



# Entity Reference

Amster 5

ForgeRock AS  
201 Mission St., Suite 2900  
San Francisco, CA 94105, USA  
+1 415-599-1100 (US)  
[www.forgerock.com](http://www.forgerock.com)

---

Copyright © 2017 ForgeRock AS.

## Abstract

Reference of the ForgeRock® Access Management command-line interface entities.



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

ForgeRock® and ForgeRock Identity Platform™ are trademarks of ForgeRock Inc. or its subsidiaries in the U.S. and in other countries. Trademarks are the property of their respective owners.

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

DejaVu Fonts

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of Gnome, the Gnome Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the Gnome Foundation or Bitstream Inc., respectively. For further information, contact: fonts at gnome dot org.

Arev Fonts Copyright

Copyright (c) 2006 by Tavmjong Bah. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: tavmjong @ free . fr.

Admonition graphics by Yannick Lung. Free for commercial use. Available at Freecn's Cumulus.

---

# Table of Contents

Preface .....	vii
1. Amster Entity Reference .....	1
1.1. ActiveDirectory .....	1
1.2. ActiveDirectoryApplicationModeADAM .....	16
1.3. ActiveDirectoryModule .....	30
1.4. AdaptiveRiskModule .....	44
1.5. AdvancedProperties .....	72
1.6. AgentGroups .....	73
1.7. AgentService .....	74
1.8. Agents .....	75
1.9. AmsterModule .....	76
1.10. AnonymousModule .....	81
1.11. ApplicationTypes .....	87
1.12. Applications .....	88
1.13. AuditEvent .....	93
1.14. AuditLogging .....	105
1.15. Authentication .....	110
1.16. AuthenticationChains .....	136
1.17. AuthenticationModules .....	142
1.18. AuthenticatorOath .....	143
1.19. AuthenticatorOathModule .....	150
1.20. AuthenticatorPush .....	159
1.21. AuthenticatorPushModule .....	166
1.22. AuthenticatorPushRegistrationModule .....	171
1.23. BaseUrlSource .....	178
1.24. CertificateModule .....	183
1.25. CircleOfTrust .....	199
1.26. ClientDetection .....	202
1.27. CommonFederationConfiguration .....	204
1.28. ConditionTypes .....	210
1.29. Csv .....	210
1.30. CtsDataStoreProperties .....	230
1.31. Dashboard .....	233
1.32. DashboardInstance .....	237
1.33. Dashboards .....	241
1.34. DataStoreModule .....	242
1.35. DatabaseRepositoryEarlyAccess .....	246
1.36. DecisionCombiners .....	254
1.37. DefaultAdvancedProperties .....	255
1.38. DefaultCtsDataStoreProperties .....	256
1.39. DefaultDirectoryConfiguration .....	258
1.40. DefaultGeneralProperties .....	260
1.41. DefaultSdkProperties .....	263
1.42. DefaultSecurityProperties .....	266

1.43. DefaultSessionProperties .....	271
1.44. DefaultUmaDataStoreProperties .....	274
1.45. DeviceIdMatchModule .....	280
1.46. DeviceIdSaveModule .....	285
1.47. DirectoryConfiguration .....	290
1.48. ElasticSearch .....	292
1.49. EmailService .....	307
1.50. FederationModule .....	315
1.51. Files .....	319
1.52. ForgottenPassword .....	324
1.53. ForgottenUsername .....	325
1.54. GeneralProperties .....	326
1.55. GenericLDAPv3 .....	331
1.56. GlobalScripts .....	346
1.57. Globalization .....	351
1.58. HotpModule .....	355
1.59. HttpBasicModule .....	365
1.60. IdRepository .....	370
1.61. IdRepositoryUser .....	374
1.62. IdffEntity .....	381
1.63. J2EEAgentGroups .....	383
1.64. J2eeAgents .....	439
1.65. Jdbc .....	495
1.66. JdbcModule .....	512
1.67. Jms .....	521
1.68. Json .....	538
1.69. KbaQuestions .....	555
1.70. LdapModule .....	556
1.71. LegacyUserSelfService .....	571
1.72. Logging .....	578
1.73. MembershipModule .....	585
1.74. Monitoring .....	591
1.75. MsisdnModule .....	593
1.76. MultiFederationProtocol .....	604
1.77. Naming .....	605
1.78. OAuth2ClientAgentGroups .....	609
1.79. OAuth2Clients .....	626
1.80. OAuth2Module .....	644
1.81. OAuth2Provider .....	666
1.82. OAuth2UserApplications .....	698
1.83. OathModule .....	699
1.84. OathUserDevices .....	710
1.85. OpenDJ .....	713
1.86. OpenIdConnectModule .....	728
1.87. PendingUmaRequests .....	737
1.88. PersistentCookieModule .....	740
1.89. Platform .....	746

1.90. Policies .....	747
1.91. PolicyAgents .....	758
1.92. PolicyConfiguration .....	762
1.93. PushAuthenticationUserDevices .....	773
1.94. PushNotification .....	774
1.95. PushNotificationResponse .....	781
1.96. RadiusClient .....	783
1.97. RadiusModule .....	788
1.98. RadiusServer .....	795
1.99. Realms .....	798
1.100. Records .....	800
1.101. ResourceSets .....	803
1.102. ResourceTypes .....	805
1.103. RestApis .....	809
1.104. SaeModule .....	811
1.105. Saml2Entity .....	815
1.106. Saml2Module .....	818
1.107. SamlV2ServiceConfiguration .....	828
1.108. SamlV2SoapBinding .....	834
1.109. ScriptStore .....	836
1.110. ScriptTypes .....	841
1.111. ScriptedModule .....	843
1.112. Scripting .....	848
1.113. ScriptingEngineConfiguration .....	850
1.114. Scripts .....	855
1.115. SdkProperties .....	860
1.116. SecurIdModule .....	866
1.117. SecurityProperties .....	871
1.118. ServerInformation .....	880
1.119. ServerVersion .....	880
1.120. Servers .....	881
1.121. Services .....	883
1.122. Session .....	885
1.123. SessionProperties .....	895
1.124. SessionPropertyWhiteList .....	899
1.125. Sessions .....	903
1.126. SharedAgents .....	906
1.127. Sites .....	910
1.128. SoapSTSAgentGroups .....	914
1.129. SoapStsAgents .....	917
1.130. SocialAuthentication .....	920
1.131. Splunk .....	926
1.132. SubjectAttributes .....	938
1.133. SubjectTypes .....	939
1.134. SunDSWithOpenAMSchema .....	940
1.135. SupportedIds .....	958
1.136. Syslog .....	960

1.137. TivoliDirectoryServer .....	972
1.138. TrustedUserDevices .....	987
1.139. UmaDataStoreProperties .....	988
1.140. UmaPolicies .....	999
1.141. UmaProvider .....	1003
1.142. UmaResourceSetLabels .....	1010
1.143. UmaUserAuditHistory .....	1012
1.144. User .....	1013
1.145. UserRegistration .....	1017
1.146. UserSelfService .....	1018
1.147. ValidationService .....	1042
1.148. WebAgentGroups .....	1047
1.149. WebAgents .....	1083
1.150. WindowsDesktopSsoModule .....	1119
1.151. WindowsNtModule .....	1127
1.152. WsEntity .....	1132
A. Getting Support .....	1136
A.1. Accessing Documentation Online .....	1136
A.2. Joining the ForgeRock Community .....	1137
A.3. Getting Support and Contacting ForgeRock .....	1137

# Preface

This reference contains the entities and actions you can perform using Amster.

This guide is written for anyone using Amster to configure and manage ForgeRock Access Management deployments.

## About ForgeRock Identity Platform™ Software

ForgeRock Identity Platform™ is the only offering for access management, identity management, user-managed access, directory services, and an identity gateway, designed and built as a single, unified platform.

The platform includes the following components that extend what is available in open source projects to provide fully featured, enterprise-ready software:

- ForgeRock Access Management (AM)
- ForgeRock Identity Management (IDM)
- ForgeRock Directory Services (DS)
- ForgeRock Identity Gateway (IG)

## Chapter 1

# Amster Entity Reference

This chapter contains details of the entities available to Amster in AM 14.0.0.

## 1.1. ActiveDirectory

### 1.1.1. Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForAD`

Resource version: `1.0`

#### 1.1.1.1. create

Usage:

```
am> create ActiveDirectory --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunIdRepoClass" : {
      "title" : "LDAPv3 Repository Plug-in Class Name",
      "description" : "",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-dncache-size" : {
      "title" : "DN Cache Size",
      "description" : "In DN items, only used when DN Cache is enabled.",
      "propertyOrder" : 6000,

```



```

    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sunIdRepoSupportedOperations" : {
    "title" : "LDAPv3 Plug-in Supported Types and Operations",
    "description" : "",
    "propertyOrder" : 1900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-interval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-name" : {
    "title" : "LDAP People Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-attributes" : {
    "title" : "LDAP User Attributes",
    "description" : "",
    "propertyOrder" : 2400,

```

```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "com.ipplanet.am.ldap.connection.delay.between.retries" : {
    "title" : "The Delay Time Between Retries",
    "description" : "In milliseconds.",
    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-enabled" : {
    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository  

implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during  

authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying  

LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP  

store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-attribute" : {
    "title" : "LDAP Groups Search Attribute",
    "description" : "",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-attr" : {
    "title" : "Knowledge Based Authentication Attribute Name",
    "description" : "",
    "propertyOrder" : 5300,
    "required" : true,
    "items" : {
      "type" : "string"
    }
  },

```

```

    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-naming-attr" : {
    "title" : "Authentication Naming Attribute",
    "description" : "",
    "propertyOrder" : 5200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
},

```

```

"sun-idrepo-ldapv3-config-users-search-filter" : {
  "title" : "LDAP Users Search Filter",
  "description" : "",
  "propertyOrder" : 2200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-name" : {
  "title" : "LDAP Groups Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 3100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-max-result" : {
  "title" : "Maximum Results Returned from Search",
  "description" : "",
  "propertyOrder" : 1500,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-attributes" : {
  "title" : "LDAP Groups Attributes",
  "description" : "",
  "propertyOrder" : 3400,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-time-limit" : {
  "title" : "Search Timeout",
  "description" : "In seconds.",
  "propertyOrder" : 1600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"openam-idrepo-ldapv3-heartbeat-timeunit" : {
  "title" : "LDAP Connection Heartbeat Time Unit",
  "description" : "Defines the time unit corresponding to the Heartbeat Interval  

  setting. This setting controls how often OpenAM should send a heartbeat search request  

  to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then  

  it may take up to the interval period before the problem is detected. Use along with the Heartbeat  

  Interval parameter to define the exact interval.",
  "propertyOrder" : 1400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-isactive" : {
  "title" : "Attribute Name of User Status",
  "description" : "",
  "propertyOrder" : 2600,

```



```

    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-active" : {
    "title" : "User Status Active Value",
    "description" : "",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-filter" : {
    "title" : "LDAP Groups Search Filter",
    "description" : "",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-value" : {
    "title" : "LDAP People Container Value",
    "description" : "",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}

```

```
}  
}
```

### 1.1.1.2. delete

Usage:

```
am> delete ActiveDirectory --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.1.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ActiveDirectory --realm Realm --actionName getAllTypes
```

### 1.1.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ActiveDirectory --realm Realm --actionName getCreatableTypes
```

### 1.1.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ActiveDirectory --realm Realm --actionName nextdescendents
```

### 1.1.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query ActiveDirectory --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.1.1.7. read

Usage:

```
am> read ActiveDirectory --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.1.1.8. update

Usage:

```
am> update ActiveDirectory --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunIdRepoClass" : {
      "title" : "LDAPv3 Repository Plug-in Class Name",
      "description" : "",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-dncache-size" : {
      "title" : "DN Cache Size",
      "description" : "In DN items, only used when DN Cache is enabled.",
      "propertyOrder" : 6000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sunIdRepoSupportedOperations" : {
      "title" : "LDAPv3 Plug-in Supported Types and Operations",
      "description" : "",
      "propertyOrder" : 1900,

```



```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-interval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-name" : {
    "title" : "LDAP People Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-attributes" : {
    "title" : "LDAP User Attributes",
    "description" : "",
    "propertyOrder" : 2400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "com.ipplanet.am.ldap.connection.delay.between.retries" : {

```

```

    "title" : "The Delay Time Between Retries",
    "description" : "In milliseconds.",
    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-enabled" : {
    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-attribute" : {
    "title" : "LDAP Groups Search Attribute",
    "description" : "",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-attr" : {
    "title" : "Knowledge Based Authentication Attribute Name",
    "description" : "",
    "propertyOrder" : 5300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
    "propertyOrder" : 700,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-naming-attr" : {
    "title" : "Authentication Naming Attribute",
    "description" : "",
    "propertyOrder" : 5200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-filter" : {
    "title" : "LDAP Users Search Filter",
    "description" : "",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
},

```

```

"sun-idrepo-ldapv3-config-group-container-name" : {
  "title" : "LDAP Groups Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 3100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-max-result" : {
  "title" : "Maximum Results Returned from Search",
  "description" : "",
  "propertyOrder" : 1500,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-attributes" : {
  "title" : "LDAP Groups Attributes",
  "description" : "",
  "propertyOrder" : 3400,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-time-limit" : {
  "title" : "Search Timeout",
  "description" : "In seconds.",
  "propertyOrder" : 1600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"openam-idrepo-ldapv3-heartbeat-timeunit" : {
  "title" : "LDAP Connection Heartbeat Time Unit",
  "description" : "Defines the time unit corresponding to the Heartbeat Interval  

  setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request  

  to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then  

  it may take up to the interval period before the problem is detected. Use along with the Heartbeat  

  Interval parameter to define the exact interval.",
  "propertyOrder" : 1400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-isactive" : {
  "title" : "Attribute Name of User Status",
  "description" : "",
  "propertyOrder" : 2600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-inactive" : {
  "title" : "User Status Inactive Value",
  "description" : "",
  "propertyOrder" : 2800,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-value" : {
    "title" : "LDAP Groups Container Value",
    "description" : "",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authpw" : {
    "title" : "LDAP Bind Password",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-objectclass" : {
    "title" : "LDAP User Object Class",
    "description" : "",
    "propertyOrder" : 2300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-unique-member" : {
        "title" : "Attribute Name of Unique Member",
        "description" : "",
        "propertyOrder" : 3600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-search-scope" : {
        "title" : "LDAPv3 Plug-in Search Scope",
        "description" : "",
        "propertyOrder" : 2000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-active" : {
        "title" : "User Status Active Value",
        "description" : "",
        "propertyOrder" : 2700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-groups-search-filter" : {
        "title" : "LDAP Groups Search Filter",
        "description" : "",
        "propertyOrder" : 3000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-psearch-scope" : {
        "title" : "Persistent Search Scope",
        "description" : "",
        "propertyOrder" : 5700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-people-container-value" : {
        "title" : "LDAP People Container Value",
        "description" : "",
        "propertyOrder" : 5100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

## 1.2. ActiveDirectoryApplicationModeADAM

### 1.2.1. Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForADAM`

Resource version: `1.0`

#### 1.2.1.1. create

Usage:

```
am> create ActiveDirectoryApplicationModeADAM --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "openam-idrepo-ldapv3-heartbeat-interval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-max-result" : {
      "title" : "Maximum Results Returned from Search",
      "description" : "",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-dncache-size" : {
      "title" : "DN Cache Size",
      "description" : "In DN items, only used when DN Cache is enabled.",
      "propertyOrder" : 6000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

```

    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-naming-attr" : {
    "title" : "Authentication Naming Attribute",
    "description" : "",
    "propertyOrder" : 5200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-filter" : {
    "title" : "LDAP Users Search Filter",
    "description" : "",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoSupportedOperations" : {
    "title" : "LDAPv3 Plug-in Supported Types and Operations",
    "description" : "",
    "propertyOrder" : 1900,
    "required" : true,
    "items" : {

```



```

    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-uniquemember" : {
  "title" : "Attribute Name of Unique Member",
  "description" : "",
  "propertyOrder" : 3600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-isactive" : {
  "title" : "Attribute Name of User Status",
  "description" : "",
  "propertyOrder" : 2600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-people-container-value" : {
  "title" : "LDAP People Container Value",
  "description" : "",
  "propertyOrder" : 5100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-users-search-attribute" : {
  "title" : "LDAP Users Search Attribute",
  "description" : "",
  "propertyOrder" : 2100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"openam-idrepo-ldapv3-heartbeat-timeunit" : {
  "title" : "LDAP Connection Heartbeat Time Unit",
  "description" : "Defines the time unit corresponding to the Heartbeat Interval  

  setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request  

  to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then  

  it may take up to the interval period before the problem is detected. Use along with the Heartbeat  

  Interval parameter to define the exact interval.",
  "propertyOrder" : 1400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-user-attributes" : {
  "title" : "LDAP User Attributes",
  "description" : "",
  "propertyOrder" : 2400,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
}

```

```

},
"sun-idrepo-ldapv3-config-groups-search-filter" : {
  "title" : "LDAP Groups Search Filter",
  "description" : "",
  "propertyOrder" : 3000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-time-limit" : {
  "title" : "Search Timeout",
  "description" : "In seconds.",
  "propertyOrder" : 1600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-attributes" : {
  "title" : "LDAP Groups Attributes",
  "description" : "",
  "propertyOrder" : 3400,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-dncache-enabled" : {
  "title" : "DN Cache",
  "description" : "Used to enable/disable the DN Cache within the OpenAM repository  
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during  
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying  
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP  
store supports persistent search and move/rename (mod_dn) results are available.",
  "propertyOrder" : 5900,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-organization_name" : {
  "title" : "LDAP Organization DN",
  "description" : "",
  "propertyOrder" : 900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-groups-search-attribute" : {
  "title" : "LDAP Groups Search Attribute",
  "description" : "",
  "propertyOrder" : 2900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-name" : {
  "title" : "LDAP Groups Container Naming Attribute",
  "description" : "",

```

```

    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "LDAPv3 Repository Plug-in Class Name",
    "description" : "",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authpw" : {
    "title" : "LDAP Bind Password",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-value" : {
    "title" : "LDAP Groups Container Value",
    "description" : "",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",

```

```

    "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-objectclass" : {
    "title" : "LDAP User Object Class",
    "description" : "",
    "propertyOrder" : 2300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "com.ipplanet.am.ldap.connection.delay.between.retries" : {
    "title" : "The Delay Time Between Retries",
    "description" : "In milliseconds.",
    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-active" : {
    "title" : "User Status Active Value",
    "description" : "",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-name" : {
    "title" : "LDAP People Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 5000,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-attr" : {
    "title" : "Knowledge Based Authentication Attribute Name",
    "description" : "",
    "propertyOrder" : 5300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }
}
}

```

### 1.2.1.2. delete

Usage:

```
am> delete ActiveDirectoryApplicationModeADAM --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.2.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ActiveDirectoryApplicationModeADAM --realm Realm --actionName getAllTypes
```

### 1.2.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ActiveDirectoryApplicationModeADAM --realm Realm --actionName getCreatableTypes
```

### 1.2.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ActiveDirectoryApplicationModeADAM --realm Realm --actionName nextdescendents
```

### 1.2.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query ActiveDirectoryApplicationModeADAM --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.2.1.7. read

Usage:

```
am> read ActiveDirectoryApplicationModeADAM --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.2.1.8. update

Usage:

```
am> update ActiveDirectoryApplicationModeADAM --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "openam-idrepo-ldapv3-heartbeat-interval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-max-result" : {
      "title" : "Maximum Results Returned from Search",
      "description" : "",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-dncache-size" : {
      "title" : "DN Cache Size",
      "description" : "In DN items, only used when DN Cache is enabled.",
      "propertyOrder" : 6000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-auth-naming-attr" : {
      "title" : "Authentication Naming Attribute",
      "description" : "",
      "propertyOrder" : 5200,
      "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-filter" : {
    "title" : "LDAP Users Search Filter",
    "description" : "",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoSupportedOperations" : {
    "title" : "LDAPv3 Plug-in Supported Types and Operations",
    "description" : "",
    "propertyOrder" : 1900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",

```



```

    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-isactive" : {
    "title" : "Attribute Name of User Status",
    "description" : "",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-value" : {
    "title" : "LDAP People Container Value",
    "description" : "",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-timeunit" : {
    "title" : "LDAP Connection Heartbeat Time Unit",
    "description" : "Defines the time unit corresponding to the Heartbeat Interval  

    setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request  

    to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then  

    it may take up to the interval period before the problem is detected. Use along with the Heartbeat  

    Interval parameter to define the exact interval.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-attributes" : {
    "title" : "LDAP User Attributes",
    "description" : "",
    "propertyOrder" : 2400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-filter" : {
    "title" : "LDAP Groups Search Filter",
    "description" : "",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",

```

```

    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-time-limit" : {
    "title" : "Search Timeout",
    "description" : "In seconds.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",
    "description" : "",
    "propertyOrder" : 3400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-enabled" : {
    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository  
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during  
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying  
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP  
store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-attribute" : {
    "title" : "LDAP Groups Search Attribute",
    "description" : "",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-name" : {
    "title" : "LDAP Groups Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",

```

```

    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "LDAPv3 Repository Plug-in Class Name",
    "description" : "",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authpw" : {
    "title" : "LDAP Bind Password",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-value" : {
    "title" : "LDAP Groups Container Value",
    "description" : "",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  },

```

```

"sun-idrepo-ldapv3-config-user-objectclass" : {
  "title" : "LDAP User Object Class",
  "description" : "",
  "propertyOrder" : 2300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-psearchbase" : {
  "title" : "Persistent Search Base DN",
  "description" : "",
  "propertyOrder" : 5500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-connection-mode" : {
  "title" : "LDAP Connection Mode",
  "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
  "propertyOrder" : 1000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"com.ipplanet.am.ldap.connection.delay.between.retries" : {
  "title" : "The Delay Time Between Retries",
  "description" : "In milliseconds.",
  "propertyOrder" : 5800,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-active" : {
  "title" : "User Status Active Value",
  "description" : "",
  "propertyOrder" : 2700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-people-container-name" : {
  "title" : "LDAP People Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 5000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-auth-kba-attr" : {
  "title" : "Knowledge Based Authentication Attribute Name",
  "description" : "",
  "propertyOrder" : 5300,

```

```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }
}
}

```

## 1.3. ActiveDirectoryModule

### 1.3.1. Realm Operations

Resource path: `/realm-config/authentication/modules/activedirectory`

Resource version: `1.0`

#### 1.3.1.1. create

Usage:

```
am> create ActiveDirectoryModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userBindPassword" : {
      "title" : "Bind User Password",
      "description" : "The password of the administration account.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "userSearchFilter" : {
      "title" : "User Search Filter",
      "description" : "This search filter will be appended to the standard user search
filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
For example: <code>(objectClass=person)</code>would result in the following user search filter:<br>
<br><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "profileAttributeMappings" : {
      "title" : "User Creation Attributes",
      "description" : "Controls the mapping of local attribute to external attribute for dynamic
profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
between the attribute/values retrieved from the users authenticated profile and the attribute/values
that will be provisioned into their matching account in the data store.<br><br>The format of this
property is: <br><br><code> local attr|external attr</code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "openam-auth-ldap-connection-mode" : {
      "title" : "LDAP Connection Mode",
      "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
      "propertyOrder" : 1000,
      "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "userBindDN" : {
    "title" : "Bind User DN",
    "description" : "The DN of an admin user used by the module to authentication to the LDAP
server<br><br>The LDAP module requires an administration account in order to perform functionality
such as password reset.<br><br><i>NB </i><code>cn=Directory Manager</code> should not be used in
production systems.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "returnUserDN" : {
    "title" : "Return User DN to DataStore",
    "description" : "Controls whether the DN or the username is returned as the authentication
principal.",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "operationTimeout" : {
    "title" : "LDAP operations timeout",
    "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
will apply.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "secondaryLdapServer" : {
    "title" : "Secondary Active Directory Server",
    "description" : "Use this list to set the secondary (failover) Active Directory server used
for authentication.<br><br>If the primary Active Directory server fails, the Active Directory
authentication module will failover to the secondary server. A single entry must be in the
format:<br><br><code>server:port</code><br><br>Multiple entries allow associations between
OpenAM servers and an Active Directory server. The format is:<br><br><code>local server name |
server:port</code><br><br><i>NB </i>The local server name is the full name of the server from the
list of servers and sites.",
    "propertyOrder" : 200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default). ",
    "propertyOrder" : 1800,

```

```

    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "userSearchStartDN" : {
    "title" : "DN to Start User Search",
    "description" : "The search for accounts to be authenticated start from this base DN <br><br>For
a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different
base DN's for the search The format is as follows:<br><br><code>local server name | search DN</
code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers
and sites.",
    "propertyOrder" : 300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "trustAllServerCertificates" : {
    "title" : "Trust All Server Certificates",
    "description" : "Enables a <code>X509TrustManager</code> that trusts all
certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
servers protected by self signed or invalid certificates (such as invalid hostname).<br><br><i>NB
</i>Use this feature with care as it bypasses the normal certificate verification process",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userSearchAttributes" : {
    "title" : "Attributes Used to Search for a User to be Authenticated",
    "description" : "The attributes specified in this list form the LDAP search filter.<br><br>The
default value of uid will form the following search filter of <code>uid=<i>user</i></code>, if there
are multiple values such as uid and cn, the module will create a search filter as follows <code>(|
(uid=<i>user</i>)(cn=<i>user</i>))</code>",
    "propertyOrder" : 700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userProfileRetrievalAttribute" : {
    "title" : "Attribute Used to Retrieve User Profile",
    "description" : "The LDAP module will use this attribute to search of the profile of an
authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
Normally this will be the same attribute used to find the user account. The value will be the name of
the user used for authentication.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "primaryLdapServer" : {
    "title" : "Primary Active Directory Server ",
    "description" : "Use this list to set the primary Active Directory server used for
authentication. <br><br>The Active Directory authentication module will use this list as the primary

```



```

server for authentication. A single entry must be in the format:<br><br><code>server:port</code><br><br>Multiple entries allow associations between OpenAM servers and an Active Directory server. The format is:<br><br><code>local server name | server:port</code><br><br>The local server name is the full name of the server from the list of servers and sites.",
  "propertyOrder" : 100,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"connectionHeartbeatInterval" : {
  "title" : "LDAP Connection Heartbeat Interval",
  "description" : "Specifies how often should OpenAM send a heartbeat request to the directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the heartbeat requests will ensure that the connections won't become idle. Use along with the Heartbeat Time Unit parameter to define the correct interval. Zero or negative value will result in disabling heartbeat requests.",
  "propertyOrder" : 1500,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"connectionHeartbeatTimeUnit" : {
  "title" : "LDAP Connection Heartbeat Time Unit",
  "description" : "Defines the time unit corresponding to the Heartbeat Interval setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the heartbeat requests will ensure that the connections won't become idle.",
  "propertyOrder" : 1600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"searchScope" : {
  "title" : "Search Scope",
  "description" : "The level in the Directory Server that will be searched for a matching user profile.<br><br>This attribute controls how the directory is searched.<br><br><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and all levels below are searched</li></ul>",
  "propertyOrder" : 900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
}

```

### 1.3.1.2. delete

Usage:

```
am> delete ActiveDirectoryModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.3.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ActiveDirectoryModule --realm Realm --actionName getAllTypes
```

### 1.3.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ActiveDirectoryModule --realm Realm --actionName getCreatableTypes
```

### 1.3.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ActiveDirectoryModule --realm Realm --actionName nextdescendents
```

### 1.3.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query ActiveDirectoryModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.3.1.7. read

Usage:

```
am> read ActiveDirectoryModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.3.1.8. update

Usage:

```
am> update ActiveDirectoryModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userBindPassword" : {
      "title" : "Bind User Password",
      "description" : "The password of the administration account.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "userSearchFilter" : {
      "title" : "User Search Filter",
      "description" : "This search filter will be appended to the standard user search
filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
For example: <code>(objectClass=person)</code>would result in the following user search filter:<br>
<br><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "profileAttributeMappings" : {
      "title" : "User Creation Attributes",
      "description" : "Controls the mapping of local attribute to external attribute for dynamic
profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
between the attribute/values retrieved from the users authenticated profile and the attribute/values
that will be provisioned into their matching account in the data store.<br><br>The format of this
property is: <br><br><code> local attr|external attr</code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

```

    },
    "openam-auth-ldap-connection-mode" : {
      "title" : "LDAP Connection Mode",
      "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userBindDN" : {
      "title" : "Bind User DN",
      "description" : "The DN of an admin user used by the module to authentication to the LDAP
server<br><br>The LDAP module requires an administration account in order to perform functionality
such as password reset.<br><br><i>NB </i><code>cn=Directory Manager</code> should not be used in
production systems.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication
principal.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "operationTimeout" : {
      "title" : "LDAP operations timeout",
      "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
will apply.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "secondaryLdapServer" : {
      "title" : "Secondary Active Directory Server",
      "description" : "Use this list to set the secondary (failover) Active Directory server used
for authentication.<br><br>If the primary Active Directory server fails, the Active Directory
authentication module will failover to the secondary server. A single entry must be in the
format:<br><br><code>server:port</code><br><br>Multiple entries allow associations between
OpenAM servers and an Active Directory server. The format is:<br><br><code>local server name |
server:port</code><br><br><i>NB </i>The local server name is the full name of the server from the
list of servers and sites.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      }
    }
  }

```

```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "userSearchStartDN" : {
    "title" : "DN to Start User Search",
    "description" : "The search for accounts to be authenticated start from this base DN <br><br>For a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different base DN's for the search The format is as follows:<br><br><code>local server name | search DN</code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "trustAllServerCertificates" : {
    "title" : "Trust All Server Certificates",
    "description" : "Enables a <code>X509TrustManager</code> that trusts all certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP servers protected by self signed or invalid certificates (such as invalid hostname).<br><br><i>NB </i>Use this feature with care as it bypasses the normal certificate verification process",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userSearchAttributes" : {
    "title" : "Attributes Used to Search for a User to be Authenticated",
    "description" : "The attributes specified in this list form the LDAP search filter.<br><br>The default value of uid will form the following search filter of <code>uid=<i>user</i></code>, if there are multiple values such as uid and cn, the module will create a search filter as follows <code>(|uid=<i>user</i>)(cn=<i>user</i>))</code>",
    "propertyOrder" : 700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userProfileRetrievalAttribute" : {
    "title" : "Attribute Used to Retrieve User Profile",
    "description" : "The LDAP module will use this attribute to search of the profile of an authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.

```

Normally this will be the same attribute used to find the user account. The value will be the name of the user used for authentication.",

```

    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "primaryLdapServer" : {
    "title" : "Primary Active Directory Server ",
    "description" : "Use this list to set the primary Active Directory server used for authentication. <br><br>The Active Directory authentication module will use this list as the primary server for authentication. A single entry must be in the format:<br><br><code>server:port</code><br><br>Multiple entries allow associations between OpenAM servers and an Active Directory server. The format is:<br><br><code>local server name | server:port</code><br><br>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "connectionHeartbeatInterval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the heartbeat requests will ensure that the connections won't become idle. Use along with the Heartbeat Time Unit parameter to define the correct interval. Zero or negative value will result in disabling heartbeat requests.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "connectionHeartbeatTimeUnit" : {
    "title" : "LDAP Connection Heartbeat Time Unit",
    "description" : "Defines the time unit corresponding to the Heartbeat Interval setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the heartbeat requests will ensure that the connections won't become idle.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "searchScope" : {
    "title" : "Search Scope",
    "description" : "The level in the Directory Server that will be searched for a matching user profile.<br><br>This attribute controls how the directory is searched.<br><br><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and all levels below are searched</li></ul>",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}

```

```
}
```

## 1.3.2. Global Operations

Resource path: `/global-config/authentication/modules/activedirectory`

Resource version: `1.0`

### 1.3.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ActiveDirectoryModule --global --actionName getAllTypes
```

### 1.3.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ActiveDirectoryModule --global --actionName getCreatableTypes
```

### 1.3.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ActiveDirectoryModule --global --actionName nextdescendents
```

### 1.3.2.4. read

Usage:

```
am> read ActiveDirectoryModule --global
```

### 1.3.2.5. update

Usage:

```
am> update ActiveDirectoryModule --global --body body
```

## Parameters:

### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "operationTimeout" : {
          "title" : "LDAP operations timeout",
          "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
will apply.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "userSearchStartDN" : {
          "title" : "DN to Start User Search",
          "description" : "The search for accounts to be authenticated start from this base DN
<br><br>For a single server just enter the Base DN to be searched. Multiple OpenAM servers can have
different base DNS for the search The format is as follows:<br><br><code>local server name | search
DN</code><br><br><i>NB </i>The local server name is the full name of the server from the list of
servers and sites.",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "openam-auth-ldap-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectionHeartbeatTimeUnit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the
heartbeat requests will ensure that the connections won't become idle.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",

```



```

    "exampleValue" : ""
  },
  "searchScope" : {
    "title" : "Search Scope",
    "description" : "The level in the Directory Server that will be searched for a
matching user profile.<br><br>This attribute controls how the directory is searched.<br><br>
<ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
all levels below are searched</li></ul>",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "connectionHeartbeatInterval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections,
since the heartbeat requests will ensure that the connections won't become idle. Use along with the
Heartbeat Time Unit parameter to define the correct interval. Zero or negative value will result in
disabling heartbeat requests.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "userProfileRetrievalAttribute" : {
    "title" : "Attribute Used to Retrieve User Profile",
    "description" : "The LDAP module will use this attribute to search of the profile of an
authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
Normally this will be the same attribute used to find the user account. The value will be the name of
the user used for authentication.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "primaryLdapServer" : {
    "title" : "Primary Active Directory Server ",
    "description" : "Use this list to set the primary Active Directory server used for
authentication. <br><br>The Active Directory authentication module will use this list as the primary
server for authentication. A single entry must be in the format:<br><br><code>server:port</code>
<br><br>Multiple entries allow associations between OpenAM servers and an Active Directory
server. The format is:<br><br><code>local server name | server:port</code><br><br>The local
server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "trustAllServerCertificates" : {
    "title" : "Trust All Server Certificates",
    "description" : "Enables a <code>X509TrustManager</code> that trusts all
certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
servers protected by self signed or invalid certificates (such as invalid hostname).<br><br><i>NB
</i>Use this feature with care as it bypasses the normal certificate verification process",

```

```

    "propertyOrder" : 1400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "returnUserDN" : {
    "title" : "Return User DN to DataStore",
    "description" : "Controls whether the DN or the username is returned as the authentication principal.",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userSearchFilter" : {
    "title" : "User Search Filter",
    "description" : "This search filter will be appended to the standard user search filter.<br><br>This attribute can be used to append a custom search filter to the standard filter. For example: <code>(objectClass=person)</code>would result in the following user search filter:<br><br><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "secondaryLdapServer" : {
    "title" : "Secondary Active Directory Server",
    "description" : "Use this list to set the secondary (failover) Active Directory server used for authentication.<br><br>If the primary Active Directory server fails, the Active Directory authentication module will failover to the secondary server. A single entry must be in the format:<br><br><code>server:port</code><br><br>Multiple entries allow associations between OpenAM servers and an Active Directory server. The format is:<br><br><code>local server name | server:port</code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "userBindPassword" : {
    "title" : "Bind User Password",
    "description" : "The password of the administration account.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "format" : "password",

```

```

    "exampleValue" : ""
  },
  "profileAttributeMappings" : {
    "title" : "User Creation Attributes",
    "description" : "Controls the mapping of local attribute to external attribute for dynamic
profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
between the attribute/values retrieved from the users authenticated profile and the attribute/values
that will be provisioned into their matching account in the data store.<br><br>The format of this
property is: <br><br><code> local attr|external attr</code>",
    "propertyOrder" : 1300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userBindDN" : {
    "title" : "Bind User DN",
    "description" : "The DN of an admin user used by the module to authentication to the LDAP
server<br><br>The LDAP module requires an administration account in order to perform functionality
such as password reset.<br><br><i>NB </i><code>cn=Directory Manager</code> should not be used in
production systems.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userSearchAttributes" : {
    "title" : "Attributes Used to Search for a User to be Authenticated",
    "description" : "The attributes specified in this list form the LDAP search
filter.<br><br>The default value of uid will form the following search filter of <code>uid=<i>user</i></code>
if there are multiple values such as uid and cn, the module will create a search filter as
follows <code>(|(uid=<i>user</i>)(cn=<i>user</i>))</code>",
    "propertyOrder" : 700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.4. AdaptiveRiskModule

### 1.4.1. Realm Operations

Resource path: `/realm-config/authentication/modules/adaptiverisk`

Resource version: `1.0`

### 1.4.1.1. create

Usage:

```
am> create AdaptiveRiskModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "invertRequestHeaderScore" : {
      "title" : "Invert Result",
      "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
      "propertyOrder" : 4700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "knownCookieScore" : {
      "title" : "Score",
      "description" : "The amount to increment the score if this check fails.",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "ipHistoryProfileAttribute" : {
      "title" : "Profile Attribute Name",
      "description" : "The name of the attribute used to store the IP history list in the data store.<br><br>IP history list is stored in the Data Store meaning your Data Store should be able to store values under the configured attribute name. If you're using a directory server as backend, make sure your Data Store configuration contains the necessary objectclass and attribute related settings.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ipHistoryCheckEnabled" : {
      "title" : "IP History Check",
      "description" : "Enables the checking of client IP address against a list of past IP addresses.<br><br>If this check is enabled; a set number of past IP addresses used by the client to access OpenAM is recorded in the user profile. This check passes if the current client IP address
```

is present in the history list. If the IP address is not present, the check fails and the IP address is added to list if the overall authentication is successful (causing the oldest IP address to be removed).",

```

    "propertyOrder" : 1000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "timeSinceLastLoginScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "ipHistoryScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "invertProfileRiskAttributeScore" : {
    "title" : "Invert Result",
    "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "knownCookieName" : {
    "title" : "Cookie Name",
    "description" : "The name of the cookie to set on the client.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileRiskAttributeName" : {
    "title" : "Attribute Name",
    "description" : "The name of the attribute to retrieve from the user profile in the data store.",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "timeSinceLastLoginCheckEnabled" : {
    "title" : "Time since Last login Check",
    "description" : "Enables the checking of the last time the user successfully authenticated.<br><br>If this check is enabled, the check ensures the user has successfully authenticated within a given interval. If the interval has been exceeded the check will fail. The last authentication for the user is stored in a client cookie.",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "deviceCookieName" : {
    "title" : "Cookie Name",
    "description" : "The name of the cookie to be checked for (and optionally set) on the client request",
    "propertyOrder" : 3400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "requestHeaderScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 4600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "geolocationScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 4100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "invertKnownCookieScore" : {
    "title" : "Invert Result",
    "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "profileRiskAttributeCheckEnabled" : {
    "title" : "Profile Risk Attribute check",
    "description" : "Enables the checking of the user profile for a matching attribute and value.<br><br>If this check is enabled, the check will pass if the users profile contains the required risk attribute and value.",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invertDeviceCookieScore" : {
    "title" : "Invert Result",
    "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
    "propertyOrder" : 3700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "saveLastLoginTimeOnSuccessfulLogin" : {
    "title" : "Save time of Successful Login",
    "description" : "The last login time will be saved in a client cookie<br><br>The Adaptive Risk Post Authentication Plug-in will update the last login time",

```

```

    "propertyOrder" : 2500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "geolocationDatabaseLocation" : {
    "title" : "Geolocation Database location",
    "description" : "The path to the location of the GEO location database.<br><br>The Geolocation
database is not distributed with OpenAM, you can get it in binary format from <a href=\"http://
www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
    "propertyOrder" : 3900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "geolocationCheckEnabled" : {
    "title" : "Geolocation Country Code Check",
    "description" : "Enables the checking of the client IP address against the geolocation
database.<br><br>The geolocation database associates IP addresses against their known location. This
check passes if the country associated with the client IP address is matched against the list of
valid country codes.<br><br>The geolocation database is available in binary format at <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
    "propertyOrder" : 3800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "maxTimeSinceLastLogin" : {
    "title" : "Max Time since Last login",
    "description" : "The maximum number of days that can elapse before this test.",
    "propertyOrder" : 2400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "failedAuthenticationCheckEnabled" : {
    "title" : "Failed Authentication Check",
    "description" : "Checks if the user has past authentication failures.<br><br>Check if the OpenAM
account lockout mechanism has recorded past authentication failures for the user.<br><br><i>NB </
i>For this check to function, Account Lockout must be enabled.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ipRangeCheckEnabled" : {
    "title" : "IP Range Check",
    "description" : "Enables the checking of the client IP address against a list of IP
addresses.<br><br>The IP range check compares the IP of the client against a list of IP addresses, if
the client IP is found within said list the check is successful.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "saveSuccessfulIP" : {
    "title" : "Save Successful IP Address",

```

```

    "description" : "The IP History list will be updated in the data store<br><br>The Adaptive Risk Post Authentication Plug-in will update the IP history list if the overall authentication is successful.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invertIPRangeScoreEnabled" : {
    "title" : "Invert Result",
    "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invertIPHHistoryScore" : {
    "title" : "Invert Result",
    "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ipRange" : {
    "title" : "IP Range",
    "description" : "The list of IP address to compare against the client IP address.<br><br>The format of the IP address is as follows:<br><br><ul><li>Single IP address: <code>172.16.90.1</code></li><li>CIDR notation: <code>172.16.90.0/24</code></li><li>IP net-block with netmask: <code>172.16.90.0:255.255.255.0</code></li></ul>",
    "propertyOrder" : 700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "timeSinceLastLoginCookieName" : {
    "title" : "Cookie Name",
    "description" : "The name of the cookie used to store the time of the last successful authentication.",
    "propertyOrder" : 2300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "knownCookieCheckEnabled" : {
    "title" : "Cookie Value Check",
    "description" : "Enables the checking of a known cookie value in the client request<br><br>If this check is enabled, the check looks for a known cookie in the client request. If the cookie exists and has the correct value then the check will pass. ",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  },

```



```

"invertTimeSinceLastLoginScore" : {
  "title" : "Invert Result",
  "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
  "propertyOrder" : 2700,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"invertGeolocationScore" : {
  "title" : "Invert Result",
  "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
  "propertyOrder" : 4200,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"authenticationLevel" : {
  "title" : "Authentication Level",
  "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"saveDeviceCookieValueOnSuccessfulLogin" : {
  "title" : "Save Device Registration on Successful Login",
  "description" : "Set the device cookie on the client response<br><br>The Adaptive Risk Post
Authentication Plug-in will set the device cookie on the client response",
  "propertyOrder" : 3500,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"deviceCookieCheckEnabled" : {
  "title" : "Device Registration Cookie Check",
  "description" : "Enables the checking of the client request for a known cookie.<br><br>If this
check is enabled, the check will pass if the client request contains the named cookie.",
  "propertyOrder" : 3300,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"requestHeaderValue" : {
  "title" : "Request Header Value",
  "description" : "The required value of the named HTTP header.",
  "propertyOrder" : 4500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"requestHeaderName" : {
  "title" : "Request Header Name",
  "description" : "The name of the required HTTP header ",
  "propertyOrder" : 4400,
  "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "deviceCookieScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "failureScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "riskThreshold" : {
    "title" : "Risk Threshold",
    "description" : "If the risk threshold value is not reached after executing the different tests,
the authentication is considered to be successful.<br><br>Associated with many of the adaptive risk
checks is a score; if a check does not passes then the score is added to the current running total.
The final score is then compared with the <i>Risk Threshold</i>, if the score is lesser than said
threshold the module will be successful. ",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "profileRiskAttributeScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "createKnownCookieOnSuccessfulLogin" : {
    "title" : "Save Cookie Value on Successful Login",
    "description" : "The cookie will be created on the client after successful login<br><br>The
Adaptive Risk Post Authentication Plug-in will set the cookie on the client response",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "knownCookieValue" : {
    "title" : "Cookie Value",
    "description" : "The value to be set on the cookie.",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "requestHeaderCheckEnabled" : {
    "title" : "Request Header Check",

```

```

        "description" : "Enables the checking of the client request for a known header name and
value.<br><br>The request header check will pass if the client request contains the required named
header and value.",
        "propertyOrder" : 4300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "ipHistoryCount" : {
        "title" : "History size",
        "description" : "The number of client IP addresses to save in the history list.",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "geolocationValidCountryCodes" : {
        "title" : "Valid Country Codes",
        "description" : "The list of country codes that are considered as valid locations for client
IPs.<br><br>The list is made up of country codes separated by a | character; for example:<br><br>
><code>gb|us|no|fr</code>",
        "propertyOrder" : 4000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "ipRangeScore" : {
        "title" : "Score",
        "description" : "The amount to increment the score if this check fails.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "profileRiskAttributeValue" : {
        "title" : "Attribute Value",
        "description" : "The required value of the named attribute.",
        "propertyOrder" : 3000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "invertFailureScore" : {
        "title" : "Invert Result",
        "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
}
}

```

### 1.4.1.2. delete

Usage:

```
am> delete AdaptiveRiskModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.4.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AdaptiveRiskModule --realm Realm --actionName getAllTypes
```

### 1.4.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AdaptiveRiskModule --realm Realm --actionName getCreatableTypes
```

### 1.4.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AdaptiveRiskModule --realm Realm --actionName nextdescendents
```

### 1.4.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query AdaptiveRiskModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.4.1.7. read

Usage:

```
am> read AdaptiveRiskModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.4.1.8. update

Usage:

```
am> update AdaptiveRiskModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "invertRequestHeaderScore" : {
      "title" : "Invert Result",
      "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
      "propertyOrder" : 4700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "knownCookieScore" : {
      "title" : "Score",
      "description" : "The amount to increment the score if this check fails.",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "ipHistoryProfileAttribute" : {
      "title" : "Profile Attribute Name",
      "description" : "The name of the attribute used to store the IP history list in the data store.<br><br>IP history list is stored in the Data Store meaning your Data Store should be able to store values under the configured attribute name. If you're using a directory server as backend, make sure your Data Store configuration contains the necessary objectclass and attribute related settings.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ipHistoryCheckEnabled" : {
```

```

        "title" : "IP History Check",
        "description" : "Enables the checking of client IP address against a list of past IP
addresses.<br><br>If this check is enabled; a set number of past IP addresses used by the client to
access OpenAM is recorded in the user profile. This check passes if the current client IP address
is present in the history list. If the IP address is not present, the check fails and the IP address
is added to list if the overall authentication is successful (causing the oldest IP address to be
removed).",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "timeSinceLastLoginScore" : {
        "title" : "Score",
        "description" : "The amount to increment the score if this check fails.",
        "propertyOrder" : 2600,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "ipHistoryScore" : {
        "title" : "Score",
        "description" : "The amount to increment the score if this check fails.",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "invertProfileRiskAttributeScore" : {
        "title" : "Invert Result",
        "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
        "propertyOrder" : 3200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "knownCookieName" : {
        "title" : "Cookie Name",
        "description" : "The name of the cookie to set on the client.",
        "propertyOrder" : 1700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "profileRiskAttributeName" : {
        "title" : "Attribute Name",
        "description" : "The name of the attribute to retrieve from the user profile in the data
store.",
        "propertyOrder" : 2900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "timeSinceLastLoginCheckEnabled" : {
        "title" : "Time since Last login Check",
        "description" : "Enables the checking of the last time the user successfully
authenticated.<br><br>If this check is enabled, the check ensures the user has successfully

```

```

authenticated within a given interval. If the interval has been exceeded the check will fail. The
last authentication for the user is stored in a client cookie.",
  "propertyOrder" : 2200,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"deviceCookieName" : {
  "title" : "Cookie Name",
  "description" : "The name of the cookie to be checked for (and optionally set) on the client
request",
  "propertyOrder" : 3400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"requestHeaderScore" : {
  "title" : "Score",
  "description" : "The amount to increment the score if this check fails.",
  "propertyOrder" : 4600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"geolocationScore" : {
  "title" : "Score",
  "description" : "The amount to increment the score if this check fails.",
  "propertyOrder" : 4100,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"invertKnownCookieScore" : {
  "title" : "Invert Result",
  "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
  "propertyOrder" : 2100,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"profileRiskAttributeCheckEnabled" : {
  "title" : "Profile Risk Attribute check",
  "description" : "Enables the checking of the user profile for a matching attribute and
value.<br><br>If this check is enabled, the check will pass if the users profile contains the
required risk attribute and value.",
  "propertyOrder" : 2800,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"invertDeviceCookieScore" : {
  "title" : "Invert Result",
  "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
  "propertyOrder" : 3700,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
}

```

```

    },
    "saveLastLoginTimeOnSuccessfulLogin" : {
      "title" : "Save time of Successful Login",
      "description" : "The last login time will be saved in a client cookie<br><br>The Adaptive Risk
Post Authentication Plug-in will update the last login time",
      "propertyOrder" : 2500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "geolocationDatabaseLocation" : {
      "title" : "Geolocation Database location",
      "description" : "The path to the location of the GEO location database.<br><br>The Geolocation
database is not distributed with OpenAM, you can get it in binary format from <a href=\"http://
www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
      "propertyOrder" : 3900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "geolocationCheckEnabled" : {
      "title" : "Geolocation Country Code Check",
      "description" : "Enables the checking of the client IP address against the geolocation
database.<br><br>The geolocation database associates IP addresses against their known location. This
check passes if the country associated with the client IP address is matched against the list of
valid country codes.<br><br>The geolocation database is available in binary format at <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
      "propertyOrder" : 3800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "maxTimeSinceLastLogin" : {
      "title" : "Max Time since Last login",
      "description" : "The maximum number of days that can elapse before this test.",
      "propertyOrder" : 2400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "failedAuthenticationCheckEnabled" : {
      "title" : "Failed Authentication Check",
      "description" : "Checks if the user has past authentication failures.<br><br>Check if the OpenAM
account lockout mechanism has recorded past authentication failures for the user.<br><br><i>NB </
i>For this check to function, Account Lockout must be enabled.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ipRangeCheckEnabled" : {
      "title" : "IP Range Check",
      "description" : "Enables the checking of the client IP address against a list of IP
addresses.<br><br>The IP range check compares the IP of the client against a list of IP addresses, if
the client IP is found within said list the check is successful.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }

```



```

    },
    "saveSuccessfulIP" : {
      "title" : "Save Successful IP Address",
      "description" : "The IP History list will be updated in the data store<br><br>The Adaptive Risk Post Authentication Plug-in will update the IP history list if the overall authentication is successful.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "invertIPRangeScoreEnabled" : {
      "title" : "Invert Result",
      "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "invertIPHHistoryScore" : {
      "title" : "Invert Result",
      "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ipRange" : {
      "title" : "IP Range",
      "description" : "The list of IP address to compare against the client IP address.<br><br>The format of the IP address is as follows:<br><br><ul><li>Single IP address: <code>172.16.90.1</code></li><li>CIDR notation: <code>172.16.90.0/24</code></li><li>IP net-block with netmask: <code>172.16.90.0:255.255.255.0</code></li></ul>",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "timeSinceLastLoginCookieName" : {
      "title" : "Cookie Name",
      "description" : "The name of the cookie used to store the time of the last successful authentication.",
      "propertyOrder" : 2300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "knownCookieCheckEnabled" : {
      "title" : "Cookie Value Check",
      "description" : "Enables the checking of a known cookie value in the client request<br><br>If this check is enabled, the check looks for a known cookie in the client request. If the cookie exists and has the correct value then the check will pass. ",
      "propertyOrder" : 1600,
      "required" : true,

```

```

    "type" : "boolean",
    "exampleValue" : ""
  },
  "invertTimeSinceLastLoginScore" : {
    "title" : "Invert Result",
    "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invertGeolocationScore" : {
    "title" : "Invert Result",
    "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
    "propertyOrder" : 4200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "saveDeviceCookieValueOnSuccessfulLogin" : {
    "title" : "Save Device Registration on Successful Login",
    "description" : "Set the device cookie on the client response<br><br>The Adaptive Risk Post
Authentication Plug-in will set the device cookie on the client response",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "deviceCookieCheckEnabled" : {
    "title" : "Device Registration Cookie Check",
    "description" : "Enables the checking of the client request for a known cookie.<br><br>If this
check is enabled, the check will pass if the client request contains the named cookie.",
    "propertyOrder" : 3300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "requestHeaderValue" : {
    "title" : "Request Header Value",
    "description" : "The required value of the named HTTP header.",
    "propertyOrder" : 4500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "requestHeaderName" : {
    "title" : "Request Header Name",

```

```

    "description" : "The name of the required HTTP header ",
    "propertyOrder" : 4400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "deviceCookieScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "failureScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "riskThreshold" : {
    "title" : "Risk Threshold",
    "description" : "If the risk threshold value is not reached after executing the different tests,
the authentication is considered to be successful.<br><br>Associated with many of the adaptive risk
checks is a score; if a check does not passes then the score is added to the current running total.
The final score is then compared with the <i>Risk Threshold</i>, if the score is lesser than said
threshold the module will be successful. ",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "profileRiskAttributeScore" : {
    "title" : "Score",
    "description" : "The amount to increment the score if this check fails.",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "createKnownCookieOnSuccessfulLogin" : {
    "title" : "Save Cookie Value on Successful Login",
    "description" : "The cookie will be created on the client after successful login<br><br>The
Adaptive Risk Post Authentication Plug-in will set the cookie on the client response",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "knownCookieValue" : {
    "title" : "Cookie Value",
    "description" : "The value to be set on the cookie.",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
},

```

```

    "requestHeaderCheckEnabled" : {
      "title" : "Request Header Check",
      "description" : "Enables the checking of the client request for a known header name and
value.<br><br>The request header check will pass if the client request contains the required named
header and value.",
      "propertyOrder" : 4300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ipHistoryCount" : {
      "title" : "History size",
      "description" : "The number of client IP addresses to save in the history list.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "geolocationValidCountryCodes" : {
      "title" : "Valid Country Codes",
      "description" : "The list of country codes that are considered as valid locations for client
IPs.<br><br>The list is made up of country codes separated by a | character; for example:<br><br>
><code>gb|us|no|fr</code>",
      "propertyOrder" : 4000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ipRangeScore" : {
      "title" : "Score",
      "description" : "The amount to increment the score if this check fails.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "profileRiskAttributeValue" : {
      "title" : "Attribute Value",
      "description" : "The required value of the named attribute.",
      "propertyOrder" : 3000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "invertFailureScore" : {
      "title" : "Invert Result",
      "description" : "If the check succeeds the score will be included in the total, for failure the
score will not be incremented.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}

```

## 1.4.2. Global Operations

Resource path: `/global-config/authentication/modules/adaptiverisk`

Resource version: `1.0`

### 1.4.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AdaptiveRiskModule --global --actionName getAllTypes
```

### 1.4.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AdaptiveRiskModule --global --actionName getCreatableTypes
```

### 1.4.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AdaptiveRiskModule --global --actionName nextdescendents
```

### 1.4.2.4. read

Usage:

```
am> read AdaptiveRiskModule --global
```

### 1.4.2.5. update

Usage:

```
am> update AdaptiveRiskModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "attributecheck" : {
          "type" : "object",
          "title" : "Profile Attribute",
          "propertyOrder" : 7,
          "properties" : {
            "profileRiskAttributeName" : {
              "title" : "Attribute Name",
              "description" : "The name of the attribute to retrieve from the user profile in the data
store.",
              "propertyOrder" : 2900,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "profileRiskAttributeValue" : {
              "title" : "Attribute Value",
              "description" : "The required value of the named attribute.",
              "propertyOrder" : 3000,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "invertProfileRiskAttributeScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 3200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "profileRiskAttributeCheckEnabled" : {
              "title" : "Profile Risk Attribute check",
              "description" : "Enables the checking of the user profile for a matching attribute
and value.<br><br>If this check is enabled, the check will pass if the users profile contains the
required risk attribute and value.",
              "propertyOrder" : 2800,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "profileRiskAttributeScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 3100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            }
          }
        }
      }
    }
  }
}
```

```

    },
    "iprange" : {
      "type" : "object",
      "title" : "IP Address Range",
      "propertyOrder" : 2,
      "properties" : {
        "ipRangeCheckEnabled" : {
          "title" : "IP Range Check",
          "description" : "Enables the checking of the client IP address against a list of IP
addresses.<br><br>The IP range check compares the IP of the client against a list of IP addresses, if
the client IP is found within said list the check is successful.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ipRangeScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "ipRange" : {
        "title" : "IP Range",
        "description" : "The list of IP address to compare against the client IP
address.<br><br>The format of the IP address is as follows:<br><br><ul><li>Single IP address:
<code>172.16.90.1</code></li><li>CIDR notation: <code>172.16.90.0/24</code></li><li>IP net-block with
netmask: <code>172.16.90.0:255.255.255.0</code></li></ul>",
        "propertyOrder" : 700,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "invertIPRangeScoreEnabled" : {
        "title" : "Invert Result",
        "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  },
  "devicecookie" : {
    "type" : "object",
    "title" : "Device Cookie",
    "propertyOrder" : 5,
    "properties" : {
      "deviceCookieScore" : {
        "title" : "Score",
        "description" : "The amount to increment the score if this check fails.",
        "propertyOrder" : 3600,
        "required" : true,

```

```

        "type" : "integer",
        "exampleValue" : ""
    },
    "saveDeviceCookieValueOnSuccessfulLogin" : {
        "title" : "Save Device Registration on Successful Login",
        "description" : "Set the device cookie on the client response<br><br>The Adaptive Risk
Post Authentication Plug-in will set the device cookie on the client response",
        "propertyOrder" : 3500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "deviceCookieName" : {
        "title" : "Cookie Name",
        "description" : "The name of the cookie to be checked for (and optionally set) on the
client request",
        "propertyOrder" : 3400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "invertDeviceCookieScore" : {
        "title" : "Invert Result",
        "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
        "propertyOrder" : 3700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "deviceCookieCheckEnabled" : {
        "title" : "Device Registration Cookie Check",
        "description" : "Enables the checking of the client request for a known
cookie.<br><br>If this check is enabled, the check will pass if the client request contains the named
cookie.",
        "propertyOrder" : 3300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"lastlogin" : {
    "type" : "object",
    "title" : "Time Since Last Login",
    "propertyOrder" : 6,
    "properties" : {
        "timeSinceLastLoginCookieName" : {
            "title" : "Cookie Name",
            "description" : "The name of the cookie used to store the time of the last successful
authentication.",
            "propertyOrder" : 2300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "timeSinceLastLoginScore" : {
            "title" : "Score",
            "description" : "The amount to increment the score if this check fails.",

```



```

        "propertyOrder" : 2600,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "timeSinceLastLoginCheckEnabled" : {
        "title" : "Time since Last login Check",
        "description" : "Enables the checking of the last time the user successfully
authenticated.<br><br>If this check is enabled, the check ensures the user has successfully
authenticated within a given interval. If the interval has been exceeded the check will fail. The
last authentication for the user is stored in a client cookie.",
        "propertyOrder" : 2200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "invertTimeSinceLastLoginScore" : {
        "title" : "Invert Result",
        "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
        "propertyOrder" : 2700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "maxTimeSinceLastLogin" : {
        "title" : "Max Time since Last login",
        "description" : "The maximum number of days that can elapse before this test.",
        "propertyOrder" : 2400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "saveLastLoginTimeOnSuccessfulLogin" : {
        "title" : "Save time of Successful Login",
        "description" : "The last login time will be saved in a client cookie<br><br>The
Adaptive Risk Post Authentication Plug-in will update the last login time",
        "propertyOrder" : 2500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
},
"geolocation" : {
    "type" : "object",
    "title" : "Geo Location",
    "propertyOrder" : 8,
    "properties" : {
        "geolocationValidCountryCodes" : {
            "title" : "Valid Country Codes",
            "description" : "The list of country codes that are considered as valid locations for
client IPs.<br><br>The list is made up of country codes separated by a | character; for example:<br>
><br><code>gb|us|no|fr</code>",
            "propertyOrder" : 4000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},

```

```

    "geolocationCheckEnabled" : {
      "title" : "Geolocation Country Code Check",
      "description" : "Enables the checking of the client IP address against the geolocation
database.<br><br>The geolocation database associates IP addresses against their known location. This
check passes if the country associated with the client IP address is matched against the list of
valid country codes.<br><br>The geolocation database is available in binary format at <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
      "propertyOrder" : 3800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "invertGeolocationScore" : {
      "title" : "Invert Result",
      "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
      "propertyOrder" : 4200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "geolocationScore" : {
      "title" : "Score",
      "description" : "The amount to increment the score if this check fails.",
      "propertyOrder" : 4100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "geolocationDatabaseLocation" : {
      "title" : "Geolocation Database location",
      "description" : "The path to the location of the GEO location database.<br><br>The
Geolocation database is not distributed with OpenAM, you can get it in binary format from <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
      "propertyOrder" : 3900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "iphistory" : {
    "type" : "object",
    "title" : "IP Address History",
    "propertyOrder" : 3,
    "properties" : {
      "ipHistoryCheckEnabled" : {
        "title" : "IP History Check",
        "description" : "Enables the checking of client IP address against a list of past IP
addresses.<br><br>If this check is enabled; a set number of past IP addresses used by the client to
access OpenAM is recorded in the user profile. This check passes if the current client IP address
is present in the history list. If the IP address is not present, the check fails and the IP address
is added to list if the overall authentication is successful (causing the oldest IP address to be
removed).",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  },

```

```

    "invertIPHHistoryScore" : {
      "title" : "Invert Result",
      "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ipHistoryScore" : {
      "title" : "Score",
      "description" : "The amount to increment the score if this check fails.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "ipHistoryProfileAttribute" : {
      "title" : "Profile Attribute Name",
      "description" : "The name of the attribute used to store the IP history list in the data
store.<br><br>IP history list is stored in the Data Store meaning your Data Store should be able
to store values under the configured attribute name. If you're using a directory server as backend,
make sure your Data Store configuration contains the necessary objectclass and attribute related
settings.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ipHistoryCount" : {
      "title" : "History size",
      "description" : "The number of client IP addresses to save in the history list.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "saveSuccessfulIP" : {
      "title" : "Save Successful IP Address",
      "description" : "The IP History list will be updated in the data store<br><br>The
Adaptive Risk Post Authentication Plug-in will update the IP history list if the overall
authentication is successful.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "requestheader" : {
    "type" : "object",
    "title" : "Request Header",
    "propertyOrder" : 9,
    "properties" : {
      "requestHeaderValue" : {
        "title" : "Request Header Value",
        "description" : "The required value of the named HTTP header.",
        "propertyOrder" : 4500,
        "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "requestHeaderCheckEnabled" : {
        "title" : "Request Header Check",
        "description" : "Enables the checking of the client request for a known header name and value.<br><br>The request header check will pass if the client request contains the required named header and value.",
        "propertyOrder" : 4300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "requestHeaderName" : {
        "title" : "Request Header Name",
        "description" : "The name of the required HTTP header ",
        "propertyOrder" : 4400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "invertRequestHeaderScore" : {
        "title" : "Invert Result",
        "description" : "If the check succeeds the score will be included in the total, for failure the score will not be incremented.",
        "propertyOrder" : 4700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "requestHeaderScore" : {
        "title" : "Score",
        "description" : "The amount to increment the score if this check fails.",
        "propertyOrder" : 4600,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
    },
    "authfailed" : {
        "type" : "object",
        "title" : "Failed Authentications",
        "propertyOrder" : 1,
        "properties" : {
            "failedAuthenticationCheckEnabled" : {
                "title" : "Failed Authentication Check",
                "description" : "Checks if the user has past authentication failures.<br><br>Check if the OpenAM account lockout mechanism has recorded past authentication failures for the user.<br><br><i>NB </i>For this check to function, Account Lockout must be enabled.",
                "propertyOrder" : 300,
                "required" : true,
                "type" : "boolean",
                "exampleValue" : ""
            },
            "failureScore" : {
                "title" : "Score",
                "description" : "The amount to increment the score if this check fails.",
                "propertyOrder" : 400,

```

```

        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "invertFailureScore" : {
        "title" : "Invert Result",
        "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
},
"general" : {
    "type" : "object",
    "title" : "General",
    "propertyOrder" : 0,
    "properties" : {
        "riskThreshold" : {
            "title" : "Risk Threshold",
            "description" : "If the risk threshold value is not reached after executing the
different tests, the authentication is considered to be successful.<br><br>Associated with many
of the adaptive risk checks is a score; if a check does not passes then the score is added to the
current running total. The final score is then compared with the <i>Risk Threshold</i>, if the score
is lesser than said threshold the module will be successful. ",
            "propertyOrder" : 200,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "authenticationLevel" : {
            "title" : "Authentication Level",
            "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
            "propertyOrder" : 100,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        }
    }
},
"knowncookie" : {
    "type" : "object",
    "title" : "Known Cookie",
    "propertyOrder" : 4,
    "properties" : {
        "knownCookieValue" : {
            "title" : "Cookie Value",
            "description" : "The value to be set on the cookie.",
            "propertyOrder" : 1800,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "knownCookieCheckEnabled" : {
            "title" : "Cookie Value Check",

```

```

        "description" : "Enables the checking of a known cookie value in the client
request<br><br>If this check is enabled, the check looks for a known cookie in the client request. If
the cookie exists and has the correct value then the check will pass. ",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "createKnownCookieOnSuccessfulLogin" : {
        "title" : "Save Cookie Value on Successful Login",
        "description" : "The cookie will be created on the client after successful
login<br><br>The Adaptive Risk Post Authentication Plug-in will set the cookie on the client
response",
        "propertyOrder" : 1900,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "invertKnownCookieScore" : {
        "title" : "Invert Result",
        "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
        "propertyOrder" : 2100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "knownCookieScore" : {
        "title" : "Score",
        "description" : "The amount to increment the score if this check fails.",
        "propertyOrder" : 2000,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "knownCookieName" : {
        "title" : "Cookie Name",
        "description" : "The name of the cookie to set on the client.",
        "propertyOrder" : 1700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
    }
}
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.5. AdvancedProperties

### 1.5.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/advanced`

Resource version: `1.0`

#### 1.5.1.1. read

Usage:

```
am> read AdvancedProperties --global --serverName serverName
```

Parameters:

**--serverName**

An object of property key-value pairs

#### 1.5.1.2. update

Usage:

```
am> update AdvancedProperties --global --serverName serverName --body body
```

Parameters:

**--serverName**

An object of property key-value pairs

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "patternProperties" : {
    ".+" : {
      "type" : "string",
      "title" : "Value",
      "description" : "Any string value"
    }
  },
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "An object of property key-value pairs",
  "type" : "object",
  "title" : "Advanced Properties"
}
```

## 1.6. AgentGroups

### 1.6.1. Realm Operations

Aggregating Agent Groups handler that is responsible for querying the aggregating agent groups

Resource path: `/realm-config/agents/groups`

Resource version: `1.0`

#### 1.6.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AgentGroups --realm Realm --actionName getAllTypes
```

#### 1.6.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AgentGroups --realm Realm --actionName getCreatableTypes
```

#### 1.6.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AgentGroups --realm Realm --actionName nextdescendents
```

#### 1.6.1.4. query

Querying the aggregating agent groups

Usage:

```
am> query AgentGroups --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: `[*]`



## 1.7. AgentService

### 1.7.1. Global Operations

Resource path: `/global-config/agents/AgentService`

Resource version: `1.0`

#### 1.7.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AgentService --global --actionName getAllTypes
```

#### 1.7.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AgentService --global --actionName getCreatableTypes
```

#### 1.7.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AgentService --global --actionName nextdescendents
```

#### 1.7.1.4. read

Usage:

```
am> read AgentService --global
```

#### 1.7.1.5. update

Usage:

```
am> update AgentService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

## 1.8. Agents

### 1.8.1. Realm Operations

Aggregating Agents handler that is responsible for querying the aggregating agents

Resource path: `/realm-config/agents`

Resource version: `1.0`

#### 1.8.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Agents --realm Realm --actionName getAllTypes
```

#### 1.8.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Agents --realm Realm --actionName getCreatableTypes
```

#### 1.8.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Agents --realm Realm --actionName nextdescendents
```

#### 1.8.1.4. query

Querying the aggregating agents

Usage:

```
am> query Agents --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

## 1.8.2. Global Operations

Global and default configuration for agents

Resource path: `/global-config/agents`

Resource version: `1.0`

### 1.8.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Agents --global --actionName getAllTypes
```

### 1.8.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Agents --global --actionName getCreatableTypes
```

### 1.8.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Agents --global --actionName nextdescendents
```

## 1.9. AmsterModule

### 1.9.1. Realm Operations

Resource path: `/realm-config/authentication/modules/amster`

Resource version: `1.0`

### 1.9.1.1. create

Usage:

```
am> create AmsterModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabled" : {
      "title" : "Enabled",
      "description" : "If not enabled, prevents PKI login using the Amster module.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "authorizedKeys" : {
      "title" : "Authorized Keys",
      "description" : "The location of the authorized_keys file (which has the same format as an OpenSSH authorized_keys file) to use to validate remote Amster connections.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

### 1.9.1.2. delete

Usage:

```
am> delete AmsterModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.9.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AmsterModule --realm Realm --actionName getAllTypes
```

### 1.9.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AmsterModule --realm Realm --actionName getCreatableTypes
```

### 1.9.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AmsterModule --realm Realm --actionName nextdescendents
```

### 1.9.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query AmsterModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.9.1.7. read

Usage:

```
am> read AmsterModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.9.1.8. update

Usage:

```
am> update AmsterModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabled" : {
      "title" : "Enabled",
      "description" : "If not enabled, prevents PKI login using the Amster module.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "authorizedKeys" : {
      "title" : "Authorized Keys",
      "description" : "The location of the authorized_keys file (which has the same format as an
OpenSSH authorized_keys file) to use to validate remote Amster connections.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.9.2. Global Operations

Resource path: </global-config/authentication/modules/amster>

Resource version: 1.0

### 1.9.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AmsterModule --global --actionName getAllTypes
```

### 1.9.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AmsterModule --global --actionName getCreatableTypes
```

### 1.9.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AmsterModule --global --actionName nextdescendents
```

### 1.9.2.4. read

Usage:

```
am> read AmsterModule --global
```

### 1.9.2.5. update

Usage:

```
am> update AmsterModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authorizedKeys" : {
```

```

    "title" : "Authorized Keys",
    "description" : "The location of the authorized_keys file (which has the same format as an
OpenSSH authorized keys file) to use to validate remote Amster connections.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "enabled" : {
    "title" : "Enabled",
    "description" : "If not enabled, prevents PKI login using the Amster module.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.10. AnonymousModule

### 1.10.1. Realm Operations

Resource path: `/realm-config/authentication/modules/anonymous`

Resource version: `1.0`

#### 1.10.1.1. create

Usage:

```
am> create AnonymousModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.



--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultAnonymousUsername" : {
      "title" : "Default Anonymous User Name",
      "description" : "The default username to use if no username is supplied during authentication.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "validAnonymousUsers" : {
      "title" : "Valid Anonymous Users",
      "description" : "List of accounts that are allowed to login without providing
credentials.<br><br>Any username on this list will be allows anonymous access to OpenAM. Usernames
listed here must have matching profiles in the data store or the user profile requirement must be
disabled. The username can be specified during anonymous authentication as follows:<br><br><code>/
openam/UI/Login?module=anonymous&IDToken1=<i>username</i></code>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "caseSensitiveUsernameMatchingEnabled" : {
      "title" : "Case Sensitive User IDs",
      "description" : "If enabled, username matching will be case sensitive.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

### 1.10.1.2. delete

Usage:

```
am> delete AnonymousModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.10.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AnonymousModule --realm Realm --actionName getAllTypes
```

### 1.10.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AnonymousModule --realm Realm --actionName getCreatableTypes
```

### 1.10.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AnonymousModule --realm Realm --actionName nextdescendents
```

### 1.10.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query AnonymousModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.10.1.7. read

Usage:

```
am> read AnonymousModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.10.1.8. update

Usage:

```
am> update AnonymousModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultAnonymousUsername" : {
      "title" : "Default Anonymous User Name",
      "description" : "The default username to use if no username is supplied during authentication.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "validAnonymousUsers" : {
      "title" : "Valid Anonymous Users",
      "description" : "List of accounts that are allowed to login without providing
credentials.<br><br>Any username on this list will be allows anonymous access to OpenAM. Usernames
listed here must have matching profiles in the data store or the user profile requirement must be
disabled. The username can be specified during anonymous authentication as follows:<br><br><code>/
openam/UI/Login?module=anonymous&IDToken1=<i>username</i></code>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "caseSensitiveUsernameMatchingEnabled" : {
      "title" : "Case Sensitive User IDs",
      "description" : "If enabled, username matching will be case sensitive.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
}
```

```
"authenticationLevel" : {  
  "title" : "Authentication Level",  
  "description" : "The authentication level associated with this module.<br><br>Each  
authentication module has an authentication level that can be used to indicate the level of security  
associated with the module; 0 is the lowest (and the default).",  
  "propertyOrder" : 400,  
  "required" : true,  
  "type" : "integer",  
  "exampleValue" : ""  
}  
}  
}
```

## 1.10.2. Global Operations

Resource path: `/global-config/authentication/modules/anonymous`

Resource version: `1.0`

### 1.10.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AnonymousModule --global --actionName getAllTypes
```

### 1.10.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AnonymousModule --global --actionName getCreatableTypes
```

### 1.10.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AnonymousModule --global --actionName nextdescendents
```

### 1.10.2.4. read

Usage:

```
am> read AnonymousModule --global
```

## 1.10.2.5. update

Usage:

```
am> update AnonymousModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "defaultAnonymousUsername" : {
          "title" : "Default Anonymous User Name",
          "description" : "The default username to use if no username is supplied during authentication.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "validAnonymousUsers" : {
          "title" : "Valid Anonymous Users",
          "description" : "List of accounts that are allowed to login without providing credentials.<br><br>Any username on this list will be allows anonymous access to OpenAM. Usernames listed here must have matching profiles in the data store or the user profile requirement must be disabled. The username can be specified during anonymous authentication as follows:<br><br><code>/openam/UI/Login?module=anonymous&IDToken1=<i>username</i></code>",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "caseSensitiveUsernameMatchingEnabled" : {
          "title" : "Case Sensitive User IDs",
          "description" : "If enabled, username matching will be case sensitive.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
```

```
        "exampleValue" : ""
      },
    },
    "type" : "object",
    "title" : "Realm Defaults"
  }
}
```

## 1.11. ApplicationTypes

### 1.11.1. Realm Operations

Service for reading and listing the available application types. Application types act as templates for policy sets, and define how to compare resources and index policies. OpenAM provides a default application type that represents web resources called iPlanetAMWebAgentService

Resource path: `/applicationtypes`

Resource version: `1.0`

#### 1.11.1.1. query

Lists the application types using a query filter

Usage:

```
am> query ApplicationTypes --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

#### 1.11.1.2. read

Reads an individual application type by the provided application type name

Usage:

```
am> read ApplicationTypes --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.12. Applications

### 1.12.1. Realm Operations

Service for manipulating Applications. It supports the CRUDQ operations.

Resource path: `/applications`

Resource version: `2.1`

#### 1.12.1.1. create

Creates a new Application in a realm

Usage:

```
am> create Applications --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Application schema",
  "type" : "object",
  "title" : "Application",
  "properties" : {
    "name" : {
      "type" : "string",
      "title" : "Name",
      "description" : "Unique application identifier."
    },
    "displayName" : {
      "type" : "string",
      "title" : "Display name",
      "description" : "When defined, it is displayed in the UI instead of application name."
    },
    "description" : {
      "type" : "string",
      "title" : "Description",
      "description" : "String describing the application."
    },
    "applicationType" : {
      "type" : "string",
      "title" : "Application type",
      "description" : "Name of the application type used as a template for the policy set."
    },
    "conditions" : {
```

```

    "type" : "array",
    "items" : {
      "type" : "string",
      "title" : "Conditions",
      "description" : "Condition types allowed in the context of the policy set."
    }
  },
  "subjects" : {
    "type" : "array",
    "items" : {
      "type" : "string",
      "title" : "Subjects",
      "description" : "Subject types allowed in the context of the policy set."
    }
  },
  "resourceTypeUuids" : {
    "type" : "array",
    "items" : {
      "type" : "string",
      "title" : "Resource type uuids",
      "description" : "A list of the UUIDs of the resource types associated with the policy set."
    }
  },
  "entitlementCombiner" : {
    "type" : "string",
    "title" : "Entitlement combiner",
    "description" : "Name of the decision combiner, such as \"DenyOverride\"."
  },
  "searchIndex" : {
    "type" : "string",
    "title" : "Search index",
    "description" : "Class name of the implementation for searching indexes for resource names, such
as \"com.sun.identity.entitlement.util.ResourceNameSplitter\" for URL resource names."
  },
  "saveIndex" : {
    "type" : "string",
    "title" : "Save index",
    "description" : "Class name of the implementation for creating indexes for resource names, such
as \"com.sun.identity.entitlement.util.ResourceNameIndexGenerator\" for URL resource names."
  },
  "resourceComparator" : {
    "type" : "string",
    "title" : "Resource comparator",
    "description" : "Class name of the resource comparator implementation
used in the context of the policy set. The following implementations
are available: \"com.sun.identity.entitlement.ExactMatchResourceName\",
\"com.sun.identity.entitlement.PrefixResourceName\", \"com.sun.identity.entitlement.RegExResourceName
\", \"com.sun.identity.entitlement.URLResourceName\"."
  },
  "attributeNames" : {
    "type" : "array",
    "items" : {
      "type" : "string",
      "title" : "Attribute names",
      "description" : "A list of attribute names such as cn. The list is used to aid policy indexing
and lookup."
    }
  },
  "createdBy" : {

```



```

    "type" : "string",
    "title" : "Created by",
    "description" : "A string containing the universal identifier DN of the subject that created the
application."
  },
  "lastModifiedBy" : {
    "type" : "string",
    "title" : "Last modified by",
    "description" : "A string containing the universal identifier DN of the subject that most
recently updated the application. If the application has not been modified since it was created, this
will be the same value as createdBy."
  },
  "creationDate" : {
    "type" : "integer",
    "title" : "Creation date",
    "description" : "An integer containing the creation date and time, in number of seconds since
the Unix Epoch."
  },
  "lastModifiedDate" : {
    "type" : "integer",
    "title" : "Last modified date",
    "description" : "An integer containing the last modified date and time, in number of seconds
since the Unix Epoch. If the application has not been modified since it was created, this will be the
same value as creationDate."
  },
  "editable" : {
    "type" : "boolean",
    "title" : "Editable",
    "description" : "It indicates if application is editable."
  }
},
"required" : [ "name", "applicationType" ]
}

```

### 1.12.1.2. delete

Deletes an individual Application in a realm specified by its name

Usage:

```
am> delete Applications --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.12.1.3. query

Lists all the Applications in a realm

Usage:

```
am> query Applications --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

### 1.12.1.4. read

Reads an individual Application in a realm specified by its name

Usage:

```
am> read Applications --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.12.1.5. update

Updates an individual Application in a realm specified by its name

Usage:

```
am> update Applications --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Application schema",
  "type" : "object",
  "title" : "Application",
  "properties" : {
    "name" : {
      "type" : "string",
      "title" : "Name",
      "description" : "Unique application identifier."
    },
    "displayName" : {
      "type" : "string",
      "title" : "Display name",
      "description" : "When defined, it is displayed in the UI instead of application name."
    },
    "description" : {
      "type" : "string",
      "title" : "Description",
    }
  }
}
```

```

    "description" : "String describing the application."
  },
  "applicationType" : {
    "type" : "string",
    "title" : "Application type",
    "description" : "Name of the application type used as a template for the policy set."
  },
  "conditions" : {
    "type" : "array",
    "items" : {
      "type" : "string",
      "title" : "Conditions",
      "description" : "Condition types allowed in the context of the policy set."
    }
  },
  "subjects" : {
    "type" : "array",
    "items" : {
      "type" : "string",
      "title" : "Subjects",
      "description" : "Subject types allowed in the context of the policy set."
    }
  },
  "resourceTypeUuids" : {
    "type" : "array",
    "items" : {
      "type" : "string",
      "title" : "Resource type uuids",
      "description" : "A list of the UUIDs of the resource types associated with the policy set."
    }
  },
  "entitlementCombiner" : {
    "type" : "string",
    "title" : "Entitlement combiner",
    "description" : "Name of the decision combiner, such as \"DenyOverride\"."
  },
  "searchIndex" : {
    "type" : "string",
    "title" : "Search index",
    "description" : "Class name of the implementation for searching indexes for resource names, such as \"com.sun.identity.entitlement.util.ResourceNameSplitter\" for URL resource names."
  },
  "saveIndex" : {
    "type" : "string",
    "title" : "Save index",
    "description" : "Class name of the implementation for creating indexes for resource names, such as \"com.sun.identity.entitlement.util.ResourceNameIndexGenerator\" for URL resource names."
  },
  "resourceComparator" : {
    "type" : "string",
    "title" : "Resource comparator",
    "description" : "Class name of the resource comparator implementation used in the context of the policy set. The following implementations are available: \"com.sun.identity.entitlement.ExactMatchResourceName\", \"com.sun.identity.entitlement.PrefixResourceName\", \"com.sun.identity.entitlement.RegExResourceName\", \"com.sun.identity.entitlement.URLResourceName\"."
  },
  "attributeNames" : {
    "type" : "array",

```

```

    "items" : {
      "type" : "string",
      "title" : "Attribute names",
      "description" : "A list of attribute names such as cn. The list is used to aid policy indexing
and lookup."
    },
    "createdBy" : {
      "type" : "string",
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject that created the
application."
    },
    "lastModifiedBy" : {
      "type" : "string",
      "title" : "Last modified by",
      "description" : "A string containing the universal identifier DN of the subject that most
recently updated the application. If the application has not been modified since it was created, this
will be the same value as createdBy."
    },
    "creationDate" : {
      "type" : "integer",
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in number of seconds since
the Unix Epoch."
    },
    "lastModifiedDate" : {
      "type" : "integer",
      "title" : "Last modified date",
      "description" : "An integer containing the last modified date and time, in number of seconds
since the Unix Epoch. If the application has not been modified since it was created, this will be the
same value as creationDate."
    },
    "editable" : {
      "type" : "boolean",
      "title" : "Editable",
      "description" : "It indicates if application is editable."
    }
  },
  "required" : [ "name", "applicationType" ]
}

```

## 1.13. AuditEvent

### 1.13.1. Realm Operations

Audit events are logged through a realm audit service.

Resource path: `/realm-audit/{topic}`

Resource version: 1.0

### 1.13.1.1. create

Create a new audit event, which will be handled and logged by the configured audit service.

Usage:

```
am> create AuditEvent --realm Realm --topic topic --body body
```

Parameters:

**--topic**

Audit events are logged through a realm audit service.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The schema contains properties that are common to all topics and some that are
  unique to a specific topic. The description of each property indicates which topic the property
  applies to.",
  "title" : "Audit event schema",
  "type" : "object",
  "properties" : {
    "_id" : {
      "title" : "ID",
      "description" : "The ID of the event, used by all topics",
      "type" : "string"
    },
    "timestamp" : {
      "title" : "Timestamp",
      "description" : "The time at which the event occurred, used by all topics",
      "type" : "string"
    },
    "eventName" : {
      "title" : "Event name",
      "description" : "The name of the event, used by all topics",
      "type" : "string"
    },
    "transactionId" : {
      "title" : "Transaction ID",
      "description" : "The transaction ID of the event, used by all topics",
      "type" : "string"
    },
    "userId" : {
      "title" : "User ID",
      "description" : "The ID of the user responsible for the event, used by all topics",
      "type" : "string"
    },
    "trackingIds" : {
      "title" : "Tracking IDs",
      "description" : "The tracking IDs of the event, used by all topics",
      "type" : "array",
      "items" : {
        "id" : "0",
        "type" : "string"
      }
    }
  }
}
```

```

},
"component" : {
  "title" : "Component",
  "description" : "The component responsible for the event, used by all topics",
  "type" : "string"
},
"realm" : {
  "title" : "Realm",
  "description" : "The realm in which the event occurred, used by all topics",
  "type" : "string"
},
"server" : {
  "title" : "Server",
  "description" : "The server details for an access event",
  "type" : "object",
  "properties" : {
    "ip" : {
      "title" : "Server IP address",
      "description" : "The server ip address for an access event",
      "type" : "string"
    },
    "port" : {
      "title" : "Server port",
      "description" : "The server port for an access event",
      "type" : "integer"
    }
  }
},
"client" : {
  "title" : "Client",
  "description" : "The client details for an access event",
  "type" : "object",
  "properties" : {
    "ip" : {
      "title" : "Client IP address",
      "description" : "The client IP address for an access event",
      "type" : "string"
    },
    "port" : {
      "title" : "Client port",
      "description" : "The client port for an access event",
      "type" : "integer"
    }
  }
},
"request" : {
  "title" : "Request",
  "description" : "The request details for an access event",
  "type" : "object",
  "properties" : {
    "protocol" : {
      "title" : "Request protocol",
      "description" : "The request protocol for an access event",
      "type" : "string"
    },
    "operation" : {
      "title" : "Request operation",
      "description" : "The request operation for an access event",
      "type" : "string"
    }
  }
}

```

```

    },
    "detail" : {
      "title" : "Request detail",
      "description" : "The request detail for an access event",
      "type" : "object"
    }
  },
  "http" : {
    "title" : "Http details",
    "description" : "The Http details for an access event",
    "type" : "object",
    "properties" : {
      "request" : {
        "title" : "Http request",
        "description" : "The http request for an access event",
        "type" : "object",
        "properties" : {
          "secure" : {
            "title" : "Http secure",
            "description" : "The http secure property for an access event",
            "type" : "boolean"
          },
          "method" : {
            "title" : "Http method",
            "description" : "The http method for an access event",
            "type" : "string"
          },
          "path" : {
            "title" : "Http path",
            "description" : "The http path for an access event",
            "type" : "string"
          },
          "queryParameters" : {
            "title" : "Http query parameters",
            "description" : "The http query parameters for an access event",
            "type" : "object",
            "additionalProperties" : {
              "type" : "array",
              "items" : {
                "type" : "string"
              }
            }
          }
        }
      },
      "headers" : {
        "title" : "Http headers",
        "description" : "The http headers for an access event",
        "type" : "object",
        "additionalProperties" : {
          "type" : "array",
          "items" : {
            "type" : "string"
          }
        }
      },
      "cookies" : {
        "title" : "Http cookies",
        "description" : "The http cookies for an access event",
        "type" : "object",

```

```

        "additionalProperties" : {
            "type" : "string"
        }
    }
},
"response" : {
    "title" : "Http response",
    "description" : "The http response for an access event",
    "type" : "object",
    "properties" : {
        "headers" : {
            "title" : "Http request headers",
            "description" : "The http request headers for an access event",
            "type" : "object",
            "additionalProperties" : {
                "type" : "array",
                "items" : {
                    "type" : "string"
                }
            }
        }
    }
},
},
"response" : {
    "title" : "Response",
    "description" : "The response details for an access event",
    "type" : "object",
    "properties" : {
        "status" : {
            "title" : "Response status",
            "description" : "The response status for an access event",
            "type" : "string"
        },
        "statusCode" : {
            "title" : "Response status code",
            "description" : "The response status code for an access event",
            "type" : "string"
        },
        "detail" : {
            "title" : "Response detail",
            "description" : "The response detail for an access event",
            "type" : "object"
        },
        "elapsedTime" : {
            "title" : "Response elapsed time",
            "description" : "The response elapsedTime for an access event",
            "type" : "integer"
        },
        "elapsedTimeUnits" : {
            "title" : "Response elapsed time units",
            "description" : "The response elapsed time units for an access event",
            "type" : "string"
        }
    }
},
"runAs" : {

```



```

    "title" : "Run as",
    "description" : "What the change that triggered an activity or config event was run as",
    "type" : "string"
  },
  "objectId" : {
    "title" : "Object ID",
    "description" : "The object ID of the change that triggered an activity or config event",
    "type" : "string"
  },
  "operation" : {
    "title" : "Operation",
    "description" : "The operation that triggered an activity or config event",
    "type" : "string"
  },
  "before" : {
    "title" : "Before state",
    "description" : "The state before an activity or config event occurred",
    "type" : "object"
  },
  "after" : {
    "title" : "After state",
    "description" : "The state after an activity or config event occurred",
    "type" : "object"
  },
  "changedFields" : {
    "title" : "Changed fields",
    "description" : "The changed fields after an activity or config event occurred",
    "type" : "array",
    "items" : {
      "id" : "1",
      "type" : "string"
    }
  },
  "revision" : {
    "title" : "Revision",
    "description" : "The revision for an activity or config event",
    "type" : "string"
  },
  "result" : {
    "title" : "Result",
    "description" : "The result of the authentication event",
    "type" : "string"
  },
  "principal" : {
    "title" : "Principal",
    "description" : "The principal responsible for the authentication event",
    "type" : "array",
    "items" : {
      "type" : "string"
    }
  },
  "context" : {
    "title" : "Context",
    "description" : "The context of an authentication event",
    "type" : "object",
    "properties" : { }
  },
  "entries" : {
    "title" : "Entries",

```

```

    "description" : "The entries for an authentication event",
    "type" : "array",
    "items" : {
      "type" : "object",
      "properties" : {
        "moduleId" : {
          "title" : "Module ID",
          "description" : "The module ID for the authentication event",
          "type" : "string"
        },
        "result" : {
          "title" : "Module result",
          "description" : "The result of the module authentication event",
          "type" : "string"
        },
        "info" : {
          "title" : "Entries information",
          "description" : "The entries information for an authentication event",
          "type" : "object",
          "properties" : { }
        }
      }
    }
  },
  "required" : [ "transactionId", "timestamp" ]
}

```

## 1.13.2. Global Operations

Audit events are logged through the global audit service.

Resource path: `/global-audit/{topic}`

Resource version: **1.0**

### 1.13.2.1. create

Create a new audit event, which will be handled and logged by the configured audit service.

Usage:

```
am> create AuditEvent --global --topic topic --body body
```

Parameters:

**--topic**

Audit events are logged through the global audit service.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",

```

```

"description" : "The schema contains properties that are common to all topics and some that are
unique to a specific topic. The description of each property indicates which topic the property
applies to.",
"title" : "Audit event schema",
"type" : "object",
"properties" : {
  "_id" : {
    "title" : "ID",
    "description" : "The ID of the event, used by all topics",
    "type" : "string"
  },
  "timestamp" : {
    "title" : "Timestamp",
    "description" : "The time at which the event occurred, used by all topics",
    "type" : "string"
  },
  "eventName" : {
    "title" : "Event name",
    "description" : "The name of the event, used by all topics",
    "type" : "string"
  },
  "transactionId" : {
    "title" : "Transaction ID",
    "description" : "The transaction ID of the event, used by all topics",
    "type" : "string"
  },
  "userId" : {
    "title" : "User ID",
    "description" : "The ID of the user responsible for the event, used by all topics",
    "type" : "string"
  },
  "trackingIds" : {
    "title" : "Tracking IDs",
    "description" : "The tracking IDs of the event, used by all topics",
    "type" : "array",
    "items" : {
      "id" : "0",
      "type" : "string"
    }
  },
  "component" : {
    "title" : "Component",
    "description" : "The component responsible for the event, used by all topics",
    "type" : "string"
  },
  "realm" : {
    "title" : "Realm",
    "description" : "The realm in which the event occurred, used by all topics",
    "type" : "string"
  },
  "server" : {
    "title" : "Server",
    "description" : "The server details for an access event",
    "type" : "object",
    "properties" : {
      "ip" : {
        "title" : "Server IP address",
        "description" : "The server ip address for an access event",
        "type" : "string"
      }
    }
  }
}

```

```

    },
    "port" : {
      "title" : "Server port",
      "description" : "The server port for an access event",
      "type" : "integer"
    }
  }
},
"client" : {
  "title" : "Client",
  "description" : "The client details for an access event",
  "type" : "object",
  "properties" : {
    "ip" : {
      "title" : "Client IP address",
      "description" : "The client IP address for an access event",
      "type" : "string"
    },
    "port" : {
      "title" : "Client port",
      "description" : "The client port for an access event",
      "type" : "integer"
    }
  }
},
"request" : {
  "title" : "Request",
  "description" : "The request details for an access event",
  "type" : "object",
  "properties" : {
    "protocol" : {
      "title" : "Request protocol",
      "description" : "The request protocol for an access event",
      "type" : "string"
    },
    "operation" : {
      "title" : "Request operation",
      "description" : "The request operation for an access event",
      "type" : "string"
    },
    "detail" : {
      "title" : "Request detail",
      "description" : "The request detail for an access event",
      "type" : "object"
    }
  }
},
"http" : {
  "title" : "Http details",
  "description" : "The Http details for an access event",
  "type" : "object",
  "properties" : {
    "request" : {
      "title" : "Http request",
      "description" : "The http request for an access event",
      "type" : "object",
      "properties" : {
        "secure" : {
          "title" : "Http secure",

```

```

        "description" : "The http secure property for an access event",
        "type" : "boolean"
    },
    "method" : {
        "title" : "Http method",
        "description" : "The http method for an access event",
        "type" : "string"
    },
    "path" : {
        "title" : "Http path",
        "description" : "The http path for an access event",
        "type" : "string"
    },
    "queryParameters" : {
        "title" : "Http query parameters",
        "description" : "The http query parameters for an access event",
        "type" : "object",
        "additionalProperties" : {
            "type" : "array",
            "items" : {
                "type" : "string"
            }
        }
    },
    "headers" : {
        "title" : "Http headers",
        "description" : "The http headers for an access event",
        "type" : "object",
        "additionalProperties" : {
            "type" : "array",
            "items" : {
                "type" : "string"
            }
        }
    },
    "cookies" : {
        "title" : "Http cookies",
        "description" : "The http cookies for an access event",
        "type" : "object",
        "additionalProperties" : {
            "type" : "string"
        }
    }
},
"response" : {
    "title" : "Http response",
    "description" : "The http response for an access event",
    "type" : "object",
    "properties" : {
        "headers" : {
            "title" : "Http request headers",
            "description" : "The http request headers for an access event",
            "type" : "object",
            "additionalProperties" : {
                "type" : "array",
                "items" : {
                    "type" : "string"
                }
            }
        }
    }
}

```

```

    }
  }
}
},
"response" : {
  "title" : "Response",
  "description" : "The response details for an access event",
  "type" : "object",
  "properties" : {
    "status" : {
      "title" : "Response status",
      "description" : "The response status for an access event",
      "type" : "string"
    },
    "statusCode" : {
      "title" : "Response status code",
      "description" : "The response status code for an access event",
      "type" : "string"
    },
    "detail" : {
      "title" : "Response detail",
      "description" : "The response detail for an access event",
      "type" : "object"
    },
    "elapsedTime" : {
      "title" : "Response elapsed time",
      "description" : "The response elapsedTime for an access event",
      "type" : "integer"
    },
    "elapsedTimeUnits" : {
      "title" : "Response elapsed time units",
      "description" : "The response elapsed time units for an access event",
      "type" : "string"
    }
  }
},
"runAs" : {
  "title" : "Run as",
  "description" : "What the change that triggered an activity or config event was run as",
  "type" : "string"
},
"objectId" : {
  "title" : "Object ID",
  "description" : "The object ID of the change that triggered an activity or config event",
  "type" : "string"
},
"operation" : {
  "title" : "Operation",
  "description" : "The operation that triggered an activity or config event",
  "type" : "string"
},
"before" : {
  "title" : "Before state",
  "description" : "The state before an activity or config event occurred",
  "type" : "object"
},
"after" : {

```

```

    "title" : "After state",
    "description" : "The state after an activity or config event occurred",
    "type" : "object"
  },
  "changedFields" : {
    "title" : "Changed fields",
    "description" : "The changed fields after an activity or config event occurred",
    "type" : "array",
    "items" : {
      "id" : "1",
      "type" : "string"
    }
  },
  "revision" : {
    "title" : "Revision",
    "description" : "The revision for an activity or config event",
    "type" : "string"
  },
  "result" : {
    "title" : "Result",
    "description" : "The result of the authentication event",
    "type" : "string"
  },
  "principal" : {
    "title" : "Principal",
    "description" : "The principal responsible for the authentication event",
    "type" : "array",
    "items" : {
      "type" : "string"
    }
  },
  "context" : {
    "title" : "Context",
    "description" : "The context of an authentication event",
    "type" : "object",
    "properties" : { }
  },
  "entries" : {
    "title" : "Entries",
    "description" : "The entries for an authentication event",
    "type" : "array",
    "items" : {
      "type" : "object",
      "properties" : {
        "moduleId" : {
          "title" : "Module ID",
          "description" : "The module ID for the authentication event",
          "type" : "string"
        }
      },
      "result" : {
        "title" : "Module result",
        "description" : "The result of the module authentication event",
        "type" : "string"
      }
    },
    "info" : {
      "title" : "Entries information",
      "description" : "The entries information for an authentication event",
      "type" : "object",
      "properties" : { }
    }
  }
}

```

```
    }  
  }  
},  
"required" : [ "transactionId", "timestamp" ]  
}
```

## 1.14. AuditLogging

### 1.14.1. Realm Operations

Resource path: `/realm-config/services/audit`

Resource version: `1.0`

#### 1.14.1.1. create

Usage:

```
am> create AuditLogging --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:



```
{
  "type" : "object",
  "properties" : {
    "auditEnabled" : {
      "title" : "Audit logging",
      "description" : "Enable audit logging in OpenAM.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "fieldFilterPolicy" : {
      "title" : "Field exclusion policies",
      "description" : "A list of fields or values (JSON pointers) to exclude from the audit event.<br><br>To specify a field or value within a field to be filtered out of the event, start the pointer with the event topic, for example access, activity, authentication, or config, followed by the field name or the path to the value in the field.<p><p>For example, to filter out the <code>userId</code> field in an access event the pointer will be <code>/access/userId</code>.<p>To filter out the <code>content-type</code> value in the <code>http.request.headers</code> field the pointer will be <code>/access/http/request/headers/content-type</code>.<p>Only values that are made up of JSON strings can be manipulated in this way.",
      "propertyOrder" : 200,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

### 1.14.1.2. delete

Usage:

```
am> delete AuditLogging --realm Realm
```

### 1.14.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuditLogging --realm Realm --actionName getAllTypes
```

### 1.14.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuditLogging --realm Realm --actionName getCreatableTypes
```

#### 1.14.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuditLogging --realm Realm --actionName nextdescendents
```

#### 1.14.1.6. read

Usage:

```
am> read AuditLogging --realm Realm
```

#### 1.14.1.7. update

Usage:

```
am> update AuditLogging --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "auditEnabled" : {
      "title" : "Audit logging",
      "description" : "Enable audit logging in OpenAM.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "fieldFilterPolicy" : {
      "title" : "Field exclusion policies",
      "description" : "A list of fields or values (JSON pointers) to exclude from the audit event.<br><br>To specify a field or value within a field to be filtered out of the event, start the pointer with the event topic, for example access, activity, authentication, or config, followed by the field name or the path to the value in the field.<p><p>For example, to filter out the <code>userId</code> field in an access event the pointer will be <code>/access/userId</code>.<p>To filter out the <code>content-type</code> value in the <code>http.request.headers</code> field the pointer will be <code>/access/http/request/headers/content-type</code>.<p>Only values that are made up of JSON strings can be manipulated in this way.",
      "propertyOrder" : 200,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.14.2. Global Operations

Resource path: `/global-config/services/audit`

Resource version: `1.0`

### 1.14.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuditLogging --global --actionName getAllTypes
```

### 1.14.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuditLogging --global --actionName getCreatableTypes
```

### 1.14.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuditLogging --global --actionName nextdescendents
```

### 1.14.2.4. read

Usage:

```
am> read AuditLogging --global
```

### 1.14.2.5. update

Usage:

```
am> update AuditLogging --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "auditEnabled" : {
      "title" : "Audit logging",
      "description" : "Enable audit logging in OpenAM.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "fieldFilterPolicy" : {
      "title" : "Field exclusion policies",
      "description" : "A list of fields or values (JSON pointers) to exclude from the audit event.<br><br>To specify a field or value within a field to be filtered out of the event, start the pointer with the event topic, for example access, activity, authentication, or config, followed by the field name or the path to the value in the field.<p><p>For example, to filter out the <code>userId</code> field in an access event the pointer will be <code>/access/userId</code>.<p>To filter out the <code>content-type</code> value in the <code>http.request.headers</code> field the pointer will be <code>/access/http/request/headers/content-type</code>.<p>Only values that are made up of JSON strings can be manipulated in this way.",
      "propertyOrder" : 200,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

```

    },
    "defaults" : {
      "properties" : {
        "fieldFilterPolicy" : {
          "title" : "Field exclusion policies",
          "description" : "A list of fields or values (JSON pointers) to exclude from the audit event.<br><br>To specify a field or value within a field to be filtered out of the event, start the pointer with the event topic, for example access, activity, authentication, or config, followed by the field name or the path to the value in the field.<p><p>For example, to filter out the <code>userId</code> field in an access event the pointer will be <code>/access/userId</code>.<p>To filter out the <code>content-type</code> value in the <code>http.request.headers</code> field the pointer will be <code>/access/http/request/headers/content-type</code>.<p>Only values that are made up of JSON strings can be manipulated in this way.",
          "propertyOrder" : 200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "auditEnabled" : {
          "title" : "Audit logging",
          "description" : "Enable audit logging in OpenAM.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}

```

## 1.15. Authentication

### 1.15.1. Realm Operations

Resource path: `/realm-config/authentication`

Resource version: `1.0`

#### 1.15.1.1. create

Usage:

```
am> create Authentication --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "general" : {
      "type" : "object",
      "title" : "General",
      "propertyOrder" : 3,
      "properties" : {
        "identityType" : {
          "title" : "Identity Types",
          "description" : "",
          "propertyOrder" : 2500,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userStatusCallbackPlugins" : {
          "title" : "Pluggable User Status Event Classes",
          "description" : "List of classes to be called when status of the user account
changes.<br><br>When the status of a users account changes, OpenAM can be configured to call into
a custom class. The custom class can then be used to perform some action as required. The built in
status change events are:<br><br><ul><li>Account locked</li><li>Password changed</li></ul><br>
>Custom code can also extend this mechanism.",
          "propertyOrder" : 2600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "twoFactorRequired" : {
          "title" : "Two Factor Authentication Mandatory",
          "description" : "",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "locale" : {
          "title" : "Default Authentication Locale",
          "description" : "",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultAuthLevel" : {
          "title" : "Default Authentication Level",
          "description" : "The default authentication level for modules in this realm.<br><br>If
the authentication module does not set it's own auth level then the module will have the default
authentication level for the realm.",

```

```

    "propertyOrder" : 4100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "statelessSessionsEnabled" : {
    "title" : "Use Stateless Sessions",
    "description" : "Enables stateless sessions.<br><br>Stateless sessions provide elastic
scalability by storing all session state on the client in the SSO cookie. See Session service
configuration to enable signing and encryption (HIGHLY RECOMMENDED).",
    "propertyOrder" : 3800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }
},
"core" : {
  "type" : "object",
  "title" : "Core",
  "propertyOrder" : -1,
  "properties" : {
    "orgConfig" : {
      "title" : "Organization Authentication Configuration",
      "description" : "Default Authentication Chain for users<br><br>This is the authentication
chain that will be used to authenticate users to this realm.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "adminAuthModule" : {
      "title" : "Administrator Authentication Configuration",
      "description" : "Default Authentication Chain for administrators<br><br>This is the
authentication chain that will be used to authentication administrative users to this realm.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
},
"security" : {
  "type" : "object",
  "title" : "Security",
  "propertyOrder" : 4,
  "properties" : {
    "sharedSecret" : {
      "title" : "Organization Authentication Signing Secret",
      "description" : "HMAC shared secret for signing RESTful Authentication requests.<br><br>This
is the shared secret for signing state used in RESTful authentication requests. Should be at Base-64
encoded and at least 128-bits in length. By default a cryptographically secure random value is
generated.",
      "propertyOrder" : 4000,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
},

```

```

    "zeroPageLoginAllowedWithoutReferrer" : {
      "title" : "Zero Page Login Allowed without Referrer?",
      "description" : "Whether to allow Zero Page Login if the HTTP Referer header is
missing.<br><br>The HTTP Referer header is sometimes missing from requests (e.g., if making a request
to HTTP from HTTPS). This setting controls whether such requests should be allowed or not. Setting
to 'true' will reduce the risk of Login CSRF attacks with Zero Page Login, but may potentially deny
legitimate requests.",
      "propertyOrder" : 3700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "keyAlias" : {
      "title" : "Persistent Cookie Encryption Certificate Alias",
      "description" : "Keystore Alias for encrypting Persistent Cookies.<br><br>This is the alias
for the private/public keys in the Keystore used in Persistent Cookie authentication requests.",
      "propertyOrder" : 3300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "zeroPageLoginReferrerWhiteList" : {
      "title" : "Zero Page Login Referrer Whitelist",
      "description" : "List of allowed HTTP Referer (sic) URLs from which Zero Page Login requests
are allowed.<br><br>Enter here all URLs from which you want to allow Zero Page Login. This provides
some mitigation against Login CSRF attacks. Leave empty to allow from any Referer. Applies to both
GET and POST login requests.",
      "propertyOrder" : 3600,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "moduleBasedAuthEnabled" : {
      "title" : "Module Based Authentication",
      "description" : "Allows a user to authenticate via module based authentication.<br><br>The
feature allow users to override the realm configuration and use a named authentication module to
authenticate.<br><br><i>NB </i>Recommended to turn this feature off in production environments.",
      "propertyOrder" : 2800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "zeroPageLoginEnabled" : {
      "title" : "Zero Page Login",
      "description" : "Allows a user to authenticate using GET request parameters without
showing the login screen.<br><br>Enable this feature if the authentication mechanism uses a single
authentication screen or the first authentication screen should always be invisible to users (since
it is auto-submitted). Use caution when enabling this feature as it can be used to authenticate using
regular GET parameters, which could be cached by browsers and logged in server and proxy access logs
exposing the values of the GET parameters.",
      "propertyOrder" : 3400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}

```



```

},
"userprofile" : {
  "type" : "object",
  "title" : "User Profile",
  "propertyOrder" : 0,
  "properties" : {
    "dynamicProfileCreation" : {
      "title" : "User Profile",
      "description" : "Controls the result of the user profile success post successful authentication.<br><br>Controls whether a user profile is required for authentication to be successful or if the profile will be dynamically created if none already exists. Choose ignore if you do not have a data store configured in the realm.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "aliasAttributeName" : {
      "title" : "Alias Search Attribute Name",
      "description" : "The secondary LDAP attribute retrieves the user profile if the primary LDAP attribute specified in 'User Naming Attribute' fails.<br><br>This list of LDAP attributes is used to extend the set of attributes searched by OpenAM to find the users profile.<br>For example: <ul><li>cn</li><li>mail</li><li>givenname</li></ul><br>A user authenticates to OpenAM under the id of steve, OpenAM will first search using the naming attribute (uid by default) so uid=steve, if no match is found then cn=steve will be searched until a match is found or the list is exhausted.<br><br><i>NB </i> Only used when User Profile searching is enabled.",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaultRole" : {
      "title" : "User Profile Dynamic Creation Default Roles",
      "description" : "List of roles of which dynamically created users will be a member.<br><br>Enter the DN for each role that will be assigned to a new user when their profile has been dynamically created by OpenAM.<br><br><i>NB </i> Deprecated functionality in OpenAM.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
},
"accountlockout" : {
  "type" : "object",
  "title" : "Account Lockout",
  "propertyOrder" : 2,
  "properties" : {
    "lockoutEmailAddress" : {
      "title" : "Email Address to Send Lockout Notification",
      "description" : "An email address or set of email addresses that receive notifications about account lockout events.<br><br>OpenAM can be configured to send a localisable email message to a set of email addresses when account lockout events occur. The contents of the

```

email message is configured using the following properties in the `amAuth.properties` file.

- `lockOutEmailFrom` : The `"From"` address of the email message
- `lockOutEmailSub` : The subject of the email message
- `lockOutEmailMsg` : The contents of the email message

The identity for whom the account has been locked is included in the email message.

The format of this property is: `<emailaddress|locale|charset>`. Multiple email addresses are space-separated. Email addresses must include the domain name, such as `admin@example.com`.

```

    "propertyOrder" : 1100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lockoutWarnUserCount" : {
    "title" : "Warn User After N Failures",
    "description" : "Warn the user when they reach this level of failed
authentications.

The user will be given a warning when they reach this level of failed
authentications during the lockout interval.

The text of the lockout warning is configured using the
lockOutWarning property in the amAuth.properties file.",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "lockoutDurationMultiplier" : {
    "title" : "Lockout Duration Multiplier",
    "description" : "Value multiplied to the Login Failure Lockout Duration for each successive
lockout.

This property is used to enable OpenAM to increase the account lockout duration for
each successive account lockout. For example: If the lockout duration is set to 10 and the duration
multiplier is set to 2; the duration of the first lockout will be 10 minutes and the duration of the
second lockout will be 20 minutes.

The default value of 1 disables this function. ",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "loginFailureDuration" : {
    "title" : "Login Failure Lockout Interval",
    "description" : "The lockout interval time is in minutes.

OpenAM tracks the failed
authentication count for a user over the lockout interval.

For example: If the lockout
interval is 5 minutes and the lockout count is 5; the user will have to have failed to authenticate
5 times over the previous 5 minutes for the account to be locked. Failed authentications the occurred
outside of the 5 minute interval are ignored.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "lockoutAttributeValue" : {
    "title" : "Lockout Attribute Value",
    "description" : "Value to set in custom lockout attribute

This is the value that will
be set on the custom attribute in the users profile when they account is locked.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lockoutDuration" : {
    "title" : "Login Failure Lockout Duration",

```

```

    "description" : "The duration of the users account lockout, in minutes.<br><br>OpenAM can
either lockout the users account indefinitely (until administration action) by setting the duration
to 0, (the default) or OpenAM can lock the users account for a given number of minutes. After the
lockout interval, the user will be able to successfully authenticate to OpenAM.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "loginFailureCount" : {
    "title" : "Login Failure Lockout Count",
    "description" : "The maximum number of failed authentications for a user before their
account is locked.<br><br>This setting controls the maximum number of failed authentications a user
can have during the lockout interval before OpenAM locks the users account.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "loginFailureLockoutMode" : {
    "title" : "Login Failure Lockout Mode",
    "description" : "Enables account lockout functionality for users authenticating to this
realm.<br><br>OpenAM can track the number of failed authentications by a user over time and if a pre-
defined limit is breached, OpenAM can lockout the users account and perform additional functions.<br>
<br><i>NB </i>This functionality is in addition to any account lockout behaviour implemented by the
LDAP Directory Server.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invalidAttemptsDataAttributeName" : {
    "title" : "Invalid Attempts Data Attribute Name",
    "description" : "The name of the attribute used to store information about failed
authentications.<br><br>OpenAM can be configured to store information about invalid authentications
in the users profile. This allows multiple instances of OpenAM in the same site to share
information about a users invalid authentication attempts. By default the custom attribute;
<code>sunAMAuthInvalidAttemptsData</code> defined in the <code>sunAMAuthAccountLockout</code>
objectclass is used to store this data. Use this property to change the attribute used by OpenAM to
store this information.<br><br><i>NB </i>Any attribute specified must be a valid attribute in the
data store.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "storeInvalidAttemptsInDataStore" : {
    "title" : "Store Invalid Attempts in Data Store",
    "description" : "Enables sharing of login failure attempts across AM Instances<br><br>When
this setting is enabled OpenAM will store the users invalid authentication information in the data
store under the attribute configured in the <i>Invalid Attempts Data Attribute Name</i> property.",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "lockoutAttributeName" : {
    "title" : "Lockout Attribute Name",

```

```

        "description" : "Name of custom lockout attribute <br><br>When OpenAM locks an account, the
<code>inetuserstatus</code> attribute in the locked account is set to Inactive. In addition, OpenAM
can set the value of another attribute in the users profile. ",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"postauthprocess" : {
    "type" : "object",
    "title" : "Post Authentication Processing",
    "propertyOrder" : 5,
    "properties" : {
        "usernameGeneratorClass" : {
            "title" : "Pluggable User Name Generator Class",
            "description" : "The name of the default implementation of the user name
generator class.<br><br>The name of the class used to return a list of usernames to
the Membership auth module.<br><br><i>NB </i>This class must implement the interface
<code>com.sun.identity.authentication.spi.UserIDGenerator</code>",
            "propertyOrder" : 2200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "userAttributeSessionMapping" : {
            "title" : "User Attribute Mapping to Session Attribute",
            "description" : "Mapping of user profile attribute name to session attribute
name.<br><br>The setting causes OpenAM to read the named attributes from the users profile in the
data store and store their values in the users session.<br><br>Format: User Profile Attribute|
Session Attribute name. ",
            "propertyOrder" : 3000,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "loginSuccessUrl" : {
            "title" : "Default Success Login URL",
            "description" : "Successful logins will be forwarded to this URL<br><br>This is the URL to
which clients will be forwarded upon successful authentication. Enter a URL or URI relative to the
local OpenAM. URL or URI can be prefixed with the ClientType|URL if client specific. URL without
http(s) protocol will be appended to the current URI of OpenAM.",
            "propertyOrder" : 1800,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "usernameGeneratorEnabled" : {
            "title" : "Generate UserID Mode",
            "description" : "Enables this mode in the Membership auth module.<br><br>When this mode is
enabled, if the Membership auth module detects that the supplied username already exists in the data
store then a list of valid usernames can be shown to the user, if requested by said user.",

```

```

        "propertyOrder" : 2100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "loginFailureUrl" : {
        "title" : "Default Failure Login URL ",
        "description" : "Failed logins will be forwarded to this URL<br><br>This is the URL to
which clients will be forwarded upon failed authentication. Enter a URL or URI relative to the
local OpenAM. URL or URI can be prefixed with ClientType|URL if client specific. URL without http(s)
protocol will be appended to the current URI of OpenAM.",
        "propertyOrder" : 1900,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "loginPostProcessClass" : {
        "title" : "Authentication Post Processing Classes",
        "description" : "A list of post authentication processing classes for all users
in this realm.<br><br>This is a list of Post Processing Classes that will be called by
OpenAM for all users that authenticate to this realm. Refer to the documentation for the
places where the list of post authentication classes can be set and their precedence.
<br><br>For example: org.forgerock.auth.PostProcessClass<br><i>NB </i>OpenAM must be
able to find these classes on the <code>CLASSPATH</code> and must implement the interface
<code>com.sun.identity.authentication.spi.AMPostAuthProcessInterface</code>.",
        "propertyOrder" : 2000,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    }
}
}
}
}
}

```

### 1.15.1.2. delete

Usage:

```
am> delete Authentication --realm Realm
```

### 1.15.1.3. read

Usage:

```
am> read Authentication --realm Realm
```

## 1.15.1.4. update

Usage:

```
am> update Authentication --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "general" : {
      "type" : "object",
      "title" : "General",
      "propertyOrder" : 3,
      "properties" : {
        "identityType" : {
          "title" : "Identity Types",
          "description" : "",
          "propertyOrder" : 2500,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userStatusCallbackPlugins" : {
          "title" : "Pluggable User Status Event Classes",
          "description" : "List of classes to be called when status of the user account changes.<br><br>When the status of a users account changes, OpenAM can be configured to call into a custom class. The custom class can then be used to perform some action as required. The built in status change events are:<br><br><ul><li>Account locked</li><li>Password changed</li></ul><br>>Custom code can also extend this mechanism.",
          "propertyOrder" : 2600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "twoFactorRequired" : {
          "title" : "Two Factor Authentication Mandatory",
          "description" : "",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "locale" : {
          "title" : "Default Authentication Locale",
          "description" : "",
          "propertyOrder" : 600,

```

```

        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "defaultAuthLevel" : {
        "title" : "Default Authentication Level",
        "description" : "The default authentication level for modules in this realm.<br><br>If
the authentication module does not set it's own auth level then the module will have the default
authentication level for the realm.",
        "propertyOrder" : 4100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "statelessSessionsEnabled" : {
        "title" : "Use Stateless Sessions",
        "description" : "Enables stateless sessions.<br><br>Stateless sessions provide elastic
scalability by storing all session state on the client in the SSO cookie. See Session service
configuration to enable signing and encryption (HIGHLY RECOMMENDED).",
        "propertyOrder" : 3800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
    },
    "core" : {
        "type" : "object",
        "title" : "Core",
        "propertyOrder" : -1,
        "properties" : {
            "orgConfig" : {
                "title" : "Organization Authentication Configuration",
                "description" : "Default Authentication Chain for users<br><br>This is the authentication
chain that will be used to authenticate users to this realm.",
                "propertyOrder" : 700,
                "required" : true,
                "type" : "string",
                "exampleValue" : ""
            },
            "adminAuthModule" : {
                "title" : "Administrator Authentication Configuration",
                "description" : "Default Authentication Chain for administrators<br><br>This is the
authentication chain that will be used to authentication administrative users to this realm.",
                "propertyOrder" : 200,
                "required" : true,
                "type" : "string",
                "exampleValue" : ""
            }
        }
    },
    "security" : {
        "type" : "object",
        "title" : "Security",
        "propertyOrder" : 4,
        "properties" : {
            "sharedSecret" : {
                "title" : "Organization Authentication Signing Secret",

```

```

    "description" : "HMAC shared secret for signing RESTful Authentication requests.<br><br>This is the shared secret for signing state used in RESTful authentication requests. Should be at Base-64 encoded and at least 128-bits in length. By default a cryptographically secure random value is generated.",
    "propertyOrder" : 4000,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "zeroPageLoginAllowedWithoutReferrer" : {
    "title" : "Zero Page Login Allowed without Referrer?",
    "description" : "Whether to allow Zero Page Login if the HTTP Referrer header is missing.<br><br>The HTTP Referrer header is sometimes missing from requests (e.g., if making a request to HTTP from HTTPS). This setting controls whether such requests should be allowed or not. Setting to 'true' will reduce the risk of Login CSRF attacks with Zero Page Login, but may potentially deny legitimate requests.",
    "propertyOrder" : 3700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "keyAlias" : {
    "title" : "Persistent Cookie Encryption Certificate Alias",
    "description" : "Keystore Alias for encrypting Persistent Cookies.<br><br>This is the alias for the private/public keys in the Keystore used in Persistent Cookie authentication requests.",
    "propertyOrder" : 3300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "zeroPageLoginReferrerWhiteList" : {
    "title" : "Zero Page Login Referrer Whitelist",
    "description" : "List of allowed HTTP Referrer (sic) URLs from which Zero Page Login requests are allowed.<br><br>Enter here all URLs from which you want to allow Zero Page Login. This provides some mitigation against Login CSRF attacks. Leave empty to allow from any Referrer. Applies to both GET and POST login requests.",
    "propertyOrder" : 3600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "moduleBasedAuthEnabled" : {
    "title" : "Module Based Authentication",
    "description" : "Allows a user to authenticate via module based authentication.<br><br>The feature allow users to override the realm configuration and use a named authentication module to authenticate.<br><br><i>NB Recommended to turn this feature off in production environments.",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "zeroPageLoginEnabled" : {
    "title" : "Zero Page Login",
    "description" : "Allows a user to authenticate using GET request parameters without showing the login screen.<br><br>Enable this feature if the authentication mechanism uses a single

```



```

authentication screen or the first authentication screen should always be invisible to users (since
it is auto-submitted). Use caution when enabling this feature as it can be used to authenticate using
regular GET parameters, which could be cached by browsers and logged in server and proxy access logs
exposing the values of the GET parameters.",
    "propertyOrder" : 3400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }
},
"userprofile" : {
  "type" : "object",
  "title" : "User Profile",
  "propertyOrder" : 0,
  "properties" : {
    "dynamicProfileCreation" : {
      "title" : "User Profile",
      "description" : "Controls the result of the user profile success post successful
authentication.<br><br>Controls whether a user profile is required for authentication to be
successful or if the profile will be dynamically created if none already exists. Choose ignore if you
do not have a data store configured in the realm.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "aliasAttributeName" : {
      "title" : "Alias Search Attribute Name",
      "description" : "The secondary LDAP attribute retrieves the user profile if the primary
LDAP attribute specified in 'User Naming Attribute' fails.<br><br>This list of LDAP attributes
is used to extend the set of attributes searched by OpenAM to find the users profile.<br>For
example: <ul><li>cn</li><li>mail</li><li>givenname</li></ul><br>A user authenticates to OpenAM
under the id of steve, OpenAM will first search using the naming attribute (uid by default) so
uid=steve, if no match is found then cn=steve will be searched until a match is found or the list is
exhausted.<br><br><i>NB </i> Only used when User Profile searching is enabled.",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaultRole" : {
      "title" : "User Profile Dynamic Creation Default Roles",
      "description" : "List of roles of which dynamically created users will be a
member.<br><br>Enter the DN for each role that will be assigned to a new user when their profile has
been dynamically created by OpenAM.<br><br><i>NB </i> Deprecated functionality in OpenAM.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
},

```

```

"accountlockout" : {
  "type" : "object",
  "title" : "Account Lockout",
  "propertyOrder" : 2,
  "properties" : {
    "lockoutEmailAddress" : {
      "title" : "Email Address to Send Lockout Notification",
      "description" : "An email address or set of email addresses that receive notifications
about account lockout events.<br><br>OpenAM can be configured to send a localisable email
message to a set of email addresses when account lockout events occur. The contents of the
email message is configured using the following properties in the <code>amAuth.properties</code>
file.<br><ul><li><code>lockOutEmailFrom</code> : The \"From\" address of the email message</li>
<li><code>lockOutEmailSub</code> : The subject of the email message</li>
<li><code>lockOutEmailMsg</code> : The contents of the email message</li></ul><br>The identity for whom the account has
been locked is included in the email message.<br><br>The format of this property is:<br>
<code>emailaddress|locale|charset</code>. Multiple email addresses are space-separated.<br>Email
addresses must include the domain name, such as <code>admin@example.com</code>.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "lockoutWarnUserCount" : {
      "title" : "Warn User After N Failures",
      "description" : "Warn the user when they reach this level of failed
authentications.<br><br>The user will be given a warning when they reach this level of failed
authentications during the lockout interval.<br>The text of the lockout warning is configured using
the <code>lockOutWarning</code> property in the <code>amAuth.properties</code> file.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "lockoutDurationMultiplier" : {
      "title" : "Lockout Duration Multiplier",
      "description" : "Value multiplied to the Login Failure Lockout Duration for each successive
lockout.<br><br>This property is used to enable OpenAM to increase the account lockout duration for
each successive account lockout. For example: If the lockout duration is set to 10 and the duration
multiplier is set to 2; the duration of the first lockout will be 10 minutes and the duration of the
second lockout will be 20 minutes.<br><br>The default value of 1 disables this function. ",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "loginFailureDuration" : {
      "title" : "Login Failure Lockout Interval",
      "description" : "The lockout interval time is in minutes.<br><br>OpenAM tracks the failed
authentication count for a user over the lockout interval.<br><br>For example: If the lockout
interval is 5 minutes and the lockout count is 5; the user will have to have failed to authenticate
5 times over the previous 5 minutes for the account to be locked. Failed authentications the occurred
outside of the 5 minute interval are ignored.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "lockoutAttributeValue" : {
      "title" : "Lockout Attribute Value",

```

```

    "description" : "Value to set in custom lockout attribute<br><br>This is the value that will
    be set on the custom attribute in the users profile when they account is locked.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lockoutDuration" : {
    "title" : "Login Failure Lockout Duration",
    "description" : "The duration of the users account lockout, in minutes.<br><br>OpenAM can
    either lockout the users account indefinitely (until administration action) by setting the duration
    to 0, (the default) or OpenAM can lock the users account for a given number of minutes. After the
    lockout interval, the user will be able to successfully authenticate to OpenAM.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "loginFailureCount" : {
    "title" : "Login Failure Lockout Count",
    "description" : "The maximum number of failed authentications for a user before their
    account is locked.<br><br>This setting controls the maximum number of failed authentications a user
    can have during the lockout interval before OpenAM locks the users account.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "loginFailureLockoutMode" : {
    "title" : "Login Failure Lockout Mode",
    "description" : "Enables account lockout functionality for users authenticating to this
    realm.<br><br>OpenAM can track the number of failed authentications by a user over time and if a pre-
    defined limit is breached, OpenAM can lockout the users account and perform additional functions.<br>
    <br><i>NB </i>This functionality is in addition to any account lockout behaviour implemented by the
    LDAP Directory Server.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invalidAttemptsDataAttributeName" : {
    "title" : "Invalid Attempts Data Attribute Name",
    "description" : "The name of the attribute used to store information about failed
    authentications.<br><br>OpenAM can be configured to store information about invalid authentications
    in the users profile. This allows multiple instances of OpenAM in the same site to share
    information about a users invalid authentication attempts. By default the custom attribute;
    <code>sunAMAuthInvalidAttemptsData</code> defined in the <code>sunAMAuthAccountLockout</code>
    objectclass is used to store this data. Use this property to change the attribute used by OpenAM to
    store this information.<br><br><i>NB </i>Any attribute specified must be a valid attribute in the
    data store.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "storeInvalidAttemptsInDataStore" : {
    "title" : "Store Invalid Attempts in Data Store",

```

```

    "description" : "Enables sharing of login failure attempts across AM Instances<br><br>When
this setting is enabled OpenAM will store the users invalid authentication information in the data
store under the attribute configured in the <i>Invalid Attempts Data Attribute Name</i> property.",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "lockoutAttributeName" : {
    "title" : "Lockout Attribute Name",
    "description" : "Name of custom lockout attribute <br><br>When OpenAM locks an account, the
<code>inetuserstatus</code> attribute in the locked account is set to Inactive. In addition, OpenAM
can set the value of another attribute in the users profile. ",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
},
"postauthprocess" : {
  "type" : "object",
  "title" : "Post Authentication Processing",
  "propertyOrder" : 5,
  "properties" : {
    "usernameGeneratorClass" : {
      "title" : "Pluggable User Name Generator Class",
      "description" : "The name of the default implementation of the user name
generator class.<br><br>The name of the class used to return a list of usernames to
the Membership auth module.<br><br><i>NB </i>This class must implement the interface
<code>com.sun.identity.authentication.spi.UserIDGenerator</code>",
      "propertyOrder" : 2200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userAttributeSessionMapping" : {
      "title" : "User Attribute Mapping to Session Attribute",
      "description" : "Mapping of user profile attribute name to session attribute
name.<br><br>The setting causes OpenAM to read the named attributes from the users profile in the
data store and store their values in the users session.<br><br>Format: User Profile Attribute|
Session Attribute name. ",
      "propertyOrder" : 3000,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "loginSuccessUrl" : {
      "title" : "Default Success Login URL",
      "description" : "Successful logins will be forwarded to this URL<br><br>This is the URL to
which clients will be forwarded upon successful authentication. Enter a URL or URI relative to the
local OpenAM. URL or URI can be prefixed with the ClientType|URL if client specific. URL without
http(s) protocol will be appended to the current URI of OpenAM.",
      "propertyOrder" : 1800,
      "required" : true,
      "items" : {

```

```

        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "usernameGeneratorEnabled" : {
      "title" : "Generate UserID Mode",
      "description" : "Enables this mode in the Membership auth module.<br><br>When this mode is enabled, if the Membership auth module detects that the supplied username already exists in the data store then a list of valid usernames can be shown to the user, if requested by said user.",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "loginFailureUrl" : {
      "title" : "Default Failure Login URL ",
      "description" : "Failed logins will be forwarded to this URL<br><br>This is the URL to which clients will be forwarded upon failed authentication. Enter a URL or URI relative to the local OpenAM. URL or URI can be prefixed with ClientType|URL if client specific. URL without http(s) protocol will be appended to the current URI of OpenAM.",
      "propertyOrder" : 1900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "loginPostProcessClass" : {
      "title" : "Authentication Post Processing Classes",
      "description" : "A list of post authentication processing classes for all users in this realm.<br><br>This is a list of Post Processing Classes that will be called by OpenAM for all users that authenticate to this realm. Refer to the documentation for the places where the list of post authentication classes can be set and their precedence.<br><br>For example: org.forgerock.auth.PostProcessClass<br><i>NB </i>OpenAM must be able to find these classes on the <code>CLASSPATH</code> and must implement the interface <code>com.sun.identity.authentication.spi.AMPostAuthProcessInterface</code>.",
      "propertyOrder" : 2000,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
}
}
}

```

## 1.15.2. Global Operations

Resource path: </global-config/authentication>

Resource version: 1.0

### 1.15.2.1. read

Usage:

```
am> read Authentication --global
```

### 1.15.2.2. update

Usage:

```
am> update Authentication --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "ldapConnectionPoolDefaultSize" : {
      "title" : "Default LDAP Connection Pool Size",
      "description" : "The default connection pool size; format is: minimum:maximum",
      "propertyOrder" : 2400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteAuthSecurityEnabled" : {
      "title" : "Remote Auth Security",
      "description" : "OpenAM requires authentication client to authenticate itself before authenticating users.<br><br>When this setting is enabled, OpenAM will require the authentication client (such as a policy agent) to authentication itself to OpenAM before the client will be allow to use the remote authentication API to authenticate users. ",
      "propertyOrder" : 2900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "keepPostProcessInstances" : {
      "title" : "Keep Post Process Objects for Logout Processing",
      "description" : "Store Post Processing Classes for the duration of the session.<br><br>Enabling this setting will cause OpenAM to store instances of post processing classes into the users session. When the user logs out the original instances of the post processing classes will be called instead of new instances. This may be needed for special logout processing.<br><br><i>NB </i>Enabling this setting will increase the memory usage of OpenAM.",
      "propertyOrder" : 3100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapConnectionPoolSize" : {
      "title" : "LDAP Connection Pool Size",
      "description" : "Controls the size of the LDAP connection pool used for authentication<br><br>Control the size of the connection pool to the LDAP directory server used by
```

any of the authentication modules that use LDAP directly such as LDAP or Active Directory. Different OpenAM servers can be configured with different connection pool settings. Format:

```
host:port:minimum:maximum",
  "propertyOrder" : 2300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"authenticators" : {
  "title" : "Pluggable Authentication Module Classes",
  "description" : "List of configured authentication modules<br><br>The list of
configured authentication modules available to OpenAM. All modules must extend from the
<code>com.sun.identity.authentication.spi.AMLoginModule</code> class.",
  "propertyOrder" : 500,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"defaults" : {
  "properties" : {
    "postauthprocess" : {
      "type" : "object",
      "title" : "Post Authentication Processing",
      "propertyOrder" : 5,
      "properties" : {
        "loginFailureUrl" : {
          "title" : "Default Failure Login URL ",
          "description" : "Failed logins will be forwarded to this URL<br><br>This is the URL
to which clients will be forwarded upon failed authentication. Enter a URL or URI relative to the
local OpenAM. URL or URI can be prefixed with ClientType|URL if client specific. URL without http(s)
protocol will be appended to the current URI of OpenAM.",
          "propertyOrder" : 1900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "usernameGeneratorClass" : {
          "title" : "Pluggable User Name Generator Class",
          "description" : "The name of the default implementation of the user name
generator class.<br><br>The name of the class used to return a list of usernames to
the Membership auth module.<br><br><i>NB</i>This class must implement the interface
<code>com.sun.identity.authentication.spi.UserIDGenerator</code>",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "userAttributeSessionMapping" : {
      "title" : "User Attribute Mapping to Session Attribute",
```

```

        "description" : "Mapping of user profile attribute name to session attribute
name.<br><br>The setting causes OpenAM to read the named attributes from the users profile in the
data store and store their values in the users session.<br></br>Format: User Profile Attribute|
Session Attribute name. ",
        "propertyOrder" : 3000,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "loginSuccessUrl" : {
        "title" : "Default Success Login URL",
        "description" : "Successful logins will be forwarded to this URL<br><br>This is the URL
to which clients will be forwarded upon successful authentication. Enter a URL or URI relative to
the local OpenAM. URL or URI can be prefixed with the ClientType|URL if client specific. URL without
http(s) protocol will be appended to the current URI of OpenAM.",
        "propertyOrder" : 1800,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "usernameGeneratorEnabled" : {
        "title" : "Generate UserID Mode",
        "description" : "Enables this mode in the Membership auth module.<br><br>When this mode
is enabled, if the Membership auth module detects that the supplied username already exists in the
data store then a list of valid usernames can be shown to the user, if requested by said user.",
        "propertyOrder" : 2100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "loginPostProcessClass" : {
        "title" : "Authentication Post Processing Classes",
        "description" : "A list of post authentication processing classes for all
users in this realm.<br><br>This is a list of Post Processing Classes that will be called
by OpenAM for all users that authenticate to this realm. Refer to the documentation for
the places where the list of post authentication classes can be set and their precedence.
<br><br>For example: org.forgerock.auth.PostProcessClass<br><i>NB </i>OpenAM must be
able to find these classes on the <code>CLASSPATH</code> and must implement the interface
<code>com.sun.identity.authentication.spi.AMPostAuthProcessInterface</code>.",
        "propertyOrder" : 2000,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    }
}
},
"security" : {
    "type" : "object",
    "title" : "Security",
    "propertyOrder" : 4,

```



```

    "properties" : {
      "moduleBasedAuthEnabled" : {
        "title" : "Module Based Authentication",
        "description" : "Allows a user to authenticate via module based
authentication.<br><br>The feature allow users to override the realm configuration and use a named
authentication module to authenticate.<br><br><i>NB </i>Recommended to turn this feature off in
production environments.",
        "propertyOrder" : 2800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "zeroPageLoginReferrerWhiteList" : {
        "title" : "Zero Page Login Referer Whitelist",
        "description" : "List of allowed HTTP Referer (sic) URLs from which Zero Page Login
requests are allowed.<br><br>Enter here all URLs from which you want to allow Zero Page Login. This
provides some mitigation against Login CSRF attacks. Leave empty to allow from any Referer. Applies
to both GET and POST login requests.",
        "propertyOrder" : 3600,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "zeroPageLoginEnabled" : {
        "title" : "Zero Page Login",
        "description" : "Allows a user to authenticate using GET request parameters without
showing the login screen.<br><br>Enable this feature if the authentication mechanism uses a single
authentication screen or the first authentication screen should always be invisible to users (since
it is auto-submitted). Use caution when enabling this feature as it can be used to authenticate using
regular GET parameters, which could be cached by browsers and logged in server and proxy access logs
exposing the values of the GET parameters.",
        "propertyOrder" : 3400,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "sharedSecret" : {
        "title" : "Organization Authentication Signing Secret",
        "description" : "HMAC shared secret for signing RESTful Authentication
requests.<br><br>This is the shared secret for signing state used in RESTful authentication requests.
Should be at Base-64 encoded and at least 128-bits in length. By default a cryptographically secure
random value is generated.",
        "propertyOrder" : 4000,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
      },
      "zeroPageLoginAllowedWithoutReferrer" : {
        "title" : "Zero Page Login Allowed without Referer?",
        "description" : "Whether to allow Zero Page Login if the HTTP Referer header is
missing.<br><br>The HTTP Referer header is sometimes missing from requests (e.g., if making a request
to HTTP from HTTPS). This setting controls whether such requests should be allowed or not. Setting
to 'true' will reduce the risk of Login CSRF attacks with Zero Page Login, but may potentially deny
legitimate requests.",
        "propertyOrder" : 3700,

```

```

        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "keyAlias" : {
        "title" : "Persistent Cookie Encryption Certificate Alias",
        "description" : "Keystore Alias for encrypting Persistent Cookies.<br><br>This is
the alias for the private/public keys in the Keystore used in Persistent Cookie authentication
requests.",
        "propertyOrder" : 3300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"core" : {
    "type" : "object",
    "title" : "Core",
    "propertyOrder" : -1,
    "properties" : {
        "adminAuthModule" : {
            "title" : "Administrator Authentication Configuration",
            "description" : "Default Authentication Chain for administrators<br><br>This is the
authentication chain that will be used to authentication administrative users to this realm.",
            "propertyOrder" : 200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "orgConfig" : {
            "title" : "Organization Authentication Configuration",
            "description" : "Default Authentication Chain for users<br><br>This is the
authentication chain that will be used to authenticate users to this realm.",
            "propertyOrder" : 700,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"general" : {
    "type" : "object",
    "title" : "General",
    "propertyOrder" : 3,
    "properties" : {
        "twoFactorRequired" : {
            "title" : "Two Factor Authentication Mandatory",
            "description" : "",
            "propertyOrder" : 3900,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "userStatusCallbackPlugins" : {
            "title" : "Pluggable User Status Event Classes",
            "description" : "List of classes to be called when status of the user account
changes.<br><br>When the status of a users account changes, OpenAM can be configured to call into
a custom class. The custom class can then be used to perform some action as required. The built in

```

```

status change events are:<br/><br/><ul><li>Account locked</li><li>Password changed</li></ul><br/>
>Custom code can also extend this mechanism.",
  "propertyOrder" : 2600,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"statelessSessionsEnabled" : {
  "title" : "Use Stateless Sessions",
  "description" : "Enables stateless sessions.<br><br>Stateless sessions provide elastic
scalability by storing all session state on the client in the SSO cookie. See Session service
configuration to enable signing and encryption (HIGHLY RECOMMENDED).",
  "propertyOrder" : 3800,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"identityType" : {
  "title" : "Identity Types",
  "description" : "",
  "propertyOrder" : 2500,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"defaultAuthLevel" : {
  "title" : "Default Authentication Level",
  "description" : "The default authentication level for modules in this realm.<br><br>If
the authentication module does not set it's own auth level then the module will have the default
authentication level for the realm.",
  "propertyOrder" : 4100,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"locale" : {
  "title" : "Default Authentication Locale",
  "description" : "",
  "propertyOrder" : 600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
},
"accountlockout" : {
  "type" : "object",
  "title" : "Account Lockout",
  "propertyOrder" : 2,
  "properties" : {
    "loginFailureLockoutMode" : {
      "title" : "Login Failure Lockout Mode",

```

```

        "description" : "Enables account lockout functionality for users authenticating to this realm.<br><br>OpenAM can track the number of failed authentications by a user over time and if a pre-defined limit is breached, OpenAM can lockout the users account and perform additional functions.<br>><br><i>NB </i>This functionality is in addition to any account lockout behaviour implemented by the LDAP Directory Server.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "loginFailureCount" : {
        "title" : "Login Failure Lockout Count",
        "description" : "The maximum number of failed authentications for a user before their account is locked.<br><br>This setting controls the maximum number of failed authentications a user can have during the lockout interval before OpenAM locks the users account.",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "lockoutAttributeName" : {
        "title" : "Lockout Attribute Name",
        "description" : "Name of custom lockout attribute <br><br>When OpenAM locks an account, the <code>inetuserstatus</code> attribute in the locked account is set to Inactive. In addition, OpenAM can set the value of another attribute in the users profile. ",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "loginFailureDuration" : {
        "title" : "Login Failure Lockout Interval",
        "description" : "The lockout interval time is in minutes.<br><br>OpenAM tracks the failed authentication count for a user over the lockout interval.<br><br>For example: If the lockout interval is 5 minutes and the lockout count is 5; the user will have to have failed to authenticate 5 times over the previous 5 minutes for the account to be locked. Failed authentications the occurred outside of the 5 minute interval are ignored.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "lockoutEmailAddress" : {
        "title" : "Email Address to Send Lockout Notification",
        "description" : "An email address or set of email addresses that receive notifications about account lockout events.<br><br>OpenAM can be configured to send a localisable email message to a set of email addresses when account lockout events occur. The contents of the email message is configured using the following properties in the <code>amAuth.properties</code> file.<br><ul><li><code>lockOutEmailFrom</code> : The \"From\" address of the email message</li><li><code>lockOutEmailSub</code> : The subject of the email message</li><li><code>lockOutEmailMsg</code> : The contents of the email message</li></ul><br>The identity for whom the account has been locked is included in the email message.<br><br>The format of this property is:<br>><code>emailaddress|locale|charset</code>. Multiple email addresses are space-separated.<br>Email addresses must include the domain name, such as <code>admin@example.com</code>.",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    },

```

```

    "lockoutWarnUserCount" : {
      "title" : "Warn User After N Failures",
      "description" : "Warn the user when they reach this level of failed
authentications.<br><br>The user will be given a warning when they reach this level of failed
authentications during the lockout interval.<br>The text of the lockout warning is configured using
the <code>lockOutWarning</code> property in the <code>amAuth.properties</code> file.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "lockoutAttributeValue" : {
      "title" : "Lockout Attribute Value",
      "description" : "Value to set in custom lockout attribute<br><br>This is the value that
will be set on the custom attribute in the users profile when they account is locked.",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "lockoutDurationMultiplier" : {
      "title" : "Lockout Duration Multiplier",
      "description" : "Value multiplied to the Login Failure Lockout Duration for each
successive lockout.<br><br>This property is used to enable OpenAM to increase the account lockout
duration for each successive account lockout. For example: If the lockout duration is set to 10 and
the duration multiplier is set to 2; the duration of the first lockout will be 10 minutes and the
duration of the second lockout will be 20 minutes.<br><br>The default value of 1 disables this
function. ",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "storeInvalidAttemptsInDataStore" : {
      "title" : "Store Invalid Attempts in Data Store",
      "description" : "Enables sharing of login failure attempts across AM
Instances<br><br>When this setting is enabled OpenAM will store the users invalid authentication
information in the data store under the attribute configured in the <i>Invalid Attempts Data
Attribute Name</i> property.",
      "propertyOrder" : 2700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "lockoutDuration" : {
      "title" : "Login Failure Lockout Duration",
      "description" : "The duration of the users account lockout, in minutes.<br><br>OpenAM
can either lockout the users account indefinitely (until administration action) by setting the
duration to 0, (the default) or OpenAM can lock the users account for a given number of minutes.
After the lockout interval, the user will be able to successfully authenticate to OpenAM.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "invalidAttemptsDataAttributeName" : {
      "title" : "Invalid Attempts Data Attribute Name",
      "description" : "The name of the attribute used to store information about failed
authentications.<br><br>OpenAM can be configured to store information about invalid authentications

```

in the users profile. This allows multiple instances of OpenAM in the same site to share information about a users invalid authentication attempts. By default the custom attribute; `<code>sunAMAuthInvalidAttemptsData</code>` defined in the `<code>sunAMAuthAccountLockout</code>` objectclass is used to store this data. Use this property to change the attribute used by OpenAM to store this information.  
*NB* Any attribute specified must be a valid attribute in the data store.",

```

        "propertyOrder" : 1700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"userprofile" : {
    "type" : "object",
    "title" : "User Profile",
    "propertyOrder" : 0,
    "properties" : {
        "defaultRole" : {
            "title" : "User Profile Dynamic Creation Default Roles",
            "description" : "List of roles of which dynamically created users will be a
member.<br><br>Enter the DN for each role that will be assigned to a new user when their profile has
been dynamically created by OpenAM.<br><br><i>NB </i> Deprecated functionality in OpenAM.",
            "propertyOrder" : 300,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "aliasAttributeName" : {
            "title" : "Alias Search Attribute Name",
            "description" : "The secondary LDAP attribute retrieves the user profile if the primary
LDAP attribute specified in 'User Naming Attribute' fails.<br><br>This list of LDAP attributes
is used to extend the set of attributes searched by OpenAM to find the users profile.<br>For
example: <ul><li>cn</li><li>mail</li><li>givenname</li></ul><br>A user authenticates to OpenAM
under the id of steve, OpenAM will first search using the naming attribute (uid by default) so
uid=steve, if no match is found then cn=steve will be searched until a match is found or the list is
exhausted.<br><br><i>NB </i> Only used when User Profile searching is enabled.",
            "propertyOrder" : 400,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "dynamicProfileCreation" : {
            "title" : "User Profile",
            "description" : "Controls the result of the user profile success post successful
authentication.<br><br>Controls whether a user profile is required for authentication to be
successful or if the profile will be dynamically created if none already exists. Choose ignore if you
do not have a data store configured in the realm.",
            "propertyOrder" : 100,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}

```

```
    }  
  },  
  "type" : "object",  
  "title" : "Realm Defaults"  
}  
}
```

## 1.16. AuthenticationChains

### 1.16.1. Realm Operations

Resource path: `/realm-config/authentication/chains`

Resource version: `1.0`

#### 1.16.1.1. create

Usage:

```
am> create AuthenticationChains --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "type" : "object",  
  "properties" : {  
    "loginSuccessUrl" : {  
      "title" : "Login Success URL",  
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be  
appended to the current URI.",  
      "propertyOrder" : 200,  
      "required" : true,  
      "items" : {  
        "type" : "string"  
      },  
      "type" : "array",  
      "exampleValue" : ""  
    },  
    "loginFailureUrl" : {  
      "title" : "Login Failed URL",
```





**--id**

The unique identifier for the resource.

### 1.16.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationChains --realm Realm --actionName getAllTypes
```

### 1.16.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationChains --realm Realm --actionName getCreatableTypes
```

### 1.16.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationChains --realm Realm --actionName nextdescendents
```

### 1.16.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query AuthenticationChains --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.16.1.7. read

Usage:

```
am> read AuthenticationChains --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.16.1.8. update

Usage:

```
am> update AuthenticationChains --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "loginSuccessUrl" : {
      "title" : "Login Success URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
appended to the current URI.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "loginFailureUrl" : {
      "title" : "Login Failed URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
appended to the current URI.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "loginPostProcessClass" : {
      "title" : "Authentication Post Processing Classes",
      "description" : "Example: com.abc.authentication.PostProcessClass",
      "propertyOrder" : 400,
```

```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "authChainConfiguration" : {
    "title" : "Authentication Configuration",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "exampleValue" : "",
    "type" : "array",
    "items" : {
      "type" : "object",
      "properties" : {
        "module" : {
          "type" : "string"
        },
        "criteria" : {
          "type" : "string"
        },
        "options" : {
          "type" : "object",
          "patternProperties" : {
            ".*" : "string"
          }
        }
      }
    }
  }
}

```

## 1.16.2. Global Operations

Resource path: `/global-config/authentication/chains`

Resource version: `1.0`

### 1.16.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationChains --global --actionName getAllTypes
```

### 1.16.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationChains --global --actionName getCreatableTypes
```

### 1.16.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationChains --global --actionName nextdescendents
```

### 1.16.2.4. read

Usage:

```
am> read AuthenticationChains --global
```

### 1.16.2.5. update

Usage:

```
am> update AuthenticationChains --global --body body
```

Parameters:

#### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "authChainConfiguration" : {
          "title" : "Authentication Configuration",
          "description" : "",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}
```

## 1.17. AuthenticationModules

### 1.17.1. Realm Operations

The collection of all authentication modules in a realm allows querying for all module instances.

Resource path: `/realm-config/authentication/modules`

Resource version: `1.0`

#### 1.17.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationModules --realm Realm --actionName getAllTypes
```

#### 1.17.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationModules --realm Realm --actionName getCreatableTypes
```

#### 1.17.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationModules --realm Realm --actionName nextdescendents
```

#### 1.17.1.4. query

Query for authentication module instances

Usage:

```
am> query AuthenticationModules --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\_id]

## 1.17.2. Global Operations

Global and default configuration for authentication modules

Resource path: `/global-config/authentication/modules`

Resource version: `1.0`

### 1.17.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationModules --global --actionName getAllTypes
```

### 1.17.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationModules --global --actionName getCreatableTypes
```

### 1.17.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationModules --global --actionName nextdescendents
```

## 1.18. AuthenticatorOath

### 1.18.1. Realm Operations

Resource path: `/realm-config/services/authenticatorOathService`

Resource version: `1.0`

#### 1.18.1.1. create

Usage:

```
am> create AuthenticatorOath --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorOATHDeviceSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme for securing device profiles stored on the server.<br><br>If enabled, each device profile is encrypted using a unique random secret key using the given strength of AES encryption in CBC mode with PKCS#5 padding. A HMAC-SHA of the given strength (truncated to half-size) is used to ensure integrity protection and authenticated encryption. The unique random key is encrypted with the given RSA key-pair and stored with the device profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the keystore. The private key is used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of encryption keystore.<br><br><i>Note:</i> PKCS#11 keystores require hardware support such as a security device or smart card and is not available by default in most JVM installations.<p><p>See the <a href='\"https://docs.oracle.com/javase/8/docs/technotes/guides/security/pllguide.html\"' target='\"_blank\"'>JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oathAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "Attribute for storing ForgeRock Authenticator OATH profiles.<br><br>The default attribute is added to the user store during OpenAM installation. If you want to use a different attribute, you must make sure to add it to your user store schema prior to deploying two-step verification with a ForgeRock OATH authenticator app in OpenAM. OpenAM must be able to write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the keystore. This password will be encrypted.",
      "propertyOrder" : 500,
      "required" : false,

```

```

    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "authenticatorOATHDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
    "title" : "Private Key Password",
    "description" : "Password to unlock the private key.",
    "propertyOrder" : 700,
    "required" : false,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "authenticatorOATHDeviceSettingsEncryptionKeystore" : {
    "title" : "Encryption Key Store",
    "description" : "Path to the keystore from which to load encryption keys.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticatorOATHSkippableName" : {
    "title" : "ForgeRock Authenticator (OATH) Device Skippable Attribute Name",
    "description" : "The data store attribute that holds the user's decision to enable or disable obtaining and providing a password obtained from the ForgeRock Authenticator app. This attribute must be writeable.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

### 1.18.1.2. delete

Usage:

```
am> delete AuthenticatorOath --realm Realm
```

### 1.18.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorOath --realm Realm --actionName getAllTypes
```

### 1.18.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:



```
am> action AuthenticatorOath --realm Realm --actionName getCreatableTypes
```

### 1.18.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorOath --realm Realm --actionName nextdescendents
```

### 1.18.1.6. read

Usage:

```
am> read AuthenticatorOath --realm Realm
```

### 1.18.1.7. update

Usage:

```
am> update AuthenticatorOath --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorOATHDeviceSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme for securing device profiles stored on the server.<br><br>If enabled, each device profile is encrypted using a unique random secret key using the given strength of AES encryption in CBC mode with PKCS#5 padding. A HMAC-SHA of the given strength (truncated to half-size) is used to ensure integrity protection and authenticated encryption. The unique random key is encrypted with the given RSA key-pair and stored with the device profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the keystore. The private key is used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

```

"authenticatorOATHDeviceSettingsEncryptionKeystoreType" : {
  "title" : "Key Store Type",
  "description" : "Type of encryption keystore.<br><br><i>Note:</i> PKCS#11 keystores require hardware support such as a security device or smart card and is not available by default in most JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
  "propertyOrder" : 400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"oathAttrName" : {
  "title" : "Profile Storage Attribute",
  "description" : "Attribute for storing ForgeRock Authenticator OATH profiles.<br><br>The default attribute is added to the user store during OpenAM installation. If you want to use a different attribute, you must make sure to add it to your user store schema prior to deploying two-step verification with a ForgeRock OATH authenticator app in OpenAM. OpenAM must be able to write to the attribute.",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"authenticatorOATHDeviceSettingsEncryptionKeystorePassword" : {
  "title" : "Key Store Password",
  "description" : "Password to unlock the keystore. This password will be encrypted.",
  "propertyOrder" : 500,
  "required" : false,
  "type" : "string",
  "format" : "password",
  "exampleValue" : ""
},
"authenticatorOATHDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
  "title" : "Private Key Password",
  "description" : "Password to unlock the private key.",
  "propertyOrder" : 700,
  "required" : false,
  "type" : "string",
  "format" : "password",
  "exampleValue" : ""
},
"authenticatorOATHDeviceSettingsEncryptionKeystore" : {
  "title" : "Encryption Key Store",
  "description" : "Path to the keystore from which to load encryption keys.",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"authenticatorOATHSkippableName" : {
  "title" : "ForgeRock Authenticator (OATH) Device Skippable Attribute Name",
  "description" : "The data store attribute that holds the user's decision to enable or disable obtaining and providing a password obtained from the ForgeRock Authenticator app. This attribute must be writeable.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}

```

```
}  
}
```

## 1.18.2. Global Operations

Resource path: `/global-config/services/authenticatorOathService`

Resource version: `1.0`

### 1.18.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorOath --global --actionName getAllTypes
```

### 1.18.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorOath --global --actionName getCreatableTypes
```

### 1.18.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorOath --global --actionName nextdescendents
```

### 1.18.2.4. read

Usage:

```
am> read AuthenticatorOath --global
```

### 1.18.2.5. update

Usage:

```
am> update AuthenticatorOath --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticatorOATHDeviceSettingsEncryptionScheme" : {
          "title" : "Device Profile Encryption Scheme",
          "description" : "Encryption scheme for securing device profiles stored on the
server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
using the given strength of AES encryption in CBC mode with PKCS#5 padding. A HMAC-SHA of the
given strength (truncated to half-size) is used to ensure integrity protection and authenticated
encryption. The unique random key is encrypted with the given RSA key-pair and stored with the device
profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
files.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorOATHSkippableName" : {
          "title" : "ForgeRock Authenticator (OATH) Device Skippable Attribute Name",
          "description" : "The data store attribute that holds the user's decision to enable or
disable obtaining and providing a password obtained from the ForgeRock Authenticator app. This
attribute must be writeable.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionKeystore" : {
          "title" : "Encryption Key Store",
          "description" : "Path to the keystore from which to load encryption keys.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionKeystoreType" : {
          "title" : "Key Store Type",
          "description" : "Type of encryption keystore.<br><br><i>Note:</i> PKCS#11 keystores require
hardware support such as a security device or smart card and is not available by default in most
JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/pllguide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
          "title" : "Private Key Password",
          "description" : "Password to unlock the private key.",
          "propertyOrder" : 700,
          "required" : false,

```

```

        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
        "title" : "Key-Pair Alias",
        "description" : "Alias of the certificate and private key in the keystore. The private key
is used to encrypt and decrypt device profiles.",
        "propertyOrder" : 600,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystorePassword" : {
        "title" : "Key Store Password",
        "description" : "Password to unlock the keystore. This password will be encrypted.",
        "propertyOrder" : 500,
        "required" : false,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "oathAttrName" : {
        "title" : "Profile Storage Attribute",
        "description" : "Attribute for storing ForgeRock Authenticator OATH profiles.<br><br>The
default attribute is added to the user store during OpenAM installation. If you want to use a
different attribute, you must make sure to add it to your user store schema prior to deploying two-
step verification with a ForgeRock OATH authenticator app in OpenAM. OpenAM must be able to write to
the attribute.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.19. AuthenticatorOathModule

### 1.19.1. Realm Operations

Resource path: `/realm-config/authentication/modules/authenticator oath`

Resource version: `1.0`

#### 1.19.1.1. create

## Usage:

```
am> create AuthenticatorOathModule --realm Realm --id id --body body
```

## Parameters:

### --id

The unique identifier for the resource.

### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every few seconds as specified by the time step interval.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oathIssuerName" : {
      "title" : "Name of the Issuer",
      "description" : "Name to identify the OTP issuer.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "ForgeRock"
    },
    "minimumSecretKeyLength" : {
      "title" : "Minimum Secret Key Length",
      "description" : "Number of hexadecimal characters allowed for the Secret Key.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "totpMaximumClockDrift" : {
      "title" : "Maximum Allowed Clock Drift",
      "description" : "Number of time steps a client is allowed to get out of sync with the server before manual resynchronisation is required. For example, with 3 allowed drifts and a time step interval of 30 seconds the server will allow codes from up to 90 seconds from the current time to be treated as the current time step. The drift for a user's device is calculated each time they enter a new code. If the drift exceeds this value, the user's authentication code will be rejected.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "totpTimeStepInterval" : {
      "title" : "TOTP Time Step Interval",
      "description" : "The TOTP time step in seconds that the OTP device uses to generate the OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
```

```
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"authenticationLevel" : {
  "title" : "Authentication Level",
  "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"hotpWindowSize" : {
  "title" : "HOTP Window Size",
  "description" : "The size of the window to resynchronize with the client.<br><br>This sets the
window that the OTP device and the server counter can be out of sync. For example, if the window size
is 100 and the servers last successful login was at counter value 2, then the server will accept a
OTP from the OTP device that is from device counter 3 to 102.",
  "propertyOrder" : 500,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"totpTimeStepsInWindow" : {
  "title" : "TOTP Time Steps",
  "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This
is the number of time step intervals to check the received OTP against both forward in time and back
in time. For example, with 1 time steps and a time step interval of 30 seconds the server will allow
a code between the previous code, the current code and the next code.",
  "propertyOrder" : 900,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"addChecksumToOtpEnabled" : {
  "title" : "Add Checksum Digit",
  "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
addition to the actual password length. You should only set this if your device supports it.",
  "propertyOrder" : 600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"passwordLength" : {
  "title" : "One Time Password Length ",
  "description" : "The length of the generated OTP in digits, must be at least 6 and compatible
with the hardware/software OTP generators you expect your end-users to use. For example, Google and
ForgeRock authenticators support values of 6 and 8.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
},
```

```
"truncationOffset" : {  
  "title" : "Truncation Offset",  
  "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used  
by the HOTP algorithm that not all devices support. This should be left default unless you know your  
device uses a offset.",  
  "propertyOrder" : 700,  
  "required" : true,  
  "type" : "integer",  
  "exampleValue" : ""  
}  
}  
}
```

### 1.19.1.2. delete

Usage:

```
am> delete AuthenticatorOathModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.19.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorOathModule --realm Realm --actionName getAllTypes
```

### 1.19.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorOathModule --realm Realm --actionName getCreatableTypes
```

### 1.19.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorOathModule --realm Realm --actionName nextdescendents
```



### 1.19.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query AuthenticatorOathModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.19.1.7. read

Usage:

```
am> read AuthenticatorOathModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.19.1.8. update

Usage:

```
am> update AuthenticatorOathModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every few seconds as specified by the time step interval.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
  },
}
```

```

"oathIssuerName" : {
  "title" : "Name of the Issuer",
  "description" : "Name to identify the OTP issuer.",
  "propertyOrder" : 1100,
  "required" : true,
  "type" : "string",
  "exampleValue" : "ForgeRock"
},
"minimumSecretKeyLength" : {
  "title" : "Minimum Secret Key Length",
  "description" : "Number of hexadecimal characters allowed for the Secret Key.",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"totpMaximumClockDrift" : {
  "title" : "Maximum Allowed Clock Drift",
  "description" : "Number of time steps a client is allowed to get out of sync with the server
before manual resynchronisation is required. For example, with 3 allowed drifts and a time step
interval of 30 seconds the server will allow codes from up to 90 seconds from the current time to be
treated as the current time step. The drift for a user's device is calculated each time they enter a
new code. If the drift exceeds this value, the user's authentication code will be rejected.",
  "propertyOrder" : 1000,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"totpTimeStepInterval" : {
  "title" : "TOTP Time Step Interval",
  "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"authenticationLevel" : {
  "title" : "Authentication Level",
  "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"hotpWindowSize" : {
  "title" : "HOTP Window Size",
  "description" : "The size of the window to resynchronize with the client.<br><br>This sets the
window that the OTP device and the server counter can be out of sync. For example, if the window size
is 100 and the servers last successful login was at counter value 2, then the server will accept a
OTP from the OTP device that is from device counter 3 to 102.",
  "propertyOrder" : 500,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
}

```

```

    },
    "totpTimeStepsInWindow" : {
      "title" : "TOTP Time Steps",
      "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This is the number of time step intervals to check the received OTP against both forward in time and back in time. For example, with 1 time steps and a time step interval of 30 seconds the server will allow a code between the previous code, the current code and the next code.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "addChecksumToOtpEnabled" : {
      "title" : "Add Checksum Digit",
      "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in addition to the actual password length. You should only set this if your device supports it.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "passwordLength" : {
      "title" : "One Time Password Length ",
      "description" : "The length of the generated OTP in digits, must be at least 6 and compatible with the hardware/software OTP generators you expect your end-users to use. For example, Google and ForgeRock authenticators support values of 6 and 8.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "truncationOffset" : {
      "title" : "Truncation Offset",
      "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used by the HOTP algorithm that not all devices support. This should be left default unless you know your device uses a offset.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}

```

## 1.19.2. Global Operations

Resource path: </global-config/authentication/modules/authenticatororauth>

Resource version: 1.0

### 1.19.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorOathModule --global --actionName getAllTypes
```

### 1.19.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorOathModule --global --actionName getCreatableTypes
```

### 1.19.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorOathModule --global --actionName nextdescendents
```

### 1.19.2.4. read

Usage:

```
am> read AuthenticatorOathModule --global
```

### 1.19.2.5. update

Usage:

```
am> update AuthenticatorOathModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "truncationOffset" : {
          "title" : "Truncation Offset",
          "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used by the HOTP algorithm that not all devices support. This should be left default unless you know your device uses a offset.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    },
    "passwordLength" : {
      "title" : "One Time Password Length ",
      "description" : "The length of the generated OTP in digits, must be at least 6 and
compatible with the hardware/software OTP generators you expect your end-users to use. For example,
Google and ForgeRock authenticators support values of 6 and 8.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "totpTimeStepsInWindow" : {
      "title" : "TOTP Time Steps",
      "description" : "The number of time steps to check before and after receiving a
OTP.<br><br>This is the number of time step intervals to check the received OTP against both forward
in time and back in time. For example, with 1 time steps and a time step interval of 30 seconds the
server will allow a code between the previous code, the current code and the next code.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "minimumSecretKeyLength" : {
      "title" : "Minimum Secret Key Length",
      "description" : "Number of hexadecimal characters allowed for the Secret Key.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "hotpWindowSize" : {
      "title" : "HOTP Window Size",
      "description" : "The size of the window to resynchronize with the client.<br><br>This sets
the window that the OTP device and the server counter can be out of sync. For example, if the window
size is 100 and the servers last successful login was at counter value 2, then the server will accept
a OTP from the OTP device that is from device counter 3 to 102.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses
a counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every
few seconds as specified by the time step interval.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "oathIssuerName" : {
      "title" : "Name of the Issuer",
      "description" : "Name to identify the OTP issuer.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "ForgeRock"
    },
    },
  },

```

```

    "addChecksumToOtpEnabled" : {
      "title" : "Add Checksum Digit",
      "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
addition to the actual password length. You should only set this if your device supports it.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "totpTimeStepInterval" : {
      "title" : "TOTP Time Step Interval",
      "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "totpMaximumClockDrift" : {
      "title" : "Maximum Allowed Clock Drift",
      "description" : "Number of time steps a client is allowed to get out of sync with the server
before manual resynchronisation is required. For example, with 3 allowed drifts and a time step
interval of 30 seconds the server will allow codes from up to 90 seconds from the current time to be
treated as the current time step. The drift for a user's device is calculated each time they enter a
new code. If the drift exceeds this value, the user's authentication code will be rejected.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "type" : "object",
  "title" : "Realm Defaults"
}
}
}

```

## 1.20. AuthenticatorPush

### 1.20.1. Realm Operations

Resource path: `/realm-config/services/authenticatorPushService`

Resource version: `1.0`

### 1.20.1.1. create

Usage:

```
am> create AuthenticatorPush --realm Realm --body body
```

Parameters:

#### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorPushDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of KeyStore to load.<br><br><i>Note:</i> PKCS#11 keystores require hardware support such as a security device or smart card and is not available by default in most JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/security/pllguide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the server.<br><br>If enabled, each device profile is encrypted using a unique random secret key using the given strength of AES encryption in CBC mode with PKCS#5 padding. A HMAC-SHA of the given strength (truncated to half-size) is used to ensure integrity protection and authenticated encryption. The unique random key is encrypted with the given RSA key-pair and stored with the device profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "pushAttrName" : {
      "title" : "Profile Storage Attribute",
```

```

        "description" : "The user's attribute in which to store Push Notification profiles.<br><br>The default attribute is added to the schema when you prepare a user store for use with OpenAM. If you want to use a different attribute, you must make sure to add it to your user store schema prior to deploying push notifications with the ForgeRock Authenticator app in OpenAM. OpenAM must be able to write to the attribute.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
        "title" : "Key-Pair Alias",
        "description" : "Alias of the certificate and private key in the keystore. The private key is used to encrypt and decrypt device profiles.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystorePassword" : {
        "title" : "Key Store Password",
        "description" : "Password to unlock the keystore. This password is encrypted when it is saved in the OpenAM configuration. You should modify the default value.",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystore" : {
        "title" : "Encryption Key Store",
        "description" : "Path to the keystore from which to load encryption keys.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

### 1.20.1.2. delete

Usage:

```
am> delete AuthenticatorPush --realm Realm
```

### 1.20.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPush --realm Realm --actionName getAllTypes
```



#### 1.20.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPush --realm Realm --actionName getCreatableTypes
```

#### 1.20.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPush --realm Realm --actionName nextdescendents
```

#### 1.20.1.6. read

Usage:

```
am> read AuthenticatorPush --realm Realm
```

#### 1.20.1.7. update

Usage:

```
am> update AuthenticatorPush --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorPushDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of KeyStore to load.<br><br><i>Note:</i> PKCS#11 keystores require hardware support such as a security device or smart card and is not available by default in most JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/security/pllguide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : true,

```

```

    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "authenticatorPushDeviceSettingsEncryptionScheme" : {
    "title" : "Device Profile Encryption Scheme",
    "description" : "Encryption scheme to use to secure device profiles stored on the
server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
using the given strength of AES encryption in CBC mode with PKCS#5 padding. A HMAC-SHA of the
given strength (truncated to half-size) is used to ensure integrity protection and authenticated
encryption. The unique random key is encrypted with the given RSA key-pair and stored with the device
profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
files.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "pushAttrName" : {
    "title" : "Profile Storage Attribute",
    "description" : "The user's attribute in which to store Push Notification profiles.<br><br>The
default attribute is added to the schema when you prepare a user store for use with OpenAM. If you
want to use a different attribute, you must make sure to add it to your user store schema prior to
deploying push notifications with the ForgeRock Authenticator app in OpenAM. OpenAM must be able to
write to the attribute.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticatorPushDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
    "title" : "Key-Pair Alias",
    "description" : "Alias of the certificate and private key in the keystore. The private key is
used to encrypt and decrypt device profiles.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticatorPushDeviceSettingsEncryptionKeystorePassword" : {
    "title" : "Key Store Password",
    "description" : "Password to unlock the keystore. This password is encrypted when it is saved in
the OpenAM configuration. You should modify the default value.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "authenticatorPushDeviceSettingsEncryptionKeystore" : {
    "title" : "Encryption Key Store",
    "description" : "Path to the keystore from which to load encryption keys.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}

```

```
}
```

## 1.20.2. Global Operations

Resource path: `/global-config/services/authenticatorPushService`

Resource version: `1.0`

### 1.20.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPush --global --actionName getAllTypes
```

### 1.20.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPush --global --actionName getCreatableTypes
```

### 1.20.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPush --global --actionName nextdescendents
```

### 1.20.2.4. read

Usage:

```
am> read AuthenticatorPush --global
```

### 1.20.2.5. update

Usage:

```
am> update AuthenticatorPush --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticatorPushDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
          "title" : "Private Key Password",
          "description" : "Password to unlock the private key.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionKeystoreType" : {
          "title" : "Key Store Type",
          "description" : "Type of KeyStore to load.<br><br><i>Note:</i> PKCS#11 keystores require hardware support such as a security device or smart card and is not available by default in most JVM installations.<p><p>See the <a href="https://docs.oracle.com/javase/8/docs/technotes/guides/security/pllguide.html\" target="_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionKeystorePassword" : {
          "title" : "Key Store Password",
          "description" : "Password to unlock the keystore. This password is encrypted when it is saved in the OpenAM configuration. You should modify the default value.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionScheme" : {
          "title" : "Device Profile Encryption Scheme",
          "description" : "Encryption scheme to use to secure device profiles stored on the server.<br><br>If enabled, each device profile is encrypted using a unique random secret key using the given strength of AES encryption in CBC mode with PKCS#5 padding. A HMAC-SHA of the given strength (truncated to half-size) is used to ensure integrity protection and authenticated encryption. The unique random key is encrypted with the given RSA key-pair and stored with the device profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy files.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionKeystore" : {
          "title" : "Encryption Key Store",
          "description" : "Path to the keystore from which to load encryption keys.",
          "propertyOrder" : 300,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "pushAttrName" : {
    "title" : "Profile Storage Attribute",
    "description" : "The user's attribute in which to store Push Notification
profiles.<br><br>The default attribute is added to the schema when you prepare a user store for use
with OpenAM. If you want to use a different attribute, you must make sure to add it to your user
store schema prior to deploying push notifications with the ForgeRock Authenticator app in OpenAM.
OpenAM must be able to write to the attribute.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticatorPushDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
    "title" : "Key-Pair Alias",
    "description" : "Alias of the certificate and private key in the keystore. The private key
is used to encrypt and decrypt device profiles.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.21. AuthenticatorPushModule

### 1.21.1. Realm Operations

Resource path: `/realm-config/authentication/modules/authPush`

Resource version: `1.0`

#### 1.21.1.1. create

Usage:

```
am> create AuthenticatorPushModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "timeoutInMilliseconds" : {
      "title" : "Return Message Timeout (ms)",
      "description" : "The period of time (in milliseconds) within which a push notification should be
replied to.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "pushMessage" : {
      "title" : "Login Message",
      "description" : "Message transmitted over Push. Use the label {{user}} to replace with the
registered login's username, and {{issuer}} to replace with the name of the issuer stored at
registration.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

### 1.21.1.2. delete

Usage:

```
am> delete AuthenticatorPushModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

### 1.21.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPushModule --realm Realm --actionName getAllTypes
```

#### 1.21.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPushModule --realm Realm --actionName getCreatableTypes
```

#### 1.21.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPushModule --realm Realm --actionName nextdescendents
```

#### 1.21.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query AuthenticatorPushModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.21.1.7. read

Usage:

```
am> read AuthenticatorPushModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.21.1.8. update

Usage:

```
am> update AuthenticatorPushModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "timeoutInMilliSeconds" : {
      "title" : "Return Message Timeout (ms)",
      "description" : "The period of time (in milliseconds) within which a push notification should be
replied to.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "pushMessage" : {
      "title" : "Login Message",
      "description" : "Message transmitted over Push. Use the label {{user}} to replace with the
registered login's username, and {{issuer}} to replace with the name of the issuer stored at
registration.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

## 1.21.2. Global Operations

Resource path: </global-config/authentication/modules/authPush>

Resource version: [1.0](#)



### 1.21.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPushModule --global --actionName getAllTypes
```

### 1.21.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPushModule --global --actionName getCreatableTypes
```

### 1.21.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPushModule --global --actionName nextdescendents
```

### 1.21.2.4. read

Usage:

```
am> read AuthenticatorPushModule --global
```

### 1.21.2.5. update

Usage:

```
am> update AuthenticatorPushModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
```

```

        "title" : "Authentication Level",
        "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "pushMessage" : {
        "title" : "Login Message",
        "description" : "Message transmitted over Push. Use the label {{user}} to replace with the registered login's username, and {{issuer}} to replace with the name of the issuer stored at registration.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "timeoutInMilliseconds" : {
        "title" : "Return Message Timeout (ms)",
        "description" : "The period of time (in milliseconds) within which a push notification should be replied to.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.22. AuthenticatorPushRegistrationModule

### 1.22.1. Realm Operations

Resource path: `/realm-config/authentication/modules/authPushReg`

Resource version: `1.0`

#### 1.22.1.1. create

Usage:

```
am> create AuthenticatorPushRegistrationModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "issuer" : {
      "title" : "Issuer Name",
      "description" : "The Name of the service as it will appear on the registered device.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "googleLink" : {
      "title" : "Google Play URL",
      "description" : "URL of the app to download on Google Play.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "appleLink" : {
      "title" : "App Store App URL",
      "description" : "URL of the app to download on the App Store.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "timeoutInMilliSeconds" : {
      "title" : "Registration Response Timeout (ms)",
      "description" : "The period of time (in milliseconds) within which the registration QR code should be replied to.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "imgUrl" : {
      "title" : "Image URL",
      "description" : "The location of the image to download and display as your identity issuer's logo within the mobile app.",
      "propertyOrder" : 500,

```

```
    "required" : true,
    "type" : "string",
    "exampleValue" : "http://example.com/image.png"
  },
  "bgcolour" : {
    "title" : "Background Colour",
    "description" : "The background colour of the image to display behind your identity issuer's
logo within the mobile app.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
```

### 1.22.1.2. delete

Usage:

```
am> delete AuthenticatorPushRegistrationModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.22.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --realm Realm --actionName getAllTypes
```

### 1.22.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --realm Realm --actionName getCreatableTypes
```

### 1.22.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --realm Realm --actionName nextdescendents
```

### 1.22.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query AuthenticatorPushRegistrationModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.22.1.7. read

Usage:

```
am> read AuthenticatorPushRegistrationModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.22.1.8. update

Usage:

```
am> update AuthenticatorPushRegistrationModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "issuer" : {
      "title" : "Issuer Name",
      "description" : "The Name of the service as it will appear on the registered device.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "googleLink" : {
```

```

    "title" : "Google Play URL",
    "description" : "URL of the app to download on Google Play.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "appleLink" : {
    "title" : "App Store App URL",
    "description" : "URL of the app to download on the App Store.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "timeoutInMilliseconds" : {
    "title" : "Registration Response Timeout (ms)",
    "description" : "The period of time (in milliseconds) within which the registration QR code should be replied to.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "imageUrl" : {
    "title" : "Image URL",
    "description" : "The location of the image to download and display as your identity issuer's logo within the mobile app.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : "http://example.com/image.png"
  },
  "bgcolour" : {
    "title" : "Background Colour",
    "description" : "The background colour of the image to display behind your identity issuer's logo within the mobile app.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

## 1.22.2. Global Operations

Resource path: `/global-config/authentication/modules/authPushReg`

Resource version: `1.0`

### 1.22.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --global --actionName getAllTypes
```

### 1.22.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --global --actionName getCreatableTypes
```

### 1.22.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --global --actionName nextdescendents
```

### 1.22.2.4. read

Usage:

```
am> read AuthenticatorPushRegistrationModule --global
```

### 1.22.2.5. update

Usage:

```
am> update AuthenticatorPushRegistrationModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
```

```

    "bgcolour" : {
      "title" : "Background Colour",
      "description" : "The background colour of the image to display behind your identity issuer's
logo within the mobile app.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "appleLink" : {
      "title" : "App Store App URL",
      "description" : "URL of the app to download on the App Store.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Issuer Name",
      "description" : "The Name of the service as it will appear on the registered device.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "googleLink" : {
      "title" : "Google Play URL",
      "description" : "URL of the app to download on Google Play.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "imgUrl" : {
      "title" : "Image URL",
      "description" : "The location of the image to download and display as your identity issuer's
logo within the mobile app.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : "http://example.com/image.png"
    },
    "timeoutInMilliseconds" : {
      "title" : "Registration Response Timeout (ms)",
      "description" : "The period of time (in milliseconds) within which the registration QR code
should be replied to.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",

```



```
        "exampleValue" : ""
      }
    },
    "type" : "object",
    "title" : "Realm Defaults"
  }
}
```

## 1.23. BaseUrlSource

### 1.23.1. Realm Operations

Resource path: `/realm-config/services/baseurl`

Resource version: `1.0`

#### 1.23.1.1. create

Usage:

```
am> create BaseUrlSource --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "extensionClassName" : {
      "title" : "Extension class name",
      "description" : "If Extension class is selected as the Base URL source, enter  
<code>org.forgerock.openam.services.baseurl.BaseURLProvider</code> in the Extension class name  
field.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "fixedValue" : {
      "title" : "Fixed value base URL",
      "description" : "If Fixed value is selected as the Base URL source, enter the base URL in the  
Fixed value base URL field.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

```

    },
    "source" : {
      "title" : "Base URL Source",
      "description" : "Specifies the source of the base URL. Choose from the
following:<ul> <li>Extension class. Specifies that the extension class returns a
base URL from a provided HttpServletRequest. In the Extension class name field, enter
<code>org.forgerock.openam.services.baseurl.BaseURLProvider</code>.</li><li>Fixed value. Specifies
that the base URL is retrieved from a specific base URL value. In the Fixed value base URL field,
enter the base URL value.</li><li>Forwarded header. Specifies that the base URL is retrieved from
a forwarded header field in the HTTP request. The Forwarded HTTP header field is standardized and
specified in <a href=\"https://tools.ietf.org/html/rfc7239\">RFC7239</a>.</li><li>Host/protocol
from incoming request. Specifies that the hostname, server name, and port are retrieved from the
incoming HTTP request.</li><li>X-Forwarded-* headers. Specifies that the base URL is retrieved from
non-standard header fields, such as <code>X-Forwarded-For</code>, <code>X-Forwarded-By</code>, and
<code>X-Forwarded-Proto</code>.</li></ul>",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "contextPath" : {
      "title" : "Context path",
      "description" : "Specifies the context path for the base URL.<p><p>If provided, the base URL
includes the deployment context path appended to the calculated URL.<p>For example, <code>/openam</
code>.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}

```

### 1.23.1.2. delete

Usage:

```
am> delete BaseUrlSource --realm Realm
```

### 1.23.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action BaseUrlSource --realm Realm --actionName getAllTypes
```

### 1.23.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action BaseUrlSource --realm Realm --actionName getCreatableTypes
```

### 1.23.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action BaseUrlSource --realm Realm --actionName nextdescendents
```

### 1.23.1.6. read

Usage:

```
am> read BaseUrlSource --realm Realm
```

### 1.23.1.7. update

Usage:

```
am> update BaseUrlSource --realm Realm --body body
```

Parameters:

#### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "extensionClassName" : {
      "title" : "Extension class name",
      "description" : "If Extension class is selected as the Base URL source, enter  
<code>org.forgerock.openam.services.baseurl.BaseURLProvider</code> in the Extension class name  
field.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "fixedValue" : {
      "title" : "Fixed value base URL",
      "description" : "If Fixed value is selected as the Base URL source, enter the base URL in the  
Fixed value base URL field.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

```

"source" : {
  "title" : "Base URL Source",
  "description" : "Specifies the source of the base URL. Choose from the
following:<ul> <li>Extension class. Specifies that the extension class returns a
base URL from a provided HttpServletRequest. In the Extension class name field, enter
<code>org.forgerock.openam.services.baseurl.BaseURLProvider</code>.</li><li>Fixed value. Specifies
that the base URL is retrieved from a specific base URL value. In the Fixed value base URL field,
enter the base URL value.</li><li>Forwarded header. Specifies that the base URL is retrieved from
a forwarded header field in the HTTP request. The Forwarded HTTP header field is standardized and
specified in <a href=\"https://tools.ietf.org/html/rfc7239\">RFC7239</a>.</li><li>Host/protocol
from incoming request. Specifies that the hostname, server name, and port are retrieved from the
incoming HTTP request.</li><li>X-Forwarded-* headers. Specifies that the base URL is retrieved from
non-standard header fields, such as <code>X-Forwarded-For</code>, <code>X-Forwarded-By</code>, and
<code>X-Forwarded-Proto</code>.</li></ul>",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"contextPath" : {
  "title" : "Context path",
  "description" : "Specifies the context path for the base URL.<p><p>If provided, the base URL
includes the deployment context path appended to the calculated URL.<p>For example, <code>/openam</
code>.",
  "propertyOrder" : 400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
}

```

## 1.23.2. Global Operations

Resource path: `/global-config/services/baseurl`

Resource version: `1.0`

### 1.23.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action BaseUrlSource --global --actionName getAllTypes
```

### 1.23.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action BaseUrlSource --global --actionName getCreatableTypes
```

### 1.23.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action BaseUrlSource --global --actionName nextdescendents
```

### 1.23.2.4. read

Usage:

```
am> read BaseUrlSource --global
```

### 1.23.2.5. update

Usage:

```
am> update BaseUrlSource --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "extensionClassName" : {
          "title" : "Extension class name",
          "description" : "If Extension class is selected as the Base URL source, enter
<code>org.forgerock.openam.services.baseurl.BaseURLProvider</code> in the Extension class name
field.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "source" : {
          "title" : "Base URL Source",
          "description" : "Specifies the source of the base URL. Choose from the
following:<ul> <li>Extension class. Specifies that the extension class returns a
base URL from a provided HttpServletRequest. In the Extension class name field, enter
<code>org.forgerock.openam.services.baseurl.BaseURLProvider</code>.</li><li>Fixed value. Specifies
that the base URL is retrieved from a specific base URL value. In the Fixed value base URL field,
enter the base URL value.</li><li>Forwarded header. Specifies that the base URL is retrieved from
```

```

a forwarded header field in the HTTP request. The Forwarded HTTP header field is standardized and
specified in <a href="https://tools.ietf.org/html/rfc7239">RFC7239</a>.</li><li>Host/protocol
from incoming request.</li><li>X-Forwarded-* headers. Specifies that the base URL is retrieved from
incoming HTTP request.</li></ul>.",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"contextPath" : {
  "title" : "Context path",
  "description" : "Specifies the context path for the base URL.<p><p>If provided, the base URL
includes the deployment context path appended to the calculated URL.<p>For example, <code>/openam</
code>.",
  "propertyOrder" : 400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"fixedValue" : {
  "title" : "Fixed value base URL",
  "description" : "If Fixed value is selected as the Base URL source, enter the base URL in
the Fixed value base URL field.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.24. CertificateModule

### 1.24.1. Realm Operations

Resource path: `/realm-config/authentication/modules/certificate`

Resource version: `1.0`

#### 1.24.1.1. create

Usage:

```
am> create CertificateModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "matchCertificateToCRL" : {
      "title" : "Match Certificate to CRL",
      "description" : "The Client Certificate will be checked against the Certificate Revocation list held in the directory<br><br>A Certificate Revocation List can be provisioned into the directory. Having this option enabled will cause all client certificates to be checked against this list.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "matchCACertificateToCRL" : {
      "title" : "Match CA Certificate to CRL",
      "description" : "The CA certificate that issued the client certificate will also be checked against the CRL.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapCertificateAttribute" : {
      "title" : "Subject DN Attribute Used to Search LDAP for Certificates",
      "description" : "This is the attribute used to search the directory for the certificate<br><br>The Certificate module will search the directory for the certificate using the search filter based on this attribute and the value of the Subject DN taken from the certificate.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientCertificateHttpHeaderName" : {
      "title" : "HTTP Header Name for Client Certificate",
      "description" : "The name of the HTTP request header containing the certificate, only used when <i>Trusted Remote Hosts</i> mode is enabled.",
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-auth-cert-gw-cert-preferred" : {
      "title" : "Use only Certificate from HTTP request header",
      "description" : "Strictly use client cert from HTTP header over cert from HTTPS connection/servlet attribute",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

```

    },
    "matchCertificateInLdap" : {
      "title" : "Match Certificate in LDAP",
      "description" : "The client certificate must exist in the directory for the authentication to be
successful.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "cacheCRLsInMemory" : {
      "title" : "Cache CRLs in memory",
      "description" : "The CRLs will be cached in memory",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "sslEnabled" : {
      "title" : "Use SSL/TLS for LDAP Access",
      "description" : "The certificate module will use SSL/TLS to access the LDAP server",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "userBindDN" : {
      "title" : "LDAP Server Authentication User",
      "description" : "DN of the user used by the module to authenticate to the LDAP server<br><br>The
Certificate module authenticates to the LDAP server in order to search for a matching certificate.
The DN entered here represents the account used for said authentication and must have read/search
access to the LDAP server.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "certificateLdapServers" : {
      "title" : "LDAP Server Where Certificates are Stored",
      "description" : "Use this list to set the LDAP server used to search for certificates.
<br><br>The Certificate authentication module will use this list for the LDAP server used to search
for certificates. A single entry must be in the format:<br><br><code>ldap_server:port</code><br>
><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br>
><br><code>local server name | server:port</code><br><br>The local server name is the full name of
the server from the list of servers and sites.",
      "propertyOrder" : 1000,
      "required" : true,
      "items" : {
        "type" : "string"
      }
    }
  }

```



```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "crlHttpParameters" : {
    "title" : "HTTP Parameters for CRL Update",
    "description" : "These parameters will be included in any HTTP CRL call to the Certificate Authority<br><br>If the Client or CA certificate contains the Issuing Distribution Point Extension then OpenAM will use this information to retrieve the CRL from the distribution point. This property allow custom HTTP parameters to be included in the CRL request.<br><br>The format of the parameter is as follows:<br><br><code>param1=value1,param2=value</code>",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "crlMatchingCertificateAttribute" : {
    "title" : "Issuer DN Attribute(s) Used to Search LDAP for CRLs",
    "description" : "This is the name of the attribute taken from the CA certificate that will be used to search the CRL.<br><br>If only one attribute name is specified, the ldap searchfilter will be (attrName=Value_of_the_corresponding_Attribute_from_SubjectDN)<br>e.g. SubjectDN of issuer cert 'C=US, CN=Some CA, serialNumber=123456', attribute name specified is 'CN', searchfilter used will be <code>(CN=Some CA)</code><br><br>If serveral attribute names are specified, they have to separated by <code>,</code>. The resulting ldap searchfilter value will be a comma separated list of name attribute values, the search attribute will be <code>cn</code><br>e.g. SubjectDN of issuer cert 'C=US, CN=Some CA, serialNumber=123456', attribute names specified are 'CN,serialNumber', searchfilter used will be <code>cn=CN=Some CA,serialNumber=123456</code><br>The order of the values of the attribute names matter as they must match the value of the <code>cn</code> attribute of a crlDistributionPoint entry in the directory server.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "updateCRLsFromDistributionPoint" : {
    "title" : "Update CA CRLs from CRLDistributionPoint",
    "description" : "Fetch new CA CRLs from CRLDistributionPoint and update it in Directory Server<br><br>If the CA certificate includes an IssuingDistributionPoint or has an CRLDistributionPoint extension set OpenAM tries to update the CRLs if needed (i.e. CRL is out-of-date). <br>This property controls if the update should be performed.<br>This property is only used if CA CRL checking is enabled.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ocspValidationEnabled" : {
    "title" : "OCSP Validation",
    "description" : "Enable Online Certificate Status Protocol validation for OCSP aware certificates<br><br>If the certificate contains OCSP validation information then OpenAM will use this information to check the validity of the certificate as part of the authentication process.<br><br><i>>NB </i>The OpenAM server must have Internet connectivity for OCSP to work",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "certificateAttributeToProfileMapping" : {
    "title" : "Certificate Field Used to Access User Profile",

```

```

    "description" : "The certificate module needs to read a value from the client certificate that
can be used to search the LDAP server for a matching certificate. ",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userBindPassword" : {
    "title" : "LDAP Server Authentication Password",
    "description" : "The password for the authentication user",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "certificateAttributeProfileMappingExtension" : {
    "title" : "SubjectAltNameExt Value Type to Access User Profile",
    "description" : "Use the Subject Alternative Name Field in preference to one of the standard
certificate fields.<br><br>Selecting RFC822Name or UPN will cause this field to have precedence
over the <i>Certificate Field Used to Access User Profile</i> or <i>Other Certificate Field Used
to Access User Profile</i> attribute.<br><br><i>NB </i>The client certificate must contain the
<i>Subject Alternate Name Extension</i> for this function to operate.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ldapSearchStartDN" : {
    "title" : "LDAP Search Start or Base DN",
    "description" : "The start point in the LDAP server for the certificate search<br><br>When
entering multiple entries, each entry must be prefixed with a local server name. Multiple entries
allow different search Base DNs depending on the OpenAM server in use. The format is:<br><br>
<code>local server name | base dn</code><br><br>The local server name is the full name of the
server from the list of servers and sites.",
    "propertyOrder" : 1100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "trustedRemoteHosts" : {
    "title" : "Trusted Remote Hosts",
    "description" : "A list of IP addresses trusted to supply client certificates.<br><br>If SSL/TLS
is being terminated at a load balancer or at the Distributed Authentication server then this option
can be used to ensure that only specified <i>trusted</i> hosts (identified by IP address) are allowed
to supply client certificates to the certificate module,<br><br>Valid values for this list are as
follows:<ul><li>none</li><li>any</li><li>multiple IP addresses</li></ul><br><br>The default value
of <i>none</i> disables this functionality",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
},

```

```
"otherCertificateAttributeToProfileMapping" : {  
  "title" : "Other Certificate Field Used to Access User Profile",  
  "description" : "This field is only used if the <i>Certificate Field Used to Access User  
Profile</i> attribute is set to <i>other</i>. This field allows a custom certificate field to be used  
as the basis of the user search.",  
  "propertyOrder" : 1600,  
  "required" : true,  
  "type" : "string",  
  "exampleValue" : ""  
}  
}  
}
```

#### 1.24.1.2. delete

Usage:

```
am> delete CertificateModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.24.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CertificateModule --realm Realm --actionName getAllTypes
```

#### 1.24.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CertificateModule --realm Realm --actionName getCreatableTypes
```

#### 1.24.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CertificateModule --realm Realm --actionName nextdescendents
```

### 1.24.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query CertificateModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.24.1.7. read

Usage:

```
am> read CertificateModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.24.1.8. update

Usage:

```
am> update CertificateModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "matchCertificateToCRL" : {
      "title" : "Match Certificate to CRL",
      "description" : "The Client Certificate will be checked against the Certificate Revocation list held in the directory<br><br>A Certificate Revocation List can be provisioned into the directory. Having this option enabled will cause all client certificates to be checked against this list.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
  },
}
```

```

    "matchCACertificateToCRL" : {
      "title" : "Match CA Certificate to CRL",
      "description" : "The CA certificate that issued the client certificate will also be checked
against the CRL.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapCertificateAttribute" : {
      "title" : "Subject DN Attribute Used to Search LDAP for Certificates",
      "description" : "This is the attribute used to search the directory for the
certificate<br><br>The Certificate module will search the directory for the certificate using the
search filter based on this attribute and the value of the Subject DN taken from the certificate.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientCertificateHttpRequestName" : {
      "title" : "HTTP Header Name for Client Certificate",
      "description" : "The name of the HTTP request header containing the certificate, only used when
<i>Trusted Remote Hosts</i> mode is enabled.",
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-auth-cert-gw-cert-preferred" : {
      "title" : "Use only Certificate from HTTP request header",
      "description" : "Strictly use client cert from HTTP header over cert from HTTPS connection/
servlet attribute",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "matchCertificateInLdap" : {
      "title" : "Match Certificate in LDAP",
      "description" : "The client certificate must exist in the directory for the authentication to be
successful.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "cacheCRLsInMemory" : {
      "title" : "Cache CRLs in memory",
      "description" : "The CRLs will be cached in memory",

```

```

    "propertyOrder" : 700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sslEnabled" : {
    "title" : "Use SSL/TLS for LDAP Access",
    "description" : "The certificate module will use SSL/TLS to access the LDAP server",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userBindDN" : {
    "title" : "LDAP Server Authentication User",
    "description" : "DN of the user used by the module to authenticate to the LDAP server<br><br>The Certificate module authenticates to the LDAP server in order to search for a matching certificate. The DN entered here represents the account used for said authentication and must have read/search access to the LDAP server.",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "certificateLdapServers" : {
    "title" : "LDAP Server Where Certificates are Stored",
    "description" : "Use this list to set the LDAP server used to search for certificates.
    <br><br>The Certificate authentication module will use this list for the LDAP server used to search for certificates. A single entry must be in the format:<br><br><code>ldap_server:port</code><br>
    <br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br>
    <br><code>local server name | server:port</code><br><br>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 1000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "crlHttpParameters" : {
    "title" : "HTTP Parameters for CRL Update",
    "description" : "These parameters will be included in any HTTP CRL call to the Certificate Authority<br><br>If the Client or CA certificate contains the Issuing Distribution Point Extension then OpenAM will use this information to retrieve the CRL from the distribution point. This property allow custom HTTP parameters to be included in the CRL request.<br><br>The format of the parameter is as follows:<br><br><code>param1=value1,param2=value</code>",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "crlMatchingCertificateAttribute" : {
    "title" : "Issuer DN Attribute(s) Used to Search LDAP for CRLs",
    "description" : "This is the name of the attribute taken from the CA certificate that will be used to search the CRL.<br><br>If only one attribute name is specified, the ldap searchfilter will be (attrName=Value_of_the_corresponding_Attribute_from_SubjectDN)<br>e.g. SubjectDN of issuer cert 'C=US, CN=Some CA, serialNumber=123456', attribute name specified is 'CN', searchfilter used will be <code>(CN=Some CA)</code><br><br>If serveral attribute names are specified, they have

```

to separated by `<code>,</code>`. The resulting ldap searchfilter value will be a comma separated list of name attribute values, the search attribute will be `<code>cn</code>`  
e.g. SubjectDN of issuer cert 'C=US, CN=Some CA, serialNumber=123456', attribute names specified are 'CN,serialNumber', searchfilter used will be `<code>cn=CN=Some CA,serialNumber=123456</code>`  
The order of the values of the attribute names matter as they must match the value of the `<code>cn</code>` attribute of a crlDistributionPoint entry in the directory server.",

```

    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "updateCRLsFromDistributionPoint" : {
    "title" : "Update CA CRLs from CRLDistributionPoint",
    "description" : "Fetch new CA CRLs from CRLDistributionPoint and update it in
Directory Server<br><br>If the CA certificate includes an IssuingDistributionPoint or has an
CRLDistributionPoint extension set OpenAM tries to update the CRLs if needed (i.e. CRL is out-of-
date). <br>This property controls if the update should be performed.<br>This property is only used
if CA CRL checking is enabled.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ocspValidationEnabled" : {
    "title" : "OCSP Validation",
    "description" : "Enable Online Certificate Status Protocol validation for OCSP aware
certificates<br><br>If the certificate contains OCSP validation information then OpenAM will use this
information to check the validity of the certificate as part of the authentication process.<br><br>
<i>NB </i>The OpenAM server must have Internet connectivity for OCSP to work",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "certificateAttributeToProfileMapping" : {
    "title" : "Certificate Field Used to Access User Profile",
    "description" : "The certificate module needs to read a value from the client certificate that
can be used to search the LDAP server for a matching certificate. ",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userBindPassword" : {
    "title" : "LDAP Server Authentication Password",
    "description" : "The password for the authentication user",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "certificateAttributeProfileMappingExtension" : {
    "title" : "SubjectAltNameExt Value Type to Access User Profile",
    "description" : "Use the Subject Alternative Name Field in preference to one of the standard
certificate fields.<br><br>Selecting RFC822Name or UPN will cause this field to have precedence
over the <i>Certificate Field Used to Access User Profile</i> or <i>Other Certificate Field Used
to Access User Profile</i> attribute.<br><br><i>NB </i>The client certificate must contain the
<i>Subject Alternate Name Extension</i> for this function to operate.",

```

```

    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ldapSearchStartDN" : {
    "title" : "LDAP Search Start or Base DN",
    "description" : "The start point in the LDAP server for the certificate search<br><br>When
entering multiple entries, each entry must be prefixed with a local server name. Multiple entries
allow different search Base DN's depending on the OpenAM server in use. The format is:<br><br>
<code>local server name | base dn</code><br><br>The local server name is the full name of the
server from the list of servers and sites.",
    "propertyOrder" : 1100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "trustedRemoteHosts" : {
    "title" : "Trusted Remote Hosts",
    "description" : "A list of IP addresses trusted to supply client certificates.<br><br>If SSL/TLS
is being terminated at a load balancer or at the Distributed Authentication server then this option
can be used to ensure that only specified <i>trusted</i> hosts (identified by IP address) are allowed
to supply client certificates to the certificate module,<br><br>Valid values for this list are as
follows:<ul><li>none</li><li>any</li><li>multiple IP addresses</li></ul><br><br>The default value
of <i>none</i> disables this functionality",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "otherCertificateAttributeToProfileMapping" : {
    "title" : "Other Certificate Field Used to Access User Profile",
    "description" : "This field is only used if the <i>Certificate Field Used to Access User
Profile</i> attribute is set to <i>other</i>. This field allows a custom certificate field to be used
as the basis of the user search.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

## 1.24.2. Global Operations

Resource path: `/global-config/authentication/modules/certificate`

Resource version: `1.0`



### 1.24.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CertificateModule --global --actionName getAllTypes
```

### 1.24.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CertificateModule --global --actionName getCreatableTypes
```

### 1.24.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CertificateModule --global --actionName nextdescendents
```

### 1.24.2.4. read

Usage:

```
am> read CertificateModule --global
```

### 1.24.2.5. update

Usage:

```
am> update CertificateModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "clientCertificateHttpHeaderName" : {
          "title" : "HTTP Header Name for Client Certificate",
          "description" : "The name of the HTTP request header containing the certificate, only used
when <i>Trusted Remote Hosts</i> mode is enabled.",
          "propertyOrder" : 1900,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ldapSearchStartDN" : {
    "title" : "LDAP Search Start or Base DN",
    "description" : "The start point in the LDAP server for the certificate search<br><br>When
entering multiple entries, each entry must be prefixed with a local server name. Multiple entries
allow different search Base DN's depending on the OpenAM server in use. The format is:<br><br>
<code>local server name | base dn</code><br><br>The local server name is the full name of the
server from the list of servers and sites.",
    "propertyOrder" : 1100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "iplanet-am-auth-cert-gw-cert-preferred" : {
    "title" : "Use only Certificate from HTTP request header",
    "description" : "Strictly use client cert from HTTP header over cert from HTTPS connection/
servlet attribute",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ldapCertificateAttribute" : {
    "title" : "Subject DN Attribute Used to Search LDAP for Certificates",
    "description" : "This is the attribute used to search the directory for the
certificate<br><br>The Certificate module will search the directory for the certificate using the
search filter based on this attribute and the value of the Subject DN taken from the certificate.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "crlHttpParameters" : {
    "title" : "HTTP Parameters for CRL Update",
    "description" : "These parameters will be included in any HTTP CRL call to the Certificate
Authority<br><br>If the Client or CA certificate contains the Issuing Distribution Point Extension
then OpenAM will use this information to retrieve the CRL from the distribution point. This property
allow custom HTTP parameters to be included in the CRL request.<br><br>The format of the parameter
is as follows:<br><br><code>param1=value1,param2=value</code>",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "updateCRLsFromDistributionPoint" : {
    "title" : "Update CA CRLs from CRLDistributionPoint",
    "description" : "Fetch new CA CRLs from CRLDistributionPoint and update it in
Directory Server<br><br>If the CA certificate includes an IssuingDistributionPoint or has an
CRLDistributionPoint extension set OpenAM tries to update the CRLs if needed (i.e. CRL is out-of-
date). <br>This property controls if the update should be performed.<br>This property is only used
if CA CRL checking is enabled.",
    "propertyOrder" : 800,
    "required" : true,

```

```

    "type" : "boolean",
    "exampleValue" : ""
  },
  "userBindPassword" : {
    "title" : "LDAP Server Authentication Password",
    "description" : "The password for the authentication user",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "cacheCRLsInMemory" : {
    "title" : "Cache CRLs in memory",
    "description" : "The CRLs will be cached in memory",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "crlMatchingCertificateAttribute" : {
    "title" : "Issuer DN Attribute(s) Used to Search LDAP for CRLs",
    "description" : "This is the name of the attribute taken from the CA certificate that will
be used to search the CRL.<br><br>If only one attribute name is specified, the ldap searchfilter
will be (attrName=Value_of_the_corresponding_Attribute_from_SubjectDN)<br>e.g. SubjectDN of issuer
cert 'C=US, CN=Some CA, serialNumber=123456', attribute name specified is 'CN', searchfilter used
will be <code>(CN=Some CA)</code><br><br>If several attribute names are specified, they have
to be separated by <code>,</code>. The resulting ldap searchfilter value will be a comma separated
list of name attribute values, the search attribute will be <code>cn</code><br>e.g. SubjectDN of
issuer cert 'C=US, CN=Some CA, serialNumber=123456', attribute names specified are 'CN,serialNumber',
searchfilter used will be <code>cn=CN=Some CA,serialNumber=123456</code><br>The order of the values
of the attribute names matter as they must match the value of the <code>cn</code> attribute of a
crlDistributionPoint entry in the directory server.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userBindDN" : {
    "title" : "LDAP Server Authentication User",
    "description" : "DN of the user used by the module to authenticate to the LDAP
server<br><br>The Certificate module authenticates to the LDAP server in order to search for a
matching certificate. The DN entered here represents the account used for said authentication and
must have read/search access to the LDAP server.",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ocspValidationEnabled" : {
    "title" : "OCSP Validation",
    "description" : "Enable Online Certificate Status Protocol validation for OCSP aware
certificates<br><br>If the certificate contains OCSP validation information then OpenAM will use this
information to check the validity of the certificate as part of the authentication process.<br><br>
><i>NB </i>The OpenAM server must have Internet connectivity for OCSP to work",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }

```

```

    },
    "certificateAttributeProfileMappingExtension" : {
      "title" : "SubjectAltNameExt Value Type to Access User Profile",
      "description" : "Use the Subject Alternative Name Field in preference to one of the standard
certificate fields.<br><br>Selecting RFC822Name or UPN will cause this field to have have precedence
over the <i>Certificate Field Used to Access User Profile</i> or <i>Other Certificate Field Used
to Access User Profile</i> attribute.<br><br><i>NB </i>The client certificate must contain the
<i>Subject Alternate Name Extension</i> for this function to operate.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "matchCertificateInLdap" : {
      "title" : "Match Certificate in LDAP",
      "description" : "The client certificate must exist in the directory for the authentication
to be successful.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "sslEnabled" : {
      "title" : "Use SSL/TLS for LDAP Access",
      "description" : "The certificate module will use SSL/TLS to access the LDAP server",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "trustedRemoteHosts" : {
      "title" : "Trusted Remote Hosts",
      "description" : "A list of IP addresses trusted to supply client certificates.<br><br>If
SSL/TLS is being terminated at a load balancer or at the Distributed Authentication server then this
option can be used to ensure that only specified <i>trusted</i> hosts (identified by IP address) are
allowed to supply client certificates to the certificate module,<br><br>Valid values for this list
are as follows:<ul><li>none</li><li>any</li><li>multiple IP addresses</li></ul><br><br>The default
value of <i>none</i> disables this functionality",
      "propertyOrder" : 1800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "matchCACertificateToCRL" : {
      "title" : "Match CA Certificate to CRL",

```

```

        "description" : "The CA certificate that issued the client certificate will also be checked
against the CRL.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "certificateLdapServers" : {
        "title" : "LDAP Server Where Certificates are Stored",
        "description" : "Use this list to set the LDAP server used to search for certificates.
<br><br>The Certificate authentication module will use this list for the LDAP server used to search
for certificates. A single entry must be in the format:<br><br><code>ldap_server:port</code><br>
<br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br>
<br><br><code>local server name | server:port</code><br><br>The local server name is the full name of
the server from the list of servers and sites.",
        "propertyOrder" : 1000,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "certificateAttributeToProfileMapping" : {
        "title" : "Certificate Field Used to Access User Profile",
        "description" : "The certificate module needs to read a value from the client certificate
that can be used to search the LDAP server for a matching certificate. ",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "otherCertificateAttributeToProfileMapping" : {
        "title" : "Other Certificate Field Used to Access User Profile",
        "description" : "This field is only used if the <i>Certificate Field Used to Access User
Profile</i> attribute is set to <i>other</i>. This field allows a custom certificate field to be used
as the basis of the user search.",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "matchCertificateToCRL" : {
        "title" : "Match Certificate to CRL",
        "description" : "The Client Certificate will be checked against the Certificate Revocation
list held in the directory<br><br>A Certificate Revocation List can be provisioned into the
directory. Having this option enabled will cause all client certificates to be checked against this
list.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
},
"type" : "object",
"title" : "Realm Defaults"
}
}

```

```
}
```

## 1.25. CircleOfTrust

### 1.25.1. Realm Operations

Resource path: `/realm-config/federation/circlesoftrust`

Resource version: `1.0`

#### 1.25.1.1. create

Usage:

```
am> create CircleOfTrust --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "saml2WriterServiceUrl" : {
      "title" : "a211",
      "description" : "",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status of the Circle of Trust",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedProviders" : {
      "title" : "Trusted Providers",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
```

```
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"saml2ReaderServiceUrl" : {
  "title" : "a212",
  "description" : "",
  "propertyOrder" : 500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"description" : {
  "title" : "Description of the Circle of Trust ",
  "description" : "",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"idffReaderServiceUrl" : {
  "title" : "a214",
  "description" : "",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"idffWriterServiceUrl" : {
  "title" : "a213",
  "description" : "",
  "propertyOrder" : 600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
```

### 1.25.1.2. delete

Usage:

```
am> delete CircleOfTrust --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.25.1.3. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query CircleOfTrust --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.25.1.4. read

Usage:

```
am> read CircleOfTrust --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.25.1.5. update

Usage:

```
am> update CircleOfTrust --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "saml2WriterServiceUrl" : {
      "title" : "a211",
      "description" : "",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status of the Circle of Trust",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",

```



```

    "exampleValue" : ""
  },
  "trustedProviders" : {
    "title" : "Trusted Providers",
    "description" : "",
    "propertyOrder" : 300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "saml2ReaderServiceUrl" : {
    "title" : "a212",
    "description" : "",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "description" : {
    "title" : "Description of the Circle of Trust ",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "idffReaderServiceUrl" : {
    "title" : "a214",
    "description" : "",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "idffWriterServiceUrl" : {
    "title" : "a213",
    "description" : "",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

## 1.26. ClientDetection

### 1.26.1. Global Operations

Resource path: </global-config/services/clientdetection>

Resource version: 1.0

### 1.26.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ClientDetection --global --actionName getAllTypes
```

### 1.26.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ClientDetection --global --actionName getCreatableTypes
```

### 1.26.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ClientDetection --global --actionName nextdescendents
```

### 1.26.1.4. read

Usage:

```
am> read ClientDetection --global
```

### 1.26.1.5. update

Usage:

```
am> update ClientDetection --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultClientType" : {
      "title" : "Default Client Type",
      "description" : "The name of the client type selected if no client match is found.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "detectionClass" : {
      "title" : "Client Detection Class",
      "description" : "The default client detection plug-in implementation.<br><br>The client detection plug-in is used to determine the client type. The client type is a name that uniquely identifies the client to OpenAM. The plug-in scans the HTTP request from the client in order to determine the name of the client type.<br><br>The implementation must implement the <code>com.iplanet.services.cdm.ClientDetectionInterface</code> interface.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enable Client Detection",
      "description" : "Enable/Disable the Client Detection Framework in OpenAM.<br><br>The Client Detection Framework can be used to identify the type of the client and deliver different content in the Authentication User Interface based on the client type. The default client type is HTML.<br><br><i>Note:</i> This functionality is disabled in OpenAM; customisation is required before it can be enabled.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

## 1.27. CommonFederationConfiguration

### 1.27.1. Global Operations

Resource path: </global-config/services/federation/common>

Resource version: 1.0

#### 1.27.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CommonFederationConfiguration --global --actionName getAllTypes
```

### 1.27.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CommonFederationConfiguration --global --actionName getCreatableTypes
```

### 1.27.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CommonFederationConfiguration --global --actionName nextdescendents
```

### 1.27.1.4. read

Usage:

```
am> read CommonFederationConfiguration --global
```

### 1.27.1.5. update

Usage:

```
am> update CommonFederationConfiguration --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "monitoring" : {
      "type" : "object",
      "title" : "Monitoring",
      "propertyOrder" : 3,
      "properties" : {
        "monitoringIdffClass" : {
          "title" : "Monitoring Provider Class for ID-FF",
          "description" : "The ID-FF engine uses this class to gain access to the monitoring
system.<br><br>The default implementation uses the built-in OpenAM monitoring system. A custom
implementation must implement the <code>com.sun.identity.plugin.monitoring.FedMonIDFFSvc</code>
interface.",
          "propertyOrder" : 2200,
          "required" : true,
```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "monitoringAgentClass" : {
        "title" : "Monitoring Agent Provider Class",
        "description" : "The Federation system uses this class to gain access to the monitoring
system.<br><br>The default implementation uses the built-in OpenAM monitoring system. A custom
implementation must implement the <code>com.sun.identity.plugin.monitoring.FedMonAgent</code>
interface.",
        "propertyOrder" : 1900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "monitoringSaml1Class" : {
        "title" : "Monitoring Provider Class for SAML1",
        "description" : "The SAMLv1 engine uses this class to gain access to the monitoring
system.<br><br>The default implementation uses the built-in OpenAM monitoring system. A custom
implementation must implement the <code>com.sun.identity.plugin.monitoring.FedMonSAML1Svc</code>
interface.",
        "propertyOrder" : 2000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "monitoringSaml2Class" : {
        "title" : "Monitoring Provider Class for SAML2",
        "description" : "The SAML2 engine uses this class to gain access to the monitoring
system.<br><br>The default implementation uses the built-in OpenAM monitoring system. A custom
implementation must implement the <code>com.sun.identity.plugin.monitoring.FedMonSAML2Svc</code>
interface.",
        "propertyOrder" : 2100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"generalConfig" : {
    "type" : "object",
    "title" : "General Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "certificateChecking" : {
            "title" : "Check presence of certificates",
            "description" : "Enable checking of certificates against local copy<br><br>Whether to verify
that the partner's signing certificate included in the Federation XML document is the same as the one
stored in the said partner's meta data.",
            "propertyOrder" : 900,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "maxContentLength" : {
            "title" : "Maximum allowed content length",
            "description" : "The maximum content length allowed in federation communications, in
bytes.",
            "propertyOrder" : 500,
            "required" : true,

```

```

        "type" : "integer",
        "exampleValue" : ""
    },
    "samlErrorPageHttpBinding" : {
        "title" : "SAML Error Page HTTP Binding",
        "description" : "The possible values are HTTP-Redirect or HTTP-POST.",
        "propertyOrder" : 1800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "samlErrorPageUrl" : {
        "title" : "SAML Error Page URL",
        "description" : "OpenAM redirects users here when an error occurs in the SAML2
engine.<br><br>Both relative and absolute URLs are supported. Users are redirected to an absolute URL
using the configured HTTP Binding whereas relative URLs are displayed within the request.",
        "propertyOrder" : 1700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"algorithms" : {
    "type" : "object",
    "title" : "Algorithms",
    "propertyOrder" : 2,
    "properties" : {
        "canonicalizationAlgorithm" : {
            "title" : "XML canonicalization algorithm",
            "description" : "The algorithm used to canonicalize XML documents.",
            "propertyOrder" : 1000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "QuerySignatureAlgorithmRSA" : {
            "title" : "Query String signature algorithm (RSA)",
            "description" : "The default signature algorithm to use in case of RSA keys.",
            "propertyOrder" : 1300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "transformationAlgorithm" : {
            "title" : "XML transformation algorithm",
            "description" : "The algorithm used to transform XML documents.",
            "propertyOrder" : 1600,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "DigestAlgorithm" : {
            "title" : "XML digest algorithm",
            "description" : "The default digest algorithm to use in signing XML.",
            "propertyOrder" : 1200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}

```

```

    },
    "QuerySignatureAlgorithmDSA" : {
      "title" : "Query String signature algorithm (DSA)",
      "description" : "The default signature algorithm to use in case of DSA keys.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "signatureAlgorithm" : {
      "title" : "XML signature algorithm",
      "description" : "The algorithm used to sign XML documents.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "QuerySignatureAlgorithmEC" : {
      "title" : "Query String signature algorithm (EC)",
      "description" : "The default signature algorithm to use in case of EC keys.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
},
"implementationClasses" : {
  "type" : "object",
  "title" : "Implementation Classes",
  "propertyOrder" : 1,
  "properties" : {
    "passwordDecoderClass" : {
      "title" : "PasswordDecoder SPI implementation class",
      "description" : "The Federation system uses this class to decode password  
encoded by OpenAM.<br><br>The default implementation uses the internal OpenAM  
decryption API to decode passwords. A custom implementation must implement the  
<code>com.sun.identity.saml.xmlsig.PasswordDecoder</code> interface.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "keyProviderClass" : {
      "title" : "KeyProvider SPI implementation class",
      "description" : "The Federation system uses this class to provide access to the  
underlying Java keystore.<br><br>The default implementation uses the Java Cryptographic  
Engine to provide access to the Java keystore. A custom implementation must implement the  
<code>com.sun.identity.saml.xmlsig.KeyProvider</code> interface.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "datastoreClass" : {
      "title" : "Datastore SPI implementation class",
      "description" : "The Federation system uses this class to get/set user  
profile attributes.<br><br>The default implementation uses the Identity repository

```





## 1.28. ConditionTypes

### 1.28.1. Realm Operations

Service for querying and reading the environment condition types stored in OpenAM. Environment condition types describe the JSON representation of environment conditions that you can use in policy definitions

Resource path: `/conditiontypes`

Resource version: `1.0`

#### 1.28.1.1. query

Query the list of environment condition types

Usage:

```
am> query ConditionTypes --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

#### 1.28.1.2. read

Read an individual environment condition type by providing the unique identifier title

Usage:

```
am> read ConditionTypes --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.29. Csv

### 1.29.1. Realm Operations

Resource path: `/realm-config/services/audit/CSV`

Resource version: `1.0`

### 1.29.1.1. create

Usage:

```
am> create Csv --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "csvFileRotation" : {
      "type" : "object",
      "title" : "File Rotation",
      "propertyOrder" : 3,
      "properties" : {
        "rotationTimes" : {
          "title" : "Rotation Times",
          "description" : "Durations after midnight to trigger file rotation, in seconds.",
          "propertyOrder" : 1100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "rotationFileSuffix" : {
          "title" : "File Rotation Suffix",
          "description" : "Suffix to append to audit files when they are rotated. Suffix should be a timestamp.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationInterval" : {
          "title" : "Rotation Interval",
          "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero value disables this feature.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationEnabled" : {
          "title" : "Rotation Enabled",
          "description" : "Enables and disables audit file rotation.",
          "propertyOrder" : 600,
          "required" : true,

```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "rotationMaxFileSize" : {
        "title" : "Maximum File Size",
        "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "rotationFilePrefix" : {
        "title" : "File Rotation Prefix",
        "description" : "Prefix to prepend to audit files when rotating audit files.",
        "propertyOrder" : 800,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 2100,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"csvBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 5,
    "properties" : {
        "bufferingEnabled" : {
            "title" : "Buffering Enabled",
            "description" : "Enables or disables buffering.",
            "propertyOrder" : 1500,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    },
    "bufferingAutoFlush" : {
        "title" : "Flush Each Event Immediately",
        "description" : "Performance may be improved by writing all buffered events before
flushing.",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "boolean",

```

```

        "exampleValue" : ""
    }
}
},
"csvFileRetention" : {
    "type" : "object",
    "title" : "File Retention",
    "propertyOrder" : 4,
    "properties" : {
        "retentionMaxDiskSpaceToUse" : {
            "title" : "Maximum Disk Space",
            "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
            "title" : "Maximum Number of Historical Files",
            "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
            "propertyOrder" : 1200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMinFreeSpaceRequired" : {
            "title" : "Minimum Free Space Required",
            "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"csvSecurity" : {
    "type" : "object",
    "title" : "Tamper Evident Configuration",
    "propertyOrder" : 6,
    "properties" : {
        "securityFilename" : {
            "title" : "Certificate Store Location",
            "description" : "Path to Java keystore.",
            "propertyOrder" : 1800,
            "required" : false,
            "type" : "string",
            "exampleValue" : ""
        },
        "securityEnabled" : {
            "title" : "Is Enabled",
            "description" : "Enables the CSV tamper evident feature.",
            "propertyOrder" : 1700,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
},

```

```

"securitySignatureInterval" : {
  "title" : "Signature Interval",
  "description" : "Signature generation interval, in seconds.",
  "propertyOrder" : 2000,
  "required" : false,
  "type" : "string",
  "exampleValue" : ""
},
"securityPassword" : {
  "title" : "Certificate Store Password",
  "description" : "Password for Java keystore.",
  "propertyOrder" : 1900,
  "required" : false,
  "type" : "string",
  "format" : "password",
  "exampleValue" : ""
}
},
"commonHandler" : {
  "type" : "object",
  "title" : "General Handler Configuration",
  "propertyOrder" : 0,
  "properties" : {
    "topics" : {
      "title" : "Topics",
      "description" : "List of topics handled by an audit event handler.",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "Enables or disables an audit event handler.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
},
"csvConfig" : {
  "type" : "object",
  "title" : "CSV Configuration",
  "propertyOrder" : 2,
  "properties" : {
    "location" : {
      "title" : "Log Directory",
      "description" : "Directory in which to store audit log CSV files.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
}

```

```
}  
}  
}
```

### 1.29.1.2. delete

Usage:

```
am> delete Csv --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.29.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Csv --realm Realm --actionName getAllTypes
```

### 1.29.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Csv --realm Realm --actionName getCreatableTypes
```

### 1.29.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Csv --realm Realm --actionName nextdescendents
```

### 1.29.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Csv --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

**1.29.1.7. read**

Usage:

```
am> read Csv --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

**1.29.1.8. update**

Usage:

```
am> update Csv --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "csvFileRotation" : {
      "type" : "object",
      "title" : "File Rotation",
      "propertyOrder" : 3,
      "properties" : {
        "rotationTimes" : {
          "title" : "Rotation Times",
          "description" : "Durations after midnight to trigger file rotation, in seconds.",
          "propertyOrder" : 1100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "rotationFileSuffix" : {
          "title" : "File Rotation Suffix",
          "description" : "Suffix to append to audit files when they are rotated. Suffix should be a timestamp.",

```

```

        "propertyOrder" : 900,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "rotationInterval" : {
        "title" : "Rotation Interval",
        "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "rotationEnabled" : {
        "title" : "Rotation Enabled",
        "description" : "Enables and disables audit file rotation.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "rotationMaxFileSize" : {
        "title" : "Maximum File Size",
        "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "rotationFilePrefix" : {
        "title" : "File Rotation Prefix",
        "description" : "Prefix to prepend to audit files when rotating audit files.",
        "propertyOrder" : 800,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 2100,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
},
"csvBuffering" : {

```



```

    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 5,
    "properties" : {
      "bufferingEnabled" : {
        "title" : "Buffering Enabled",
        "description" : "Enables or disables buffering.",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "bufferingAutoFlush" : {
        "title" : "Flush Each Event Immediately",
        "description" : "Performance may be improved by writing all buffered events before
flushing.",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  },
  "csvFileRetention" : {
    "type" : "object",
    "title" : "File Retention",
    "propertyOrder" : 4,
    "properties" : {
      "retentionMaxDiskSpaceToUse" : {
        "title" : "Maximum Disk Space",
        "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 1300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "retentionMaxNumberOfHistoryFiles" : {
        "title" : "Maximum Number of Historical Files",
        "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
        "propertyOrder" : 1200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "retentionMinFreeSpaceRequired" : {
        "title" : "Minimum Free Space Required",
        "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "csvSecurity" : {
    "type" : "object",

```

```

"title" : "Tamper Evident Configuration",
"propertyOrder" : 6,
"properties" : {
  "securityFilename" : {
    "title" : "Certificate Store Location",
    "description" : "Path to Java keystore.",
    "propertyOrder" : 1800,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "securityEnabled" : {
    "title" : "Is Enabled",
    "description" : "Enables the CSV tamper evident feature.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "securitySignatureInterval" : {
    "title" : "Signature Interval",
    "description" : "Signature generation interval, in seconds.",
    "propertyOrder" : 2000,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "securityPassword" : {
    "title" : "Certificate Store Password",
    "description" : "Password for Java keystore.",
    "propertyOrder" : 1900,
    "required" : false,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  }
}
},
"commonHandler" : {
  "type" : "object",
  "title" : "General Handler Configuration",
  "propertyOrder" : 0,
  "properties" : {
    "topics" : {
      "title" : "Topics",
      "description" : "List of topics handled by an audit event handler.",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "Enables or disables an audit event handler.",
      "propertyOrder" : 300,
      "required" : true,

```

```

        "type" : "boolean",
        "exampleValue" : ""
    }
},
"csvConfig" : {
    "type" : "object",
    "title" : "CSV Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "location" : {
            "title" : "Log Directory",
            "description" : "Directory in which to store audit log CSV files.",
            "propertyOrder" : 500,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
}
}
}

```

## 1.29.2. Global Operations

Resource path: `/global-config/services/audit/CSV`

Resource version: `1.0`

### 1.29.2.1. create

Usage:

```
am> create Csv --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```

{
    "type" : "object",
    "properties" : {
        "commonHandler" : {
            "type" : "object",
            "title" : "General Handler Configuration",
            "propertyOrder" : 0,
            "properties" : {
                "topics" : {

```

```

        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 400,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"csvFileRetention" : {
    "type" : "object",
    "title" : "File Retention",
    "propertyOrder" : 4,
    "properties" : {
        "retentionMaxDiskSpaceToUse" : {
            "title" : "Maximum Disk Space",
            "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
            "title" : "Maximum Number of Historical Files",
            "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
            "propertyOrder" : 1200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMinFreeSpaceRequired" : {
            "title" : "Minimum Free Space Required",
            "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
},
"csvFileRotation" : {
    "type" : "object",
    "title" : "File Rotation",
    "propertyOrder" : 3,
    "properties" : {

```

```

    "rotationEnabled" : {
      "title" : "Rotation Enabled",
      "description" : "Enables and disables audit file rotation.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "rotationMaxFileSize" : {
      "title" : "Maximum File Size",
      "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "rotationInterval" : {
      "title" : "Rotation Interval",
      "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "rotationFilePrefix" : {
      "title" : "File Rotation Prefix",
      "description" : "Prefix to prepend to audit files when rotating audit files.",
      "propertyOrder" : 800,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "rotationTimes" : {
      "title" : "Rotation Times",
      "description" : "Durations after midnight to trigger file rotation, in seconds.",
      "propertyOrder" : 1100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "rotationFileSuffix" : {
      "title" : "File Rotation Suffix",
      "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
      "propertyOrder" : 900,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "csvSecurity" : {
    "type" : "object",
    "title" : "Tamper Evident Configuration",

```

```

"propertyOrder" : 6,
"properties" : {
  "securitySignatureInterval" : {
    "title" : "Signature Interval",
    "description" : "Signature generation interval, in seconds.",
    "propertyOrder" : 2000,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "securityPassword" : {
    "title" : "Certificate Store Password",
    "description" : "Password for Java keystore.",
    "propertyOrder" : 1900,
    "required" : false,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "securityFilename" : {
    "title" : "Certificate Store Location",
    "description" : "Path to Java keystore.",
    "propertyOrder" : 1800,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "securityEnabled" : {
    "title" : "Is Enabled",
    "description" : "Enables the CSV tamper evident feature.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }
}
},
"commonHandlerPlugin" : {
  "type" : "object",
  "title" : "Audit Event Handler Factory",
  "propertyOrder" : 1,
  "properties" : {
    "handlerFactory" : {
      "title" : "Factory Class Name",
      "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
},
"csvBuffering" : {
  "type" : "object",
  "title" : "Buffering",
  "propertyOrder" : 5,
  "properties" : {

```

```

    "bufferingEnabled" : {
      "title" : "Buffering Enabled",
      "description" : "Enables or disables buffering.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "bufferingAutoFlush" : {
      "title" : "Flush Each Event Immediately",
      "description" : "Performance may be improved by writing all buffered events before
flushing.",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "csvConfig" : {
    "type" : "object",
    "title" : "CSV Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "location" : {
        "title" : "Log Directory",
        "description" : "Directory in which to store audit log CSV files.",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  }
}
}
}
}

```

### 1.29.2.2. delete

Usage:

```
am> delete Csv --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.29.2.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Csv --global --actionName getAllTypes
```

#### 1.29.2.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Csv --global --actionName getCreatableTypes
```

#### 1.29.2.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Csv --global --actionName nextdescendents
```

#### 1.29.2.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Csv --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.29.2.7. read

Usage:

```
am> read Csv --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.29.2.8. update

Usage:

```
am> update Csv --global --id id --body body
```



Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "csvFileRetention" : {
      "type" : "object",
      "title" : "File Retention",
      "propertyOrder" : 4,
      "properties" : {
        "retentionMaxDiskSpaceToUse" : {
          "title" : "Maximum Disk Space",
          "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
          "title" : "Maximum Number of Historical Files",
          "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code> disables pruning of old history files.",
          "propertyOrder" : 1200,
          "required" : true,
```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "retentionMinFreeSpaceRequired" : {
        "title" : "Minimum Free Space Required",
        "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"csvFileRotation" : {
    "type" : "object",
    "title" : "File Rotation",
    "propertyOrder" : 3,
    "properties" : {
        "rotationEnabled" : {
            "title" : "Rotation Enabled",
            "description" : "Enables and disables audit file rotation.",
            "propertyOrder" : 600,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "rotationMaxFileSize" : {
            "title" : "Maximum File Size",
            "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 700,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "rotationInterval" : {
            "title" : "Rotation Interval",
            "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
            "propertyOrder" : 1000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "rotationFilePrefix" : {
            "title" : "File Rotation Prefix",
            "description" : "Prefix to prepend to audit files when rotating audit files.",
            "propertyOrder" : 800,
            "required" : false,
            "type" : "string",
            "exampleValue" : ""
        },
        "rotationTimes" : {
            "title" : "Rotation Times",
            "description" : "Durations after midnight to trigger file rotation, in seconds.",
            "propertyOrder" : 1100,
            "required" : true,
            "items" : {

```

```

        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"rotationFileSuffix" : {
    "title" : "File Rotation Suffix",
    "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
    "propertyOrder" : 900,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
}
},
},
"csvSecurity" : {
    "type" : "object",
    "title" : "Tamper Evident Configuration",
    "propertyOrder" : 6,
    "properties" : {
        "securitySignatureInterval" : {
            "title" : "Signature Interval",
            "description" : "Signature generation interval, in seconds.",
            "propertyOrder" : 2000,
            "required" : false,
            "type" : "string",
            "exampleValue" : ""
        },
        "securityPassword" : {
            "title" : "Certificate Store Password",
            "description" : "Password for Java keystore.",
            "propertyOrder" : 1900,
            "required" : false,
            "type" : "string",
            "format" : "password",
            "exampleValue" : ""
        },
        "securityFilename" : {
            "title" : "Certificate Store Location",
            "description" : "Path to Java keystore.",
            "propertyOrder" : 1800,
            "required" : false,
            "type" : "string",
            "exampleValue" : ""
        },
        "securityEnabled" : {
            "title" : "Is Enabled",
            "description" : "Enables the CSV tamper evident feature.",
            "propertyOrder" : 1700,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
},
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",

```

```

    "propertyOrder" : 1,
    "properties" : {
      "handlerFactory" : {
        "title" : "Factory Class Name",
        "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
        "propertyOrder" : 2100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "csvBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 5,
    "properties" : {
      "bufferingEnabled" : {
        "title" : "Buffering Enabled",
        "description" : "Enables or disables buffering.",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "bufferingAutoFlush" : {
        "title" : "Flush Each Event Immediately",
        "description" : "Performance may be improved by writing all buffered events before
flushing.",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  },
  "csvConfig" : {
    "type" : "object",
    "title" : "CSV Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "location" : {
        "title" : "Log Directory",
        "description" : "Directory in which to store audit log CSV files.",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  }
}
}
}
}
}

```

## 1.30. CtsDataStoreProperties

### 1.30.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/cts`

Resource version: `1.0`

#### 1.30.1.1. read

Usage:

```
am> read CtsDataStoreProperties --global --serverName serverName
```

Parameters:

**--serverName**

An object of property key-value pairs

#### 1.30.1.2. update

Usage:

```
am> update CtsDataStoreProperties --global --serverName serverName --body body
```

Parameters:

**--serverName**

An object of property key-value pairs

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.org.forgerock.services.cts.store.common.section" : {
      "title" : "CTS Token Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "org.forgerock.services.cts.store.location" : {
          "title" : "Store Mode",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
```

```

        "value" : {
          "enum" : [ "default", "external" ],
          "options" : {
            "enum_titles" : [ "Default Token Store", "External Token Store" ]
          },
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    },
    "org.forgerock.services.cts.store.root.suffix" : {
      "title" : "Root Suffix",
      "type" : "object",
      "propertyOrder" : 1,
      "description" : "",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    },
    "org.forgerock.services.cts.store.max.connections" : {
      "title" : "Max Connections",
      "type" : "object",
      "propertyOrder" : 2,
      "description" : "",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  }
},
"amconfig.org.forgerock.services.cts.store.external.section" : {
  "title" : "External Store Configuration",
  "type" : "object",
  "propertyOrder" : 1,
  "properties" : {
    "org.forgerock.services.cts.store.ssl.enabled" : {
      "title" : "SSL/TLS Enabled",
      "type" : "object",
      "propertyOrder" : 0,
      "description" : "",
      "properties" : {

```

```

        "value" : {
          "type" : "boolean",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    },
    "org.forgerock.services.cts.store.directory.name" : {
      "title" : "Connection String(s)",
      "type" : "object",
      "propertyOrder" : 1,
      "description" : "An ordered list of connection strings for LDAP directories. Each connection
string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
IDs are optional parameters that will prioritize that connection to use from the specified nodes.
Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>.",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    },
    "org.forgerock.services.cts.store.loginid" : {
      "title" : "Login Id",
      "type" : "object",
      "propertyOrder" : 2,
      "description" : "",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    },
    "org.forgerock.services.cts.store.password" : {
      "title" : "Password",
      "type" : "object",
      "propertyOrder" : 3,
      "description" : "",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false,
          "format" : "password"
        },
        "inherited" : {
          "type" : "boolean",

```





### 1.31.1.1. create

Usage:

```
am> create Dashboard --realm Realm --body body
```

Parameters:

#### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "assignedDashboard" : {
      "title" : "Available Dashboard Apps",
      "description" : "List of application dashboard names available by default for realms with the
Dashboard service configured.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

### 1.31.1.2. delete

Usage:

```
am> delete Dashboard --realm Realm
```

### 1.31.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Dashboard --realm Realm --actionName getAllTypes
```

### 1.31.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Dashboard --realm Realm --actionName getCreatableTypes
```

### 1.31.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Dashboard --realm Realm --actionName nextdescendents
```

### 1.31.1.6. read

Usage:

```
am> read Dashboard --realm Realm
```

### 1.31.1.7. update

Usage:

```
am> update Dashboard --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "assignedDashboard" : {
      "title" : "Available Dashboard Apps",
      "description" : "List of application dashboard names available by default for realms with the
Dashboard service configured.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.31.2. Global Operations

Resource path: `/global-config/services/dashboard`

Resource version: `1.0`

### 1.31.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Dashboard --global --actionName getAllTypes
```

### 1.31.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Dashboard --global --actionName getCreatableTypes
```

### 1.31.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Dashboard --global --actionName nextdescendents
```

### 1.31.2.4. read

Usage:

```
am> read Dashboard --global
```

### 1.31.2.5. update

Usage:

```
am> update Dashboard --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "assignedDashboard" : {
          "title" : "Available Dashboard Apps",
          "description" : "List of application dashboard names available by default for realms with the Dashboard service configured.",
          "propertyOrder" : 700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

## 1.32. DashboardInstance

### 1.32.1. Global Operations

Resource path: `/global-config/services/dashboard/instances`

Resource version: `1.0`

#### 1.32.1.1. create

Usage:

```
am> create DashboardInstance --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```

"properties" : {
  "displayName" : {
    "title" : "Dashboard Display Name",
    "description" : "The application name that displays on the dashboard client.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "login" : {
    "title" : "Dashboard Login",
    "description" : "The URL that takes the user to the application.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "name" : {
    "title" : "Dashboard Name",
    "description" : "The application name as it will appear to the administrator for configuring the
dashboard.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "icon" : {
    "title" : "Dashboard Icon",
    "description" : "The icon name that will be displayed on the dashboard client identifying the
application.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "className" : {
    "title" : "Dashboard Class Name",
    "description" : "Identifies how to access the application, for example
<code>SAML2ApplicationClass</code> for a SAML v2.0 application.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "icfIdentifier" : {
    "title" : "ICF Identifier",
    "description" : "",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
}

```

### 1.32.1.2. delete

Usage:

```
am> delete DashboardInstance --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.32.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DashboardInstance --global --actionName getAllTypes
```

### 1.32.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DashboardInstance --global --actionName getCreatableTypes
```

### 1.32.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DashboardInstance --global --actionName nextdescendents
```

### 1.32.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query DashboardInstance --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.32.1.7. read

Usage:

```
am> read DashboardInstance --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.32.1.8. update

Usage:

```
am> update DashboardInstance --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "displayName" : {
      "title" : "Dashboard Display Name",
      "description" : "The application name that displays on the dashboard client.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "login" : {
      "title" : "Dashboard Login",
      "description" : "The URL that takes the user to the application.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "name" : {
      "title" : "Dashboard Name",
      "description" : "The application name as it will appear to the administrator for configuring the dashboard.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "icon" : {
      "title" : "Dashboard Icon",
```

```
    "description" : "The icon name that will be displayed on the dashboard client identifying the application.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "className" : {
    "title" : "Dashboard Class Name",
    "description" : "Identifies how to access the application, for example <code>SAML2ApplicationClass</code> for a SAML v2.0 application.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "icfIdentifier" : {
    "title" : "ICF Identifier",
    "description" : "",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
```

## 1.33. Dashboards

### 1.33.1. Realm Operations

The dashboard service is responsible for returning information from the Dashboard. The only supported operation is read.

Resource path: `/dashboard`

Resource version: `1.0`

#### 1.33.1.1. read

Read dashboard information

Usage:

```
am> read Dashboards --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.



## 1.34. DataStoreModule

### 1.34.1. Realm Operations

Resource path: `/realm-config/authentication/modules/datastore`

Resource version: `1.0`

#### 1.34.1.1. create

Usage:

```
am> create DataStoreModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

#### 1.34.1.2. delete

Usage:

```
am> delete DataStoreModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.34.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DataStoreModule --realm Realm --actionName getAllTypes
```

### 1.34.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DataStoreModule --realm Realm --actionName getCreatableTypes
```

### 1.34.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DataStoreModule --realm Realm --actionName nextdescendents
```

### 1.34.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query DataStoreModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.34.1.7. read

Usage:

```
am> read DataStoreModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.34.1.8. update

Usage:

```
am> update DataStoreModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

## 1.34.2. Global Operations

Resource path: </global-config/authentication/modules/datastore>

Resource version: [1.0](#)

### 1.34.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DataStoreModule --global --actionName getAllTypes
```

### 1.34.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DataStoreModule --global --actionName getCreatableTypes
```

### 1.34.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DataStoreModule --global --actionName nextdescendents
```

### 1.34.2.4. read

Usage:

```
am> read DataStoreModule --global
```

### 1.34.2.5. update

Usage:

```
am> update DataStoreModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

## 1.35. DatabaseRepositoryEarlyAccess

### 1.35.1. Realm Operations

Resource path: `/realm-config/services/id-repositories/Database`

Resource version: `1.0`

#### 1.35.1.1. create

Usage:

```
am> create DatabaseRepositoryEarlyAccess --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-opensso-database-JDBCdriver" : {
      "title" : "JDBC Driver Class Name",
      "description" : "Class name of JDBC driver to use to get connections. URL, JDBC username and password paramters also needed",
      "propertyOrder" : 7500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-opensso-database-JDBCdbpassword" : {
      "title" : "Password for Connecting to Database",
      "description" : "Password used as parameter by JDBC driver",
      "propertyOrder" : 7600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "sun-opensso-database-JDBCurl" : {
      "title" : "JDBC Driver URL",
      "description" : "URL used as parameter by JDBC driver",
      "propertyOrder" : 7700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-opensso-database-UserIDAttr" : {
```

```

    "title" : "User ID Attribute Name",
    "description" : "Name of attribute column name in DB table for user id",
    "propertyOrder" : 8200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-opensso-database-config-users-search-attribute" : {
    "title" : "Users Search Attribute in Database",
    "description" : "Name of attribute column name in DB table for users LIKE search queries",
    "propertyOrder" : 8700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-opensso-database-UserAttrs" : {
    "title" : "List of User Attributes Names in Database",
    "description" : "",
    "propertyOrder" : 8000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-opensso-database-config-max-result" : {
    "title" : "Maximum Results Returned from Search",
    "description" : "Value to determine the maximum number of search results to fetch",
    "propertyOrder" : 8600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-opensso-database-activeValue" : {
    "title" : "User Status Active Value",
    "description" : "Value stored in the db table's user status column to represent an Active user",
    "propertyOrder" : 8400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-opensso-database-UserTableName" : {
    "title" : "Database User Table Name",
    "description" : "",
    "propertyOrder" : 7900,
    "required" : true,
    "type" : "string",

```

```

        "exampleValue" : ""
    },
    "sunIdRepoClass" : {
        "title" : "Database Repository Plugin Class Name",
        "description" : "",
        "propertyOrder" : 7000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-inactiveValue" : {
        "title" : "User Status Inactive Value",
        "description" : "Value stored in the db table's user status column to represent an Inactive
user",
        "propertyOrder" : 8500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-UserPasswordAttr" : {
        "title" : "User Password Attribute Name",
        "description" : "Name of attribute column name in DB table for user password",
        "propertyOrder" : 8100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-membership-search-attribute" : {
        "title" : "Membership Search Attribute in Database",
        "description" : "Name of attribute column name in DB table for membership LIKE search queries",
        "propertyOrder" : 9000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-dao-JDBCConnectionType" : {
        "title" : "Connection Type",
        "description" : "",
        "propertyOrder" : 7300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-JDBCDBuser" : {
        "title" : "Connect This User to Database",
        "description" : "Connection user name used as parameter by JDBC driver",
        "propertyOrder" : 7800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-UserStatusAttr" : {
        "title" : "Attribute Name of User Status",
        "description" : "Name of attribute column name in DB table to determine if user is active or
inactive",
        "propertyOrder" : 8300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }

```

```

    },
    "sun-opensso-database-DataSourceJndiName" : {
      "title" : "Database DataSource Name",
      "description" : "Name specified when configuring a DataSource in the application server for
connections",
      "propertyOrder" : 7400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-opensso-database-dao-class-name" : {
      "title" : "Database Data Access Object Plugin Class Name",
      "description" : "",
      "propertyOrder" : 7200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-opensso-database-sunIdRepoSupportedOperations" : {
      "title" : "Database Plug-in Supported Types and Operations",
      "description" : "",
      "propertyOrder" : 7100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sun-opensso-database-MembershipIDAttr" : {
      "title" : "Membership ID Attribute Name",
      "description" : "Name of attribute column name in DB membership table to uniquely identify a
group",
      "propertyOrder" : 8900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-opensso-database-MembershipTableName" : {
      "title" : "Database Membership table name",
      "description" : "",
      "propertyOrder" : 8800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
}

```

### 1.35.1.2. delete

Usage:

```
am> delete DatabaseRepositoryEarlyAccess --realm Realm --id id
```

Parameters:



**--id**

The unique identifier for the resource.

### 1.35.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DatabaseRepositoryEarlyAccess --realm Realm --actionName getAllTypes
```

### 1.35.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DatabaseRepositoryEarlyAccess --realm Realm --actionName getCreatableTypes
```

### 1.35.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DatabaseRepositoryEarlyAccess --realm Realm --actionName nextdescendents
```

### 1.35.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query DatabaseRepositoryEarlyAccess --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.35.1.7. read

Usage:

```
am> read DatabaseRepositoryEarlyAccess --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.35.1.8. update

Usage:

```
am> update DatabaseRepositoryEarlyAccess --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-opensso-database-JDBCdriver" : {
      "title" : "JDBC Driver Class Name",
      "description" : "Class name of JDBC driver to use to get connections. URL, JDBC username and password paramters also needed",
      "propertyOrder" : 7500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-opensso-database-JDBCdbpassword" : {
      "title" : "Password for Connecting to Database",
      "description" : "Password used as parameter by JDBC driver",
      "propertyOrder" : 7600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "sun-opensso-database-JDBCurl" : {
      "title" : "JDBC Driver URL",
      "description" : "URL used as parameter by JDBC driver",
      "propertyOrder" : 7700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-opensso-database-UserIDAttr" : {
      "title" : "User ID Attribute Name",
      "description" : "Name of attribute column name in DB table for user id",
      "propertyOrder" : 8200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

```

"sun-opensso-database-config-users-search-attribute" : {
  "title" : "Users Search Attribute in Database",
  "description" : "Name of attribute column name in DB table for users LIKE search queries",
  "propertyOrder" : 8700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-opensso-database-UserAttrs" : {
  "title" : "List of User Attributes Names in Database",
  "description" : "",
  "propertyOrder" : 8000,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-opensso-database-config-max-result" : {
  "title" : "Maximum Results Returned from Search",
  "description" : "Value to determine the maximum number of search results to fetch",
  "propertyOrder" : 8600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-opensso-database-activeValue" : {
  "title" : "User Status Active Value",
  "description" : "Value stored in the db table's user status column to represent an Active user",
  "propertyOrder" : 8400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sunIdRepoAttributeMapping" : {
  "title" : "Attribute Name Mapping",
  "description" : "",
  "propertyOrder" : 1800,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-opensso-database-UserTableName" : {
  "title" : "Database User Table Name",
  "description" : "",
  "propertyOrder" : 7900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sunIdRepoClass" : {
  "title" : "Database Repository Plugin Class Name",
  "description" : "",
  "propertyOrder" : 7000,
  "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-inactiveValue" : {
        "title" : "User Status Inactive Value",
        "description" : "Value stored in the db table's user status column to represent an Inactive
user",
        "propertyOrder" : 8500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-UserPasswordAttr" : {
        "title" : "User Password Attribute Name",
        "description" : "Name of attribute column name in DB table for user password",
        "propertyOrder" : 8100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-membership-search-attribute" : {
        "title" : "Membership Search Attribute in Database",
        "description" : "Name of attribute column name in DB table for membership LIKE search queries",
        "propertyOrder" : 9000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-dao-JDBCConnectionType" : {
        "title" : "Connection Type",
        "description" : "",
        "propertyOrder" : 7300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-JDBCDBuser" : {
        "title" : "Connect This User to Database",
        "description" : "Connection user name used as parameter by JDBC driver",
        "propertyOrder" : 7800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-UserStatusAttr" : {
        "title" : "Attribute Name of User Status",
        "description" : "Name of attribute column name in DB table to determine if user is active or
inactive",
        "propertyOrder" : 8300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-DataSourceIndiName" : {
        "title" : "Database DataSource Name",
        "description" : "Name specified when configuring a DataSource in the application server for
connections",
        "propertyOrder" : 7400,
        "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-dao-class-name" : {
        "title" : "Database Data Access Object Plugin Class Name",
        "description" : "",
        "propertyOrder" : 7200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-sunIdRepoSupportedOperations" : {
        "title" : "Database Plug-in Supported Types and Operations",
        "description" : "",
        "propertyOrder" : 7100,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "sun-opensso-database-MembershipIDAttr" : {
        "title" : "Membership ID Attribute Name",
        "description" : "Name of attribute column name in DB membership table to uniquely identify a
group",
        "propertyOrder" : 8900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-opensso-database-MembershipTableName" : {
        "title" : "Database Membership table name",
        "description" : "",
        "propertyOrder" : 8800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

## 1.36. DecisionCombiners

### 1.36.1. Realm Operations

Service for querying and reading decision combiners information. Decision combiners describe how to resolve policy decisions when multiple policies apply

Resource path: [/decisioncombiners](#)

Resource version: [1.0](#)

### 1.36.1.1. query

Lists all decision combiners

Usage:

```
am> query DecisionCombiners --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [title]

### 1.36.1.2. read

Reads an individual decision combiner specified by its name

Usage:

```
am> read DecisionCombiners --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.37. DefaultAdvancedProperties

### 1.37.1. Global Operations

An object of property key-value pairs

Resource path: </global-config/servers/server-default/properties/advanced>

Resource version: [1.0](#)

### 1.37.1.1. read

Usage:

```
am> read DefaultAdvancedProperties --global
```

### 1.37.1.2. update

Usage:

```
am> update DefaultAdvancedProperties --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "patternProperties" : {
    ".+" : {
      "type" : "string",
      "title" : "Value",
      "description" : "Any string value"
    }
  },
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "An object of property key-value pairs",
  "type" : "object",
  "title" : "Advanced Properties"
}
```

## 1.38. DefaultCtsDataStoreProperties

### 1.38.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/cts`

Resource version: `1.0`

#### 1.38.1.1. read

Usage:

```
am> read DefaultCtsDataStoreProperties --global
```

#### 1.38.1.2. update

Usage:

```
am> update DefaultCtsDataStoreProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.org.forgerock.services.cts.store.common.section" : {
      "title" : "CTS Token Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "org.forgerock.services.cts.store.location" : {
          "enum" : [ "default", "external" ],
          "options" : {
            "enum_titles" : [ "Default Token Store", "External Token Store" ]
          },
          "type" : "string",
          "title" : "Store Mode",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.cts.store.root.suffix" : {
          "type" : "string",
          "title" : "Root Suffix",
          "propertyOrder" : 1,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.cts.store.max.connections" : {
          "type" : "string",
          "title" : "Max Connections",
          "propertyOrder" : 2,
          "required" : true,
          "description" : ""
        }
      }
    },
    "amconfig.org.forgerock.services.cts.store.external.section" : {
      "title" : "External Store Configuration",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "org.forgerock.services.cts.store.ssl.enabled" : {
          "type" : "boolean",
          "title" : "SSL/TLS Enabled",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.cts.store.directory.name" : {
          "type" : "string",
          "title" : "Connection String(s)",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site IDs are optional parameters that will prioritize that connection to use from the specified nodes."
        }
      }
    }
  }
}
```



Multiple connection strings should be comma-separated, e.g. `<code>host1:389,host2:50389|server1|site1,host3:50389</code>.`

```

    },
    "org.forgerock.services.cts.store.loginid" : {
      "type" : "string",
      "title" : "Login Id",
      "propertyOrder" : 2,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.cts.store.password" : {
      "type" : "string",
      "title" : "Password",
      "propertyOrder" : 3,
      "required" : true,
      "description" : "",
      "format" : "password"
    },
    "org.forgerock.services.cts.store.heartbeat" : {
      "type" : "integer",
      "title" : "Heartbeat",
      "propertyOrder" : 4,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.cts.store.affinity.enabled" : {
      "type" : "boolean",
      "title" : "Affinity Enabled",
      "propertyOrder" : 5,
      "required" : true,
      "description" : "Enables affinity based request load balancing when accessing the CTS
servers. It is imperative that the connection string setting is set to the same value for all OpenAM
servers in the deployment when this feature is enabled."
    }
  }
}
}
}

```

## 1.39. DefaultDirectoryConfiguration

### 1.39.1. Global Operations

Connection details for directory server(s).

Resource path: `/global-config/servers/server-default/properties/directoryConfiguration`

Resource version: **1.0**

#### 1.39.1.1. read

Usage:

```
am> read DefaultDirectoryConfiguration --global
```

### 1.39.1.2. update

Usage:

```
am> update DefaultDirectoryConfiguration --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "directoryConfiguration" : {
      "type" : "object",
      "title" : "Directory Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "minConnectionPool" : {
          "title" : "Minimum Connection Pool",
          "propertyOrder" : 0,
          "type" : "number"
        },
        "maxConnectionPool" : {
          "title" : "Maximum Connection Pool",
          "propertyOrder" : 1,
          "type" : "number"
        },
        "bindDn" : {
          "title" : "Bind DN",
          "propertyOrder" : 2,
          "type" : "string"
        },
        "bindPassword" : {
          "title" : "Bind Password",
          "propertyOrder" : 3,
          "type" : "string",
          "format" : "password"
        }
      }
    },
    "directoryServers" : {
      "type" : "array",
      "title" : "Server",
      "propertyOrder" : 1,
      "items" : {
        "type" : "object",
        "required" : [ "serverName", "hostName", "portNumber", "connectionType" ],
        "properties" : {
          "serverName" : {
            "title" : "Name",
```

```
        "type" : "string",
        "propertyOrder" : 0
      },
      "hostName" : {
        "title" : "Host Name",
        "type" : "string",
        "propertyOrder" : 1
      },
      "portNumber" : {
        "title" : "Port Number",
        "type" : "string",
        "propertyOrder" : 2
      },
      "connectionType" : {
        "type" : "string",
        "enum" : [ "SIMPLE", "SSL" ],
        "options" : {
          "enum_titles" : [ "SIMPLE", "SSL" ]
        },
        "title" : "Connection Type",
        "propertyOrder" : 3
      }
    }
  }
}
```

## 1.40. DefaultGeneralProperties

### 1.40.1. Global Operations

An object of property key-value pairs

Resource path: [/global-config/servers/server-default/properties/general](#)

Resource version: [1.0](#)

#### 1.40.1.1. read

Usage:

```
am> read DefaultGeneralProperties --global
```

#### 1.40.1.2. update

Usage:

```
am> update DefaultGeneralProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.installdir" : {
      "title" : "System",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "com.iplanet.services.configpath" : {
          "type" : "string",
          "title" : "Base installation directory",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Base directory where product's data resides. (property name: com.iplanet.services.configpath)"
        },
        "com.iplanet.am.locale" : {
          "type" : "string",
          "title" : "Default Locale",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Default locale for the product. (property name: com.iplanet.am.locale)"
        },
        "com.sun.identity.client.notification.url" : {
          "type" : "string",
          "title" : "Notification URL",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "The location of notification service end point. It is usually the product's deployment URI/notificationservice. (property name: com.sun.identity.client.notification.url)"
        },
        "com.iplanet.am.util.xml.validating" : {
          "enum" : [ "on", "off" ],
          "options" : {
            "enum_titles" : [ "On", "Off" ]
          },
          "type" : "string",
          "title" : "XML Validation",
          "propertyOrder" : 3,
          "required" : true,
          "description" : "Specifies if validation is required when parsing XML documents. (property name: com.iplanet.am.util.xml.validating)"
        }
      }
    },
    "amconfig.header.debug" : {
      "title" : "Debugging",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "com.iplanet.services.debug.level" : {
          "enum" : [ "off", "error", "warning", "message" ],
          "options" : {

```

```

        "enum_titles" : [ "Off", "Error", "Warning", "Message" ]
    },
    "type" : "string",
    "title" : "Debug Level",
    "propertyOrder" : 0,
    "required" : true,
    "description" : "Debug level for all components in the product. (property name:
com.ipplanet.services.debug.level)"
    },
    "com.sun.services.debug.mergeall" : {
        "enum" : [ "on", "off" ],
        "options" : {
            "enum_titles" : [ "On", "Off" ]
        },
        "type" : "string",
        "title" : "Merge Debug Files",
        "propertyOrder" : 1,
        "required" : true,
        "description" : "On : Directs all debug data to a single file (debug.out); Off : creates
separate per-component debug files (property name : com.sun.services.debug.mergeall)"
    },
    "com.ipplanet.services.debug.directory" : {
        "type" : "string",
        "title" : "Debug Directory",
        "propertyOrder" : 2,
        "required" : true,
        "description" : "Directory where debug files reside. (property name:
com.ipplanet.services.debug.directory)"
    }
    },
    "amconfig.header.mailserver" : {
        "title" : "Mail Server",
        "type" : "object",
        "propertyOrder" : 2,
        "properties" : {
            "com.ipplanet.am.smtphost" : {
                "type" : "string",
                "title" : "Mail Server Host Name",
                "propertyOrder" : 0,
                "required" : true,
                "description" : "(property name: com.ipplanet.am.smtphost)"
            },
            "com.ipplanet.am.smtpport" : {
                "type" : "integer",
                "title" : "Mail Server Port Number",
                "propertyOrder" : 1,
                "required" : true,
                "description" : "(property name: com.ipplanet.am.smtpport)"
            }
        }
    }
}
}
}
}
}

```

## 1.41. DefaultSdkProperties

### 1.41.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/sdk`

Resource version: `1.0`

#### 1.41.1.1. read

Usage:

```
am> read DefaultSdkProperties --global
```

#### 1.41.1.2. update

Usage:

```
am> update DefaultSdkProperties --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.datastore" : {
      "title" : "Data Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "com.sun.identity.sm.enableDataStoreNotification" : {
          "type" : "boolean",
          "title" : "Enable Datastore Notification",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Specifies if backend datastore notification is enabled. If
this value is set to 'false', then in-memory notification is enabled. (property name:
com.sun.identity.sm.enableDataStoreNotification)"
        },
        "com.sun.identity.sm.ldap.enableProxy" : {
          "type" : "boolean",
          "title" : "Enable Directory Proxy",
          "propertyOrder" : 1,
          "required" : true,

```

```

    "description" : "This indicates to Service Management that the Directory Proxy must be used
    for read, write, and/or modify operations to the Directory Server. This flag also determines if ACIs
    or delegation privileges are to be used. (property name: com.sun.identity.sm ldap.enableProxy)"
  },
  "com.sun.identity.sm.notification.threadpool.size" : {
    "type" : "integer",
    "title" : "Notification Pool Size",
    "propertyOrder" : 2,
    "required" : true,
    "description" : "Specifies the size of the sm notification thread pool (total number of
    threads). (property name: com.sun.identity.sm.notification.threadpool.size)"
  }
},
"amconfig.header.eventservice" : {
  "title" : "Event Service",
  "type" : "object",
  "propertyOrder" : 1,
  "properties" : {
    "com.ipplanet.am.event.connection.num.retries" : {
      "type" : "integer",
      "title" : "Number of retries for Event Service connections",
      "propertyOrder" : 0,
      "required" : true,
      "description" : "Specifies the number of attempts made to successfully re-establish the
      Event Service connections. (property name: com.ipplanet.am.event.connection.num.retries)"
    },
    "com.ipplanet.am.event.connection.delay.between.retries" : {
      "type" : "integer",
      "title" : "Delay between Event Service connection retries",
      "propertyOrder" : 1,
      "required" : true,
      "description" : "Specifies the delay in milliseconds between retries to re-establish the
      Event Service connections. (property name: com.ipplanet.am.event.connection.delay.between.retries)"
    },
    "com.ipplanet.am.event.connection.ldap.error.codes.retries" : {
      "type" : "string",
      "title" : "Error codes for Event Service connection retries",
      "propertyOrder" : 2,
      "required" : true,
      "description" : "This secifies the LDAP exception error codes for which
      retries to re-establish Event Service connections will trigger. (property name:
      com.ipplanet.am.event.connection.ldap.error.codes.retries)"
    },
    "com.sun.am.event.connection.disable.list" : {
      "type" : "string",
      "title" : "Disabled Event Service Connection",
      "propertyOrder" : 3,
      "required" : true,
      "description" : "Specifies which event connection (persistent search) to be disabled. There
      are three valid values - aci, sm and um (case insensitive). Multiple values should be separated with
      \",\". (property name: com.sun.am.event.connection.disable.list)"
    }
  }
},
"amconfig.header.ldapconnection" : {
  "title" : "LDAP Connection",
  "type" : "object",
  "propertyOrder" : 2,

```

```

    "properties" : {
      "com.ipanet.am.ldap.connection.num.retries" : {
        "type" : "integer",
        "title" : "Number of retries for LDAP Connection",
        "propertyOrder" : 0,
        "required" : true,
        "description" : "Specifies the number of attempts made to successfully re-establish LDAP
Connection. (property name: com.ipanet.am.ldap.connection.num.retries)"
      },
      "com.ipanet.am.ldap.connection.delay.between.retries" : {
        "type" : "integer",
        "title" : "Delay between LDAP connection retries",
        "propertyOrder" : 1,
        "required" : true,
        "description" : "Specifies the delay in milliseconds between retries to re-establish the
LDAP connections. (property name: com.ipanet.am.ldap.connection.delay.between.retries)"
      },
      "com.ipanet.am.ldap.connection.ldap.error.codes.retries" : {
        "type" : "string",
        "title" : "Error codes for LDAP connection retries",
        "propertyOrder" : 2,
        "required" : true,
        "description" : "This secifies the LDAP exception error codes for
which retries to re-establish LDAP connections will trigger. (property name:
com.ipanet.am.ldap.connection.ldap.error.codes.retries)"
      }
    },
    "amconfig.header.cachingreplica" : {
      "title" : "Caching and Replica",
      "type" : "object",
      "propertyOrder" : 3,
      "properties" : {
        "com.ipanet.am.sdk.cache.maxSize" : {
          "type" : "integer",
          "title" : "SDK Caching Max. Size",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Specifies the size of the cache when SDK caching is enabled. The size
should be an integer greater than 0, or default size (10000) will be used. Changing this value will
reset (clear) the contents of the cache. (property name: com.ipanet.am.sdk.cache.maxSize)"
        },
        "com.ipanet.am.replica.num.retries" : {
          "type" : "integer",
          "title" : "SDK Replica Retries",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies the number of times to retry when an Entry Not Found error is
returned to the SDK. (property name: com.ipanet.am.replica.num.retries)"
        },
        "com.ipanet.am.replica.delay.between.retries" : {
          "type" : "integer",
          "title" : "Delay between SDK Replica Retries",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "Specifies the delay time in milliseconds between the retries. (property
name: com.ipanet.am.replica.delay.between.retries)"
        }
      }
    }
  }

```



```

},
"amconfig.header.sdktimetoliveconfig" : {
  "title" : "Time To Live Configuration",
  "type" : "object",
  "propertyOrder" : 4,
  "properties" : {
    "com.iplanet.am.sdk.cache.entry.expire.enabled" : {
      "type" : "boolean",
      "title" : "Cache Entry Expiration Enabled",
      "propertyOrder" : 0,
      "required" : true,
      "description" : "If this property is set, the cache entries will expire
based on the time specified in User Entry Expiration Time property. (property name:
com.iplanet.am.sdk.cache.entry.expire.enabled)"
    },
    "com.iplanet.am.sdk.cache.entry.user.expire.time" : {
      "type" : "integer",
      "title" : "User Entry Expiration Time",
      "propertyOrder" : 1,
      "required" : true,
      "description" : "This property specifies time in minutes for which the user entries remain
valid in cache after their last modification. After this specified period of time elapses (after the
last modification/read from the directory), the data for the entry that is cached will expire. At
that instant new requests for data for these user entries will result in reading from the Directory.
(property name: com.iplanet.am.sdk.cache.entry.user.expire.time)"
    },
    "com.iplanet.am.sdk.cache.entry.default.expire.time" : {
      "type" : "integer",
      "title" : "Default Entry Expiration Time",
      "propertyOrder" : 2,
      "required" : true,
      "description" : "This property specifies time in minutes for which the non-user entries
remain valid in cache after their last modification. After this specified period of time elapses
(after the last modification/read from the directory), the data for the entry that is cached will
expire. At that instant new requests for data for these non-user entries will result in reading from
the Directory. (property name: com.iplanet.am.sdk.cache.entry.default.expire.time)"
    }
  }
}
}
}
}

```

## 1.42. DefaultSecurityProperties

### 1.42.1. Global Operations

An object of property key-value pairs

Resource path: </global-config/servers/server-default/properties/security>

Resource version: 1.0

### 1.42.1.1. read

Usage:

```
am> read DefaultSecurityProperties --global
```

### 1.42.1.2. update

Usage:

```
am> update DefaultSecurityProperties --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.encryption" : {
      "title" : "Encryption",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "am.encryption.pwd" : {
          "type" : "string",
          "title" : "Password Encryption Key",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "The encryption key value for decrypting passwords stored in the Service Management System configuration. (property name: am.encryption.pwd)"
        },
        "com.ipianet.security.encryptor" : {
          "type" : "string",
          "title" : "Encryption class",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "The default encryption class. (property name: com.ipianet.security.encryptor)"
        },
        "com.ipianet.security.SecureRandomFactoryImpl" : {
          "type" : "string",
          "title" : "Secure Random Factory Class",
          "propertyOrder" : 3,
          "required" : true,
          "description" : "This property is used for specifying SecureRandomFactory class. Available values for this property are com.ipianet.am.util.JSSSecureRandomFactoryImpl that is using JSS and com.ipianet.am.util.SecureRandomFactoryImpl that is using pure Java only. (property name: com.ipianet.security.SecureRandomFactoryImpl)"
        }
      }
    },
    "amconfig.header.validation" : {
      "title" : "Validation",
```

```

    "type" : "object",
    "propertyOrder" : 1,
    "properties" : {
      "com.ipplanet.services.comm.server.pllrequest.maxContentLength" : {
        "type" : "integer",
        "title" : "Platform Low Level Comm. Max. Content Length",
        "propertyOrder" : 0,
        "required" : true,
        "description" : "Maximum content-length for an HttpRequest. (property name:
com.ipplanet.services.comm.server.pllrequest.maxContentLength)"
      },
      "com.ipplanet.am.clientIPCheckEnabled" : {
        "type" : "boolean",
        "title" : "Client IP Address Check",
        "propertyOrder" : 1,
        "required" : true,
        "description" : "Specifies whether or not the IP address of the client is checked in all
single sign on token creations or validations. (property name: com.ipplanet.am.clientIPCheckEnabled)"
      }
    },
    "amconfig.header.cookie" : {
      "title" : "Cookie",
      "type" : "object",
      "propertyOrder" : 2,
      "properties" : {
        "com.ipplanet.am.cookie.name" : {
          "type" : "string",
          "title" : "Cookie Name",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "The cookie name used by Authentication Service to set the valid
session handler ID. This name is used to retrieve the valid session information. (property name:
com.ipplanet.am.cookie.name)"
        },
        "com.ipplanet.am.cookie.secure" : {
          "type" : "boolean",
          "title" : "Secure Cookie",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies whether to set cookie in a secure mode in which the browser
will only return the cookie when a secure protocol such as HTTP(s) is used. (property name:
com.ipplanet.am.cookie.secure)"
        },
        "com.ipplanet.am.cookie.encode" : {
          "type" : "boolean",
          "title" : "Encode Cookie Value",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "Specifies whether to URL encode the cookie value. (property name:
com.ipplanet.am.cookie.encode)"
        }
      }
    },
    "amconfig.header.securitykey" : {
      "title" : "Key Store",
      "type" : "object",
      "propertyOrder" : 3,
      "properties" : {

```

```

    "com.sun.identity.saml.xmlsig.keystore" : {
      "type" : "string",
      "title" : "Keystore File",
      "propertyOrder" : 0,
      "required" : true,
      "description" : "Specifies the location of the keystore file. (property name:
com.sun.identity.saml.xmlsig.keystore)"
    },
    "com.sun.identity.saml.xmlsig.storetype" : {
      "type" : "string",
      "title" : "Keystore Type",
      "propertyOrder" : 1,
      "required" : true,
      "description" : "Specifies the keystore type. (property name:
com.sun.identity.saml.xmlsig.storetype)"
    },
    "com.sun.identity.saml.xmlsig.storepass" : {
      "type" : "string",
      "title" : "Keystore Password File",
      "propertyOrder" : 2,
      "required" : true,
      "description" : "Specifies the location of the file that contains the password used to
access the keystore file. (property name: com.sun.identity.saml.xmlsig.storepass)"
    },
    "com.sun.identity.saml.xmlsig.keypass" : {
      "type" : "string",
      "title" : "Private Key Password File",
      "propertyOrder" : 3,
      "required" : true,
      "description" : "Specifies the location of the file that contains the
password used to protect the private key of a generated key pair. (property name:
com.sun.identity.saml.xmlsig.keypass)"
    },
    "com.sun.identity.saml.xmlsig.certalias" : {
      "type" : "string",
      "title" : "Certificate Alias",
      "propertyOrder" : 4,
      "required" : true,
      "description" : "(property name: com.sun.identity.saml.xmlsig.certalias)"
    }
  }
},
"amconfig.header.crlcache" : {
  "title" : "Certificate Revocation List Caching",
  "type" : "object",
  "propertyOrder" : 4,
  "properties" : {
    "com.sun.identity.crl.cache.directory.host" : {
      "type" : "string",
      "title" : "LDAP server host name",
      "propertyOrder" : 0,
      "required" : true,
      "description" : ""
    },
    "com.sun.identity.crl.cache.directory.port" : {
      "type" : "integer",
      "title" : "LDAP server port number",
      "propertyOrder" : 1,
      "required" : true,

```

```

        "description" : ""
    },
    "com.sun.identity.crl.cache.directory.ssl" : {
        "type" : "boolean",
        "title" : "SSL/TLS Enabled",
        "propertyOrder" : 2,
        "required" : true,
        "description" : ""
    },
    "com.sun.identity.crl.cache.directory.user" : {
        "type" : "string",
        "title" : "LDAP server bind user name",
        "propertyOrder" : 3,
        "required" : true,
        "description" : ""
    },
    "com.sun.identity.crl.cache.directory.password" : {
        "type" : "string",
        "title" : "LDAP server bind password",
        "propertyOrder" : 4,
        "required" : true,
        "description" : "",
        "format" : "password"
    },
    "com.sun.identity.crl.cache.directory.searchlocs" : {
        "type" : "string",
        "title" : "LDAP search base DN",
        "propertyOrder" : 5,
        "required" : true,
        "description" : ""
    },
    "com.sun.identity.crl.cache.directory.searchattr" : {
        "type" : "string",
        "title" : "Search Attributes",
        "propertyOrder" : 6,
        "required" : true,
        "description" : "Any DN component of issuer's subjectDN can be used to retrieve CRL from
local LDAP server. It is single value string, like, \"cn\". All Root CA need to use the same search
attribute."
    }
},
    "amconfig.header.ocsp.check" : {
        "title" : "Online Certificate Status Protocol Check",
        "type" : "object",
        "propertyOrder" : 5,
        "properties" : {
            "com.sun.identity.authentication.ocspCheck" : {
                "type" : "boolean",
                "title" : "Check Enabled",
                "propertyOrder" : 0,
                "required" : true,
                "description" : ""
            },
            "com.sun.identity.authentication.ocsp.responder.url" : {
                "type" : "string",
                "title" : "Responder URL",
                "propertyOrder" : 1,
                "required" : true,

```

```

        "description" : ""
    },
    "com.sun.identity.authentication.ocsp.responder.nickname" : {
        "type" : "string",
        "title" : "Certificate Nickname",
        "propertyOrder" : 2,
        "required" : true,
        "description" : ""
    }
},
"amconfig.header.deserialisationwhitelist" : {
    "title" : "Object Deserialisation Class Whitelist",
    "type" : "object",
    "propertyOrder" : 6,
    "properties" : {
        "openam.deserialisation.classes.whitelist" : {
            "type" : "string",
            "title" : "Whitelist",
            "propertyOrder" : 0,
            "required" : true,
            "description" : "The list of classes that are considered valid when OpenAM performs
Object deserialisation operations. The defaults should work for most installations. (property name:
openam.deserialisation.classes.whitelist)"
        }
    }
}
}
}
}

```

## 1.43. DefaultSessionProperties

### 1.43.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/session`

Resource version: `1.0`

#### 1.43.1.1. read

Usage:

```
am> read DefaultSessionProperties --global
```

#### 1.43.1.2. update

Usage:

```
am> update DefaultSessionProperties --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.sessionthresholds" : {
      "title" : "Session Limits",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "org.forgerock.openam.session.service.access.persistence.caching.maxsize" : {
          "type" : "integer",
          "title" : "Maximum Session Cache Size",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "The maximum number of sessions to cache in the per-server internal session
cache. (property name: org.forgerock.openam.session.service.access.persistence.caching.maxsize)"
        },
        "com.iplanet.am.session.invalidsessionmaxtime" : {
          "type" : "integer",
          "title" : "Invalidate Session Max Time",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Duration in minutes after which the invalid session will be removed
from the session table if it is created and the user does not login. This value should always
be greater than the timeout value in the Authentication module properties file. (property name:
com.iplanet.am.session.invalidsessionmaxtime)"
        }
      }
    },
    "amconfig.header.sessionlogging" : {
      "title" : "Statistics",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "com.iplanet.am.stats.interval" : {
          "type" : "integer",
          "title" : "Logging Interval (in seconds)",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Number of seconds to elapse between statistics logging. The interval
should be at least 5 seconds to avoid CPU saturation. An interval value less than 5 seconds will be
interpreted as 5 seconds. (property name: com.iplanet.am.stats.interval)"
        },
        "com.iplanet.services.stats.state" : {
          "enum" : [ "off", "file", "console" ],
          "options" : {
            "enum_titles" : [ "Off", "File", "Console" ]
          },
          "type" : "string",
          "title" : "State",
          "propertyOrder" : 1,
          "required" : true,

```

```

        "description" : "Statistics state 'file' will write to a file under the specified directory,
and 'console' will write into webserver log files. (property name: com.ipanet.services.stats.state)"
    },
    "com.ipanet.services.stats.directory" : {
        "type" : "string",
        "title" : "Directory",
        "propertyOrder" : 2,
        "required" : true,
        "description" : "Directory where the statistic files will be created. Use forward slashes
\"/\" to separate directories, not backslash \"\\\\\". Spaces in the file name are allowed for Windows.
(property name: com.ipanet.services.stats.directory)"
    },
    "com.sun.am.session.enableHostLookUp" : {
        "type" : "boolean",
        "title" : "Enable Host Lookup",
        "propertyOrder" : 3,
        "required" : true,
        "description" : "Enables or disables host lookup during session logging. (property name:
com.sun.am.session.enableHostLookUp)"
    }
},
"amconfig.header.sessionnotification" : {
    "title" : "Notification",
    "type" : "object",
    "propertyOrder" : 2,
    "properties" : {
        "com.ipanet.am.notification.threadpool.size" : {
            "type" : "integer",
            "title" : "Notification Pool Size",
            "propertyOrder" : 0,
            "required" : true,
            "description" : "Specifies the size of the notification thread pool (total number of
threads). (property name: com.ipanet.am.notification.threadpool.size)"
        },
        "com.ipanet.am.notification.threadpool.threshold" : {
            "type" : "integer",
            "title" : "Notification Thread Pool Threshold",
            "propertyOrder" : 1,
            "required" : true,
            "description" : "Specifies the maximum task queue length for serving notification threads.
(property name: com.ipanet.am.notification.threadpool.threshold)"
        }
    }
},
"amconfig.header.sessionvalidation" : {
    "title" : "Validation",
    "type" : "object",
    "propertyOrder" : 3,
    "properties" : {
        "com.sun.am.session.caseInsensitiveDN" : {
            "type" : "boolean",
            "title" : "Case Insensitive client DN comparison",
            "propertyOrder" : 0,
            "required" : true,
            "description" : "Specifies if client distinguished name comparison is case insensitive/
sensitive. (property name: com.sun.am.session.caseInsensitiveDN)"
        }
    }
}

```



```
}  
}  
}
```

## 1.44. DefaultUmaDataStoreProperties

### 1.44.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/uma`

Resource version: `1.0`

#### 1.44.1.1. read

Usage:

```
am> read DefaultUmaDataStoreProperties --global
```

#### 1.44.1.2. update

Usage:

```
am> update DefaultUmaDataStoreProperties --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "type" : "object",  
  "properties" : {  
    "amconfig.org.forgerock.services.resourcesets.store.common.section" : {  
      "title" : "Resource Sets Store",  
      "type" : "object",  
      "propertyOrder" : 0,  
      "properties" : {  
        "org.forgerock.services.resourcesets.store.location" : {  
          "enum" : [ "default", "external" ],  
          "options" : {  
            "enum_titles" : [ "Default Token Store", "External Token Store" ]  
          },  
          "type" : "string",  
          "title" : "Store Mode",  
          "propertyOrder" : 0,  
          "required" : true,  
          "description" : ""  
        }  
      }  
    }  
  }  
}
```

```

    },
    "org.forgerock.services.resourcesets.store.root.suffix" : {
      "type" : "string",
      "title" : "Root Suffix",
      "propertyOrder" : 1,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.resourcesets.store.max.connections" : {
      "type" : "string",
      "title" : "Max Connections",
      "propertyOrder" : 2,
      "required" : true,
      "description" : ""
    }
  }
},
"amconfig.org.forgerock.services.resourcesets.store.external.section" : {
  "title" : "External Resource Sets Store Configuration",
  "type" : "object",
  "propertyOrder" : 1,
  "properties" : {
    "org.forgerock.services.resourcesets.store.ssl.enabled" : {
      "type" : "boolean",
      "title" : "SSL/TLS Enabled",
      "propertyOrder" : 0,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.resourcesets.store.directory.name" : {
      "type" : "string",
      "title" : "Connection String(s)",
      "propertyOrder" : 1,
      "required" : true,
      "description" : "An ordered list of connection strings for LDAP directories. Each connection
string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
IDs are optional parameters that will prioritize that connection to use from the specified nodes.
Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
    },
    "org.forgerock.services.resourcesets.store.loginid" : {
      "type" : "string",
      "title" : "Login Id",
      "propertyOrder" : 2,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.resourcesets.store.password" : {
      "type" : "string",
      "title" : "Password",
      "propertyOrder" : 3,
      "required" : true,
      "description" : "",
      "format" : "password"
    },
    "org.forgerock.services.resourcesets.store.heartbeat" : {
      "type" : "integer",
      "title" : "Heartbeat",
      "propertyOrder" : 4,

```

```

        "required" : true,
        "description" : ""
    }
}
},
"amconfig.org.forgerock.services.umaaudit.store.common.section" : {
    "title" : "UMA Audit Store",
    "type" : "object",
    "propertyOrder" : 2,
    "properties" : {
        "org.forgerock.services.umaaudit.store.location" : {
            "enum" : [ "default", "external" ],
            "options" : {
                "enum_titles" : [ "Default Token Store", "External Token Store" ]
            },
            "type" : "string",
            "title" : "Store Mode",
            "propertyOrder" : 0,
            "required" : true,
            "description" : ""
        },
        "org.forgerock.services.umaaudit.store.root.suffix" : {
            "type" : "string",
            "title" : "Root Suffix",
            "propertyOrder" : 1,
            "required" : true,
            "description" : ""
        },
        "org.forgerock.services.umaaudit.store.max.connections" : {
            "type" : "string",
            "title" : "Max Connections",
            "propertyOrder" : 2,
            "required" : true,
            "description" : ""
        }
    }
},
"amconfig.org.forgerock.services.umaaudit.store.external.section" : {
    "title" : "External UMA Audit Store Configuration",
    "type" : "object",
    "propertyOrder" : 3,
    "properties" : {
        "org.forgerock.services.umaaudit.store.ssl.enabled" : {
            "type" : "boolean",
            "title" : "SSL/TLS Enabled",
            "propertyOrder" : 0,
            "required" : true,
            "description" : ""
        },
        "org.forgerock.services.umaaudit.store.directory.name" : {
            "type" : "string",
            "title" : "Connection String(s)",
            "propertyOrder" : 1,
            "required" : true,
            "description" : "An ordered list of connection strings for LDAP directories. Each connection
string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
IDs are optional parameters that will prioritize that connection to use from the specified nodes.
Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
        }
    }
}

```

```

    },
    "org.forgerock.services.umaudit.store.loginid" : {
      "type" : "string",
      "title" : "Login Id",
      "propertyOrder" : 2,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.umaudit.store.password" : {
      "type" : "string",
      "title" : "Password",
      "propertyOrder" : 3,
      "required" : true,
      "description" : "",
      "format" : "password"
    },
    "org.forgerock.services.umaudit.store.heartbeat" : {
      "type" : "integer",
      "title" : "Heartbeat",
      "propertyOrder" : 4,
      "required" : true,
      "description" : ""
    }
  }
},
"amconfig.org.forgerock.services.uma.pendingrequests.store.common.section" : {
  "title" : "Pending Requests Store",
  "type" : "object",
  "propertyOrder" : 4,
  "properties" : {
    "org.forgerock.services.uma.pendingrequests.store.location" : {
      "enum" : [ "default", "external" ],
      "options" : {
        "enum_titles" : [ "Default Token Store", "External Token Store" ]
      },
      "type" : "string",
      "title" : "Store Mode",
      "propertyOrder" : 0,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.uma.pendingrequests.store.root.suffix" : {
      "type" : "string",
      "title" : "Root Suffix",
      "propertyOrder" : 1,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.uma.pendingrequests.store.max.connections" : {
      "type" : "string",
      "title" : "Max Connections",
      "propertyOrder" : 2,
      "required" : true,
      "description" : ""
    }
  }
},
"amconfig.org.forgerock.services.uma.pendingrequests.store.external.section" : {
  "title" : "External Pending Requests Store Configuration",

```

```

    "type" : "object",
    "propertyOrder" : 5,
    "properties" : {
      "org.forgerock.services.uma.pendingrequests.store.ssl.enabled" : {
        "type" : "boolean",
        "title" : "SSL/TLS Enabled",
        "propertyOrder" : 0,
        "required" : true,
        "description" : ""
      },
      "org.forgerock.services.uma.pendingrequests.store.directory.name" : {
        "type" : "string",
        "title" : "Connection String(s)",
        "propertyOrder" : 1,
        "required" : true,
        "description" : "An ordered list of connection strings for LDAP directories. Each connection
string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
IDs are optional parameters that will prioritize that connection to use from the specified nodes.
Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
      },
      "org.forgerock.services.uma.pendingrequests.store.loginid" : {
        "type" : "string",
        "title" : "Login Id",
        "propertyOrder" : 2,
        "required" : true,
        "description" : ""
      },
      "org.forgerock.services.uma.pendingrequests.store.password" : {
        "type" : "string",
        "title" : "Password",
        "propertyOrder" : 3,
        "required" : true,
        "description" : "",
        "format" : "password"
      },
      "org.forgerock.services.uma.pendingrequests.store.heartbeat" : {
        "type" : "integer",
        "title" : "Heartbeat",
        "propertyOrder" : 4,
        "required" : true,
        "description" : ""
      }
    }
  },
  "amconfig.org.forgerock.services.uma.labels.store.common.section" : {
    "title" : "UMA Resource Set Labels Store",
    "type" : "object",
    "propertyOrder" : 6,
    "properties" : {
      "org.forgerock.services.uma.labels.store.location" : {
        "enum" : [ "default", "external" ],
        "options" : {
          "enum_titles" : [ "Default Token Store", "External Token Store" ]
        },
        "type" : "string",
        "title" : "Store Mode",
        "propertyOrder" : 0,
        "required" : true,

```

```

    "description" : ""
  },
  "org.forgerock.services.uma.labels.store.root.suffix" : {
    "type" : "string",
    "title" : "Root Suffix",
    "propertyOrder" : 1,
    "required" : true,
    "description" : ""
  },
  "org.forgerock.services.uma.labels.store.max.connections" : {
    "type" : "string",
    "title" : "Max Connections",
    "propertyOrder" : 2,
    "required" : true,
    "description" : ""
  }
}
},
"amconfig.org.forgerock.services.uma.labels.store.external.section" : {
  "title" : "External Resource Set Labels Store Configuration",
  "type" : "object",
  "propertyOrder" : 7,
  "properties" : {
    "org.forgerock.services.uma.labels.store.ssl.enabled" : {
      "type" : "boolean",
      "title" : "SSL/TLS Enabled",
      "propertyOrder" : 0,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.uma.labels.store.directory.name" : {
      "type" : "string",
      "title" : "Connection String(s)",
      "propertyOrder" : 1,
      "required" : true,
      "description" : "An ordered list of connection strings for LDAP directories. Each connection
string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
IDs are optional parameters that will prioritize that connection to use from the specified nodes.
Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
    },
    "org.forgerock.services.uma.labels.store.loginid" : {
      "type" : "string",
      "title" : "Login Id",
      "propertyOrder" : 2,
      "required" : true,
      "description" : ""
    },
    "org.forgerock.services.uma.labels.store.password" : {
      "type" : "string",
      "title" : "Password",
      "propertyOrder" : 3,
      "required" : true,
      "description" : "",
      "format" : "password"
    },
    "org.forgerock.services.uma.labels.store.heartbeat" : {
      "type" : "integer",
      "title" : "Heartbeat",

```

```
        "propertyOrder" : 4,  
        "required" : true,  
        "description" : ""  
      }  
    }  
  }  
}
```

## 1.45. DeviceIdMatchModule

### 1.45.1. Realm Operations

Resource path: `/realm-config/authentication/modules/deviceidmatch`

Resource version: `1.0`

#### 1.45.1.1. create

Usage:

```
am> create DeviceIdMatchModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "type" : "object",  
  "properties" : {  
    "serverScript" : {  
      "title" : "Server-side Script",  
      "description" : "The server-side script to execute.<br><br>This script will be run on  
the server, subsequent to any client script having returned. It can be written in the selected  
language.",  
      "propertyOrder" : 300,  
      "required" : true,  
      "type" : "string",  
      "exampleValue" : ""  
    },  
    "authenticationLevel" : {  
      "title" : "Authentication Level",  
      "description" : "The authentication level associated with the authentication module.<br><br>Each  
authentication module has an authentication level that can be used to indicate the level of security  
associated with the module; 0 is the lowest (and the default).",
```

```

        "propertyOrder" : 400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "clientScript" : {
        "title" : "Client-side Script",
        "description" : "The client-side script.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "clientScriptEnabled" : {
        "title" : "Client-side Script Enabled",
        "description" : "Enable this setting if the client-side script should be executed.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
}
}

```

#### 1.45.1.2. delete

Usage:

```
am> delete DeviceIdMatchModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.45.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIdMatchModule --realm Realm --actionName getAllTypes
```

#### 1.45.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIdMatchModule --realm Realm --actionName getCreatableTypes
```



### 1.45.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIdMatchModule --realm Realm --actionName nextdescendents
```

### 1.45.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query DeviceIdMatchModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.45.1.7. read

Usage:

```
am> read DeviceIdMatchModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.45.1.8. update

Usage:

```
am> update DeviceIdMatchModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverScript" : {
      "title" : "Server-side Script",
      "description" : "The server-side script to execute.<br><br>This script will be run on the server, subsequent to any client script having returned. It can be written in the selected language.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "clientScript" : {
      "title" : "Client-side Script",
      "description" : "The client-side script.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientScriptEnabled" : {
      "title" : "Client-side Script Enabled",
      "description" : "Enable this setting if the client-side script should be executed.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

## 1.45.2. Global Operations

Resource path: `/global-config/authentication/modules/deviceidmatch`

Resource version: `1.0`

### 1.45.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIdMatchModule --global --actionName getAllTypes
```

### 1.45.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIdMatchModule --global --actionName getCreatableTypes
```

### 1.45.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIdMatchModule --global --actionName nextdescendents
```

### 1.45.2.4. read

Usage:

```
am> read DeviceIdMatchModule --global
```

### 1.45.2.5. update

Usage:

```
am> update DeviceIdMatchModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "clientScript" : {
          "title" : "Client-side Script",
          "description" : "The client-side script.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
```

```

    "exampleValue" : ""
  },
  "clientScriptEnabled" : {
    "title" : "Client-side Script Enabled",
    "description" : "Enable this setting if the client-side script should be executed.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "serverScript" : {
    "title" : "Server-side Script",
    "description" : "The server-side script to execute.<br><br>This script will be run on the server, subsequent to any client script having returned. It can be written in the selected language.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with the authentication module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.46. DeviceIdSaveModule

### 1.46.1. Realm Operations

Resource path: `/realm-config/authentication/modules/deviceidsave`

Resource version: `1.0`

#### 1.46.1.1. create

Usage:

```
am> create DeviceIdSaveModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "autoStoreProfiles" : {
      "title" : "Automatically store new profiles",
      "description" : "Select this checkbox to assume user consent to store every new profile<br><br>If this checkbox is selected user won't be prompted for storing new profiles. After successful OTP confirmation profile will be stored automatically.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "maxProfilesAllowed" : {
      "title" : "Maximum stored profile quantity",
      "description" : "No more than specified profiles quantity will be stored in user record",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

### 1.46.1.2. delete

Usage:

```
am> delete DeviceIdSaveModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.46.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIdSaveModule --realm Realm --actionName getAllTypes
```

### 1.46.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIdSaveModule --realm Realm --actionName getCreatableTypes
```

### 1.46.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIdSaveModule --realm Realm --actionName nextdescendents
```

### 1.46.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query DeviceIdSaveModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.46.1.7. read

Usage:

```
am> read DeviceIdSaveModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.46.1.8. update

Usage:

```
am> update DeviceIdSaveModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "autoStoreProfiles" : {
      "title" : "Automatically store new profiles",
      "description" : "Select this checkbox to assume user consent to store every new profile<br><br>If this checkbox is selected user won't be prompted for storing new profiles. After successful OTP confirmation profile will be stored automatically.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "maxProfilesAllowed" : {
      "title" : "Maximum stored profile quantity",
      "description" : "No more than specified profiles quantity will be stored in user record",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

## 1.46.2. Global Operations

Resource path: </global-config/authentication/modules/deviceidsave>

Resource version: 1.0

### 1.46.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIdSaveModule --global --actionName getAllTypes
```

### 1.46.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIdSaveModule --global --actionName getCreatableTypes
```

### 1.46.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIdSaveModule --global --actionName nextdescendents
```

### 1.46.2.4. read

Usage:

```
am> read DeviceIdSaveModule --global
```

### 1.46.2.5. update

Usage:

```
am> update DeviceIdSaveModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "type" : "object",
```



```

"properties" : {
  "defaults" : {
    "properties" : {
      "autoStoreProfiles" : {
        "title" : "Automatically store new profiles",
        "description" : "Select this checkbox to assume user consent to store every new
profile<br><br>If this checkbox is selected user won't be prompted for storing new profiles. After
successful OTP confirmation profile will be stored automatically.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "maxProfilesAllowed" : {
        "title" : "Maximum stored profile quantity",
        "description" : "No more than specified profiles quantity will be stored in user record",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "authenticationLevel" : {
        "title" : "Authentication Level",
        "description" : "The authentication level associated with the authentication
module.<br><br>Each authentication module has an authentication level that can be used to indicate
the level of security associated with the module; 0 is the lowest (and the default).",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      }
    },
    "type" : "object",
    "title" : "Realm Defaults"
  }
}
}

```

## 1.47. DirectoryConfiguration

### 1.47.1. Global Operations

Connection details for directory server(s).

Resource path: `/global-config/servers/{serverName}/properties/directoryConfiguration`

Resource version: `1.0`

#### 1.47.1.1. read

Usage:

```
am> read DirectoryConfiguration --global --serverName serverName
```

Parameters:

**--serverName**

Connection details for directory server(s).

## 1.47.1.2. update

Usage:

```
am> update DirectoryConfiguration --global --serverName serverName --body body
```

Parameters:

**--serverName**

Connection details for directory server(s).

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "directoryConfiguration" : {
      "type" : "object",
      "title" : "Directory Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "minConnectionPool" : {
          "title" : "Minimum Connection Pool",
          "propertyOrder" : 0,
          "type" : "number"
        },
        "maxConnectionPool" : {
          "title" : "Maximum Connection Pool",
          "propertyOrder" : 1,
          "type" : "number"
        },
        "bindDn" : {
          "title" : "Bind DN",
          "propertyOrder" : 2,
          "type" : "string"
        },
        "bindPassword" : {
          "title" : "Bind Password",
          "propertyOrder" : 3,
          "type" : "string",
          "format" : "password"
        }
      }
    },
    "directoryServers" : {
```

```

    "type" : "array",
    "title" : "Server",
    "propertyOrder" : 1,
    "items" : {
      "type" : "object",
      "required" : [ "serverName", "hostName", "portNumber", "connectionType" ],
      "properties" : {
        "serverName" : {
          "title" : "Name",
          "type" : "string",
          "propertyOrder" : 0
        },
        "hostName" : {
          "title" : "Host Name",
          "type" : "string",
          "propertyOrder" : 1
        },
        "portNumber" : {
          "title" : "Port Number",
          "type" : "string",
          "propertyOrder" : 2
        },
        "connectionType" : {
          "type" : "string",
          "enum" : [ "SIMPLE", "SSL" ],
          "options" : {
            "enum_titles" : [ "SIMPLE", "SSL" ]
          },
          "title" : "Connection Type",
          "propertyOrder" : 3
        }
      }
    }
  }
}

```

## 1.48. ElasticSearch

### 1.48.1. Realm Operations

Resource path: `/realm-config/services/audit/Elasticsearch`

Resource version: `1.0`

#### 1.48.1.1. create

Usage:

```
am> create ElasticSearch --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elasticsearchBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 4,
      "properties" : {
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Specifies the number of audit log events to hold in the buffer before
writing them to Elasticsearch.",
          "propertyOrder" : 5800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit logs in the batch queue. Additional audit events
are dropped.",
          "propertyOrder" : 5900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Specifies the interval in milliseconds at which buffered events are written
to Elasticsearch.",
          "propertyOrder" : 6000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "elasticsearchConfig" : {
      "type" : "object",
      "title" : "Elasticsearch Configuration",
      "propertyOrder" : 2,

```

```

"properties" : {
  "port" : {
    "title" : "Server Port",
    "description" : "Specifies the port number used to access Elasticsearch's REST API.",
    "propertyOrder" : 5200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "index" : {
    "title" : "Elasticsearch Index",
    "description" : "Specifies the name of the Elasticsearch index to be used for OpenAM audit
logging.",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sslEnabled" : {
    "title" : "SSL Enabled",
    "description" : "Specifies whether SSL is configured on the Elasticsearch server.<p><p>If
SSL is enabled, be sure to import the CA certificate used to sign Elasticsearch node certificates
into the Java keystore on the host that runs OpenAM before attempting to log audit events to
Elasticsearch.",
    "propertyOrder" : 5300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "host" : {
    "title" : "Server Hostname",
    "description" : "Host name or IP address of the Elasticsearch server.",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
},
"commonHandler" : {
  "type" : "object",
  "title" : "General Handler Configuration",
  "propertyOrder" : 0,
  "properties" : {
    "enabled" : {
      "title" : "Enabled",
      "description" : "Enables or disables an audit event handler.",
      "propertyOrder" : 4900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "topics" : {
      "title" : "Topics",
      "description" : "List of topics handled by an audit event handler.",
      "propertyOrder" : 5000,
      "required" : true,
      "items" : {
        "type" : "string"
      }
    }
  }
}

```

```

    },
    "type" : "array",
    "exampleValue" : ""
  }
},
"elasticsearchAuthentication" : {
  "type" : "object",
  "title" : "Authentication",
  "propertyOrder" : 3,
  "properties" : {
    "password" : {
      "title" : "Password",
      "description" : "Specifies the password to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
      "propertyOrder" : 5600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Username",
      "description" : "Specifies the username to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
      "propertyOrder" : 5500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
},
"commonHandlerPlugin" : {
  "type" : "object",
  "title" : "Audit Event Handler Factory",
  "propertyOrder" : 1,
  "properties" : {
    "handlerFactory" : {
      "title" : "Factory Class Name",
      "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
      "propertyOrder" : 6100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
}
}
}

```

### 1.48.1.2. delete

Usage:

```
am> delete ElasticSearch --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.48.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ElasticSearch --realm Realm --actionName getAllTypes
```

### 1.48.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ElasticSearch --realm Realm --actionName getCreatableTypes
```

### 1.48.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ElasticSearch --realm Realm --actionName nextdescendents
```

### 1.48.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query ElasticSearch --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.48.1.7. read

Usage:

```
am> read ElasticSearch --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.48.1.8. update

Usage:

```
am> update ElasticSearch --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elasticsearchBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 4,
      "properties" : {
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Specifies the number of audit log events to hold in the buffer before
writing them to Elasticsearch.",
          "propertyOrder" : 5800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit logs in the batch queue. Additional audit events
are dropped.",
          "propertyOrder" : 5900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Specifies the interval in milliseconds at which buffered events are written
to Elasticsearch.",
          "propertyOrder" : 6000,
          "required" : true,
          "type" : "integer",

```



```

        "exampleValue" : ""
    },
    "bufferingEnabled" : {
        "title" : "Buffering Enabled",
        "description" : "",
        "propertyOrder" : 5700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
},
"elasticsearchConfig" : {
    "type" : "object",
    "title" : "Elasticsearch Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "port" : {
            "title" : "Server Port",
            "description" : "Specifies the port number used to access Elasticsearch's REST API.",
            "propertyOrder" : 5200,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "index" : {
            "title" : "Elasticsearch Index",
            "description" : "Specifies the name of the Elasticsearch index to be used for OpenAM audit
logging.",
            "propertyOrder" : 5400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "sslEnabled" : {
            "title" : "SSL Enabled",
            "description" : "Specifies whether SSL is configured on the Elasticsearch server.<p><p>If
SSL is enabled, be sure to import the CA certificate used to sign Elasticsearch node certificates
into the Java keystore on the host that runs OpenAM before attempting to log audit events to
Elasticsearch.",
            "propertyOrder" : 5300,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "host" : {
            "title" : "Server Hostname",
            "description" : "Host name or IP address of the Elasticsearch server.",
            "propertyOrder" : 5100,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,

```

```

    "properties" : {
      "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 4900,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "topics" : {
        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 5000,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      }
    }
  },
  "elasticsearchAuthentication" : {
    "type" : "object",
    "title" : "Authentication",
    "propertyOrder" : 3,
    "properties" : {
      "password" : {
        "title" : "Password",
        "description" : "Specifies the password to access the Elasticsearch server.<p><p>Required if  

Elasticsearch Shield authentication is configured.",
        "propertyOrder" : 5600,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
      },
      "username" : {
        "title" : "Username",
        "description" : "Specifies the username to access the Elasticsearch server.<p><p>Required if  

Elasticsearch Shield authentication is configured.",
        "propertyOrder" : 5500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
      "handlerFactory" : {
        "title" : "Factory Class Name",
        "description" : "The fully qualified class name of the factory  

responsible for creating the Audit Event Handler. The class must implement  

<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
        "propertyOrder" : 6100,

```

```
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  }
}
```

## 1.48.2. Global Operations

Resource path: `/global-config/services/audit/Elasticsearch`

Resource version: `1.0`

### 1.48.2.1. create

Usage:

```
am> create ElasticSearch --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elasticsearchAuthentication" : {
      "type" : "object",
      "title" : "Authentication",
      "propertyOrder" : 3,
      "properties" : {
        "username" : {
          "title" : "Username",
          "description" : "Specifies the username to access the Elasticsearch server.<p><p>Required if  
Elasticsearch Shield authentication is configured.",
          "propertyOrder" : 5500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "password" : {
          "title" : "Password",
          "description" : "Specifies the password to access the Elasticsearch server.<p><p>Required if  
Elasticsearch Shield authentication is configured.",
          "propertyOrder" : 5600,
          "required" : true,
```

```

        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    }
},
"elasticsearchBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 4,
    "properties" : {
        "batchSize" : {
            "title" : "Batch Size",
            "description" : "Specifies the number of audit log events to hold in the buffer before
writing them to Elasticsearch.",
            "propertyOrder" : 5800,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "maxEvents" : {
            "title" : "Queue Capacity",
            "description" : "Maximum number of audit logs in the batch queue. Additional audit events
are dropped.",
            "propertyOrder" : 5900,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "bufferingEnabled" : {
            "title" : "Buffering Enabled",
            "description" : "",
            "propertyOrder" : 5700,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "writeInterval" : {
            "title" : "Write interval (in milliseconds)",
            "description" : "Specifies the interval in milliseconds at which buffered events are written
to Elasticsearch.",
            "propertyOrder" : 6000,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        }
    }
},
"elasticsearchConfig" : {
    "type" : "object",
    "title" : "Elasticsearch Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "port" : {
            "title" : "Server Port",
            "description" : "Specifies the port number used to access Elasticsearch's REST API.",
            "propertyOrder" : 5200,
            "required" : true,
            "type" : "integer",

```

```

        "exampleValue" : ""
    },
    "index" : {
        "title" : "Elasticsearch Index",
        "description" : "Specifies the name of the Elasticsearch index to be used for OpenAM audit
logging.",
        "propertyOrder" : 5400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "host" : {
        "title" : "Server Hostname",
        "description" : "Host name or IP address of the Elasticsearch server.",
        "propertyOrder" : 5100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sslEnabled" : {
        "title" : "SSL Enabled",
        "description" : "Specifies whether SSL is configured on the Elasticsearch server.<p><p>If
SSL is enabled, be sure to import the CA certificate used to sign Elasticsearch node certificates
into the Java keystore on the host that runs OpenAM before attempting to log audit events to
Elasticsearch.",
        "propertyOrder" : 5300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 5000,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 4900,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
}
},
"commonHandlerPlugin" : {

```

```
"type" : "object",
"title" : "Audit Event Handler Factory",
"propertyOrder" : 1,
"properties" : {
  "handlerFactory" : {
    "title" : "Factory Class Name",
    "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
    "propertyOrder" : 6100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
```

### 1.48.2.2. delete

Usage:

```
am> delete ElasticSearch --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.48.2.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ElasticSearch --global --actionName getAllTypes
```

### 1.48.2.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ElasticSearch --global --actionName getCreatableTypes
```

### 1.48.2.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ElasticSearch --global --actionName nextdescendents
```

### 1.48.2.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query ElasticSearch --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.48.2.7. read

Usage:

```
am> read ElasticSearch --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.48.2.8. update

Usage:

```
am> update ElasticSearch --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elasticsearchAuthentication" : {
      "type" : "object",
      "title" : "Authentication",
      "propertyOrder" : 3,
      "properties" : {
        "username" : {
```

```

        "title" : "Username",
        "description" : "Specifies the username to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
        "propertyOrder" : 5500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "password" : {
        "title" : "Password",
        "description" : "Specifies the password to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
        "propertyOrder" : 5600,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    }
},
"elasticsearchBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 4,
    "properties" : {
        "batchSize" : {
            "title" : "Batch Size",
            "description" : "Specifies the number of audit log events to hold in the buffer before
writing them to Elasticsearch.",
            "propertyOrder" : 5800,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "maxEvents" : {
            "title" : "Queue Capacity",
            "description" : "Maximum number of audit logs in the batch queue. Additional audit events
are dropped.",
            "propertyOrder" : 5900,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "bufferingEnabled" : {
            "title" : "Buffering Enabled",
            "description" : "",
            "propertyOrder" : 5700,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "writeInterval" : {
            "title" : "Write interval (in milliseconds)",
            "description" : "Specifies the interval in milliseconds at which buffered events are written
to Elasticsearch.",
            "propertyOrder" : 6000,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        }
    }
}

```



```

    }
  },
  "elasticsearchConfig" : {
    "type" : "object",
    "title" : "Elasticsearch Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "port" : {
        "title" : "Server Port",
        "description" : "Specifies the port number used to access Elasticsearch's REST API.",
        "propertyOrder" : 5200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "index" : {
        "title" : "Elasticsearch Index",
        "description" : "Specifies the name of the Elasticsearch index to be used for OpenAM audit logging.",
        "propertyOrder" : 5400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "host" : {
        "title" : "Server Hostname",
        "description" : "Host name or IP address of the Elasticsearch server.",
        "propertyOrder" : 5100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "sslEnabled" : {
        "title" : "SSL Enabled",
        "description" : "Specifies whether SSL is configured on the Elasticsearch server.<p><p>If SSL is enabled, be sure to import the CA certificate used to sign Elasticsearch node certificates into the Java keystore on the host that runs OpenAM before attempting to log audit events to Elasticsearch.",
        "propertyOrder" : 5300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  },
  "commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
      "topics" : {
        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 5000,
        "required" : true,
        "items" : {
          "type" : "string"
        }
      }
    }
  },

```

```

        "type" : "array",
        "exampleValue" : ""
    },
    "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 4900,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 6100,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
}
}
}
}

```

## 1.49. EmailService

### 1.49.1. Realm Operations

Resource path: `/realm-config/services/email`

Resource version: `1.0`

#### 1.49.1.1. create

Usage:

```
am> create EmailService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "message" : {
      "title" : "Email Content",
      "description" : "Specifies content for notification messages. If you do not set this, OpenAM
includes only the confirmation URL in the mail body.",
      "propertyOrder" : 1000,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Mail Server Authentication Username",
      "description" : "Specifies the user name for the SMTP mail server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : "username"
    },
    "subject" : {
      "title" : "Email Subject",
      "description" : "Specifies a subject for notification messages. If you do not set this, OpenAM
does not set the subject for notification messages.",
      "propertyOrder" : 900,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "from" : {
      "title" : "Email From Address",
      "description" : "Specifies the address from which to send email notifications.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : "no-reply@example.com"
    },
    "port" : {
      "title" : "Mail Server Host Port",
      "description" : "Specifies the port number for the SMTP mail server.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "hostname" : {
      "title" : "Mail Server Host Name",
      "description" : "Specifies the fully qualified domain name of the SMTP mail server through which
to send email notifications.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : "smtp.example.com"
    },
    "sslState" : {
```

```

    "title" : "Mail Server Secure Connection",
    "description" : "Specifies whether to connect to the SMTP mail server using SSL.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "emailImplClassName" : {
    "title" : "Email Message Implementation Class",
    "description" : "Specifies the class that sends email notifications, such as those sent for user
registration and forgotten passwords.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "emailAddressAttribute" : {
    "title" : "Email Attribute Name",
    "description" : "Specifies the profile attribute from which to retrieve the end user's email
address.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "password" : {
    "title" : "Mail Server Authentication Password",
    "description" : "Specifies the password for the SMTP user name.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  }
}
}

```

### 1.49.1.2. delete

Usage:

```
am> delete EmailService --realm Realm
```

### 1.49.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action EmailService --realm Realm --actionName getAllTypes
```

#### 1.49.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action EmailService --realm Realm --actionName getCreatableTypes
```

#### 1.49.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action EmailService --realm Realm --actionName nextdescendents
```

#### 1.49.1.6. read

Usage:

```
am> read EmailService --realm Realm
```

#### 1.49.1.7. update

Usage:

```
am> update EmailService --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "message" : {
      "title" : "Email Content",
      "description" : "Specifies content for notification messages. If you do not set this, OpenAM
includes only the confirmation URL in the mail body.",
      "propertyOrder" : 1000,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Mail Server Authentication Username",
      "description" : "Specifies the user name for the SMTP mail server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : "username"
    }
  }
}
```

```

    },
    "subject" : {
      "title" : "Email Subject",
      "description" : "Specifies a subject for notification messages. If you do not set this, OpenAM
does not set the subject for notification messages.",
      "propertyOrder" : 900,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "from" : {
      "title" : "Email From Address",
      "description" : "Specifies the address from which to send email notifications.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : "no-reply@example.com"
    },
    "port" : {
      "title" : "Mail Server Host Port",
      "description" : "Specifies the port number for the SMTP mail server.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "hostname" : {
      "title" : "Mail Server Host Name",
      "description" : "Specifies the fully qualified domain name of the SMTP mail server through which
to send email notifications.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : "smtp.example.com"
    },
    "sslState" : {
      "title" : "Mail Server Secure Connection",
      "description" : "Specifies whether to connect to the SMTP mail server using SSL.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "emailImplClassName" : {
      "title" : "Email Message Implementation Class",
      "description" : "Specifies the class that sends email notifications, such as those sent for user
registration and forgotten passwords.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "emailAddressAttribute" : {
      "title" : "Email Attribute Name",
      "description" : "Specifies the profile attribute from which to retrieve the end user's email
address.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",

```

```
    "exampleValue" : ""
  },
  "password" : {
    "title" : "Mail Server Authentication Password",
    "description" : "Specifies the password for the SMTP user name.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  }
}
```

## 1.49.2. Global Operations

Resource path: `/global-config/services/email`

Resource version: `1.0`

### 1.49.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action EmailService --global --actionName getAllTypes
```

### 1.49.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action EmailService --global --actionName getCreatableTypes
```

### 1.49.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action EmailService --global --actionName nextdescendents
```

### 1.49.2.4. read

Usage:

```
am> read EmailService --global
```

## 1.49.2.5. update

Usage:

```
am> update EmailService --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "emailImplClassName" : {
          "title" : "Email Message Implementation Class",
          "description" : "Specifies the class that sends email notifications, such as those sent for
user registration and forgotten passwords.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "password" : {
          "title" : "Mail Server Authentication Password",
          "description" : "Specifies the password for the SMTP user name.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "username" : {
          "title" : "Mail Server Authentication Username",
          "description" : "Specifies the user name for the SMTP mail server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : "username"
        },
        "subject" : {
          "title" : "Email Subject",
          "description" : "Specifies a subject for notification messages. If you do not set this,
OpenAM does not set the subject for notification messages.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sslState" : {
          "title" : "Mail Server Secure Connection",
          "description" : "Specifies whether to connect to the SMTP mail server using SSL.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",

```



```

        "exampleValue" : ""
    },
    "message" : {
        "title" : "Email Content",
        "description" : "Specifies content for notification messages. If you do not set this, OpenAM
includes only the confirmation URL in the mail body.",
        "propertyOrder" : 1000,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "emailAddressAttribute" : {
        "title" : "Email Attribute Name",
        "description" : "Specifies the profile attribute from which to retrieve the end user's email
address.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "hostname" : {
        "title" : "Mail Server Host Name",
        "description" : "Specifies the fully qualified domain name of the SMTP mail server through
which to send email notifications.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : "smtp.example.com"
    },
    "from" : {
        "title" : "Email From Address",
        "description" : "Specifies the address from which to send email notifications.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : "no-reply@example.com"
    },
    "port" : {
        "title" : "Mail Server Host Port",
        "description" : "Specifies the port number for the SMTP mail server.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.50. FederationModule

### 1.50.1. Realm Operations

Resource path: `/realm-config/authentication/modules/federation`

Resource version: `1.0`

#### 1.50.1.1. create

Usage:

```
am> create FederationModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

#### 1.50.1.2. delete

Usage:

```
am> delete FederationModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.50.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action FederationModule --realm Realm --actionName getAllTypes
```

### 1.50.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action FederationModule --realm Realm --actionName getCreatableTypes
```

### 1.50.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action FederationModule --realm Realm --actionName nextdescendents
```

### 1.50.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query FederationModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.50.1.7. read

Usage:

```
am> read FederationModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.50.1.8. update

Usage:

```
am> update FederationModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

## 1.50.2. Global Operations

Resource path: </global-config/authentication/modules/federation>

Resource version: [1.0](#)

### 1.50.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action FederationModule --global --actionName getAllTypes
```

### 1.50.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action FederationModule --global --actionName getCreatableTypes
```

### 1.50.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action FederationModule --global --actionName nextdescendents
```

### 1.50.2.4. read

Usage:

```
am> read FederationModule --global
```

### 1.50.2.5. update

Usage:

```
am> update FederationModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

## 1.51. Files

### 1.51.1. Realm Operations

Resource path: `/realm-config/services/id-repositories/files`

Resource version: `1.0`

#### 1.51.1.1. create

Usage:

```
am> create Files --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunFilesMonitorForChanges" : {
      "title" : "Caching",
      "description" : "",
      "propertyOrder" : 6300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "sunFilesMonitoringTime" : {
      "title" : "Cache Update Interval",
      "description" : "In minutes.",
      "propertyOrder" : 6400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sunFilesHashAttrs" : {
      "title" : "Hashed Attributes",
      "description" : "",
      "propertyOrder" : 6800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
}
```

```

"sunFilesPasswordAttr" : {
  "title" : "Password Attribute",
  "description" : "",
  "propertyOrder" : 6600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sunFilesObjectClasses" : {
  "title" : "User Object Classes",
  "description" : "",
  "propertyOrder" : 6500,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sunIdRepoClass" : {
  "title" : "Files Repository Plugin Class Name",
  "description" : "",
  "propertyOrder" : 6100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sunFilesEncryptAttrs" : {
  "title" : "Encrypted Attributes",
  "description" : "",
  "propertyOrder" : 6900,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sunFilesIdRepoDirectory" : {
  "title" : "Files Repository Directory",
  "description" : "",
  "propertyOrder" : 6200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sunFilesStatusAttr" : {
  "title" : "Status Attribute",
  "description" : "",
  "propertyOrder" : 6700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
}

```

### 1.51.1.2. delete

Usage:

```
am> delete Files --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.51.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Files --realm Realm --actionName getAllTypes
```

### 1.51.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Files --realm Realm --actionName getCreatableTypes
```

### 1.51.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Files --realm Realm --actionName nextdescendents
```

### 1.51.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Files --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.



### 1.51.1.7. read

Usage:

```
am> read Files --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.51.1.8. update

Usage:

```
am> update Files --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunFilesMonitorForChanges" : {
      "title" : "Caching",
      "description" : "",
      "propertyOrder" : 6300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "sunFilesMonitoringTime" : {
      "title" : "Cache Update Interval",
      "description" : "In minutes.",
      "propertyOrder" : 6400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sunFilesHashAttrs" : {
      "title" : "Hashed Attributes",
      "description" : "",
      "propertyOrder" : 6800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
    }
  }
}
```

```

    "exampleValue" : ""
  },
  "sunFilesPasswordAttr" : {
    "title" : "Password Attribute",
    "description" : "",
    "propertyOrder" : 6600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunFilesObjectClasses" : {
    "title" : "User Object Classes",
    "description" : "",
    "propertyOrder" : 6500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "Files Repository Plugin Class Name",
    "description" : "",
    "propertyOrder" : 6100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunFilesEncryptAttrs" : {
    "title" : "Encrypted Attributes",
    "description" : "",
    "propertyOrder" : 6900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sunFilesIdRepoDirectory" : {
    "title" : "Files Repository Directory",
    "description" : "",
    "propertyOrder" : 6200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunFilesStatusAttr" : {
    "title" : "Status Attribute",
    "description" : "",
    "propertyOrder" : 6700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
}

```

## 1.52. ForgottenPassword

### 1.52.1. Realm Operations

Self Service endpoint for retrieving a forgotten password

Resource path: `/selfservice/forgottenPassword`

Resource version: `1.0`

#### 1.52.1.1. read

Initialise the forgotten password reclamation process. A set of requirements will be returned that will need to be fulfilled and sent to the submitRequirements action.

Usage:

```
am> read ForgottenPassword --realm Realm
```

#### 1.52.1.2. submitRequirements

Submit some fulfilled requirements. Returns either a completion status, or a token along with some more requirements. If requirements are returned, they should be submitted with the token as a fresh request to this action.

Usage:

```
am> action ForgottenPassword --realm Realm --body body --actionName submitRequirements
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The structure of a request to the submitRequirements action.",
  "type" : "object",
  "title" : "Submit requirements structure",
  "properties" : {
    "token" : {
      "type" : "string",
      "title" : "Token",
      "description" : "The token returned from the previous submitRequirements request."
    },
    "input" : {
      "type" : "object",
      "title" : "Input",
      "description" : "The input as collected from the user that has forgotten their password. This object must conform to the JSON Schema of the requirements property from the last response.",
      "patternProperties" : {
        ".*" : {
          "type" : "any",
          "title" : "Input Property",
          "description" : "Valid content according to the received JSON Schema."
        }
      }
    }
  },
  "required" : [ "input" ]
}
```

## 1.53. ForgottenUsername

### 1.53.1. Realm Operations

Self Service endpoint for retrieving a forgotten username

Resource path: `/selfservice/forgottenUsername`

Resource version: `1.0`

#### 1.53.1.1. read

Initialise the forgotten username reclamation process. A set of requirements will be returned that will need to be fulfilled and sent to the submitRequirements action.

Usage:

```
am> read ForgottenUsername --realm Realm
```

### 1.53.1.2. submitRequirements

Submit some fulfilled requirements. Returns either a completion status, or a token along with some more requirements. If requirements are returned, they should be submitted with the token as a fresh request to this action.

Usage:

```
am> action ForgottenUsername --realm Realm --body body --actionName submitRequirements
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The structure of a request to the submitRequirements action.",
  "type" : "object",
  "title" : "Submit requirements structure",
  "properties" : {
    "token" : {
      "type" : "string",
      "title" : "Token",
      "description" : "The token returned from the previous submitRequirements request."
    },
    "input" : {
      "type" : "object",
      "title" : "Input",
      "description" : "The input as collected from the user that has forgotten their username. This object must conform to the JSON Schema of the requirements property from the last response.",
      "patternProperties" : {
        ".*" : {
          "type" : "any",
          "title" : "Input Property",
          "description" : "Valid content according to the received JSON Schema."
        }
      }
    }
  },
  "required" : [ "input" ]
}
```

## 1.54. GeneralProperties

### 1.54.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/general`

Resource version: `1.0`

### 1.54.1.1. read

Usage:

```
am> read GeneralProperties --global --serverName serverName
```

Parameters:

**--serverName**

An object of property key-value pairs

### 1.54.1.2. update

Usage:

```
am> update GeneralProperties --global --serverName serverName --body body
```

Parameters:

**--serverName**

An object of property key-value pairs

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.site" : {
      "title" : "Site",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "singleChoiceSite" : {
          "enum" : null,
          "options" : {
            "enum_titles" : null
          },
          "type" : "string",
          "title" : "Parent Site",
          "propertyOrder" : 0,
          "required" : false,
          "description" : "Parent Site"
        }
      }
    },
    "amconfig.header.installdir" : {
      "title" : "System",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "com.ipplanet.services.configpath" : {
          "title" : "Base installation directory",
```

```

        "type" : "object",
        "propertyOrder" : 0,
        "description" : "Base directory where product's data resides. (property name:
com.iplanet.services.configpath)",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.iplanet.am.locale" : {
        "title" : "Default Locale",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "Default locale for the product. (property name: com.iplanet.am.locale)",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.sun.identity.client.notification.url" : {
        "title" : "Notification URL",
        "type" : "object",
        "propertyOrder" : 2,
        "description" : "The location of notification service end point. It is usually the product's
deployment URI/notificationservice. (property name: com.sun.identity.client.notification.url)",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.iplanet.am.util.xml.validating" : {
        "title" : "XML Validation",
        "type" : "object",
        "propertyOrder" : 3,
        "description" : "Specifies if validation is required when parsing XML documents. (property
name: com.iplanet.am.util.xml.validating)",
        "properties" : {
            "value" : {
                "enum" : [ "on", "off" ],
                "options" : {
                    "enum_titles" : [ "On", "Off" ]
                }
            }
        }
    }
}

```

```

        },
        "type" : "string",
        "required" : false
    },
    "inherited" : {
        "type" : "boolean",
        "required" : true
    }
}
}
},
"amconfig.header.debug" : {
    "title" : "Debugging",
    "type" : "object",
    "propertyOrder" : 2,
    "properties" : {
        "com.iplanet.services.debug.level" : {
            "title" : "Debug Level",
            "type" : "object",
            "propertyOrder" : 0,
            "description" : "Debug level for all components in the product. (property name:
com.iplanet.services.debug.level)",
            "properties" : {
                "value" : {
                    "enum" : [ "off", "error", "warning", "message" ],
                    "options" : {
                        "enum_titles" : [ "Off", "Error", "Warning", "Message" ]
                    },
                    "type" : "string",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        },
        "com.sun.services.debug.mergeall" : {
            "title" : "Merge Debug Files",
            "type" : "object",
            "propertyOrder" : 1,
            "description" : "On : Directs all debug data to a single file (debug.out); Off : creates
separate per-component debug files (property name : com.sun.services.debug.mergeall)",
            "properties" : {
                "value" : {
                    "enum" : [ "on", "off" ],
                    "options" : {
                        "enum_titles" : [ "On", "Off" ]
                    },
                    "type" : "string",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        }
    }
},
}

```



```

    "com.ipplanet.services.debug.directory" : {
      "title" : "Debug Directory",
      "type" : "object",
      "propertyOrder" : 2,
      "description" : "Directory where debug files reside. (property name:
com.ipplanet.services.debug.directory)",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  },
  "amconfig.header.mailserver" : {
    "title" : "Mail Server",
    "type" : "object",
    "propertyOrder" : 3,
    "properties" : {
      "com.ipplanet.am.smtphost" : {
        "title" : "Mail Server Host Name",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "(property name: com.ipplanet.am.smtphost)",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    },
    "com.ipplanet.am.smtpport" : {
      "title" : "Mail Server Port Number",
      "type" : "object",
      "propertyOrder" : 1,
      "description" : "(property name: com.ipplanet.am.smtpport)",
      "properties" : {
        "value" : {
          "type" : "integer",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  }
}

```

```
}
```

## 1.55. GenericLDAPv3

### 1.55.1. Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3`

Resource version: `1.0`

#### 1.55.1.1. create

Usage:

```
am> create GenericLDAPv3 --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-idrepo-ldapv3-config-users-search-filter" : {
      "title" : "LDAP Users Search Filter",
      "description" : "",
      "propertyOrder" : 2200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "openam-idrepo-ldapv3-heartbeat-interval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then it may take up to the interval period before the problem is detected. Use along with the Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in disabling heartbeat requests.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-auth-naming-attr" : {
      "title" : "Authentication Naming Attribute",
```

```

    "description" : "",
    "propertyOrder" : 5200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-filter" : {
    "title" : "Persistent Search Filter",
    "description" : "",
    "propertyOrder" : 5600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-isactive" : {
    "title" : "Attribute Name of User Status",
    "description" : "",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",

```

```

    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-dftgroupmember" : {
    "title" : "Default Group Member's User DN",
    "description" : "User automatically added when group is created.",
    "propertyOrder" : 3800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-timeunit" : {
    "title" : "LDAP Connection Heartbeat Time Unit",
    "description" : "Defines the time unit corresponding to the Heartbeat Interval  

    setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request  

    to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then  

    it may take up to the interval period before the problem is detected. Use along with the Heartbeat  

    Interval parameter to define the exact interval.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "com.ipplanet.am.ldap.connection.delay.between.retries" : {
    "title" : "The Delay Time Between Retries",
    "description" : "In milliseconds.",
    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }

```

```

},
"sun-idrepo-ldapv3-dncache-enabled" : {
  "title" : "DN Cache",
  "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
  "propertyOrder" : 5900,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-authid" : {
  "title" : "LDAP Bind DN",
  "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-memberurl" : {
  "title" : "Attribute Name of Group Member URL",
  "description" : "",
  "propertyOrder" : 3700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-user-objectclass" : {
  "title" : "LDAP User Object Class",
  "description" : "",
  "propertyOrder" : 2300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-name" : {
  "title" : "LDAP Groups Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 3100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-value" : {
  "title" : "LDAP Groups Container Value",
  "description" : "",
  "propertyOrder" : 3200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-dncache-size" : {
  "title" : "DN Cache Size",

```

```

    "description" : "In DN items, only used when DN Cache is enabled.",
    "propertyOrder" : 6000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-value" : {
    "title" : "LDAP People Container Value",
    "description" : "",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-time-limit" : {
    "title" : "Search Timeout",
    "description" : "In seconds.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "LDAPv3 Repository Plug-in Class Name",
    "description" : "",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",

```

```

    "description" : "",
    "propertyOrder" : 3400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-max-result" : {
    "title" : "Maximum Results Returned from Search",
    "description" : "",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-filter" : {
    "title" : "LDAP Groups Search Filter",
    "description" : "",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-attributes" : {
    "title" : "LDAP User Attributes",
    "description" : "",
    "propertyOrder" : 2400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }

```

```

    },
    "sun-idrepo-ldapv3-config-groups-search-attribute" : {
      "title" : "LDAP Groups Search Attribute",
      "description" : "",
      "propertyOrder" : 2900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sunIdRepoSupportedOperations" : {
      "title" : "LDAPv3 Plug-in Supported Types and Operations",
      "description" : "",
      "propertyOrder" : 1900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-active" : {
      "title" : "User Status Active Value",
      "description" : "",
      "propertyOrder" : 2700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-people-container-name" : {
      "title" : "LDAP People Container Naming Attribute",
      "description" : "",
      "propertyOrder" : 5000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-search-scope" : {
      "title" : "LDAPv3 Plug-in Search Scope",
      "description" : "",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-authpw" : {
      "title" : "LDAP Bind Password",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}

```



### 1.55.1.2. delete

Usage:

```
am> delete GenericLDAPv3 --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.55.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GenericLDAPv3 --realm Realm --actionName getAllTypes
```

### 1.55.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GenericLDAPv3 --realm Realm --actionName getCreatableTypes
```

### 1.55.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GenericLDAPv3 --realm Realm --actionName nextdescendents
```

### 1.55.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query GenericLDAPv3 --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

## 1.55.1.7. read

Usage:

```
am> read GenericLDAPv3 --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.55.1.8. update

Usage:

```
am> update GenericLDAPv3 --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-idrepo-ldapv3-config-users-search-filter" : {
      "title" : "LDAP Users Search Filter",
      "description" : "",
      "propertyOrder" : 2200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "openam-idrepo-ldapv3-heartbeat-interval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-auth-naming-attr" : {
      "title" : "Authentication Naming Attribute",
      "description" : "",
      "propertyOrder" : 5200,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-filter" : {
    "title" : "Persistent Search Filter",
    "description" : "",
    "propertyOrder" : 5600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-isactive" : {
    "title" : "Attribute Name of User Status",
    "description" : "",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
},

```

```

"sun-idrepo-ldapv3-config-dftgroupmember" : {
  "title" : "Default Group Member's User DN",
  "description" : "User automatically added when group is created.",
  "propertyOrder" : 3800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"openam-idrepo-ldapv3-heartbeat-timeunit" : {
  "title" : "LDAP Connection Heartbeat Time Unit",
  "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
  "propertyOrder" : 1400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"com.iplanet.am.ldap.connection.delay.between.retries" : {
  "title" : "The Delay Time Between Retries",
  "description" : "In milliseconds.",
  "propertyOrder" : 5800,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
  "title" : "Create User Attribute Mapping",
  "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
  "propertyOrder" : 2500,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-objectclass" : {
  "title" : "LDAP Groups Object Class",
  "description" : "",
  "propertyOrder" : 3300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-psearch-scope" : {
  "title" : "Persistent Search Scope",
  "description" : "",
  "propertyOrder" : 5700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-dncache-enabled" : {

```

```

    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-memberurl" : {
    "title" : "Attribute Name of Group Member URL",
    "description" : "",
    "propertyOrder" : 3700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-user-objectclass" : {
    "title" : "LDAP User Object Class",
    "description" : "",
    "propertyOrder" : 2300,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-name" : {
    "title" : "LDAP Groups Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-value" : {
    "title" : "LDAP Groups Container Value",
    "description" : "",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"sun-idrepo-ldapv3-dncache-size" : {
    "title" : "DN Cache Size",
    "description" : "In DN items, only used when DN Cache is enabled.",
    "propertyOrder" : 6000,

```

```

    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-value" : {
    "title" : "LDAP People Container Value",
    "description" : "",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-time-limit" : {
    "title" : "Search Timeout",
    "description" : "In seconds.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "LDAPv3 Repository Plug-in Class Name",
    "description" : "",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",
    "description" : "",
    "propertyOrder" : 3400,

```

```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-max-result" : {
    "title" : "Maximum Results Returned from Search",
    "description" : "",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-filter" : {
    "title" : "LDAP Groups Search Filter",
    "description" : "",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-attributes" : {
    "title" : "LDAP User Attributes",
    "description" : "",
    "propertyOrder" : 2400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-attribute" : {

```

```

    "title" : "LDAP Groups Search Attribute",
    "description" : "",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoSupportedOperations" : {
    "title" : "LDAPv3 Plug-in Supported Types and Operations",
    "description" : "",
    "propertyOrder" : 1900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-active" : {
    "title" : "User Status Active Value",
    "description" : "",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-name" : {
    "title" : "LDAP People Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authpw" : {
    "title" : "LDAP Bind Password",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  }
}
}

```



## 1.56. GlobalScripts

### 1.56.1. Global Operations

Resource path: `/global-config/services/scripting/globalScript`

Resource version: `1.0`

#### 1.56.1.1. create

Usage:

```
am> create GlobalScripts --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
into Base64",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "lastModifiedBy" : {
      "title" : "Last modifier",
      "description" : "A string containing the universal identifier DN of the subject that most
recently updated the script. If the script has not been modified since it was created, this property
will have the same value as createdBy",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

```

"language" : {
  "title" : "Script language",
  "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"name" : {
  "title" : "Script name",
  "description" : "The name provided for the script",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"description" : {
  "title" : "Script description",
  "description" : "An optional text string to help identify the script",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"lastModifiedDate" : {
  "title" : "Last modification date",
  "description" : "A string containing the last modified date and time, in ISO 8601 format. If
the script has not been modified since it was created, this property will have the same value as
creationDate",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"context" : {
  "title" : "Script type",
  "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
AUTHENTICATION_SERVER_SIDE : Server-side Authentication AUTHENTICATION_CLIENT_SIDE : Client-side
Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"createdBy" : {
  "title" : "Created by",
  "description" : "A string containing the universal identifier DN of the subject that created the
script",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
}

```

### 1.56.1.2. delete

Usage:

```
am> delete GlobalScripts --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.56.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GlobalScripts --global --actionName getAllTypes
```

### 1.56.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GlobalScripts --global --actionName getCreatableTypes
```

### 1.56.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GlobalScripts --global --actionName nextdescendents
```

### 1.56.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query GlobalScripts --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

## 1.56.1.7. read

Usage:

```
am> read GlobalScripts --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.56.1.8. update

Usage:

```
am> update GlobalScripts --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
into Base64",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "lastModifiedBy" : {
      "title" : "Last modifier",
      "description" : "A string containing the universal identifier DN of the subject that most
recently updated the script. If the script has not been modified since it was created, this property
will have the same value as createdBy",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",

```

```

    "exampleValue" : ""
  },
  "language" : {
    "title" : "Script language",
    "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "name" : {
    "title" : "Script name",
    "description" : "The name provided for the script",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "description" : {
    "title" : "Script description",
    "description" : "An optional text string to help identify the script",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lastModifiedDate" : {
    "title" : "Last modification date",
    "description" : "A string containing the last modified date and time, in ISO 8601 format. If
the script has not been modified since it was created, this property will have the same value as
creationDate",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "context" : {
    "title" : "Script type",
    "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
AUTHENTICATION_SERVER_SIDE : Server-side Authentication AUTHENTICATION_CLIENT_SIDE : Client-side
Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "createdBy" : {
    "title" : "Created by",
    "description" : "A string containing the universal identifier DN of the subject that created the
script",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

## 1.57. Globalization

### 1.57.1. Realm Operations

Resource path: `/realm-config/services/globalization`

Resource version: `1.0`

#### 1.57.1.1. create

Usage:

```
am> create Globalization --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonNameFormats" : {
      "title" : "Auto Generated Common Name Format",
      "description" : "Use this list to configure how OpenAM formats names shown in the console banner.<br><br>This setting allows the name of the authenticated user shown in the OpenAM console banner to be customised based on the locale of the user.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

#### 1.57.1.2. delete

Usage:

```
am> delete Globalization --realm Realm
```

#### 1.57.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Globalization --realm Realm --actionName getAllTypes
```

#### 1.57.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Globalization --realm Realm --actionName getCreatableTypes
```

#### 1.57.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Globalization --realm Realm --actionName nextdescendents
```

#### 1.57.1.6. read

Usage:

```
am> read Globalization --realm Realm
```

#### 1.57.1.7. update

Usage:

```
am> update Globalization --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonNameFormats" : {
      "title" : "Auto Generated Common Name Format",
      "description" : "Use this list to configure how OpenAM formats names shown in the console banner.<br><br>This setting allows the name of the authenticated user shown in the OpenAM console banner to be customised based on the locale of the user.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.57.2. Global Operations

Resource path: `/global-config/services/globalization`

Resource version: `1.0`

### 1.57.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Globalization --global --actionName getAllTypes
```

### 1.57.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Globalization --global --actionName getCreatableTypes
```

### 1.57.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Globalization --global --actionName nextdescendents
```



## 1.57.2.4. read

Usage:

```
am> read Globalization --global
```

## 1.57.2.5. update

Usage:

```
am> update Globalization --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-identity-glln-settings-charset-alias-mapping" : {
      "title" : "Charset Aliases",
      "description" : "Use this list to map between different character set names used in Java and in
MIME.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "charsetMappings" : {
      "title" : "Charsets Supported by Each Locale",
      "description" : "This table lets you configure the order of supported character sets used for
each supported locale. Change the settings only if the defaults are not appropriate.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaults" : {
      "properties" : {
        "commonNameFormats" : {
          "title" : "Auto Generated Common Name Format",
          "description" : "Use this list to configure how OpenAM formats names shown in the console
banner.<br><br>This setting allows the name of the authenticated user shown in the OpenAM console
banner to be customised based on the locale of the user.",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          }
        }
      }
    }
  }
}
```

```
    },
    "type" : "array",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
```

## 1.58. HotpModule

### 1.58.1. Realm Operations

Resource path: `/realm-config/authentication/modules/hotp`

Resource version: `1.0`

#### 1.58.1.1. create

Usage:

```
am> create HotpModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userProfileTelephoneAttribute" : {
      "title" : "Mobile Phone Number Attribute Name",
      "description" : "This is the attribute name used for a requested text message",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpUsername" : {
      "title" : "Mail Server Authentication Username",
      "description" : "The username to use if the mail server is using SMTP authentication",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",

```

```

    "exampleValue" : ""
  },
  "userProfileEmailAttribute" : {
    "title" : "Email Attribute Name",
    "description" : "This is the attribute name used by the OTP to email the user",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpSslEnabled" : {
    "title" : "Mail Server Secure Connection ",
    "description" : "This setting controls whether the authentication module communicates with the
mail server using SSL/TLS",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpUserPassword" : {
    "title" : "Mail Server Authentication Password",
    "description" : "The password to use if the mail server is using SMTP authentication",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "otpValidityDuration" : {
    "title" : "One Time Password Validity Length",
    "description" : "This One Time Password will remain valid for this period (in minutes)",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "smtpHostPort" : {
    "title" : "Mail Server Host Port",
    "description" : "The port of the mail server.<br><br>The default port for SMTP is 25, if using
SSL the default port is 465.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "smtpHostname" : {
    "title" : "Mail Server Host Name",
    "description" : "The name of the mail server; OpenAM will use SMTP to send the messages.",
    "propertyOrder" : 300,

```

```

        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "smsGatewayClass" : {
        "title" : "SMS Gateway Implementation Class",
        "description" : "The HOTP authentication module uses this class to send SMS
messages.<br><br>The SMS gateway class must implement the following interface<br><br>
<code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "mobileCarrierAttribute" : {
        "title" : "Mobile Carrier Attribute Name",
        "description" : "This is the attribute name used for a mobile carrier domain for sending SMS
messages",
        "propertyOrder" : 1300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "autoSendOTP" : {
        "title" : "Auto Send OTP Code",
        "description" : "Select this checkbox if the OTP should be sent automatically",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "otpDeliveryMethod" : {
        "title" : "One Time Password Delivery",
        "description" : "The mechanism used to deliver the One Time Password",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "smtpFromAddress" : {
        "title" : "Email From Address",
        "description" : "Emails from the HOTP Authentication module will come from this address.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "otpLength" : {
        "title" : "One Time Password Length ",
        "description" : "The length of the generated One Time Password (in digits)",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

### 1.58.1.2. delete

Usage:

```
am> delete HotpModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.58.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HotpModule --realm Realm --actionName getAllTypes
```

### 1.58.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HotpModule --realm Realm --actionName getCreatableTypes
```

### 1.58.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HotpModule --realm Realm --actionName nextdescendents
```

### 1.58.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query HotpModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.58.1.7. read

Usage:

```
am> read HotpModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.58.1.8. update

Usage:

```
am> update HotpModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userProfileTelephoneAttribute" : {
      "title" : "Mobile Phone Number Attribute Name",
      "description" : "This is the attribute name used for a requested text message",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpUsername" : {
      "title" : "Mail Server Authentication Username",
      "description" : "The username to use if the mail server is using SMTP authentication",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userProfileEmailAttribute" : {
      "title" : "Email Attribute Name",
      "description" : "This is the attribute name used by the OTP to email the user",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpSslEnabled" : {
```

```

    "title" : "Mail Server Secure Connection ",
    "description" : "This setting controls whether the authentication module communicates with the
mail server using SSL/TLS",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpUserPassword" : {
    "title" : "Mail Server Authentication Password",
    "description" : "The password to use if the mail server is using SMTP authentication",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "otpValidityDuration" : {
    "title" : "One Time Password Validity Length",
    "description" : "This One Time Password will remain valid for this period (in minutes)",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "smtpHostPort" : {
    "title" : "Mail Server Host Port",
    "description" : "The port of the mail server.<br><br>The default port for SMTP is 25, if using
SSL the default port is 465.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "smtpHostname" : {
    "title" : "Mail Server Host Name",
    "description" : "The name of the mail server; OpenAM will use SMTP to send the messages.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smsGatewayClass" : {
    "title" : "SMS Gateway Implementation Class",
    "description" : "The HOTP authentication module uses this class to send SMS
messages.<br><br>The SMS gateway class must implement the following interface<br><br>
<code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
    "propertyOrder" : 200,
    "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "mobileCarrierAttribute" : {
        "title" : "Mobile Carrier Attribute Name",
        "description" : "This is the attribute name used for a mobile carrier domain for sending SMS
messages",
        "propertyOrder" : 1300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "autoSendOTP" : {
        "title" : "Auto Send OTP Code",
        "description" : "Select this checkbox if the OTP should be sent automatically",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "otpDeliveryMethod" : {
        "title" : "One Time Password Delivery",
        "description" : "The mechanism used to deliver the One Time Password",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "smtpFromAddress" : {
        "title" : "Email From Address",
        "description" : "Emails from the HOTP Authentication module will come from this address.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "otpLength" : {
        "title" : "One Time Password Length ",
        "description" : "The length of the generated One Time Password (in digits)",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}

```

## 1.58.2. Global Operations

Resource path: `/global-config/authentication/modules/hotp`

Resource version: `1.0`



### 1.58.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HotpModule --global --actionName getAllTypes
```

### 1.58.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HotpModule --global --actionName getCreatableTypes
```

### 1.58.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HotpModule --global --actionName nextdescendents
```

### 1.58.2.4. read

Usage:

```
am> read HotpModule --global
```

### 1.58.2.5. update

Usage:

```
am> update HotpModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "smtpFromAddress" : {
          "title" : "Email From Address",
          "description" : "Emails from the HOTP Authentication module will come from this address.",
          "propertyOrder" : 800,
          "required" : true,
```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "userProfileEmailAttribute" : {
        "title" : "Email Attribute Name",
        "description" : "This is the attribute name used by the OTP to email the user",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "smtpUserPassword" : {
        "title" : "Mail Server Authentication Password",
        "description" : "The password to use if the mail server is using SMTP authentication",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "smtpUsername" : {
        "title" : "Mail Server Authentication Username",
        "description" : "The username to use if the mail server is using SMTP authentication",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "userProfileTelephoneAttribute" : {
        "title" : "Mobile Phone Number Attribute Name",
        "description" : "This is the attribute name used for a requested text message",
        "propertyOrder" : 1200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "smtpHostPort" : {
        "title" : "Mail Server Host Port",
        "description" : "The port of the mail server.<br><br>The default port for SMTP is 25, if
using SSL the default port is 465.",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "otpValidityDuration" : {
        "title" : "One Time Password Validity Length",
        "description" : "This One Time Password will remain valid for this period (in minutes)",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "otpDeliveryMethod" : {
        "title" : "One Time Password Delivery",
        "description" : "The mechanism used to deliver the One Time Password",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "string",

```

```

    "exampleValue" : ""
  },
  "smtpSslEnabled" : {
    "title" : "Mail Server Secure Connection ",
    "description" : "This setting controls whether the authentication module communicates with
the mail server using SSL/TLS",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "autoSendOTP" : {
    "title" : "Auto Send OTP Code",
    "description" : "Select this checkbox if the OTP should be sent automatically",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "smtpHostname" : {
    "title" : "Mail Server Host Name",
    "description" : "The name of the mail server; OpenAM will use SMTP to send the messages.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smsGatewayClass" : {
    "title" : "SMS Gateway Implementation Class",
    "description" : "The HOTP authentication module uses this class to send SMS
messages.<br><br>The SMS gateway class must implement the following interface<br><br>
<code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "mobileCarrierAttribute" : {
    "title" : "Mobile Carrier Attribute Name",
    "description" : "This is the attribute name used for a mobile carrier domain for sending SMS
messages",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "otpLength" : {
    "title" : "One Time Password Length ",
    "description" : "The length of the generated One Time Password (in digits)",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",

```

```
        "propertyOrder" : 100,  
        "required" : true,  
        "type" : "integer",  
        "exampleValue" : ""  
      }  
    },  
    "type" : "object",  
    "title" : "Realm Defaults"  
  }  
}
```

## 1.59. HttpBasicModule

### 1.59.1. Realm Operations

Resource path: `/realm-config/authentication/modules/httpbasic`

Resource version: `1.0`

#### 1.59.1.1. create

Usage:

```
am> create HttpBasicModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "backendModuleName" : {
      "title" : "Backend Module Name",
      "description" : "The name of the module that will be used to perform the authentication<br><br>The HTTP Basic authentication module collect the credentials from the user and will then supply said credentials to the backend authentication module using the shared state. ",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

### 1.59.1.2. delete

Usage:

```
am> delete HttpBasicModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.59.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HttpBasicModule --realm Realm --actionName getAllTypes
```

### 1.59.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HttpBasicModule --realm Realm --actionName getCreatableTypes
```

### 1.59.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HttpBasicModule --realm Realm --actionName nextdescendents
```

### 1.59.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query HttpBasicModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.59.1.7. read

Usage:

```
am> read HttpBasicModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.59.1.8. update

Usage:

```
am> update HttpBasicModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "backendModuleName" : {
      "title" : "Backend Module Name",
      "description" : "The name of the module that will be used to perform the authentication<br><br>The HTTP Basic authentication module collect the credentials from the user and will then supply said credentials to the backend authentication module using the shared state. ",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

## 1.59.2. Global Operations

Resource path: `/global-config/authentication/modules/httpbasic`

Resource version: `1.0`

### 1.59.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HttpBasicModule --global --actionName getAllTypes
```

### 1.59.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HttpBasicModule --global --actionName getCreatableTypes
```

### 1.59.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HttpBasicModule --global --actionName nextdescendents
```

#### 1.59.2.4. read

Usage:

```
am> read HttpBasicModule --global
```

#### 1.59.2.5. update

Usage:

```
am> update HttpBasicModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "backendModuleName" : {
          "title" : "Backend Module Name",
          "description" : "The name of the module that will be used to perform the
authentication<br><br>The HTTP Basic authentication module collect the credentials from the user and
will then supply said credentials to the backend authentication module using the shared state. ",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```



## 1.60. IdRepository

### 1.60.1. Realm Operations

Resource path: `/realm-config/services/id-repositories`

Resource version: `1.0`

#### 1.60.1.1. create

Usage:

```
am> create IdRepository --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunIdRepoAttributeValidator" : {
      "title" : "Attribute Validator Plug-in",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sunCoexistenceAttributeMapping" : {
      "title" : "Directory Attribute Mapping",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sunIdRepoAttributeCombiner" : {
      "title" : "Attribute Combiner plug-in",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

```
}  
}  
}
```

### 1.60.1.2. delete

Usage:

```
am> delete IdRepository --realm Realm
```

### 1.60.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdRepository --realm Realm --actionName getAllTypes
```

### 1.60.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdRepository --realm Realm --actionName getCreatableTypes
```

### 1.60.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdRepository --realm Realm --actionName nextdescendents
```

### 1.60.1.6. read

Usage:

```
am> read IdRepository --realm Realm
```

### 1.60.1.7. update

Usage:

```
am> update IdRepository --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunIdRepoAttributeValidator" : {
      "title" : "Attribute Validator Plug-in",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sunCoexistenceAttributeMapping" : {
      "title" : "Directory Attribute Mapping",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sunIdRepoAttributeCombiner" : {
      "title" : "Attribute Combiner plug-in",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.60.2. Global Operations

Resource path: `/global-config/services/id-repositories`

Resource version: `1.0`

### 1.60.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdRepository --global --actionName getAllTypes
```

### 1.60.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdRepository --global --actionName getCreatableTypes
```

### 1.60.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdRepository --global --actionName nextdescendents
```

### 1.60.2.4. read

Usage:

```
am> read IdRepository --global
```

### 1.60.2.5. update

Usage:

```
am> update IdRepository --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "sunCoexistenceAttributeMapping" : {
          "title" : "Directory Attribute Mapping",
          "description" : "",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
```

```
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sunIdRepoAttributeCombiner" : {
      "title" : "Attribute Combiner plug-in",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sunIdRepoAttributeValidator" : {
      "title" : "Attribute Validator Plug-in",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "type" : "object",
  "title" : "Realm Defaults"
}
}
```

## 1.61. IdRepositoryUser

### 1.61.1. Global Operations

Resource path: `/global-config/services/id-repositories/user`

Resource version: `1.0`

#### 1.61.1.1. create

Usage:

```
am> create IdRepositoryUser --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "iplanet-am-user-failure-url" : {
      "title" : "iplanet-am-user-failure-url",
      "description" : "",
      "propertyOrder" : 9600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mail" : {
      "title" : "mail",
      "description" : "",
      "propertyOrder" : 9800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sn" : {
      "title" : "sn",
      "description" : "",
      "propertyOrder" : 10200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "dn" : {
      "title" : "dn",
      "description" : "",
      "propertyOrder" : 9200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-user-alias-list" : {
      "title" : "iplanet-am-user-alias-list",
      "description" : "",
      "propertyOrder" : 9500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sunIdentityMSISDNNumber" : {
      "title" : "sunIdentityMSISDNNumber",
      "description" : "",
      "propertyOrder" : 10400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "inetUserStatus" : {
      "title" : "status",
      "description" : "",
      "propertyOrder" : 10300,
```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "postalAddress" : {
    "title" : "postalAddress",
    "description" : "",
    "propertyOrder" : 10000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cn" : {
    "title" : "Name",
    "description" : "",
    "propertyOrder" : 9100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "telephoneNumber" : {
    "title" : "telephoneNumber",
    "description" : "",
    "propertyOrder" : 10500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "givenName" : {
    "title" : "givenName",
    "description" : "",
    "propertyOrder" : 9400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userPassword" : {
    "title" : "Password",
    "description" : "",
    "propertyOrder" : 9900,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "iplanet-am-user-success-url" : {
    "title" : "iplanet-am-user-success-url",
    "description" : "",
    "propertyOrder" : 9700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "employeeNumber" : {
    "title" : "employeeNumber",
    "description" : "",
    "propertyOrder" : 9300,
    "required" : true,
    "type" : "string",

```

```
    "exampleValue" : ""
  },
  "roles" : {
    "title" : "Roles",
    "description" : "",
    "propertyOrder" : 10100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }
}
```

### 1.61.1.2. delete

Usage:

```
am> delete IdRepositoryUser --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.61.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdRepositoryUser --global --actionName getAllTypes
```

### 1.61.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdRepositoryUser --global --actionName getCreatableTypes
```

### 1.61.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdRepositoryUser --global --actionName nextdescendents
```



### 1.61.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query IdRepositoryUser --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.61.1.7. read

Usage:

```
am> read IdRepositoryUser --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.61.1.8. update

Usage:

```
am> update IdRepositoryUser --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "iplanet-am-user-failure-url" : {
      "title" : "iplanet-am-user-failure-url",
      "description" : "",
      "propertyOrder" : 9600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mail" : {
      "title" : "mail",
```

```

    "description" : "",
    "propertyOrder" : 9800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sn" : {
    "title" : "sn",
    "description" : "",
    "propertyOrder" : 10200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "dn" : {
    "title" : "dn",
    "description" : "",
    "propertyOrder" : 9200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "iplanet-am-user-alias-list" : {
    "title" : "iplanet-am-user-alias-list",
    "description" : "",
    "propertyOrder" : 9500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdentityMSISDNNumber" : {
    "title" : "sunIdentityMSISDNNumber",
    "description" : "",
    "propertyOrder" : 10400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "inetUserStatus" : {
    "title" : "status",
    "description" : "",
    "propertyOrder" : 10300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "postalAddress" : {
    "title" : "postalAddress",
    "description" : "",
    "propertyOrder" : 10000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cn" : {
    "title" : "Name",
    "description" : "",
    "propertyOrder" : 9100,
    "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "telephoneNumber" : {
        "title" : "telephoneNumber",
        "description" : "",
        "propertyOrder" : 10500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "givenName" : {
        "title" : "givenName",
        "description" : "",
        "propertyOrder" : 9400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "userPassword" : {
        "title" : "Password",
        "description" : "",
        "propertyOrder" : 9900,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "iplanet-am-user-success-url" : {
        "title" : "iplanet-am-user-success-url",
        "description" : "",
        "propertyOrder" : 9700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "employeeNumber" : {
        "title" : "employeeNumber",
        "description" : "",
        "propertyOrder" : 9300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "roles" : {
        "title" : "Roles",
        "description" : "",
        "propertyOrder" : 10100,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    }
}
}

```

## 1.62. IdffEntity

### 1.62.1. Realm Operations

Resource path: `/realm-config/federation/entityproviders/idff`

Resource version: `1.0`

#### 1.62.1.1. create

Usage:

```
am> create IdffEntity --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

#### 1.62.1.2. delete

Usage:

```
am> delete IdffEntity --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.62.1.3. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query IdffEntity --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.62.1.4. read

Usage:

```
am> read IdffEntity --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.62.1.5. update

Usage:

```
am> update IdffEntity --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.63. J2EEAgentGroups

### 1.63.1. Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/J2EEAgent`

Resource version: `1.0`

#### 1.63.1.1. create

Usage:

```
am> create J2EEAgentGroups --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userTokenName" : {
```

```

    "title" : "User Token Name",
    "description" : "Session property name for user-ID of the authenticated user in session.
(property name: com.sun.identity.agents.config.user.token) <br>Hot-swap: Yes",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "webServiceAuthenticator" : {
    "title" : "Web Service Authenticator",
    "description" : "An implementation class of interface
com.sun.identity.agents.filter.IWebServiceAuthenticator that can be used to authenticate web-service
requests. (property name: com.sun.identity.agents.config.webservice.authenticator) <br>Hot-swap:
Yes",
    "propertyOrder" : 2300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoRootUrl" : {
    "title" : "Agent Root URL for CDSSO",
    "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
    "propertyOrder" : 22700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "defaultPrivilegedAttributes" : {
    "title" : "Default Privileged Attribute",
    "description" : "List of privileged attributes that will be granted to all users who have a
valid OpenAM session. (property name: com.sun.identity.agents.config.default.privileged.attribute)
<br>Hot-swap: Yes <br> Example: <br> AUTHENTICATED_USERS",
    "propertyOrder" : 9400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "cdssoTrustedIdProvider" : {
    "title" : "CDSSO Trusted ID Provider",
    "description" : "List of OpenAM Server/ID providers that should be trusted
by the agent, when evaluating the CDC Liberty Responses. (property name:
com.sun.identity.agents.config.cdsso.trusted.id.provider) <br>Hot-swap: Yes <br> Example: <br>
http://host:port/opensso/cdcservlet",
    "propertyOrder" : 5600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }

```

```

    },
    "notEnforcedIpsCacheEnabled" : {
      "title" : "Not Enforced IP Cache Flag",
      "description" : "Enable caching of not-enforced IP list evaluation results. (property name:
com.sun.identity.agents.config.notenforced.ip.cache.enable) <br>Hot-swap: Yes",
      "propertyOrder" : 8100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "postDataStickySessionKeyValue" : {
      "title" : "PDP StickySession key-value",
      "description" : "The provided key-value pair will be used for adding to
the URL or creating the cookie. <br>Example: <br>Set 'lb=server1' to append to
the querystring or to have 'lb' cookie with 'server1' value. (property name:
com.sun.identity.agents.config.postdata.preserve.stickysession.value)",
      "propertyOrder" : 13500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "repositoryLocation" : {
      "title" : "Location of Agent Configuration Repository",
      "description" : "Indicates agent's configuration located either on agent's host or centrally on
OpenAM server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "postDataCacheTtl" : {
      "title" : "PDP entry TTL",
      "description" : "This value tells how long a given POST entry should be stored
in the local cache (in milliseconds), default value is 300000. (property name:
com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl)",
      "propertyOrder" : 13300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "redirectAttemptLimit" : {
      "title" : "Redirect Attempt Limit",
      "description" : "Number of successive single point redirects that a user can make using a
single browser session which will trigger the blocking of the user request. Set to 0 to disable this
feature. (property name: com.sun.identity.agents.config.redirect.attempt.limit) <br>Hot-swap: Yes",
      "propertyOrder" : 7100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "useRedirectForCompositeAdvice" : {
      "title" : "Use HTTP-Redirect for composite advice",
      "description" : "Configure remote policy client to use HTTP-redirect instead of HTTP-POST
for composite advices. (property name: com.sun.identity.agents.config.policy.advice.use.redirect)
<br>Hot-swap: Yes",
      "propertyOrder" : 13000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }

```



```

    },
    "auditLogLocation" : {
      "title" : "Audit Log Location",
      "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition) <br>Hot-swap: Yes",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "privilegedAttributeMappingEnabled" : {
      "title" : "Enable Privileged Attribute Mapping",
      "description" : "Enable a mapping from the original value of an attribute to another value. To
satisfy container-specific restrictions on character set being used in certain configuration files.
(property name: com.sun.identity.agents.config.privileged.attribute.mapping.enable) <br>Hot-swap:
Yes",
      "propertyOrder" : 9800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "localeLanguage" : {
      "title" : "Locale Language",
      "description" : "(property name: com.sun.identity.agents.config.locale.language) <br>Hot-swap:
No",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "postDataStickySessionMode" : {
      "title" : "PDP StickySession mode",
      "description" : "The PDP mechanism needs sticky loadbalancing, the URL mode will
append a querystring, while the Cookie mode will create a cookie. (property name:
com.sun.identity.agents.config.postdata.preserve.stickysession.mode)",
      "propertyOrder" : 13400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "clientHostnameHeader" : {
      "title" : "Client Hostname Header",
      "description" : "HTTP header name that holds the Hostname of the client. (property name:
com.sun.identity.agents.config.client.hostname.header) <br>Hot-swap: Yes",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "privilegedSessionAttribute" : {
      "title" : "Privileged Session Attribute",
      "description" : "List of session property names which hold privileged attributes for the
authenticated user. (property name: com.sun.identity.agents.config.privileged.session.attribute)
<br>Hot-swap: Yes <br> Example: <br> UserToken",
      "propertyOrder" : 9700,
      "required" : true,
      "items" : {
        "type" : "string"
      }
    },
    },
  },

```

```

    "type" : "array",
    "exampleValue" : ""
  },
  "xssDetectionRedirectUri" : {
    "title" : "XSS detection redirect URI",
    "description" : "An application-specific Map that identifies a URI of the customized page if
XSS code has been detected. (property name: com.sun.identity.agents.config.xss.redirect.uri) <br>Hot-
swap: Yes <br>Examples: <br>To set a redirect target for application BankApp: enter BankApp in Map Key
field, and enter a redirect URI in Corresponding Map Value field.",
    "propertyOrder" : 12900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"responseAttributeMap" : {
  "title" : "Response Attribute Mapping",
  "description" : "Maps the policy response attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.response.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field,
and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
  "propertyOrder" : 9200,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  }
},
"type" : "object",
"exampleValue" : ""
},
"logoutEntryUri" : {
  "title" : "Logout Entry URI",
  "description" : "An application-specific Map that identifies a URI to be used as an entry point
after successful logout and subsequent successful authentication if applicable. (property name:
com.sun.identity.agents.config.logout.entry.uri) <br>Valid key: the web application name. <br>Valid
value: the logout entry URI. <br>For this property, a global value can be set to apply to all the
applications that don't have their own specific logout entry URI. <br>Hot-swap: Yes <br> Examples:
<br>To set a global application logout entry URI: leave Map Key field empty, and enter the global
application logout entry URI /welcome.html in Corresponding Map Value field. <br> To set the logout
entry URI for application BankApp: enter BankApp in Map Key field, and enter the logout entry URI /
BankApp/welcome.html in Corresponding Map Value field.",
  "propertyOrder" : 6300,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  }
},
"type" : "object",
"exampleValue" : ""
},
"loginErrorUri" : {
  "title" : "Login Error URI",

```

```

    "description" : "List of absolute URIs corresponding to an application's web.xml form-error-
page element. (property name: com.sun.identity.agents.config.login.error.uri) <br>Hot-swap: Yes <br>
Example: <br> /BankApp/jsp/error.jsp",
    "propertyOrder" : 2900,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"webServiceEndpoints" : {
    "title" : "Web Service End Points",
    "description" : "A list of Web Application end points that represent Web Services. (property
name: com.sun.identity.agents.config.webservice.endpoint) <br>Hot-swap: Yes",
    "propertyOrder" : 2100,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"cookieResetPaths" : {
    "title" : "Cookies Reset Path Map",
    "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the path of this cookie to be used when a reset event occurs. (property name:
com.sun.identity.agents.config.cookie.reset.path) <br>Hot-swap: Yes",
    "propertyOrder" : 4900,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"sessionAttributeFetchMode" : {
    "title" : "Session Attribute Fetch Mode",
    "description" : "The mode of fetching session attributes. (property name:
com.sun.identity.agents.config.session.attribute.fetch.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 8900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"useInternalLogin" : {
    "title" : "Use Internal Login",
    "description" : "Set to false if want to customize Login Content File instead of default
internal content provided. (property name: com.sun.identity.agents.config.login.use.internal)
<br>Hot-swap: Yes",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"policyClientPollingInterval" : {
    "title" : "Policy Client Polling Interval",

```

```

    "description" : "Duration in minutes after which the cached entries are refreshed by remote
policy client. (property name: com.sun.identity.agents.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 11300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "policyNotifications" : {
    "title" : "Enable Policy Notifications",
    "description" : "Enable Notifications for remote policy client. (property name:
com.sun.identity.agents.notification.enabled) <br>Hot-swap: No",
    "propertyOrder" : 11200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "portCheckEnabled" : {
    "title" : "Port Check Enable",
    "description" : "Indicates if port check functionality is enabled or disabled. (property name:
com.sun.identity.agents.config.port.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 7200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "httpSessionBinding" : {
    "title" : "HTTP Session Binding",
    "description" : "If true will invalidate the http session when login has failed, user
has no SSO session, or principal user name does not match SSO user name. (property name:
com.sun.identity.agents.config.httpsession.binding) <br>Hot-swap: Yes",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "loginFormUri" : {
    "title" : "Login Form URI",
    "description" : "List of absolute URIs corresponding to an application's web.xml form-login-page
element. (property name: com.sun.identity.agents.config.login.form) <br>Hot-swap: Yes <br> Example:
<br> /BankApp/jsp/login.jsp",
    "propertyOrder" : 2800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "webServiceAuthorizationErrorContentFile" : {
    "title" : "Web Service Authorization Error Content File",
    "description" : "The name of file that contains content used by the
Agent to generate an authorization error fault for clients. (property name:
com.sun.identity.agents.config.webservice.autherror.content) <br>Hot-swap: Yes",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ignorePathInfo" : {

```

```

        "title" : "Ignore Path Info in Request URL",
        "description" : "The path info will be stripped from the request URL while doing Not
        Enforced List check and url policy evaluation if the value is set to true. (property name:
        com.sun.identity.agents.config.ignore.path.info) <br>Hot-swap: Yes",
        "propertyOrder" : 18600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "applicationLogoutUri" : {
        "title" : "Application Logout URI",
        "description" : "An application-specific Map that identifies a request URI which indicates
        a logout event. (property name: com.sun.identity.agents.config.logout.uri) <br>Valid key: the web
        application name. <br>Valid value: the application logout URI. <br>For this property, a global value
        can be set to apply to all the applications that don't have their own specific logout URI. <br>Hot-
        swap: Yes <br> Examples: <br>To set a global application logout URI: leave Map Key field empty, and
        enter the global application logout URI /logout.jsp in Corresponding Map Value field. <br> To set the
        logout URI for application BankApp: enter BankApp in Map Key field, and enter the application logout
        URI /BankApp/logout.jsp in Corresponding Map Value field.",
        "propertyOrder" : 6000,
        "required" : true,
        "patternProperties" : {
            ".*" : {
                "type" : "string"
            }
        },
        "type" : "object",
        "exampleValue" : ""
    },
    "agentNotificationUrl" : {
        "title" : "Agent Notification URL",
        "description" : "URL used by agent to register notification listeners. (property name:
        com.sun.identity.client.notification.url) <br>Hot-swap: No",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "probeLogoutUrl" : {
        "title" : "Logout URL Probe",
        "description" : "Specifies if agent will check the availability of these urls before redirecting
        to them. (property name: com.sun.identity.agents.config.logout.url.probe.enabled) <br>Hot-swap: Yes",
        "propertyOrder" : 12600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "localAuditRotationSize" : {
        "title" : "Local Audit Log Rotation Size",
        "description" : "Size limit when a local audit log file is rotated to a new file. (property
        name: com.sun.identity.agents.config.local.log.size) <br>Hot-swap: Yes",
        "propertyOrder" : 1900,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "authServiceProtocol" : {
        "title" : "OpenAM Authentication Service Protocol",

```

```

    "description" : "Protocol to be used by the OpenAM authentication service. (property name:
com.ipplanet.am.server.protocol) <br>Hot-swap: No",
    "propertyOrder" : 10900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cookieResetDomains" : {
    "title" : "Cookies Reset Domain Map",
    "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the domain of this cookie to be used when a reset event occurs. (property name:
com.sun.identity.agents.config.cookie.reset.domain) <br>Hot-swap: Yes",
    "propertyOrder" : 4800,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "possibleXssCodeElements" : {
    "title" : "Possible XSS code elements",
    "description" : "If one of these strings occurs in the request, the client is redirected to an
error page. (property name: com.sun.identity.agents.config.xss.code.elements) <br>Hot-swap: Yes",
    "propertyOrder" : 12800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "debugLevel" : {
    "title" : "Agent Debug Level",
    "description" : "Specifies type of agent debug messages to log. (property name:
com.ipplanet.services.debug.level) <br>Hot-swap: Yes",
    "propertyOrder" : 10000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "urlPolicyEnvJsessionParameters" : {
    "title" : "URL Policy Env jsession Parameters",
    "description" : "List of HTTP SESSION attributes whose names and values will be
set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.jsession.param) <br>Hot-swap: Yes <br> Examples: <br> name
<br> phonenumber",
    "propertyOrder" : 12000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "fqdnMapping" : {
    "title" : "FQDN Virtual Host Map",

```

```

    "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN to
access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>Hot-
swap: Yes <br> Examples: <br> To map the partial hostname myserver to myserver.mydomain.com: enter
myserver in the Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map
a virtual server rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in
the Map Key field and rst.hostname.com in the Corresponding Map Value field.",
    "propertyOrder" : 6600,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"probeLoginUrl" : {
    "title" : "Login URL Probe",
    "description" : "Specifies if agent will check the availability of these urls before redirecting
to them. (property name: com.sun.identity.agents.config.login.url.probe.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 3900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"invertNotEnforcedUris" : {
    "title" : "Invert Not Enforced URIs",
    "description" : "Inverts protection of URIs specified in Not Enforced URIs list. When set
to true, it indicates that the URIs specified should be enforced and all other URIs should be
not enforced by the Agent. (property name: com.sun.identity.agents.config.notenforced.uri.invert)
<br>Hot-swap: Yes",
    "propertyOrder" : 7600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"headerAttributeDateFormat" : {
    "title" : "Fetch Attribute Date Format",
    "description" : "Format of date attribute values to be used when the attribute is
being set as HTTP header. Format is based on java.text.SimpleDateFormat. (property name:
com.sun.identity.agents.config.attribute.date.format) <br>Hot-swap: Yes",
    "propertyOrder" : 8400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"agentConfigChangeNotificationsEnabled" : {
    "title" : "Agent Configuration Change Notification",
    "description" : "Enable agent to receive notification messages from OpenAM server for
configuration changes. (property name: com.sun.identity.agents.config.change.notification.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 12100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"logoutUrlPrioritized" : {
    "title" : "Logout URL Prioritized",

```

```

    "description" : "Specifies if failover sequence for Logout URLs should be prioritized as defined
in the OpenAM Login URL list. (property name: com.sun.identity.agents.config.logout.url.prioritized)
<br>Hot-swap: Yes",
    "propertyOrder" : 12500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "customLogoutHandlers" : {
    "title" : "Custom Logout Handler",
    "description" : "Application specific logout handler to log out a user with the application
server. (property name: com.sun.identity.agents.config.logout.handler) <br>Valid key: the web
application name. <br>Valid value: the logout handler class name. <br>Hot-swap: Yes <br> Example:
<br>To set logout handler for application BankApp: enter BankApp in Map Key field, and enter logout
handler class name BankLogoutHandler in Corresponding Map Value field.",
    "propertyOrder" : 3300,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "cookieResetEnabled" : {
    "title" : "Cookie Reset",
    "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 4600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "portCheckFile" : {
    "title" : "Port Check File",
    "description" : "Name or complete path of a file that has the necessary content needed to handle
requests that need port correction. (property name: com.sun.identity.agents.config.port.check.file)
<br>Hot-swap: Yes",
    "propertyOrder" : 7300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sessionAttributeMap" : {
    "title" : "Session Attribute Mapping",
    "description" : "Maps the session attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map
Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
    "propertyOrder" : 9000,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",

```





```

    "type" : "object",
    "exampleValue" : ""
  },
  "serviceDataCacheTime" : {
    "title" : "Service Data Cache Time",
    "description" : "Cache update time in minutes for service configuration data. If set to '0' no
updates happen. (property name: com.sun.identity.sm.cacheTime) <br>Hot-swap: No",
    "propertyOrder" : 10800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "status" : {
    "title" : "Status",
    "description" : "Status of the agent configuration.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "loginProbeTimeout" : {
    "title" : "Login URL Probe Timeout",
    "description" : "The connect timeout value in milliseconds, if also Login URL Probe is set to
true. (property name: com.sun.identity.agents.config.login.url.probe.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 4000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "privilegedAttributeType" : {
    "title" : "Privileged Attribute Type",
    "description" : "List of privileged attribute types that will be fetched for each user.
(property name: com.sun.identity.agents.config.privileged.attribute.type) <br>Hot-swap: Yes <br>
Example: <br> Group",
    "propertyOrder" : 9500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "loginUrlPrioritized" : {
    "title" : "Login URL Prioritized",
    "description" : "Specifies if failover sequence for Login URLs or CDSSO URLs
should be prioritized as defined in the OpenAM Login URL list. (property name:
com.sun.identity.agents.config.login.url.prioritized) <br>Hot-swap: Yes",
    "propertyOrder" : 3800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyEvaluationRealm" : {
    "title" : "Realm",
    "description" : "Which realm to start evaluating from. (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm) <br>Hot-swap: Yes",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",

```

```

    "exampleValue" : ""
  },
  "filterMode" : {
    "title" : "Agent Filter Mode",
    "description" : "Specifies the mode of operation of the Filter. (property name:
com.sun.identity.agents.config.filter.mode) <br>Valid key: the web application name. <br>Valid
values: ALL, J2EE_POLICY, URL_POLICY, SSO_ONLY, NONE <br>For this property, a global value can be
set to apply to all the applications that don't have their own specific filter mode. <br>Hot-swap:
No <br>Examples: <br>To set ALL as the global filter mode: leave Map Key field empty, and enter ALL
in Corresponding Map Value field. <br>To set URL_POLICY as the filter mode for application BankApp:
enter BankApp in Map Key field, and enter URL_POLICY in Corresponding Map Value field.",
    "propertyOrder" : 500,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "userMappingMode" : {
    "title" : "User Mapping Mode",
    "description" : "Specifies mechanism agent uses to determine user-ID. (property name:
com.sun.identity.agents.config.user.mapping.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributeMap" : {
    "title" : "Profile Attribute Mapping",
    "description" : "Maps the profile attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.profile.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field,
and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate the value of profile
attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in
Corresponding Map Value field.",
    "propertyOrder" : 8800,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "webServiceResponseProcessor" : {
    "title" : "Web Service Response Processor",
    "description" : "An implementation class of interface
com.sun.identity.agents.filter.IWebServiceResponseProcessor that can be used to process the web-
service responses. (property name: com.sun.identity.agents.config.webservice.responseprocessor)
<br>Hot-swap: Yes",
    "propertyOrder" : 2400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }

```

```

},
"cdssoRedirectUri" : {
  "title" : "CDSSO Redirect URI",
  "description" : "An intermediate URI that is used by the Agent for processing CDSSO requests.
(property name: com.sun.identity.agents.config.cdsso.redirect.uri) <br>Hot-swap: Yes",
  "propertyOrder" : 5100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"ssoCacheEnabled" : {
  "title" : "SSO Cache Enable",
  "description" : "Specifies if the SSO Cache is active for the agent.
Cache is used through public APIs exposed by the agent SDK. (property name:
com.sun.identity.agents.config.amsso.cache.enable) <br>Hot-swap: Yes",
  "propertyOrder" : 4500,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"bypassPrincipallist" : {
  "title" : "Bypass Principal List",
  "description" : "List of principals that are bypassed by the Agent for authentication and search
purposes. (property name: com.sun.identity.agents.config.bypass.principal) <br>Hot-swap: Yes <br>
Examples: <br> guest <br> testuser",
  "propertyOrder" : 9300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"gotoParameterName" : {
  "title" : "Goto Parameter Name",
  "description" : "Property used only when CDSSO is enabled. Default value should
be changed only when the login URL has a landing page specified <br> Example :
com.sun.identity.agents.config.cdsso.cdcservlet.url = http://host:port/opensso/cdcservlet?
goto=http://agent:port/landing.jsp <br> The parameter is used by the Agent to append the original
request URL to this cdcservlet URL. This parameter is consumed by the landing page to redirect to
the original URL. (property name: com.sun.identity.agents.config.redirect.param) <br>Hot-swap: Yes
<br> Example: com.sun.identity.agents.config.redirect.param = goto2<br> The complete URL sent for
authentication will be <br> http://host:port/opensso/cdcservlet?goto=http://agent:port/landing.jsp?
goto2=http://agent.port/original.jsp",
  "propertyOrder" : 3600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userDataCacheNotifications" : {
  "title" : "Enable Notification of User Data Caches",
  "description" : "Enable notifications for amsdk and IdRepo Caches. (property name:
com.sun.identity.idm.remote.notification.enabled) <br>Hot-swap: No",
  "propertyOrder" : 10500,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"legacyRedirectUri" : {

```

```

    "title" : "Legacy User Agent Redirect URI",
    "description" : "An intermediate URI used by the Agent to redirect legacy user agent requests.
(property name: com.sun.identity.agents.config.legacy.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 6900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authServicePort" : {
    "title" : "OpenAM Authentication Service Port",
    "description" : "Port to be used by the OpenAM authentication service. (property name:
com.iplanet.am.server.port) <br>Hot-swap: No",
    "propertyOrder" : 11100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notEnforcedUrisCacheEnabled" : {
    "title" : "Not Enforced URIs Cache Enabled",
    "description" : "Enables the caching of the Not Enforced URIs list evaluation results. (property
name: com.sun.identity.agents.config.notenforced.uri.cache.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 7700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logoutProbeTimeout" : {
    "title" : "Logout URL Probe Timeout",
    "description" : "The connect timeout value in milliseconds, if also Logout URL Probe is set to
true. (property name: com.sun.identity.agents.config.logout.url.probe.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 12700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "policyClientCacheMode" : {
    "title" : "Policy Client Cache Mode",
    "description" : "Mode of caching to be used by remote policy client. (property name:
com.sun.identity.policy.client.cacheMode) <br>Hot-swap: No",
    "propertyOrder" : 11400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributeFetchMode" : {
    "title" : "Profile Attribute Fetch Mode",
    "description" : "The mode of fetching profile attributes. (property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 8700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "encryptionProvider" : {
    "title" : "Encryption Provider",
    "description" : "Specifies the encryption provider implementation to be used by the Agent.
(property name: com.iplanet.security.encryptor) <br>Hot-swap: No",
    "propertyOrder" : 10400,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "fqdnDefault" : {
    "title" : "FQDN Default",
    "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default) <br>Hot-swap: Yes",
    "propertyOrder" : 6500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "alternativeAgentPort" : {
    "title" : "Alternative Agent Port Name",
    "description" : "Port number identifying the Agent protected server listening port
to the client browsers if different from the actual listening port. (property name:
com.sun.identity.agents.config.agent.port) <br>Hot-swap: Yes",
    "propertyOrder" : 4200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "customVerificationHandlers" : {
    "title" : "Custom Verification Handler",
    "description" : "Application specific verification handler to validate the user credentials with
the local repository. (property name: com.sun.identity.agents.config.verification.handler) <br>Valid
key: the web application name. <br>Valid value: the verification handler class name. <br>Hot-swap:
Yes <br> Example: <br> To set verification handler for application BankApp: enter BankApp in Map Key
field, and enter verification handler class name BankVerificationHandler in Corresponding Map Value
field.",
    "propertyOrder" : 3400,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "notEnforcedUrisRefreshSessionIdleTime" : {
    "title" : "Refresh Session Idle Time",
    "description" : "Indicates if opensso session idle time should be refreshed or reset for not
enforced URIs. (property name: com.sun.identity.agents.config.notenforced.refresh.session.idletime)
<br>Hot-swap: Yes",
    "propertyOrder" : 8600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "webServiceEnabled" : {
    "title" : "Web Service Enable",
    "description" : "Flag specifies if Web Service processing is enabled. (property name:
com.sun.identity.agents.config.webservice.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
},

```

```

"alternativeAgentProtocol" : {
  "title" : "Alternative Agent Protocol",
  "description" : "Protocol being used (http/https) by the client browsers to communicate with
the Agent protected server if different from the actual protocol used by the server. (property name:
com.sun.identity.agents.config.agent.protocol) <br>Hot-swap: Yes",
  "propertyOrder" : 4300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"privilegedAttributesToLowerCase" : {
  "title" : "Privileged Attributes To Lower Case",
  "description" : "Maps the privileged attribute types to whether they should be converted to
lowercase. (property name: com.sun.identity.agents.config.privileged.attribute.tolowercase) <br>
Valid Keys: the privileged attribute types, such as Group, Role. <br>Valid value: true, false.
<br>Hot-swap: Yes <br> Example: <br> Enter Group in Map Key field, and enter false in Corresponding
Map Value field.",
  "propertyOrder" : 9600,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"notEnforcedUris" : {
  "title" : "Not Enforced URIs",
  "description" : "List of URIs for which protection is not enforced by the Agent. (property
name: com.sun.identity.agents.config.notenforced.uri) <br>Hot-swap: Yes <br> Examples: <br> /BankApp/
public/* <br> /BankApp/images/*",
  "propertyOrder" : 7500,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"remoteLogFilename" : {
  "title" : "Remote Log File Name",
  "description" : "Name of file stored on OpenAM server that contains agent audit messages.
(property name: com.sun.identity.agents.config.remote.logfile) <br>Hot-swap: Yes",
  "propertyOrder" : 1700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userPrincipalFlag" : {
  "title" : "User Principal Flag",
  "description" : "Use principal instead of just the user-ID for authenticating the user.
(property name: com.sun.identity.agents.config.user.principal) <br>Hot-swap: Yes",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"legacyUserAgentList" : {

```

```

    "title" : "Legacy User Agent List",
    "description" : "List of user agent header values that identify legacy
browsers. Entries in this list can have wild card character '*'. (property name:
com.sun.identity.agents.config.legacy.user.agent) <br>Hot-swap: Yes",
    "propertyOrder" : 6800,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"serviceDataCacheNotifications" : {
    "title" : "Enable Notification of Service Data Caches",
    "description" : "Enable the notifications for service management caches. (property name:
com.sun.identity.sm.notification.enabled) <br>Hot-swap: No",
    "propertyOrder" : 10700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"cdssoDomainList" : {
    "title" : "CDSSO Domain List",
    "description" : "Domains for which cookies have to be set in a CDSSO scenario. (property name:
com.sun.identity.agents.config.cdsso.domain) <br>Hot-swap: Yes <br> Example: <br> .sun.com",
    "propertyOrder" : 5800,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"clientPollingPeriod" : {
    "title" : "Client Polling Period",
    "description" : "Time in seconds after which the session client will request update of cached
session information from the server. (property name: com.iplanet.am.session.client.polling.period)
<br>Hot-swap: No",
    "propertyOrder" : 10300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"enableClientPolling" : {
    "title" : "Enable Client Polling",
    "description" : "Specifies if the session client must use polling for updating
session information and not depend upon server notifications. (property name:
com.iplanet.am.session.client.polling.enable) <br>Hot-swap: No",
    "propertyOrder" : 10200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"loginContentFile" : {
    "title" : "Login Content File Name",
    "description" : "Complete path and name of custom login content file. (property name:
com.sun.identity.agents.config.login.content.file) <br>Hot-swap: Yes",
    "propertyOrder" : 3100,
    "required" : true,

```



```

    "type" : "string",
    "exampleValue" : ""
  },
  "applicationLogoutHandlers" : {
    "title" : "Application Logout Handler",
    "description" : "An application-specific Map that identifies a handler to be used for logout
processing. (property name: com.sun.identity.agents.config.logout.application.handler) <br>Valid
key: the web application name. <br>Valid value: the application logout handler class name. <br>For
this property, a global value can be set to apply to all the applications that don't have their own
specific logout handler. <br>Hot-swap: Yes <br> Examples: <br>To set a global application logout
handler: leave Map Key field empty, and enter the global application logout handler class name
GlobalApplicationLogoutHandler in Corresponding Map Value field. <br>To set the logout handler for
application BankApp: enter BankApp in Map Key field, and enter the application logout handler class
name BankAppLogoutHandler in Corresponding Map Value field.",
    "propertyOrder" : 5900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "logoutIntrospection" : {
    "title" : "Logout Introspect Enabled",
    "description" : "Allows the Agent to search HTTP request body to locate logout parameter.
(property name: com.sun.identity.agents.config.logout.introspect.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 6200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "configurationReloadInterval" : {
    "title" : "Configuration Reload Interval",
    "description" : "Interval in seconds between configuration reloads. (property name:
com.sun.identity.agents.config.load.interval) <br>Hot-swap: Yes",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "amCookieName" : {
    "title" : "Cookie Name",
    "description" : "Name of the SSO Token cookie used between the OpenAM server and the Agent.
(property name: com.ipplanet.am.cookie.name) <br>Hot-swap: No",
    "propertyOrder" : 10100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoSecureCookies" : {
    "title" : "CDSSO Secure Enable",
    "description" : "The SSO Token cookie set by the agent in the different domains in CDSSO mode
will be marked secure. Only transmitted if the communications channel with host is a secure one.
(property name: com.sun.identity.agents.config.cdsso.secure.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "clientIpHeader" : {
    "title" : "Client IP Address Header",
    "description" : "HTTP header name that holds the IP address of the client. (property name: com.sun.identity.agents.config.client.ip.header) <br>Hot-swap: Yes",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "customAuthenticationHandlers" : {
    "title" : "Custom Authentication Handler",
    "description" : "Application specific authentication handler to authenticate the logged on user with the application server. (property name: com.sun.identity.agents.config.auth.handler) <br>Valid key: the web application name. <br>Valid value: the authentication handler class name. <br>Hot-swap: Yes <br>Example: <br>To set authentication handler for application BankApp: enter BankApp in Map Key field, and enter authentication handler class name BankAuthHandler in Corresponding Map Value field.",
    "propertyOrder" : 3200,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "localAuditLogRotation" : {
    "title" : "Rotate Local Audit Log",
    "description" : "Flag to indicate that audit log files should be rotated when reaching a certain size. (property name: com.sun.identity.agents.config.local.log.rotate) <br>Hot-swap: Yes",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "fqdnCheck" : {
    "title" : "FQDN Check",
    "description" : "Enables checking of fqdn default value and fqdn map values. (property name: com.sun.identity.agents.config.fqdn.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 6400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "webServiceProcessGetEnabled" : {
    "title" : "Web Service Process GET Enable",
    "description" : "Flag to indicates if the processing of HTTP GET requests for Web Service endpoints is enabled. (property name: com.sun.identity.agents.config.webservice.process.get.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "customProperties" : {
    "title" : "Custom Properties",

```

```

    "description" : "Additional properties that allow users to augment the set of properties
supported by agent. (property name: com.sun.identity.agents.config.freeformproperties) <br>Hot-
swap: Yes <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-
value-0 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
    "propertyOrder" : 12200,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"shortenedPrivilegeAttributeValues" : {
    "title" : "Shortened privilege attribute values",
    "description" : "When using privileged attribute type, this setting will ensure that the
membership details will be stored in a shortened format and not in the default universal ID
format.<br><br>By default the agent maps identity memberships using their universal IDs (e.g.
id=admin,ou=group,dc=openam,dc=forgerock,dc=org), however this may not be always acceptable. Using
this setting the identity membership details will be mapped in a shortened format, only including the
group's/role's name (e.g. admin). Be aware that in case there are both roles and groups in the data
store, this setting will make them indistinguishable from each other, i.e. if there is a group and a
role with the same name it will not be possible to differentiate them.",
    "propertyOrder" : 13600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"cdssoUrls" : {
    "title" : "CDSSO Servlet URL",
    "description" : "List of URLs of the available CDSSO controllers that may be used by the Agent
for CDSSO processing. (property name: com.sun.identity.agents.config.cdsso.cdcservlet.url) <br>Hot-
swap: Yes <br> Example: <br> http://host:port/opensso/cdcservlet",
    "propertyOrder" : 5200,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"postDataPreservation" : {
    "title" : "Post Data Preservation enabled",
    "description" : "Post Data Preservation functionality basically stores any POST
data before redirecting the user to the login screen and after successful login the agent
will generate a page that autosubmits the same POST to the original URL. (property name:
com.sun.identity.agents.config.postdata.preserve.enable)",
    "propertyOrder" : 13100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"missingPostDataPreservationEntryUri" : {
    "title" : "Missing PDP entry URI",
    "description" : "An application-specific URI Map that is used in case the referenced
PDP entry cannot be found in the local cache (due to ttl). In such cases it will redirect
to the specified URI, otherwise it will show a HTTP 403 Forbidden error. (property name:
com.sun.identity.agents.config.postdata.preservice.cache.noentry.url)<br>Examples: <br>To set a

```

```

redirect target for application BankApp: enter Bankapp in Map Key field and enter a redirect URI in
corresponding Map Value field.",
  "propertyOrder" : 13200,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"webServiceInternalErrorContentFile" : {
  "title" : "Web Service Internal Error Content File",
  "description" : "The name of file that contains content used by the
Agent to generate an internal error fault for clients. (property name:
com.sun.identity.agents.config.webservice.internalerror.content) <br>Hot-swap: Yes",
  "propertyOrder" : 2500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"cookieAttributeMultiValueSeparator" : {
  "title" : "Cookie Separator Character",
  "description" : "Character that will be used to separate multiple values
of the same attribute when it is being set as a cookie. (property name:
com.sun.identity.agents.config.attribute.cookie.separator) <br>Hot-swap: Yes",
  "propertyOrder" : 8300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"invertNotEnforcedIps" : {
  "title" : "Not Enforced IP Invert List",
  "description" : "Client IP Addresses to invert protection of IP addresses listed in the related
Not Enforced Client IP List. (property name: com.sun.identity.agents.config.notenforced.ip.invert)
<br>Hot-swap: Yes",
  "propertyOrder" : 8000,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"notEnforcedIps" : {
  "title" : "Not Enforced Client IP List",
  "description" : "No authentication and authorization protection from agent are
required for the requests coming from these client IP addresses. (property name:
com.sun.identity.agents.config.notenforced.ip) <br>Hot-swap: Yes <br> Examples: <br> 192.18.145.*
<br> 192.18.146.123",
  "propertyOrder" : 7900,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"cookieAttributeUrlEncoded" : {
  "title" : "Attribute Cookie Encode",
  "description" : "Indicates if the value of the attribute should be URL encoded before being set
as a cookie. (property name: com.sun.identity.agents.config.attribute.cookie.encode) <br>Hot-swap:
Yes",

```

```

    "propertyOrder" : 8500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "privilegedAttributeMap" : {
    "title" : "Privileged Attribute Mapping",
    "description" : "Map if using Enable Privileged Attribute Mapping. (property name:
com.sun.identity.agents.config.privileged.attribute.mapping) <br>Hot-swap: Yes <br> Examples: <br>
To map UUID id=manager,ou=group,dc=openam,dc=forgerock,dc=org to the principal name am_manager_role
specified in webapp's deployment descriptor: enter id=manager,ou=group,dc=openam,dc=forgerock,dc=org
in Map Key field, and enter am_manager_role in Corresponding Map Value field. <br> To map UUID
id=employee,ou=group,dc=openam,dc=forgerock,dc=org to the principal name am_employee_role specified
in webapp's deployment descriptor: enter id=employee,ou=group,dc=openam,dc=forgerock,dc=org in Map
Key field, and enter am_employee_role in Corresponding Map Value field.",
    "propertyOrder" : 9900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "policyActionBooleanValues" : {
    "title" : "Policy Client Boolean Action Values",
    "description" : "Boolean action values for policy action names. (property name:
com.sun.identity.policy.client.booleanActionValues) <br>Hot-swap: No",
    "propertyOrder" : 11500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authServiceHost" : {
    "title" : "OpenAM Authentication Service Host Name",
    "description" : "Host name to be used by the OpenAM authentication service. (property name:
com.iplanet.am.server.host) <br>Hot-swap: No",
    "propertyOrder" : 11000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoClockSkew" : {
    "title" : "CDSSO Clock Skew",
    "description" : "Time in seconds to be used by the Agent to determine the validity of the CDSSO
AuthnResponse assertion. (property name: com.sun.identity.agents.config.cdsso.clock.skew) <br>Hot-
swap: Yes",
    "propertyOrder" : 5300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "cookieResetNames" : {
    "title" : "Cookies Reset Name List",
    "description" : "Cookie names that will be reset by the Agent if Cookie Reset is enabled.
(property name: com.sun.identity.agents.config.cdsso.cookie.reset.name) <br>Hot-swap: Yes",
    "propertyOrder" : 4700,
    "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "amLoginUrl" : {
    "title" : "OpenAM Login URL",
    "description" : "OpenAM login page URL. (property name:
com.sun.identity.agents.config.login.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Login",
    "propertyOrder" : 3700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "urlPolicyEnvPostParameters" : {
    "title" : "URL Policy Env POST Parameters",
    "description" : "List of HTTP POST request parameters whose names and values will
be set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.post.param) <br>Hot-swap: Yes <br> Examples: <br> name <br>
phonenumber",
    "propertyOrder" : 11900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "localeCountry" : {
    "title" : "Locale Country",
    "description" : "(property name: com.sun.identity.agents.config.locale.country) <br>Hot-swap:
No",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "urlPolicyEnvGetParameters" : {
    "title" : "URL Policy Env GET Parameters",
    "description" : "List of HTTP GET request parameters whose names and values will be
set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.get.param) <br>Hot-swap: Yes <br> Examples: <br> name <br>
phonenumber",
    "propertyOrder" : 11800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "auditAccessType" : {
    "title" : "Audit Access Types",

```

```

    "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype) <br>Hot-swap: Yes",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jbossWebAuthenticationAvailable" : {
    "title" : "WebAuthentication Available",
    "description" : "Enable agent to make programmatic authentication with
the JBoss web container using WebAuthentication feature. (property name:
com.sun.identity.agents.config.jboss.webauth.available) <br>Hot-swap: Yes",
    "propertyOrder" : 12300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdsso" : {
    "title" : "Cross Domain SSO",
    "description" : "Enables Cross Domain Single SignOn. (property name:
com.sun.identity.agents.config.cdsso.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logoutRequestParameters" : {
    "title" : "Logout Request Parameter",
    "description" : "An application-specific Map that identifies a parameter
which when present in the HTTP request indicates a logout event. (property name:
com.sun.identity.agents.config.logout.request.param) <br>Valid key: the web application name.
<br>Valid value: the logout request parameter. <br>For this property, a global value can be set to
apply to all the applications that don't have their own specific logout request parameter. <br>Hot-
swap: Yes <br> Examples: <br>To set a global application logout request parameter: leave Map Key
field empty, and enter the global application logout request parameter logoutparam in Corresponding
Map Value field. <br> To set the logout request parameter for application BankApp: enter BankApp in
Map Key field, and enter the logout request parameter logoutparam in Corresponding Map Value field.",
    "propertyOrder" : 6100,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "responseAttributeFetchMode" : {
    "title" : "Response Attribute Fetch Mode",
    "description" : "The mode of fetching policy response attributes. (property name:
com.sun.identity.agents.config.response.attribute.fetch.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 9100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "alternativeAgentHostname" : {
    "title" : "Alternative Agent Host Name",

```

```

    "description" : "Host name identifying the Agent protected server to the client browsers if
different from the actual host name. (property name: com.sun.identity.agents.config.agent.host)
<br>Hot-swap: Yes",
    "propertyOrder" : 4100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "legacyUserAgentSupport" : {
    "title" : "Legacy User Agent Support Enable",
    "description" : "Enables support for legacy user agents (browser). (property name:
com.sun.identity.agents.config.legacy.support.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 6700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "loginAttemptLimit" : {
    "title" : "Login Attempt Limit",
    "description" : "Limit of failed login attempts for a user's single browser session until
triggering the blocking of the user request. Value of 0 disables this feature. (property name:
com.sun.identity.agents.config.login.attempt.limit) <br>Hot-swap: Yes",
    "propertyOrder" : 4400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "policyClientResourceComparators" : {
    "title" : "Policy Client Resource Comparators",
    "description" : "Resource Comparators to be used for different service names. (property name:
com.sun.identity.policy.client.resourceComparators) <br>Hot-swap: No",
    "propertyOrder" : 11600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Password",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "notEnforcedUriCacheSize" : {
    "title" : "Not Enforced URIs Cache Size",
    "description" : "Size of the cache to be used if caching of not enforced URI list evaluation
results is enabled. (property name: com.sun.identity.agents.config.notenforced.uri.cache.size)
<br>Hot-swap: Yes",
    "propertyOrder" : 7800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "policyClientClockSkew" : {
    "title" : "Policy Client Clock Skew",

```



```

        "description" : "Time in seconds which is allowed to accommodate the time difference
between the OpenAM server machine and the remote policy client machine. (property name:
com.sun.identity.policy.client.clockSkew) <br>Hot-swap: No",
        "propertyOrder" : 11700,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "notEnforcedIpsCacheSize" : {
        "title" : "Not Enforced IP Cache Size",
        "description" : "Size of the cache to be used if Not Enforced IP Cache Flag is enabled.
(property name: com.sun.identity.agents.config.notenforced.ip.cache.size) <br>Hot-swap: Yes",
        "propertyOrder" : 8200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "portCheckSetting" : {
        "title" : "Port Check Setting",
        "description" : "Map of port versus protocol entries with the key being the listening port
number and value being the listening protocol to be used by the Agent to identify requests with
invalid port numbers. (property name: com.sun.identity.agents.config.port.check.setting) <br>Hot-
swap: Yes <br> Example: <br> To map port 80 to protocol http: enter 80 in Map Key field, and enter
http in Corresponding Map Value field.",
        "propertyOrder" : 7400,
        "required" : true,
        "patternProperties" : {
            ".*" : {
                "type" : "string"
            }
        },
        "type" : "object",
        "exampleValue" : ""
    },
    "userAttributeName" : {
        "title" : "User Attribute Name",
        "description" : "Name of the attribute which contains the user-ID. (property name:
com.sun.identity.agents.config.user.attribute.name) <br>Hot-swap: Yes",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "policyEvaluationApplication" : {
        "title" : "Application",
        "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.openam.agents.config.policy.evaluation.application) <br>Hot-swap: Yes",
        "propertyOrder" : 5500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

### 1.63.1.2. delete

Usage:

```
am> delete J2EEAgentGroups --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.63.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action J2EEAgentGroups --realm Realm --actionName getAllTypes
```

### 1.63.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action J2EEAgentGroups --realm Realm --actionName getCreatableTypes
```

### 1.63.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action J2EEAgentGroups --realm Realm --actionName nextdescendents
```

### 1.63.1.6. query

Querying the agent groups of a specific type

Usage:

```
am> query J2EEAgentGroups --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.63.1.7. read

Usage:

```
am> read J2EEAgentGroups --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.63.1.8. update

Usage:

```
am> update J2EEAgentGroups --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userTokenName" : {
      "title" : "User Token Name",
      "description" : "Session property name for user-ID of the authenticated user in session.
(property name: com.sun.identity.agents.config.user.token) <br>Hot-swap: Yes",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "webServiceAuthenticator" : {
      "title" : "Web Service Authenticator",
      "description" : "An implementation class of interface
com.sun.identity.agents.filter.IWebServiceAuthenticator that can be used to authenticate web-service
requests. (property name: com.sun.identity.agents.config.webservice.authenticator) <br>Hot-swap:
Yes",
      "propertyOrder" : 2300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "cdssoRootUrl" : {
      "title" : "Agent Root URL for CDSSO",
      "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
      "propertyOrder" : 22700,
      "required" : true,
      "items" : {
        "type" : "string"
      }
    }
  }
}
```

```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "defaultPrivilegedAttributes" : {
    "title" : "Default Privileged Attribute",
    "description" : "List of privileged attributes that will be granted to all users who have a
valid OpenAM session. (property name: com.sun.identity.agents.config.default.privileged.attribute)
<br>Hot-swap: Yes <br> Example: <br> AUTHENTICATED_USERS",
    "propertyOrder" : 9400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "cdssoTrustedIdProvider" : {
    "title" : "CDSSO Trusted ID Provider",
    "description" : "List of OpenAM Server/ID providers that should be trusted
by the agent, when evaluating the CDC Liberty Responses. (property name:
com.sun.identity.agents.config.cdsso.trusted.id.provider) <br>Hot-swap: Yes <br> Example: <br>
http://host:port/opensso/cdcservlet",
    "propertyOrder" : 5600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "notEnforcedIpsCacheEnabled" : {
    "title" : "Not Enforced IP Cache Flag",
    "description" : "Enable caching of not-enforced IP list evaluation results. (property name:
com.sun.identity.agents.config.notenforced.ip.cache.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 8100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "postDataStickySessionKeyValue" : {
    "title" : "PDP Stickysession key-value",
    "description" : "The provided key-value pair will be used for adding to
the URL or creating the cookie. <br>Example: <br>Set 'lb=server1' to append to
the querystring or to have 'lb' cookie with 'server1' value. (property name:
com.sun.identity.agents.config.postdata.preserve.stickysession.value)",
    "propertyOrder" : 13500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "repositoryLocation" : {
    "title" : "Location of Agent Configuration Repository",
    "description" : "Indicates agent's configuration located either on agent's host or centrally on
OpenAM server.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}

```

```

    },
    "postDataCacheTtl" : {
      "title" : "PDP entry TTL",
      "description" : "This value tells how long a given POST entry should be stored
in the local cache (in milliseconds), default value is 300000. (property name:
com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl)",
      "propertyOrder" : 13300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "redirectAttemptLimit" : {
      "title" : "Redirect Attempt Limit",
      "description" : "Number of successive single point redirects that a user can make using a
single browser session which will trigger the blocking of the user request. Set to 0 to disable this
feature. (property name: com.sun.identity.agents.config.redirect.attempt.limit) <br>Hot-swap: Yes",
      "propertyOrder" : 7100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useRedirectForCompositeAdvice" : {
      "title" : "Use HTTP-Redirect for composite advice",
      "description" : "Configure remote policy client to use HTTP-redirect instead of HTTP-POST
for composite advices. (property name: com.sun.identity.agents.config.policy.advice.use.redirect)
<br>Hot-swap: Yes",
      "propertyOrder" : 13000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "auditLogLocation" : {
      "title" : "Audit Log Location",
      "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition) <br>Hot-swap: Yes",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "privilegedAttributeMappingEnabled" : {
      "title" : "Enable Privileged Attribute Mapping",
      "description" : "Enable a mapping from the original value of an attribute to another value. To
satisfy container-specific restrictions on character set being used in certain configuration files.
(property name: com.sun.identity.agents.config.privileged.attribute.mapping.enable) <br>Hot-swap:
Yes",
      "propertyOrder" : 9800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "localeLanguage" : {
      "title" : "Locale Language",
      "description" : "(property name: com.sun.identity.agents.config.locale.language) <br>Hot-swap:
No",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }

```

```

    },
    "postDataStickySessionMode" : {
      "title" : "PDP Stickysession mode",
      "description" : "The PDP mechanism needs sticky loadbalancing, the URL mode will
append a querystring, while the Cookie mode will create a cookie. (property name:
com.sun.identity.agents.config.postdata.preserve.stickysession.mode)",
      "propertyOrder" : 13400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientHostnameHeader" : {
      "title" : "Client Hostname Header",
      "description" : "HTTP header name that holds the Hostname of the client. (property name:
com.sun.identity.agents.config.client.hostname.header) <br>Hot-swap: Yes",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "privilegedSessionAttribute" : {
      "title" : "Privileged Session Attribute",
      "description" : "List of session property names which hold privileged attributes for the
authenticated user. (property name: com.sun.identity.agents.config.privileged.session.attribute)
<br>Hot-swap: Yes <br> Example: <br> UserToken",
      "propertyOrder" : 9700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "xssDetectionRedirectUri" : {
      "title" : "XSS detection redirect URI",
      "description" : "An application-specific Map that identifies a URI of the customized page if
XSS code has been detected. (property name: com.sun.identity.agents.config.xss.redirect.uri) <br>Hot-
swap: Yes <br>Examples: <br>To set a redirect target for application BankApp: enter BankApp in Map Key
field, and enter a redirect URI in Corresponding Map Value field.",
      "propertyOrder" : 12900,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "responseAttributeMap" : {
      "title" : "Response Attribute Mapping",
      "description" : "Maps the policy response attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.response.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field,
and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
      "propertyOrder" : 9200,
      "required" : true,
      "patternProperties" : {

```

```

        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"logoutEntryUri" : {
    "title" : "Logout Entry URI",
    "description" : "An application-specific Map that identifies a URI to be used as an entry point
after successful logout and subsequent successful authentication if applicable. (property name:
com.sun.identity.agents.config.logout.entry.uri) <br>Valid key: the web application name. <br>Valid
value: the logout entry URI. <br>For this property, a global value can be set to apply to all the
applications that don't have their own specific logout entry URI. <br>Hot-swap: Yes <br> Examples:
<br>To set a global application logout entry URI: leave Map Key field empty, and enter the global
application logout entry URI /welcome.html in Corresponding Map Value field. <br> To set the logout
entry URI for application BankApp: enter BankApp in Map Key field, and enter the logout entry URI /
BankApp/welcome.html in Corresponding Map Value field.",
    "propertyOrder" : 6300,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"loginErrorUri" : {
    "title" : "Login Error URI",
    "description" : "List of absolute URIs corresponding to an application's web.xml form-error-
page element. (property name: com.sun.identity.agents.config.login.error.uri) <br>Hot-swap: Yes <br>
Example: <br> /BankApp/jsp/error.jsp",
    "propertyOrder" : 2900,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"webServiceEndpoints" : {
    "title" : "Web Service End Points",
    "description" : "A list of Web Application end points that represent Web Services. (property
name: com.sun.identity.agents.config.webservice.endpoint) <br>Hot-swap: Yes",
    "propertyOrder" : 2100,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"cookieResetPaths" : {
    "title" : "Cookies Reset Path Map",
    "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the path of this cookie to be used when a reset event occurs. (property name:
com.sun.identity.agents.config.cookie.reset.path) <br>Hot-swap: Yes",
    "propertyOrder" : 4900,

```

```

    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "sessionAttributeFetchMode" : {
    "title" : "Session Attribute Fetch Mode",
    "description" : "The mode of fetching session attributes. (property name: com.sun.identity.agents.config.session.attribute.fetch.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 8900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "useInternalLogin" : {
    "title" : "Use Internal Login",
    "description" : "Set to false if want to customize Login Content File instead of default internal content provided. (property name: com.sun.identity.agents.config.login.use.internal) <br>Hot-swap: Yes",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyClientPollingInterval" : {
    "title" : "Policy Client Polling Interval",
    "description" : "Duration in minutes after which the cached entries are refreshed by remote policy client. (property name: com.sun.identity.agents.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 11300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "policyNotifications" : {
    "title" : "Enable Policy Notifications",
    "description" : "Enable Notifications for remote policy client. (property name: com.sun.identity.agents.notification.enabled) <br>Hot-swap: No",
    "propertyOrder" : 11200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "portCheckEnabled" : {
    "title" : "Port Check Enable",
    "description" : "Indicates if port check functionality is enabled or disabled. (property name: com.sun.identity.agents.config.port.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 7200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "httpSessionBinding" : {
    "title" : "HTTP Session Binding",

```



```

        "description" : "If true will invalidate the http session when login has failed, user
has no SSO session, or principal user name does not match SSO user name. (property name:
com.sun.identity.agents.config.httpsession.binding) <br>Hot-swap: Yes",
        "propertyOrder" : 3500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "loginFormUri" : {
        "title" : "Login Form URI",
        "description" : "List of absolute URIs corresponding to an application's web.xml form-login-page
element. (property name: com.sun.identity.agents.config.login.form) <br>Hot-swap: Yes <br> Example:
<br> /BankApp/jsp/login.jsp",
        "propertyOrder" : 2800,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "webServiceAuthorizationErrorContentFile" : {
        "title" : "Web Service Authorization Error Content File",
        "description" : "The name of file that contains content used by the
Agent to generate an authorization error fault for clients. (property name:
com.sun.identity.agents.config.webservice.autherror.content) <br>Hot-swap: Yes",
        "propertyOrder" : 2600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "ignorePathInfo" : {
        "title" : "Ignore Path Info in Request URL",
        "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info) <br>Hot-swap: Yes",
        "propertyOrder" : 18600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "applicationLogoutUri" : {
        "title" : "Application Logout URI",
        "description" : "An application-specific Map that identifies a request URI which indicates
a logout event. (property name: com.sun.identity.agents.config.logout.uri) <br>Valid key: the web
application name. <br>Valid value: the application logout URI. <br>For this property, a global value
can be set to apply to all the applications that don't have their own specific logout URI. <br>Hot-
swap: Yes <br> Examples: <br>To set a global application logout URI: leave Map Key field empty, and
enter the global application logout URI /logout.jsp in Corresponding Map Value field. <br> To set the
logout URI for application BankApp: enter BankApp in Map Key field, and enter the application logout
URI /BankApp/logout.jsp in Corresponding Map Value field.",
        "propertyOrder" : 6000,
        "required" : true,
        "patternProperties" : {
            ".*" : {
                "type" : "string"
            }
        },
        "type" : "object",
    }

```

```

    "exampleValue" : ""
  },
  "agentNotificationUrl" : {
    "title" : "Agent Notification URL",
    "description" : "URL used by agent to register notification listeners. (property name:
com.sun.identity.client.notification.url) <br>Hot-swap: No",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "probeLogoutUrl" : {
    "title" : "Logout URL Probe",
    "description" : "Specifies if agent will check the availability of these urls before redirecting
to them. (property name: com.sun.identity.agents.config.logout.url.probe.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 12600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "localAuditRotationSize" : {
    "title" : "Local Audit Log Rotation Size",
    "description" : "Size limit when a local audit log file is rotated to a new file. (property
name: com.sun.identity.agents.config.local.log.size) <br>Hot-swap: Yes",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "authServiceProtocol" : {
    "title" : "OpenAM Authentication Service Protocol",
    "description" : "Protocol to be used by the OpenAM authentication service. (property name:
com.iplanet.am.server.protocol) <br>Hot-swap: No",
    "propertyOrder" : 10900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cookieResetDomains" : {
    "title" : "Cookies Reset Domain Map",
    "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the domain of this cookie to be used when a reset event occurs. (property name:
com.sun.identity.agents.config.cookie.reset.domain) <br>Hot-swap: Yes",
    "propertyOrder" : 4800,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "possibleXssCodeElements" : {
    "title" : "Possible XSS code elements",
    "description" : "If one of these strings occurs in the request, the client is redirected to an
error page. (property name: com.sun.identity.agents.config.xss.code.elements) <br>Hot-swap: Yes",
    "propertyOrder" : 12800,
    "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "debugLevel" : {
    "title" : "Agent Debug Level",
    "description" : "Specifies type of agent debug messages to log. (property name: com.ipplanet.services.debug.level) <br>Hot-swap: Yes",
    "propertyOrder" : 10000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "urlPolicyEnvJsessionParameters" : {
    "title" : "URL Policy Env jsession Parameters",
    "description" : "List of HTTP SESSION attributes whose names and values will be set in the environment map for URL policy evaluation at OpenAM server. (property name: com.sun.identity.agents.config.policy.env.jsession.param) <br>Hot-swap: Yes <br> Examples: <br> name <br> phonenumber",
    "propertyOrder" : 12000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "fqdnMapping" : {
    "title" : "FQDN Virtual Host Map",
    "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN to access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>Hot-swap: Yes <br> Examples: <br> To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field and rst.hostname.com in the Corresponding Map Value field.",
    "propertyOrder" : 6600,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "probeLoginUrl" : {
    "title" : "Login URL Probe",
    "description" : "Specifies if agent will check the availability of these urls before redirecting to them. (property name: com.sun.identity.agents.config.login.url.probe.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 3900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invertNotEnforcedUris" : {
    "title" : "Invert Not Enforced URIs",

```

```

    "description" : "Inverts protection of URIs specified in Not Enforced URIs list. When set
to true, it indicates that the URIs specified should be enforced and all other URIs should be
not enforced by the Agent. (property name: com.sun.identity.agents.config.notenforced.uri.invert)
<br>Hot-swap: Yes",
    "propertyOrder" : 7600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"headerAttributeDateFormat" : {
    "title" : "Fetch Attribute Date Format",
    "description" : "Format of date attribute values to be used when the attribute is
being set as HTTP header. Format is based on java.text.SimpleDateFormat. (property name:
com.sun.identity.agents.config.attribute.date.format) <br>Hot-swap: Yes",
    "propertyOrder" : 8400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"agentConfigChangeNotificationsEnabled" : {
    "title" : "Agent Configuration Change Notification",
    "description" : "Enable agent to receive notification messages from OpenAM server for
configuration changes. (property name: com.sun.identity.agents.config.change.notification.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 12100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"logoutUrlPrioritized" : {
    "title" : "Logout URL Prioritized",
    "description" : "Specifies if failover sequence for Logout URLs should be prioritized as defined
in the OpenAM Login URL list. (property name: com.sun.identity.agents.config.logout.url.prioritized)
<br>Hot-swap: Yes",
    "propertyOrder" : 12500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"customLogoutHandlers" : {
    "title" : "Custom Logout Handler",
    "description" : "Application specific logout handler to log out a user with the application
server. (property name: com.sun.identity.agents.config.logout.handler) <br>Valid key: the web
application name. <br>Valid value: the logout handler class name. <br>Hot-swap: Yes <br> Example:
<br>To set logout handler for application BankApp: enter BankApp in Map Key field, and enter logout
handler class name BankLogoutHandler in Corresponding Map Value field.",
    "propertyOrder" : 3300,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"cookieResetEnabled" : {
    "title" : "Cookie Reset",

```

```

    "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 4600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "portCheckFile" : {
    "title" : "Port Check File",
    "description" : "Name or complete path of a file that has the necessary content needed to handle
requests that need port correction. (property name: com.sun.identity.agents.config.port.check.file)
<br>Hot-swap: Yes",
    "propertyOrder" : 7300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sessionAttributeMap" : {
    "title" : "Session Attribute Mapping",
    "description" : "Maps the session attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map
Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
    "propertyOrder" : 9000,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "customResponseHeader" : {
    "title" : "Custom Response Header",
    "description" : "Map specifies the custom headers that are set by the Agent on the client
browser. The key is the header name and the value represents the header value. (property name:
com.sun.identity.agents.config.response.header) <br>Hot-swap: Yes <br> Example: <br> To set the
custom header Cache-Control to value no-cache: enter Cache-Control in Map Key field, and enter no-
cache in Corresponding Map Value field.",
    "propertyOrder" : 7000,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "amLogoutUrl" : {
    "title" : "OpenAM Logout URL",
    "description" : "OpenAM logout page URL. (property name:
com.sun.identity.agents.config.logout.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opnsso/UI/Logout",
    "propertyOrder" : 12400,
    "required" : true,
    "items" : {

```

```

    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"userDataCachePollingTime" : {
  "title" : "User Data Cache Polling Time",
  "description" : "Cache update time in minutes for user management data. If set to '0' no updates happen. (property name: com.iplanet.am.sdk.remote.pollingTime) <br>Hot-swap: No",
  "propertyOrder" : 10600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"resourceAccessDeniedUri" : {
  "title" : "Resource Access Denied URI",
  "description" : "An application-specific Map that identifies a URI of the customized access denied page. (property name: com.sun.identity.agents.config.access.denied.uri) <br>Valid key: the web application name. <br>Valid value: the customized application access denied page URI. <br>For this property, a global value can be set to apply to all the applications that don't have their own specific access denied page. <br>Hot-swap: Yes <br> Examples: <br>To set a global access denied page: leave Map Key field empty, and enter the global access denied page URI /sample/accessdenied.html in Corresponding Map Value field. <br> To set the access denied page URI for application BankApp: enter BankApp in Map Key field, and enter the application access denied page URI /BankApp/accessdenied.html in Corresponding Map Value field.",
  "propertyOrder" : 2700,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"serviceDataCacheTime" : {
  "title" : "Service Data Cache Time",
  "description" : "Cache update time in minutes for service configuration data. If set to '0' no updates happen. (property name: com.sun.identity.sm.cacheTime) <br>Hot-swap: No",
  "propertyOrder" : 10800,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"status" : {
  "title" : "Status",
  "description" : "Status of the agent configuration.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"loginProbeTimeout" : {
  "title" : "Login URL Probe Timeout",
  "description" : "The connect timeout value in milliseconds, if also Login URL Probe is set to true. (property name: com.sun.identity.agents.config.login.url.probe.timeout) <br>Hot-swap: Yes",
  "propertyOrder" : 4000,
  "required" : true,
  "type" : "integer",

```

```

    "exampleValue" : ""
  },
  "privilegedAttributeType" : {
    "title" : "Privileged Attribute Type",
    "description" : "List of privileged attribute types that will be fetched for each user.
(property name: com.sun.identity.agents.config.privileged.attribute.type) <br>Hot-swap: Yes <br>
Example: <br> Group",
    "propertyOrder" : 9500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "loginUrlPrioritized" : {
    "title" : "Login URL Prioritized",
    "description" : "Specifies if failover sequence for Login URLs or CDSO URLs
should be prioritized as defined in the OpenAM Login URL list. (property name:
com.sun.identity.agents.config.login.url.prioritized) <br>Hot-swap: Yes",
    "propertyOrder" : 3800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyEvaluationRealm" : {
    "title" : "Realm",
    "description" : "Which realm to start evaluating from. (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm) <br>Hot-swap: Yes",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "filterMode" : {
    "title" : "Agent Filter Mode",
    "description" : "Specifies the mode of operation of the Filter. (property name:
com.sun.identity.agents.config.filter.mode) <br>Valid key: the web application name. <br>Valid
values: ALL, J2EE_POLICY, URL_POLICY, SSO_ONLY, NONE <br>For this property, a global value can be
set to apply to all the applications that don't have their own specific filter mode. <br>Hot-swap:
No <br>Examples: <br>To set ALL as the global filter mode: leave Map Key field empty, and enter ALL
in Corresponding Map Value field. <br>To set URL_POLICY as the filter mode for application BankApp:
enter BankApp in Map Key field, and enter URL_POLICY in Corresponding Map Value field.",
    "propertyOrder" : 500,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "userMappingMode" : {
    "title" : "User Mapping Mode",
    "description" : "Specifies mechanism agent uses to determine user-ID. (property name:
com.sun.identity.agents.config.user.mapping.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 600,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributeMap" : {
    "title" : "Profile Attribute Mapping",
    "description" : "Maps the profile attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.profile.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field,
and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate the value of profile
attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in
Corresponding Map Value field.",
    "propertyOrder" : 8800,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"webServiceResponseProcessor" : {
  "title" : "Web Service Response Processor",
  "description" : "An implementation class of interface
com.sun.identity.agents.filter.IWebServiceResponseProcessor that can be used to process the web-
service responses. (property name: com.sun.identity.agents.config.webservice.responseprocessor)
<br>Hot-swap: Yes",
  "propertyOrder" : 2400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"cdssoRedirectUri" : {
  "title" : "CDSSO Redirect URI",
  "description" : "An intermediate URI that is used by the Agent for processing CDSSO requests.
(property name: com.sun.identity.agents.config.cdsso.redirect.uri) <br>Hot-swap: Yes",
  "propertyOrder" : 5100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"ssoCacheEnabled" : {
  "title" : "SSO Cache Enable",
  "description" : "Specifies if the SSO Cache is active for the agent.
Cache is used through public APIs exposed by the agent SDK. (property name:
com.sun.identity.agents.config.amsso.cache.enable) <br>Hot-swap: Yes",
  "propertyOrder" : 4500,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"bypassPrincipalList" : {
  "title" : "Bypass Principal List",
  "description" : "List of principals that are bypassed by the Agent for authentication and search
purposes. (property name: com.sun.identity.agents.config.bypass.principal) <br>Hot-swap: Yes <br>
Examples: <br> guest <br> testuser",
  "propertyOrder" : 9300,
  "required" : true,

```



```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "gotoParameterName" : {
    "title" : "Goto Parameter Name",
    "description" : "Property used only when CDSSO is enabled. Default value should
be changed only when the login URL has a landing page specified <br> Example :
com.sun.identity.agents.config.cdssso.cdcservlet.url = http://host:port/opensso/cdcservlet?
goto=http://agent:port/landing.jsp <br> The parameter is used by the Agent to append the original
request URL to this cdcservlet URL. This parameter is consumed by the landing page to redirect to
the original URL. (property name: com.sun.identity.agents.config.redirect.param) <br>Hot-swap: Yes
<br> Example: com.sun.identity.agents.config.redirect.param = goto2<br> The complete URL sent for
authentication will be <br> http://host:port/opensso/cdcservlet?goto=http://agent:port/landing.jsp?
goto2=http://agent:port/original.jsp",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userDataCacheNotifications" : {
    "title" : "Enable Notification of User Data Caches",
    "description" : "Enable notifications for amsdk and IdRepo Caches. (property name:
com.sun.identity.idm.remote.notification.enabled) <br>Hot-swap: No",
    "propertyOrder" : 10500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "legacyRedirectUri" : {
    "title" : "Legacy User Agent Redirect URI",
    "description" : "An intermediate URI used by the Agent to redirect legacy user agent requests.
(property name: com.sun.identity.agents.config.legacy.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 6900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authServicePort" : {
    "title" : "OpenAM Authentication Service Port",
    "description" : "Port to be used by the OpenAM authentication service. (property name:
com.ipplanet.am.server.port) <br>Hot-swap: No",
    "propertyOrder" : 11100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notEnforcedUrisCacheEnabled" : {
    "title" : "Not Enforced URIs Cache Enabled",
    "description" : "Enables the caching of the Not Enforced URIs list evaluation results. (property
name: com.sun.identity.agents.config.notenforced.uri.cache.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 7700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logoutProbeTimeout" : {

```

```

    "title" : "Logout URL Probe Timeout",
    "description" : "The connect timeout value in milliseconds, if also Logout URL Probe is set to
true. (property name: com.sun.identity.agents.config.logout.url.probe.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 12700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "policyClientCacheMode" : {
    "title" : "Policy Client Cache Mode",
    "description" : "Mode of caching to be used by remote policy client. (property name:
com.sun.identity.policy.client.cacheMode) <br>Hot-swap: No",
    "propertyOrder" : 11400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributeFetchMode" : {
    "title" : "Profile Attribute Fetch Mode",
    "description" : "The mode of fetching profile attributes. (property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 8700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "encryptionProvider" : {
    "title" : "Encryption Provider",
    "description" : "Specifies the encryption provider implementation to be used by the Agent.
(property name: com.iplanet.security.encryptor) <br>Hot-swap: No",
    "propertyOrder" : 10400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "fqdnDefault" : {
    "title" : "FQDN Default",
    "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default) <br>Hot-swap: Yes",
    "propertyOrder" : 6500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "alternativeAgentPort" : {
    "title" : "Alternative Agent Port Name",
    "description" : "Port number identifying the Agent protected server listening port
to the client browsers if different from the actual listening port. (property name:
com.sun.identity.agents.config.agent.port) <br>Hot-swap: Yes",
    "propertyOrder" : 4200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "customVerificationHandlers" : {
    "title" : "Custom Verification Handler",
    "description" : "Application specific verification handler to validate the user credentials with
the local repository. (property name: com.sun.identity.agents.config.verification.handler) <br>Valid
key: the web application name. <br>Valid value: the verification handler class name. <br>Hot-swap:

```

Yes <br> Example: <br> To set verification handler for application BankApp: enter BankApp in Map Key field, and enter verification handler class name BankVerificationHandler in Corresponding Map Value field.",

```

    "propertyOrder" : 3400,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "notEnforcedUriRefreshSessionIdleTime" : {
    "title" : "Refresh Session Idle Time",
    "description" : "Indicates if opensso session idle time should be refreshed or reset for not enforced URIs. (property name: com.sun.identity.agents.config.notenforced.refresh.session.idletime) <br>Hot-swap: Yes",
    "propertyOrder" : 8600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "webServiceEnabled" : {
    "title" : "Web Service Enable",
    "description" : "Flag specifies if Web Service processing is enabled. (property name: com.sun.identity.agents.config.webservice.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "alternativeAgentProtocol" : {
    "title" : "Alternative Agent Protocol",
    "description" : "Protocol being used (http/https) by the client browsers to communicate with the Agent protected server if different from the actual protocol used by the server. (property name: com.sun.identity.agents.config.agent.protocol) <br>Hot-swap: Yes",
    "propertyOrder" : 4300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "privilegedAttributesToLowerCase" : {
    "title" : "Privileged Attributes To Lower Case",
    "description" : "Maps the privileged attribute types to whether they should be converted to lowercase. (property name: com.sun.identity.agents.config.privileged.attribute.lowercase) <br>Valid Keys: the privileged attribute types, such as Group, Role. <br>Valid value: true, false. <br>Hot-swap: Yes <br> Example: <br> Enter Group in Map Key field, and enter false in Corresponding Map Value field.",
    "propertyOrder" : 9600,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
},

```

```

"notEnforcedUri" : {
  "title" : "Not Enforced URIs",
  "description" : "List of URIs for which protection is not enforced by the Agent. (property
name: com.sun.identity.agents.config.notenforced.uri) <br>Hot-swap: Yes <br> Examples: <br> /BankApp/
public/* <br> /BankApp/images/*",
  "propertyOrder" : 7500,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"remoteLogFilename" : {
  "title" : "Remote Log File Name",
  "description" : "Name of file stored on OpenAM server that contains agent audit messages.
(property name: com.sun.identity.agents.config.remote.logfile) <br>Hot-swap: Yes",
  "propertyOrder" : 1700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userPrincipalFlag" : {
  "title" : "User Principal Flag",
  "description" : "Use principal instead of just the user-ID for authenticating the user.
(property name: com.sun.identity.agents.config.user.principal) <br>Hot-swap: Yes",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"legacyUserAgentList" : {
  "title" : "Legacy User Agent List",
  "description" : "List of user agent header values that identify legacy
browsers. Entries in this list can have wild card character '*'. (property name:
com.sun.identity.agents.config.legacy.user.agent) <br>Hot-swap: Yes",
  "propertyOrder" : 6800,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"serviceDataCacheNotifications" : {
  "title" : "Enable Notification of Service Data Caches",
  "description" : "Enable the notifications for service management caches. (property name:
com.sun.identity.sm.notification.enabled) <br>Hot-swap: No",
  "propertyOrder" : 10700,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"cdssoDomainList" : {
  "title" : "CDSSO Domain List",
  "description" : "Domains for which cookies have to be set in a CDSSO scenario. (property name:
com.sun.identity.agents.config.cdsso.domain) <br>Hot-swap: Yes <br> Example: <br> .sun.com",
  "propertyOrder" : 5800,
  "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "clientPollingPeriod" : {
    "title" : "Client Polling Period",
    "description" : "Time in seconds after which the session client will request update of cached session information from the server. (property name: com.iplanet.am.session.client.polling.period) <br>Hot-swap: No",
    "propertyOrder" : 10300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "enableClientPolling" : {
    "title" : "Enable Client Polling",
    "description" : "Specifies if the session client must use polling for updating session information and not depend upon server notifications. (property name: com.iplanet.am.session.client.polling.enable) <br>Hot-swap: No",
    "propertyOrder" : 10200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "loginContentFile" : {
    "title" : "Login Content File Name",
    "description" : "Complete path and name of custom login content file. (property name: com.sun.identity.agents.config.login.content.file) <br>Hot-swap: Yes",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "applicationLogoutHandlers" : {
    "title" : "Application Logout Handler",
    "description" : "An application-specific Map that identifies a handler to be used for logout processing. (property name: com.sun.identity.agents.config.logout.application.handler) <br>Valid key: the web application name. <br>Valid value: the application logout handler class name. <br>For this property, a global value can be set to apply to all the applications that don't have their own specific logout handler. <br>Hot-swap: Yes <br> Examples: <br>To set a global application logout handler: leave Map Key field empty, and enter the global application logout handler class name GlobalApplicationLogoutHandler in Corresponding Map Value field. <br>To set the logout handler for application BankApp: enter BankApp in Map Key field, and enter the application logout handler class name BankAppLogoutHandler in Corresponding Map Value field.",
    "propertyOrder" : 5900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "logoutIntrospection" : {
    "title" : "Logout Introspect Enabled",

```

```

    "description" : "Allows the Agent to search HTTP request body to locate logout parameter.
(property name: com.sun.identity.agents.config.logout.introspect.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 6200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "configurationReloadInterval" : {
    "title" : "Configuration Reload Interval",
    "description" : "Interval in seconds between configuration reloads. (property name:
com.sun.identity.agents.config.load.interval) <br>Hot-swap: Yes",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "amCookieName" : {
    "title" : "Cookie Name",
    "description" : "Name of the SSO Token cookie used between the OpenAM server and the Agent.
(property name: com.ipplanet.am.cookie.name) <br>Hot-swap: No",
    "propertyOrder" : 10100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoSecureCookies" : {
    "title" : "CDSSO Secure Enable",
    "description" : "The SSO Token cookie set by the agent in the different domains in CDSSO mode
will be marked secure. Only transmitted if the communications channel with host is a secure one.
(property name: com.sun.identity.agents.config.cdsso.secure.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "clientIpHeader" : {
    "title" : "Client IP Address Header",
    "description" : "HTTP header name that holds the IP address of the client. (property name:
com.sun.identity.agents.config.client.ip.header) <br>Hot-swap: Yes",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "customAuthenticationHandlers" : {
    "title" : "Custom Authentication Handler",
    "description" : "Application specific authentication handler to authenticate the logged on user
with the application server. (property name: com.sun.identity.agents.config.auth.handler) <br>Valid
key: the web application name. <br>Valid value: the authentication handler class name. <br>Hot-swap:
Yes <br>Example: <br>To set authentication handler for application BankApp: enter BankApp in Map
Key field, and enter authentication handler class name BankAuthHandler in Corresponding Map Value
field.",
    "propertyOrder" : 3200,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  },
},

```

```

    "type" : "object",
    "exampleValue" : ""
  },
  "localAuditLogRotation" : {
    "title" : "Rotate Local Audit Log",
    "description" : "Flag to indicate that audit log files should be rotated when reaching a certain size. (property name: com.sun.identity.agents.config.local.log.rotate) <br>Hot-swap: Yes",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "fqdnCheck" : {
    "title" : "FQDN Check",
    "description" : "Enables checking of fqdn default value and fqdn map values. (property name: com.sun.identity.agents.config.fqdn.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 6400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "webServiceProcessGetEnabled" : {
    "title" : "Web Service Process GET Enable",
    "description" : "Flag to indicates if the processing of HTTP GET requests for Web Service endpoints is enabled. (property name: com.sun.identity.agents.config.webservice.process.get.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "customProperties" : {
    "title" : "Custom Properties",
    "description" : "Additional properties that allow users to augment the set of properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties) <br>Hot-swap: Yes <br>Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br> custommap[key2]=custommap-value-2",
    "propertyOrder" : 12200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "shortenedPrivilegeAttributeValues" : {
    "title" : "Shortened privilege attribute values",
    "description" : "When using privileged attribute type, this setting will ensure that the membership details will be stored in a shortened format and not in the default universal ID format.<br><br>By default the agent maps identity memberships using their universal IDs (e.g. id=admin,ou=group,dc=openam,dc=forgerock,dc=org), however this may not be always acceptable. Using this setting the identity membership details will be mapped in a shortened format, only including the group's/role's name (e.g. admin). Be aware that in case there are both roles and groups in the data store, this setting will make them indistinguishable from each other, i.e. if there is a group and a role with the same name it will not be possible to differentiate them.",
    "propertyOrder" : 13600,
    "required" : true,
    "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "cdssoUrls" : {
    "title" : "CDSSO Servlet URL",
    "description" : "List of URLs of the available CDSSO controllers that may be used by the Agent
for CDSSO processing. (property name: com.sun.identity.agents.config.cdsso.cdcservlet.url) <br>Hot-
swap: Yes <br> Example: <br> http://host:port/opensso/cdcservlet",
    "propertyOrder" : 5200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "postDataPreservation" : {
    "title" : "Post Data Preservation enabled",
    "description" : "Post Data Preservation functionality basically stores any POST
data before redirecting the user to the login screen and after successful login the agent
will generate a page that autosubmits the same POST to the original URL. (property name:
com.sun.identity.agents.config.postdata.preserve.enable)",
    "propertyOrder" : 13100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "missingPostDataPreservationEntryUri" : {
    "title" : "Missing PDP entry URI",
    "description" : "An application-specific URI Map that is used in case the referenced
PDP entry cannot be found in the local cache (due to ttl). In such cases it will redirect
to the specified URI, otherwise it will show a HTTP 403 Forbidden error. (property name:
com.sun.identity.agents.config.postdata.preserve.cache.noentry.url)<br>Examples: <br>To set a
redirect target for application BankApp: enter Bankapp in Map Key field and enter a redirect URI in
corresponding Map Value field.",
    "propertyOrder" : 13200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "webServiceInternalErrorContentFile" : {
    "title" : "Web Service Internal Error Content File",
    "description" : "The name of file that contains content used by the
Agent to generate an internal error fault for clients. (property name:
com.sun.identity.agents.config.webservice.internalerror.content) <br>Hot-swap: Yes",
    "propertyOrder" : 2500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cookieAttributeMultiValueSeparator" : {
    "title" : "Cookie Separator Character",
    "description" : "Character that will be used to separate multiple values
of the same attribute when it is being set as a cookie. (property name:
com.sun.identity.agents.config.attribute.cookie.separator) <br>Hot-swap: Yes",
    "propertyOrder" : 8300,
    "required" : true,

```



```

    "type" : "string",
    "exampleValue" : ""
  },
  "invertNotEnforcedIps" : {
    "title" : "Not Enforced IP Invert List",
    "description" : "Client IP Addresses to invert protection of IP addresses listed in the related
Not Enforced Client IP List. (property name: com.sun.identity.agents.config.notenforced.ip.invert)
<br>Hot-swap: Yes",
    "propertyOrder" : 8000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "notEnforcedIps" : {
    "title" : "Not Enforced Client IP List",
    "description" : "No authentication and authorization protection from agent are
required for the requests coming from these client IP addresses. (property name:
com.sun.identity.agents.config.notenforced.ip) <br>Hot-swap: Yes <br> Examples: <br> 192.18.145.*
<br> 192.18.146.123",
    "propertyOrder" : 7900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "cookieAttributeUrlEncoded" : {
    "title" : "Attribute Cookie Encode",
    "description" : "Indicates if the value of the attribute should be URL encoded before being set
as a cookie. (property name: com.sun.identity.agents.config.attribute.cookie.encode) <br>Hot-swap:
Yes",
    "propertyOrder" : 8500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "privilegedAttributeMap" : {
    "title" : "Privileged Attribute Mapping",
    "description" : "Map if using Enable Privileged Attribute Mapping. (property name:
com.sun.identity.agents.config.privileged.attribute.mapping) <br>Hot-swap: Yes <br> Examples: <br>
To map UUID id=manager,ou=group,dc=openam,dc=forgerock,dc=org to the principal name am_manager_role
specified in webapp's deployment descriptor: enter id=manager,ou=group,dc=openam,dc=forgerock,dc=org
in Map Key field, and enter am_manager_role in Corresponding Map Value field. <br> To map UUID
id=employee,ou=group,dc=openam,dc=forgerock,dc=org to the principal name am_employee_role specified
in webapp's deployment descriptor: enter id=employee,ou=group,dc=openam,dc=forgerock,dc=org in Map
Key field, and enter am_employee_role in Corresponding Map Value field.",
    "propertyOrder" : 9900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "policyActionBooleanValues" : {
    "title" : "Policy Client Boolean Action Values",

```

```

    "description" : "Boolean action values for policy action names. (property name:
com.sun.identity.policy.client.booleanActionValues) <br>Hot-swap: No",
    "propertyOrder" : 11500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authServiceHost" : {
    "title" : "OpenAM Authentication Service Host Name",
    "description" : "Host name to be used by the OpenAM authentication service. (property name:
com.ipplanet.am.server.host) <br>Hot-swap: No",
    "propertyOrder" : 11000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoClockSkew" : {
    "title" : "CDSSO Clock Skew",
    "description" : "Time in seconds to be used by the Agent to determine the validity of the CDSSO
AuthnResponse assertion. (property name: com.sun.identity.agents.config.cdsso.clock.skew) <br>Hot-
swap: Yes",
    "propertyOrder" : 5300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "cookieResetNames" : {
    "title" : "Cookies Reset Name List",
    "description" : "Cookie names that will be reset by the Agent if Cookie Reset is enabled.
(property name: com.sun.identity.agents.config.cdsso.cookie.reset.name) <br>Hot-swap: Yes",
    "propertyOrder" : 4700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "amLoginUrl" : {
    "title" : "OpenAM Login URL",
    "description" : "OpenAM login page URL. (property name:
com.sun.identity.agents.config.login.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Login",
    "propertyOrder" : 3700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "urlPolicyEnvPostParameters" : {
    "title" : "URL Policy Env POST Parameters",
    "description" : "List of HTTP POST request parameters whose names and values will
be set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.post.param) <br>Hot-swap: Yes <br> Examples: <br> name <br>
phoneNumber",
    "propertyOrder" : 11900,
    "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "localeCountry" : {
    "title" : "Locale Country",
    "description" : "(property name: com.sun.identity.agents.config.locale.country) <br>Hot-swap:
No",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "urlPolicyEnvGetParameters" : {
    "title" : "URL Policy Env GET Parameters",
    "description" : "List of HTTP GET request parameters whose names and values will be
set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.get.param) <br>Hot-swap: Yes <br> Examples: <br> name <br>
phonenumber",
    "propertyOrder" : 11800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "auditAccessType" : {
    "title" : "Audit Access Types",
    "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype) <br>Hot-swap: Yes",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jbossWebAuthenticationAvailable" : {
    "title" : "WebAuthentication Available",
    "description" : "Enable agent to make programmatic authentication with
the JBoss web container using WebAuthentication feature. (property name:
com.sun.identity.agents.config.jboss.webauth.available) <br>Hot-swap: Yes",
    "propertyOrder" : 12300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdsso" : {
    "title" : "Cross Domain SSO",
    "description" : "Enables Cross Domain Single SignOn. (property name:
com.sun.identity.agents.config.cdsso.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logoutRequestParameters" : {
    "title" : "Logout Request Parameter",

```

```

    "description" : "An application-specific Map that identifies a parameter
which when present in the HTTP request indicates a logout event. (property name:
com.sun.identity.agents.config.logout.request.param) <br>Valid key: the web application name.
<br>Valid value: the logout request parameter. <br>For this property, a global value can be set to
apply to all the applications that don't have their own specific logout request parameter. <br>Hot-
swap: Yes <br> Examples: <br>To set a global application logout request parameter: leave Map Key
field empty, and enter the global application logout request parameter logoutparam in Corresponding
Map Value field. <br> To set the logout request parameter for application BankApp: enter BankApp in
Map Key field, and enter the logout request parameter logoutparam in Corresponding Map Value field.",
    "propertyOrder" : 6100,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"responseAttributeFetchMode" : {
    "title" : "Response Attribute Fetch Mode",
    "description" : "The mode of fetching policy response attributes. (property name:
com.sun.identity.agents.config.response.attribute.fetch.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 9100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"alternativeAgentHostname" : {
    "title" : "Alternative Agent Host Name",
    "description" : "Host name identifying the Agent protected server to the client browsers if
different from the actual host name. (property name: com.sun.identity.agents.config.agent.host)
<br>Hot-swap: Yes",
    "propertyOrder" : 4100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"legacyUserAgentSupport" : {
    "title" : "Legacy User Agent Support Enable",
    "description" : "Enables support for legacy user agents (browser). (property name:
com.sun.identity.agents.config.legacy.support.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 6700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"loginAttemptLimit" : {
    "title" : "Login Attempt Limit",
    "description" : "Limit of failed login attempts for a user's single browser session until
triggering the blocking of the user request. Value of 0 disables this feature. (property name:
com.sun.identity.agents.config.login.attempt.limit) <br>Hot-swap: Yes",
    "propertyOrder" : 4400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"policyClientResourceComparators" : {
    "title" : "Policy Client Resource Comparators",

```

```

    "description" : "Resource Comparators to be used for different service names. (property name:
com.sun.identity.policy.client.resourceComparators) <br>Hot-swap: No",
    "propertyOrder" : 11600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Password",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "notEnforcedUriCacheSize" : {
    "title" : "Not Enforced URIs Cache Size",
    "description" : "Size of the cache to be used if caching of not enforced URI list evaluation
results is enabled. (property name: com.sun.identity.agents.config.notenforced.uri.cache.size)
<br>Hot-swap: Yes",
    "propertyOrder" : 7800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "policyClientClockSkew" : {
    "title" : "Policy Client Clock Skew",
    "description" : "Time in seconds which is allowed to accommodate the time difference
between the OpenAM server machine and the remote policy client machine. (property name:
com.sun.identity.policy.client.clockSkew) <br>Hot-swap: No",
    "propertyOrder" : 11700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notEnforcedIpsCacheSize" : {
    "title" : "Not Enforced IP Cache Size",
    "description" : "Size of the cache to be used if Not Enforced IP Cache Flag is enabled.
(property name: com.sun.identity.agents.config.notenforced.ip.cache.size) <br>Hot-swap: Yes",
    "propertyOrder" : 8200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "portCheckSetting" : {
    "title" : "Port Check Setting",
    "description" : "Map of port versus protocol entries with the key being the listening port
number and value being the listening protocol to be used by the Agent to identify requests with
invalid port numbers. (property name: com.sun.identity.agents.config.port.check.setting) <br>Hot-
swap: Yes <br> Example: <br> To map port 80 to protocol http: enter 80 in Map Key field, and enter
http in Corresponding Map Value field.",
    "propertyOrder" : 7400,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  },
},

```

```
{
  "type" : "object",
  "exampleValue" : ""
},
"userAttributeName" : {
  "title" : "User Attribute Name",
  "description" : "Name of the attribute which contains the user-ID. (property name: com.sun.identity.agents.config.user.attribute.name) <br>Hot-swap: Yes",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"policyEvaluationApplication" : {
  "title" : "Application",
  "description" : "Which application contains the policies to evaluate with. (property name: org.forgerock.openam.agents.config.policy.evaluation.application) <br>Hot-swap: Yes",
  "propertyOrder" : 5500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
```

## 1.64. J2eeAgents

### 1.64.1. Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/J2EEAgent`

Resource version: `1.0`

#### 1.64.1.1. create

Usage:

```
am> create J2eeAgents --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```

"properties" : {
  "probeLogoutUrl" : {
    "title" : "Logout URL Probe",
    "description" : "Specifies if agent will check the availability of these urls before redirecting
to them. (property name: com.sun.identity.agents.config.logout.url.probe.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 12600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "headerAttributeDateFormat" : {
    "title" : "Fetch Attribute Date Format",
    "description" : "Format of date attribute values to be used when the attribute is
being set as HTTP header. Format is based on java.text.SimpleDateFormat. (property name:
com.sun.identity.agents.config.attribute.date.format) <br>Hot-swap: Yes",
    "propertyOrder" : 8400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "loginAttemptLimit" : {
    "title" : "Login Attempt Limit",
    "description" : "Limit of failed login attempts for a user's single browser session until
triggering the blocking of the user request. Value of 0 disables this feature. (property name:
com.sun.identity.agents.config.login.attempt.limit) <br>Hot-swap: Yes",
    "propertyOrder" : 4400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "resourceAccessDeniedUri" : {
    "title" : "Resource Access Denied URI",
    "description" : "An application-specific Map that identifies a URI of the customized access
denied page. (property name: com.sun.identity.agents.config.access.denied.uri) <br>Valid key: the
web application name. <br>Valid value: the customized application access denied page URI. <br>For
this property, a global value can be set to apply to all the applications that don't have their own
specific access denied page. <br>Hot-swap: Yes <br> Examples: <br>To set a global access denied page:
leave Map Key field empty, and enter the global access denied page URI /sample/accessdenied.html in
Corresponding Map Value field. <br> To set the access denied page URI for application BankApp: enter
BankApp in Map Key field, and enter the application access denied page URI /BankApp/accessdenied.html
in Corresponding Map Value field.",
    "propertyOrder" : 2700,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "logoutUrlPrioritized" : {
    "title" : "Logout URL Prioritized",
    "description" : "Specifies if failover sequence for Logout URLs should be prioritized as defined
in the OpenAM Login URL list. (property name: com.sun.identity.agents.config.logout.url.prioritized)
<br>Hot-swap: Yes",
    "propertyOrder" : 12500,
    "required" : true,
    "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "useRedirectForCompositeAdvice" : {
    "title" : "Use HTTP-Redirect for composite advice",
    "description" : "Configure remote policy client to use HTTP-redirect instead of HTTP-POST
for composite advices. (property name: com.sun.identity.agents.config.policy.advice.use.redirect)
<br>Hot-swap: Yes",
    "propertyOrder" : 13000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Password",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "legacyUserAgentList" : {
    "title" : "Legacy User Agent List",
    "description" : "List of user agent header values that identify legacy
browsers. Entries in this list can have wild card character '*'. (property name:
com.sun.identity.agents.config.legacy.user.agent) <br>Hot-swap: Yes",
    "propertyOrder" : 6800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "clientHostnameHeader" : {
    "title" : "Client Hostname Header",
    "description" : "HTTP header name that holds the Hostname of the client. (property name:
com.sun.identity.agents.config.client.hostname.header) <br>Hot-swap: Yes",
    "propertyOrder" : 1100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cookieAttributeUrlEncoded" : {
    "title" : "Attribute Cookie Encode",
    "description" : "Indicates if the value of the attribute should be URL encoded before being set
as a cookie. (property name: com.sun.identity.agents.config.attribute.cookie.encode) <br>Hot-swap:
Yes",
    "propertyOrder" : 8500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "jbossWebAuthenticationAvailable" : {
    "title" : "WebAuthentication Available",
    "description" : "Enable agent to make programmatic authentication with
the JBoss web container using WebAuthentication feature. (property name:
com.sun.identity.agents.config.jboss.webauth.available) <br>Hot-swap: Yes",
    "propertyOrder" : 12300,

```



```

    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "loginErrorUri" : {
    "title" : "Login Error URI",
    "description" : "List of absolute URIs corresponding to an application's web.xml form-error-
page element. (property name: com.sun.identity.agents.config.login.error.uri) <br>Hot-swap: Yes <br>
Example: <br> /BankApp/jsp/error.jsp",
    "propertyOrder" : 2900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "notEnforcedUris" : {
    "title" : "Not Enforced URIs",
    "description" : "List of URIs for which protection is not enforced by the Agent. (property
name: com.sun.identity.agents.config.notenforced.uri) <br>Hot-swap: Yes <br> Examples: <br> /BankApp/
public/* <br> /BankApp/images/*",
    "propertyOrder" : 7500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "fqdnCheck" : {
    "title" : "FQDN Check",
    "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 6400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "applicationLogoutHandlers" : {
    "title" : "Application Logout Handler",
    "description" : "An application-specific Map that identifies a handler to be used for logout
processing. (property name: com.sun.identity.agents.config.logout.application.handler) <br>Valid
key: the web application name. <br>Valid value: the application logout handler class name. <br>For
this property, a global value can be set to apply to all the applications that don't have their own
specific logout handler. <br>Hot-swap: Yes <br> Examples: <br>To set a global application logout
handler: leave Map Key field empty, and enter the global application logout handler class name
GlobalApplicationLogoutHandler in Corresponding Map Value field. <br>To set the logout handler for
application BankApp: enter BankApp in Map Key field, and enter the application logout handler class
name BankAppLogoutHandler in Corresponding Map Value field.",
    "propertyOrder" : 5900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  }

```

```

    },
    "policyEvaluationApplication" : {
      "title" : "Application",
      "description" : "Which application contains the policies to evaluate with. (property name: org.forgerock.openam.agents.config.policy.evaluation.application) <br>Hot-swap: Yes",
      "propertyOrder" : 5500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "loginProbeTimeout" : {
      "title" : "Login URL Probe Timeout",
      "description" : "The connect timeout value in milliseconds, if also Login URL Probe is set to true. (property name: com.sun.identity.agents.config.login.url.probe.timeout) <br>Hot-swap: Yes",
      "propertyOrder" : 4000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "notEnforcedIpsCacheSize" : {
      "title" : "Not Enforced IP Cache Size",
      "description" : "Size of the cache to be used if Not Enforced IP Cache Flag is enabled. (property name: com.sun.identity.agents.config.notenforced.ip.cache.size) <br>Hot-swap: Yes",
      "propertyOrder" : 8200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "alternativeAgentHostname" : {
      "title" : "Alternative Agent Host Name",
      "description" : "Host name identifying the Agent protected server to the client browsers if different from the actual host name. (property name: com.sun.identity.agents.config.agent.host) <br>Hot-swap: Yes",
      "propertyOrder" : 4100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "cdssoRedirectUri" : {
      "title" : "CDSSO Redirect URI",
      "description" : "An intermediate URI that is used by the Agent for processing CDSSO requests. (property name: com.sun.identity.agents.config.cdsso.redirect.uri) <br>Hot-swap: Yes",
      "propertyOrder" : 5100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "customVerificationHandlers" : {
      "title" : "Custom Verification Handler",
      "description" : "Application specific verification handler to validate the user credentials with the local repository. (property name: com.sun.identity.agents.config.verification.handler) <br>Valid key: the web application name. <br>Valid value: the verification handler class name. <br>Hot-swap: Yes <br> Example: <br> To set verification handler for application BankApp: enter BankApp in Map Key field, and enter verification handler class name BankVerificationHandler in Corresponding Map Value field.",
      "propertyOrder" : 3400,
      "required" : true,
      "patternProperties" : {
        ".*" : {

```

```

        "type" : "string"
    },
    "type" : "object",
    "exampleValue" : ""
},
"postDataPreservation" : {
    "title" : "Post Data Preservation enabled",
    "description" : "Post Data Preservation functionality basically stores any POST
data before redirecting the user to the login screen and after successful login the agent
will generate a page that autosubmits the same POST to the original URL. (property name:
com.sun.identity.agents.config.postdata.preserve.enable)",
    "propertyOrder" : 13100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"localeLanguage" : {
    "title" : "Locale Language",
    "description" : "(property name: com.sun.identity.agents.config.locale.language) <br>Hot-swap:
No",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"privilegedAttributeType" : {
    "title" : "Privileged Attribute Type",
    "description" : "List of privileged attribute types that will be fetched for each user.
(property name: com.sun.identity.agents.config.privileged.attribute.type) <br>Hot-swap: Yes <br>
Example: <br> Group",
    "propertyOrder" : 9500,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"legacyRedirectUri" : {
    "title" : "Legacy User Agent Redirect URI",
    "description" : "An intermediate URI used by the Agent to redirect legacy user agent requests.
(property name: com.sun.identity.agents.config.legacy.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 6900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"policyClientResourceComparators" : {
    "title" : "Policy Client Resource Comparators",
    "description" : "Resource Comparators to be used for different service names. (property name:
com.sun.identity.policy.client.resourceComparators) <br>Hot-swap: No",
    "propertyOrder" : 11600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"cdssoDomainList" : {
    "title" : "CDSSO Domain List",

```

```

    "description" : "Domains for which cookies have to be set in a CDSO scenario. (property name:
com.sun.identity.agents.config.cdsso.domain) <br>Hot-swap: Yes <br> Example: <br> .sun.com",
    "propertyOrder" : 5800,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"urlPolicyEnvJsessionParameters" : {
    "title" : "URL Policy Env jsession Parameters",
    "description" : "List of HTTP SESSION attributes whose names and values will be
set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.jsession.param) <br>Hot-swap: Yes <br> Examples: <br> name
<br> phonenumber",
    "propertyOrder" : 12000,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"shortenedPrivilegeAttributeValues" : {
    "title" : "Shortened privilege attribute values",
    "description" : "When using privileged attribute type, this setting will ensure that the
membership details will be stored in a shortened format and not in the default universal ID
format.<br><br>By default the agent maps identity memberships using their universal IDs (e.g.
id=admin,ou=group,dc=openam,dc=forgerock,dc=org), however this may not be always acceptable. Using
this setting the identity membership details will be mapped in a shortened format, only including the
group's/role's name (e.g. admin). Be aware that in case there are both roles and groups in the data
store, this setting will make them indistinguishable from each other, i.e. if there is a group and a
role with the same name it will not be possible to differentiate them.",
    "propertyOrder" : 13600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"authServiceProtocol" : {
    "title" : "OpenAM Authentication Service Protocol",
    "description" : "Protocol to be used by the OpenAM authentication service. (property name:
com.ipanet.am.server.protocol) <br>Hot-swap: No",
    "propertyOrder" : 10900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"cookieResetEnabled" : {
    "title" : "Cookie Reset",
    "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 4600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"localAuditRotationSize" : {
    "title" : "Local Audit Log Rotation Size",

```

```

    "description" : "Size limit when a local audit log file is rotated to a new file. (property
name: com.sun.identity.agents.config.local.log.size) <br>Hot-swap: Yes",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "policyClientPollingInterval" : {
    "title" : "Policy Client Polling Interval",
    "description" : "Duration in minutes after which the cached entries are refreshed by remote
policy client. (property name: com.sun.identity.agents.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 11300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notEnforcedUriCacheSize" : {
    "title" : "Not Enforced URIs Cache Size",
    "description" : "Size of the cache to be used if caching of not enforced URI list evaluation
results is enabled. (property name: com.sun.identity.agents.config.notenforced.uri.cache.size)
<br>Hot-swap: Yes",
    "propertyOrder" : 7800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sessionAttributeMap" : {
    "title" : "Session Attribute Mapping",
    "description" : "Maps the session attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map
Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
    "propertyOrder" : 9000,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "ssoCacheEnabled" : {
    "title" : "SSO Cache Enable",
    "description" : "Specifies if the SSO Cache is active for the agent.
Cache is used through public APIs exposed by the agent SDK. (property name:
com.sun.identity.agents.config.amsso.cache.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 4500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "urlPolicyEnvGetParameters" : {
    "title" : "URL Policy Env GET Parameters",
    "description" : "List of HTTP GET request parameters whose names and values will be
set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.get.param) <br>Hot-swap: Yes <br> Examples: <br> name <br>
phonenummer",

```

```

    "propertyOrder" : 11800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "profileAttributeMap" : {
    "title" : "Profile Attribute Mapping",
    "description" : "Maps the profile attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.profile.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field,
and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate the value of profile
attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in
Corresponding Map Value field.",
    "propertyOrder" : 8800,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "responseAttributeMap" : {
    "title" : "Response Attribute Mapping",
    "description" : "Maps the policy response attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.response.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field,
and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
    "propertyOrder" : 9200,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "webServiceEndpoints" : {
    "title" : "Web Service End Points",
    "description" : "A list of Web Application end points that represent Web Services. (property
name: com.sun.identity.agents.config.webservice.endpoint) <br>Hot-swap: Yes",
    "propertyOrder" : 2100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "invertNotEnforcedUris" : {
    "title" : "Invert Not Enforced URIs",

```

```

    "description" : "Inverts protection of URIs specified in Not Enforced URIs list. When set
to true, it indicates that the URIs specified should be enforced and all other URIs should be
not enforced by the Agent. (property name: com.sun.identity.agents.config.notenforced.uri.invert)
<br>Hot-swap: Yes",
    "propertyOrder" : 7600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "useInternalLogin" : {
    "title" : "Use Internal Login",
    "description" : "Set to false if want to customize Login Content File instead of default
internal content provided. (property name: com.sun.identity.agents.config.login.use.internal)
<br>Hot-swap: Yes",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "postDataStickySessionKeyValue" : {
    "title" : "PDP Stickysession key-value",
    "description" : "The provided key-value pair will be used for adding to
the URL or creating the cookie. <br>Example: <br>Set 'lb=server1' to append to
the querystring or to have 'lb' cookie with 'server1' value. (property name:
com.sun.identity.agents.config.postdata.preserve.stickysession.value)",
    "propertyOrder" : 13500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "logoutIntrospection" : {
    "title" : "Logout Introspect Enabled",
    "description" : "Allows the Agent to search HTTP request body to locate logout parameter.
(property name: com.sun.identity.agents.config.logout.introspect.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 6200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "webServiceAuthorizationErrorContentFile" : {
    "title" : "Web Service Authorization Error Content File",
    "description" : "The name of file that contains content used by the
Agent to generate an authorization error fault for clients. (property name:
com.sun.identity.agents.config.webservice.autherror.content) <br>Hot-swap: Yes",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "policyClientClockSkew" : {
    "title" : "Policy Client Clock Skew",
    "description" : "Time in seconds which is allowed to accommodate the time difference
between the OpenAM server machine and the remote policy client machine. (property name:
com.sun.identity.policy.client.clockSkew) <br>Hot-swap: No",
    "propertyOrder" : 11700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
},

```

```

"customAuthenticationHandlers" : {
  "title" : "Custom Authentication Handler",
  "description" : "Application specific authentication handler to authenticate the logged on user
with the application server. (property name: com.sun.identity.agents.config.auth.handler) <br>Valid
key: the web application name. <br>Valid value: the authentication handler class name. <br>Hot-swap:
Yes <br>Example: <br>To set authentication handler for application BankApp: enter BankApp in Map
Key field, and enter authentication handler class name BankAuthHandler in Corresponding Map Value
field.",
  "propertyOrder" : 3200,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"userMappingMode" : {
  "title" : "User Mapping Mode",
  "description" : "Specifies mechanism agent uses to determine user-ID. (property name:
com.sun.identity.agents.config.user.mapping.mode) <br>Hot-swap: Yes",
  "propertyOrder" : 600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"debugLevel" : {
  "title" : "Agent Debug Level",
  "description" : "Specifies type of agent debug messages to log. (property name:
com.ipplanet.services.debug.level) <br>Hot-swap: Yes",
  "propertyOrder" : 10000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"notEnforcedUrisCacheEnabled" : {
  "title" : "Not Enforced URIs Cache Enabled",
  "description" : "Enables the caching of the Not Enforced URIs list evaluation results. (property
name: com.sun.identity.agents.config.notenforced.uri.cache.enable) <br>Hot-swap: Yes",
  "propertyOrder" : 7700,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"postDataCacheTtl" : {
  "title" : "PDP entry TTL",
  "description" : "This value tells how long a given POST entry should be stored
in the local cache (in milliseconds), default value is 300000. (property name:
com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl)",
  "propertyOrder" : 13300,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"ignorePathInfo" : {
  "title" : "Ignore Path Info in Request URL",

```



```

    "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info) <br>Hot-swap: Yes",
    "propertyOrder" : 18600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userDataCacheNotifications" : {
    "title" : "Enable Notification of User Data Caches",
    "description" : "Enable notifications for amsdk and IdRepo Caches. (property name:
com.sun.identity.idm.remote.notification.enabled) <br>Hot-swap: No",
    "propertyOrder" : 10500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cookieResetDomains" : {
    "title" : "Cookies Reset Domain Map",
    "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the domain of this cookie to be used when a reset event occurs. (property name:
com.sun.identity.agents.config.cookie.reset.domain) <br>Hot-swap: Yes",
    "propertyOrder" : 4800,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "customLogoutHandlers" : {
    "title" : "Custom Logout Handler",
    "description" : "Application specific logout handler to log out a user with the application
server. (property name: com.sun.identity.agents.config.logout.handler) <br>Valid key: the web
application name. <br>Valid value: the logout handler class name. <br>Hot-swap: Yes <br> Example:
<br>To set logout handler for application BankApp: enter BankApp in Map Key field, and enter logout
handler class name BankLogoutHandler in Corresponding Map Value field.",
    "propertyOrder" : 3300,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "encryptionProvider" : {
    "title" : "Encryption Provider",
    "description" : "Specifies the encryption provider implementation to be used by the Agent.
(property name: com.iplanet.security.encryptor) <br>Hot-swap: No",
    "propertyOrder" : 10400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "auditLogLocation" : {

```

```

    "title" : "Audit Log Location",
    "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition) <br>Hot-swap: Yes",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "policyEvaluationRealm" : {
    "title" : "Realm",
    "description" : "Which realm to start evaluating from. (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm) <br>Hot-swap: Yes",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authServiceHost" : {
    "title" : "OpenAM Authentication Service Host Name",
    "description" : "Host name to be used by the OpenAM authentication service. (property name:
com.iplanet.am.server.host) <br>Hot-swap: No",
    "propertyOrder" : 11000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "portCheckEnabled" : {
    "title" : "Port Check Enable",
    "description" : "Indicates if port check functionality is enabled or disabled. (property name:
com.sun.identity.agents.config.port.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 7200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "repositoryLocation" : {
    "title" : "Location of Agent Configuration Repository",
    "description" : "Indicates agent's configuration located either on agent's host or centrally on
OpenAM server.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "filterMode" : {
    "title" : "Agent Filter Mode",
    "description" : "Specifies the mode of operation of the Filter. (property name:
com.sun.identity.agents.config.filter.mode) <br>Valid key: the web application name. <br>Valid
values: ALL, J2EE_POLICY, URL_POLICY, SSO_ONLY, NONE <br>For this property, a global value can be
set to apply to all the applications that don't have their own specific filter mode. <br>Hot-swap:
No <br>Examples: <br>To set ALL as the global filter mode: leave Map Key field empty, and enter ALL
in Corresponding Map Value field. <br>To set URL_POLICY as the filter mode for application BankApp:
enter BankApp in Map Key field, and enter URL_POLICY in Corresponding Map Value field.",
    "propertyOrder" : 500,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  }
}

```

```

    },
    "type" : "object",
    "exampleValue" : ""
  },
  "applicationLogoutUri" : {
    "title" : "Application Logout URI",
    "description" : "An application-specific Map that identifies a request URI which indicates
a logout event. (property name: com.sun.identity.agents.config.logout.uri) <br>Valid key: the web
application name. <br>Valid value: the application logout URI. <br>For this property, a global value
can be set to apply to all the applications that don't have their own specific logout URI. <br>Hot-
swap: Yes <br>Examples: <br>To set a global application logout URI: leave Map Key field empty, and
enter the global application logout URI /logout.jsp in Corresponding Map Value field. <br>To set the
logout URI for application BankApp: enter BankApp in Map Key field, and enter the application logout
URI /BankApp/logout.jsp in Corresponding Map Value field.",
    "propertyOrder" : 6000,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "agentNotificationUrl" : {
    "title" : "Agent Notification URL",
    "description" : "URL used by agent to register notification listeners. (property name:
com.sun.identity.client.notification.url) <br>Hot-swap: No",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "defaultPrivilegedAttributes" : {
    "title" : "Default Privileged Attribute",
    "description" : "List of privileged attributes that will be granted to all users who have a
valid OpenAM session. (property name: com.sun.identity.agents.config.default.privileged.attribute)
<br>Hot-swap: Yes <br>Example: <br> AUTHENTICATED_USERS",
    "propertyOrder" : 9400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "fqdnMapping" : {
    "title" : "FQDN Virtual Host Map",
    "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN to
access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>Hot-
swap: Yes <br>Examples: <br>To map the partial hostname myserver to myserver.mydomain.com: enter
myserver in the Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map
a virtual server rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in
the Map Key field and rst.hostname.com in the Corresponding Map Value field.",
    "propertyOrder" : 6600,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  }
}

```

```

    },
    "type" : "object",
    "exampleValue" : ""
  },
  "cdssoUrls" : {
    "title" : "CDSSO Servlet URL",
    "description" : "List of URLs of the available CDSSO controllers that may be used by the Agent
for CDSSO processing. (property name: com.sun.identity.agents.config.cdsso.cdcservlet.url) <br>Hot-
swap: Yes <br> Example: <br> http://host:port/opensso/cdcservlet",
    "propertyOrder" : 5200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "policyActionBooleanValues" : {
    "title" : "Policy Client Boolean Action Values",
    "description" : "Boolean action values for policy action names. (property name:
com.sun.identity.policy.client.booleanActionValues) <br>Hot-swap: No",
    "propertyOrder" : 11500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "policyNotifications" : {
    "title" : "Enable Policy Notifications",
    "description" : "Enable Notifications for remote policy client. (property name:
com.sun.identity.agents.notification.enabled) <br>Hot-swap: No",
    "propertyOrder" : 11200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "status" : {
    "title" : "Status",
    "description" : "Status of the agent configuration.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "privilegedAttributeMap" : {
    "title" : "Privileged Attribute Mapping",
    "description" : "Map if using Enable Privileged Attribute Mapping. (property name:
com.sun.identity.agents.config.privileged.attribute.mapping) <br>Hot-swap: Yes <br> Examples: <br>
To map UUID id=manager,ou=group,dc=openam,dc=forgerock,dc=org to the principal name am_manager_role
specified in webapp's deployment descriptor: enter id=manager,ou=group,dc=openam,dc=forgerock,dc=org
in Map Key field, and enter am_manager_role in Corresponding Map Value field. <br> To map UUID
id=employee,ou=group,dc=openam,dc=forgerock,dc=org to the principal name am_employee_role specified
in webapp's deployment descriptor: enter id=employee,ou=group,dc=openam,dc=forgerock,dc=org in Map
Key field, and enter am_employee_role in Corresponding Map Value field.",
    "propertyOrder" : 9900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  }
}

```

```

    },
    "type" : "object",
    "exampleValue" : ""
  },
  "urlPolicyEnvPostParameters" : {
    "title" : "URL Policy Env POST Parameters",
    "description" : "List of HTTP POST request parameters whose names and values will
be set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.post.param) <br>Hot-swap: Yes <br> Examples: <br> name <br>
phonenumber",
    "propertyOrder" : 11900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "privilegedSessionAttribute" : {
    "title" : "Privileged Session Attribute",
    "description" : "List of session property names which hold privileged attributes for the
authenticated user. (property name: com.sun.identity.agents.config.privileged.session.attribute)
<br>Hot-swap: Yes <br> Example: <br> UserToken",
    "propertyOrder" : 9700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "responseAttributeFetchMode" : {
    "title" : "Response Attribute Fetch Mode",
    "description" : "The mode of fetching policy response attributes. (property name:
com.sun.identity.agents.config.response.attribute.fetch.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 9100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "privilegedAttributesToLowerCase" : {
    "title" : "Privileged Attributes To Lower Case",
    "description" : "Maps the privileged attribute types to whether they should be converted to
lowercase. (property name: com.sun.identity.agents.config.privileged.attribute.lowercase) <br>
Valid Keys: the privileged attribute types, such as Group, Role. <br>Valid value: true, false.
<br>Hot-swap: Yes <br> Example: <br> Enter Group in Map Key field, and enter false in Corresponding
Map Value field.",
    "propertyOrder" : 9600,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "policyClientCacheMode" : {

```

```

    "title" : "Policy Client Cache Mode",
    "description" : "Mode of caching to be used by remote policy client. (property name:
com.sun.identity.policy.client.cacheMode) <br>Hot-swap: No",
    "propertyOrder" : 11400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "webServiceProcessGetEnabled" : {
    "title" : "Web Service Process GET Enable",
    "description" : "Flag to indicates if the processing of HTTP GET requests for Web Service
endpoints is enabled. (property name: com.sun.identity.agents.config.webservice.process.get.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdssoSecureCookies" : {
    "title" : "CDSSO Secure Enable",
    "description" : "The SSO Token cookie set by the agent in the different domains in CDSSO mode
will be marked secure. Only transmitted if the communications channel with host is a secure one.
(property name: com.sun.identity.agents.config.cdsso.secure.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "portCheckFile" : {
    "title" : "Port Check File",
    "description" : "Name or complete path of a file that has the necessary content needed to handle
requests that need port correction. (property name: com.sun.identity.agents.config.port.check.file)
<br>Hot-swap: Yes",
    "propertyOrder" : 7300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "privilegedAttributeMappingEnabled" : {
    "title" : "Enable Privileged Attribute Mapping",
    "description" : "Enable a mapping from the original value of an attribute to another value. To
satisfy container-specific restrictions on character set being used in certain configuration files.
(property name: com.sun.identity.agents.config.privileged.attribute.mapping.enable) <br>Hot-swap:
Yes",
    "propertyOrder" : 9800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "legacyUserAgentSupport" : {
    "title" : "Legacy User Agent Support Enable",
    "description" : "Enables support for legacy user agents (browser). (property name:
com.sun.identity.agents.config.legacy.support.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 6700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "gotoParameterName" : {

```

```

        "title" : "Goto Parameter Name",
        "description" : "Property used only when CDSSO is enabled. Default value should
        be changed only when the login URL has a landing page specified <br> Example :
        com.sun.identity.agents.config.cdssso.cdcservlet.url = http://host:port/opensso/cdcservlet?
        goto=http://agent:port/landing.jsp <br> The parameter is used by the Agent to append the original
        request URL to this cdcservlet URL. This parameter is consumed by the landing page to redirect to
        the original URL. (property name: com.sun.identity.agents.config.redirect.param) <br>Hot-swap: Yes
        <br> Example: com.sun.identity.agents.config.redirect.param = goto2<br> The complete URL sent for
        authentication will be <br> http://host:port/opensso/cdcservlet?goto=http://agent:port/landing.jsp?
        goto2=http://agent:port/original.jsp",
        "propertyOrder" : 3600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "cookieResetPaths" : {
        "title" : "Cookies Reset Path Map",
        "description" : "Maps cookie names specified in Cookie Reset Name List to value
        being the path of this cookie to be used when a reset event occurs. (property name:
        com.sun.identity.agents.config.cookie.reset.path) <br>Hot-swap: Yes",
        "propertyOrder" : 4900,
        "required" : true,
        "patternProperties" : {
            ".*" : {
                "type" : "string"
            }
        },
        "type" : "object",
        "exampleValue" : ""
    },
    "clientPollingPeriod" : {
        "title" : "Client Polling Period",
        "description" : "Time in seconds after which the session client will request update of cached
        session information from the server. (property name: com.iplanet.am.session.client.polling.period)
        <br>Hot-swap: No",
        "propertyOrder" : 10300,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "missingPostDataPreservationEntryUri" : {
        "title" : "Missing PDP entry URI",
        "description" : "An application-specific URI Map that is used in case the referenced
        PDP entry cannot be found in the local cache (due to ttl). In such cases it will redirect
        to the specified URI, otherwise it will show a HTTP 403 Forbidden error. (property name:
        com.sun.identity.agents.config.postdata.preserve.cache.noentry.url)<br>Examples: <br>To set a
        redirect target for application BankApp: enter Bankapp in Map Key field and enter a redirect URI in
        corresponding Map Value field.",
        "propertyOrder" : 13200,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "xssDetectionRedirectUri" : {
        "title" : "XSS detection redirect URI",

```

```

    "description" : "An application-specific Map that identifies a URI of the customized page if
XSS code has been detected. (property name: com.sun.identity.agents.config.xss.redirect.uri) <br>Hot-
swap: Yes <br>Examples: <br>To set a redirect target for application BankApp: enter BankApp in Map Key
field, and enter a redirect URI in Corresponding Map Value field.",
    "propertyOrder" : 12900,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"localeCountry" : {
    "title" : "Locale Country",
    "description" : "(property name: com.sun.identity.agents.config.locale.country) <br>Hot-swap:
No",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"amLoginUrl" : {
    "title" : "OpenAM Login URL",
    "description" : "OpenAM login page URL. (property name:
com.sun.identity.agents.config.login.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Login",
    "propertyOrder" : 3700,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"customProperties" : {
    "title" : "Custom Properties",
    "description" : "Additional properties that allow users to augment the set of properties
supported by agent. (property name: com.sun.identity.agents.config.freeformproperties) <br>Hot-
swap: Yes <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-
value-0 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
    "propertyOrder" : 12200,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"alternativeAgentProtocol" : {
    "title" : "Alternative Agent Protocol",
    "description" : "Protocol being used (http/https) by the client browsers to communicate with
the Agent protected server if different from the actual protocol used by the server. (property name:
com.sun.identity.agents.config.agent.protocol) <br>Hot-swap: Yes",
    "propertyOrder" : 4300,
    "required" : true,
    "type" : "string",

```



```

    "exampleValue" : ""
  },
  "cdssoRootUrl" : {
    "title" : "Agent Root URL for CDSSO",
    "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
    "propertyOrder" : 22700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "bypassPrincipallist" : {
    "title" : "Bypass Principal List",
    "description" : "List of principals that are bypassed by the Agent for authentication and search
purposes. (property name: com.sun.identity.agents.config.bypass.principal) <br>Hot-swap: Yes <br>
Examples: <br> guest <br> testuser",
    "propertyOrder" : 9300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "authServicePort" : {
    "title" : "OpenAM Authentication Service Port",
    "description" : "Port to be used by the OpenAM authentication service. (property name:
com.ipplanet.am.server.port) <br>Hot-swap: No",
    "propertyOrder" : 11100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notEnforcedIps" : {
    "title" : "Not Enforced Client IP List",
    "description" : "No authentication and authorization protection from agent are
required for the requests coming from these client IP addresses. (property name:
com.sun.identity.agents.config.notenforced.ip) <br>Hot-swap: Yes <br> Examples: <br> 192.18.145.*
<br> 192.18.146.123",
    "propertyOrder" : 7900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "configurationReloadInterval" : {
    "title" : "Configuration Reload Interval",
    "description" : "Interval in seconds between configuration reloads. (property name:
com.sun.identity.agents.config.load.interval) <br>Hot-swap: Yes",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",

```

```

    "exampleValue" : ""
  },
  "logoutProbeTimeout" : {
    "title" : "Logout URL Probe Timeout",
    "description" : "The connect timeout value in milliseconds, if also Logout URL Probe is set to
true. (property name: com.sun.identity.agents.config.logout.url.probe.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 12700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "logoutRequestParameters" : {
    "title" : "Logout Request Parameter",
    "description" : "An application-specific Map that identifies a parameter
which when present in the HTTP request indicates a logout event. (property name:
com.sun.identity.agents.config.logout.request.param) <br>Valid key: the web application name.
<br>Valid value: the logout request parameter. <br>For this property, a global value can be set to
apply to all the applications that don't have their own specific logout request parameter. <br>Hot-
swap: Yes <br> Examples: <br>To set a global application logout request parameter: leave Map Key
field empty, and enter the global application logout request parameter logoutparam in Corresponding
Map Value field. <br> To set the logout request parameter for application BankApp: enter BankApp in
Map Key field, and enter the logout request parameter logoutparam in Corresponding Map Value field.",
    "propertyOrder" : 6100,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "webServiceResponseProcessor" : {
    "title" : "Web Service Response Processor",
    "description" : "An implementation class of interface
com.sun.identity.agents.filter.IWebServiceResponseProcessor that can be used to process the web-
service responses. (property name: com.sun.identity.agents.config.webservice.responseprocessor)
<br>Hot-swap: Yes",
    "propertyOrder" : 2400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cookieAttributeMultiValueSeparator" : {
    "title" : "Cookie Separator Character",
    "description" : "Character that will be used to separate multiple values
of the same attribute when it is being set as a cookie. (property name:
com.sun.identity.agents.config.attribute.cookie.separator) <br>Hot-swap: Yes",
    "propertyOrder" : 8300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "agentConfigChangeNotificationsEnabled" : {
    "title" : "Agent Configuration Change Notification",
    "description" : "Enable agent to receive notification messages from OpenAM server for
configuration changes. (property name: com.sun.identity.agents.config.change.notification.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 12100,

```

```

    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userTokenName" : {
    "title" : "User Token Name",
    "description" : "Session property name for user-ID of the authenticated user in session.
(property name: com.sun.identity.agents.config.user.token) <br>Hot-swap: Yes",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "loginFormUri" : {
    "title" : "Login Form URI",
    "description" : "List of absolute URIs corresponding to an application's web.xml form-login-page
element. (property name: com.sun.identity.agents.config.login.form) <br>Hot-swap: Yes <br> Example:
<br> /BankApp/jsp/login.jsp",
    "propertyOrder" : 2800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "serviceDataCacheNotifications" : {
    "title" : "Enable Notification of Service Data Caches",
    "description" : "Enable the notifications for service management caches. (property name:
com.sun.identity.sm.notification.enabled) <br>Hot-swap: No",
    "propertyOrder" : 10700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "possibleXssCodeElements" : {
    "title" : "Possible XSS code elements",
    "description" : "If one of these strings occurs in the request, the client is redirected to an
error page. (property name: com.sun.identity.agents.config.xss.code.elements) <br>Hot-swap: Yes",
    "propertyOrder" : 12800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "amLogoutUrl" : {
    "title" : "OpenAM Logout URL",
    "description" : "OpenAM logout page URL. (property name:
com.sun.identity.agents.config.logout.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Logout",
    "propertyOrder" : 12400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }

```

```

    },
    "remoteLogFilename" : {
      "title" : "Remote Log File Name",
      "description" : "Name of file stored on OpenAM server that contains agent audit messages.
(property name: com.sun.identity.agents.config.remote.logfile) <br>Hot-swap: Yes",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "customResponseHeader" : {
      "title" : "Custom Response Header",
      "description" : "Map specifies the custom headers that are set by the Agent on the client
browser. The key is the header name and the value represents the header value. (property name:
com.sun.identity.agents.config.response.header) <br>Hot-swap: Yes <br> Example: <br> To set the
custom header Cache-Control to value no-cache: enter Cache-Control in Map Key field, and enter no-
cache in Corresponding Map Value field.",
      "propertyOrder" : 7000,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    },
    "webServiceInternalErrorContentFile" : {
      "title" : "Web Service Internal Error Content File",
      "description" : "The name of file that contains content used by the
Agent to generate an internal error fault for clients. (property name:
com.sun.identity.agents.config.webservice.internalerror.content) <br>Hot-swap: Yes",
      "propertyOrder" : 2500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "webServiceAuthenticator" : {
      "title" : "Web Service Authenticator",
      "description" : "An implementation class of interface
com.sun.identity.agents.filter.IWebServiceAuthenticator that can be used to authenticate web-service
requests. (property name: com.sun.identity.agents.config.webservice.authenticator) <br>Hot-swap:
Yes",
      "propertyOrder" : 2300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "profileAttributeFetchMode" : {
      "title" : "Profile Attribute Fetch Mode",
      "description" : "The mode of fetching profile attributes. (property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode) <br>Hot-swap: Yes",
      "propertyOrder" : 8700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "auditAccessType" : {
      "title" : "Audit Access Types",

```

```

    "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype) <br>Hot-swap: Yes",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "amCookieName" : {
    "title" : "Cookie Name",
    "description" : "Name of the SSO Token cookie used between the OpenAM server and the Agent.
(property name: com.iplanet.am.cookie.name) <br>Hot-swap: No",
    "propertyOrder" : 10100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sessionAttributeFetchMode" : {
    "title" : "Session Attribute Fetch Mode",
    "description" : "The mode of fetching session attributes. (property name:
com.sun.identity.agents.config.session.attribute.fetch.mode) <br>Hot-swap: Yes",
    "propertyOrder" : 8900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "serviceDataCacheTime" : {
    "title" : "Service Data Cache Time",
    "description" : "Cache update time in minutes for service configuration data. If set to '0' no
updates happen. (property name: com.sun.identity.sm.cacheTime) <br>Hot-swap: No",
    "propertyOrder" : 10800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "localAuditLogRotation" : {
    "title" : "Rotate Local Audit Log",
    "description" : "Flag to indicate that audit log files should be rotated when reaching a certain
size. (property name: com.sun.identity.agents.config.local.log.rotate) <br>Hot-swap: Yes",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logoutEntryUri" : {
    "title" : "Logout Entry URI",
    "description" : "An application-specific Map that identifies a URI to be used as an entry point
after successful logout and subsequent successful authentication if applicable. (property name:
com.sun.identity.agents.config.logout.entry.uri) <br>Valid key: the web application name. <br>Valid
value: the logout entry URI. <br>For this property, a global value can be set to apply to all the
applications that don't have their own specific logout entry URI. <br>Hot-swap: Yes <br> Examples:
<br>To set a global application logout entry URI: leave Map Key field empty, and enter the global
application logout entry URI /welcome.html in Corresponding Map Value field. <br> To set the logout
entry URI for application BankApp: enter BankApp in Map Key field, and enter the logout entry URI /
BankApp/welcome.html in Corresponding Map Value field.",
    "propertyOrder" : 6300,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  }

```

```

    },
    "type" : "object",
    "exampleValue" : ""
  },
  "cookieResetNames" : {
    "title" : "Cookies Reset Name List",
    "description" : "Cookie names that will be reset by the Agent if Cookie Reset is enabled.
(property name: com.sun.identity.agents.config.cdsso.cookie.reset.name) <br>Hot-swap: Yes",
    "propertyOrder" : 4700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userDataCachePollingTime" : {
    "title" : "User Data Cache Polling Time",
    "description" : "Cache update time in minutes for user management data. If set to '0' no updates
happen. (property name: com.ipplanet.am.sdk.remote.pollingTime) <br>Hot-swap: No",
    "propertyOrder" : 10600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "portCheckSetting" : {
    "title" : "Port Check Setting",
    "description" : "Map of port versus protocol entries with the key being the listening port
number and value being the listening protocol to be used by the Agent to identify requests with
invalid port numbers. (property name: com.sun.identity.agents.config.port.check.setting) <br>Hot-
swap: Yes <br> Example: <br> To map port 80 to protocol http: enter 80 in Map Key field, and enter
http in Corresponding Map Value field.",
    "propertyOrder" : 7400,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "probeLoginUrl" : {
    "title" : "Login URL Probe",
    "description" : "Specifies if agent will check the availability of these urls before redirecting
to them. (property name: com.sun.identity.agents.config.login.url.probe.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 3900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdsso" : {
    "title" : "Cross Domain SSO",
    "description" : "Enables Cross Domain Single SignOn. (property name:
com.sun.identity.agents.config.cdsso.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "redirectAttemptLimit" : {
    "title" : "Redirect Attempt Limit",
    "description" : "Number of successive single point redirects that a user can make using a
single browser session which will trigger the blocking of the user request. Set to 0 to disable this
feature. (property name: com.sun.identity.agents.config.redirect.attempt.limit) <br>Hot-swap: Yes",
    "propertyOrder" : 7100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "loginContentFile" : {
    "title" : "Login Content File Name",
    "description" : "Complete path and name of custom login content file. (property name:
com.sun.identity.agents.config.login.content.file) <br>Hot-swap: Yes",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "invertNotEnforcedIps" : {
    "title" : "Not Enforced IP Invert List",
    "description" : "Client IP Addresses to invert protection of IP addresses listed in the related
Not Enforced Client IP List. (property name: com.sun.identity.agents.config.notenforced.ip.invert)
<br>Hot-swap: Yes",
    "propertyOrder" : 8000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "postDataStickySessionMode" : {
    "title" : "PDP StickySession mode",
    "description" : "The PDP mechanism needs sticky loadbalancing, the URL mode will
append a querystring, while the Cookie mode will create a cookie. (property name:
com.sun.identity.agents.config.postdata.preserve.stickysession.mode)",
    "propertyOrder" : 13400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userPrincipalFlag" : {
    "title" : "User Principal Flag",
    "description" : "Use principal instead of just the user-ID for authenticating the user.
(property name: com.sun.identity.agents.config.user.principal) <br>Hot-swap: Yes",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "webServiceEnabled" : {
    "title" : "Web Service Enable",
    "description" : "Flag specifies if Web Service processing is enabled. (property name:
com.sun.identity.agents.config.webservice.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
},

```

```

"cdssoClockSkew" : {
  "title" : "CDSSO Clock Skew",
  "description" : "Time in seconds to be used by the Agent to determine the validity of the CDSSO
AuthnResponse assertion. (property name: com.sun.identity.agents.config.cdsso.clock.skew) <br>Hot-
swap: Yes",
  "propertyOrder" : 5300,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"notEnforcedUrisRefreshSessionIdleTime" : {
  "title" : "Refresh Session Idle Time",
  "description" : "Indicates if opensso session idle time should be refreshed or reset for not
enforced URIs. (property name: com.sun.identity.agents.config.notenforced.refresh.session.idletime)
<br>Hot-swap: Yes",
  "propertyOrder" : 8600,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"fqdnDefault" : {
  "title" : "FQDN Default",
  "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default) <br>Hot-swap: Yes",
  "propertyOrder" : 6500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"alternativeAgentPort" : {
  "title" : "Alternative Agent Port Name",
  "description" : "Port number identifying the Agent protected server listening port
to the client browsers if different from the actual listening port. (property name:
com.sun.identity.agents.config.agent.port) <br>Hot-swap: Yes",
  "propertyOrder" : 4200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userAttributeName" : {
  "title" : "User Attribute Name",
  "description" : "Name of the attribute which contains the user-ID. (property name:
com.sun.identity.agents.config.user.attribute.name) <br>Hot-swap: Yes",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"clientIpHeader" : {
  "title" : "Client IP Address Header",
  "description" : "HTTP header name that holds the IP address of the client. (property name:
com.sun.identity.agents.config.client.ip.header) <br>Hot-swap: Yes",
  "propertyOrder" : 1000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"notEnforcedIpsCacheEnabled" : {
  "title" : "Not Enforced IP Cache Flag",

```



```

        "description" : "Enable caching of not-enforced IP list evaluation results. (property name:
com.sun.identity.agents.config.notenforced.ip.cache.enable) <br>Hot-swap: Yes",
        "propertyOrder" : 8100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "cdssoTrustedIdProvider" : {
        "title" : "CDSSO Trusted ID Provider",
        "description" : "List of OpenAM Server/ID providers that should be trusted
by the agent, when evaluating the CDC Liberty Responses. (property name:
com.sun.identity.agents.config.cdsso.trusted.id.provider) <br>Hot-swap: Yes <br> Example: <br>
http://host:port/opensso/cdcservlet",
        "propertyOrder" : 5600,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "enableClientPolling" : {
        "title" : "Enable Client Polling",
        "description" : "Specifies if the session client must use polling for updating
session information and not depend upon server notifications. (property name:
com.ipplanet.am.session.client.polling.enable) <br>Hot-swap: No",
        "propertyOrder" : 10200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "loginUrlPrioritized" : {
        "title" : "Login URL Prioritized",
        "description" : "Specifies if failover sequence for Login URLs or CDSSO URLs
should be prioritized as defined in the OpenAM Login URL list. (property name:
com.sun.identity.agents.config.login.url.prioritized) <br>Hot-swap: Yes",
        "propertyOrder" : 3800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "httpSessionBinding" : {
        "title" : "HTTP Session Binding",
        "description" : "If true will invalidate the http session when login has failed, user
has no SSO session, or principal user name does not match SSO user name. (property name:
com.sun.identity.agents.config.httpsession.binding) <br>Hot-swap: Yes",
        "propertyOrder" : 3500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
}
}

```

## 1.64.1.2. delete

Usage:

```
am> delete J2eeAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.64.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action J2eeAgents --realm Realm --actionName getAllTypes
```

### 1.64.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action J2eeAgents --realm Realm --actionName getCreatableTypes
```

### 1.64.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action J2eeAgents --realm Realm --actionName nextdescendents
```

### 1.64.1.6. query

Querying the agents of a specific type

Usage:

```
am> query J2eeAgents --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.64.1.7. read

Usage:

```
am> read J2eeAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.64.1.8. update

Usage:

```
am> update J2eeAgents --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "probeLogoutUrl" : {
      "title" : "Logout URL Probe",
      "description" : "Specifies if agent will check the availability of these urls before redirecting
to them. (property name: com.sun.identity.agents.config.logout.url.probe.enabled) <br>Hot-swap: Yes",
      "propertyOrder" : 12600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "headerAttributeDateFormat" : {
      "title" : "Fetch Attribute Date Format",
      "description" : "Format of date attribute values to be used when the attribute is
being set as HTTP header. Format is based on java.text.SimpleDateFormat. (property name:
com.sun.identity.agents.config.attribute.date.format) <br>Hot-swap: Yes",
      "propertyOrder" : 8400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "loginAttemptLimit" : {
      "title" : "Login Attempt Limit",
      "description" : "Limit of failed login attempts for a user's single browser session until
triggering the blocking of the user request. Value of 0 disables this feature. (property name:
com.sun.identity.agents.config.login.attempt.limit) <br>Hot-swap: Yes",
      "propertyOrder" : 4400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "resourceAccessDeniedUri" : {
```

```

    "title" : "Resource Access Denied URI",
    "description" : "An application-specific Map that identifies a URI of the customized access
denied page. (property name: com.sun.identity.agents.config.access.denied.uri) <br>Valid key: the
web application name. <br>Valid value: the customized application access denied page URI. <br>For
this property, a global value can be set to apply to all the applications that don't have their own
specific access denied page. <br>Hot-swap: Yes <br> Examples: <br>To set a global access denied page:
leave Map Key field empty, and enter the global access denied page URI /sample/accessdenied.html in
Corresponding Map Value field. <br> To set the access denied page URI for application BankApp: enter
BankApp in Map Key field, and enter the application access denied page URI /BankApp/accessdenied.html
in Corresponding Map Value field.",
    "propertyOrder" : 2700,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"logoutUrlPrioritized" : {
    "title" : "Logout URL Prioritized",
    "description" : "Specifies if failover sequence for Logout URLs should be prioritized as defined
in the OpenAM Login URL list. (property name: com.sun.identity.agents.config.logout.url.prioritized)
<br>Hot-swap: Yes",
    "propertyOrder" : 12500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"useRedirectForCompositeAdvice" : {
    "title" : "Use HTTP-Redirect for composite advice",
    "description" : "Configure remote policy client to use HTTP-redirect instead of HTTP-POST
for composite advices. (property name: com.sun.identity.agents.config.policy.advice.use.redirect)
<br>Hot-swap: Yes",
    "propertyOrder" : 13000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"userpassword" : {
    "title" : "Password",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
},
"legacyUserAgentList" : {
    "title" : "Legacy User Agent List",
    "description" : "List of user agent header values that identify legacy
browsers. Entries in this list can have wild card character '*'. (property name:
com.sun.identity.agents.config.legacy.user.agent) <br>Hot-swap: Yes",
    "propertyOrder" : 6800,
    "required" : true,
    "items" : {
        "type" : "string"
    }
},

```

```

    "type" : "array",
    "exampleValue" : ""
  },
  "clientHostnameHeader" : {
    "title" : "Client Hostname Header",
    "description" : "HTTP header name that holds the Hostname of the client. (property name: com.sun.identity.agents.config.client.hostname.header) <br>Hot-swap: Yes",
    "propertyOrder" : 1100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cookieAttributeUrlEncoded" : {
    "title" : "Attribute Cookie Encode",
    "description" : "Indicates if the value of the attribute should be URL encoded before being set as a cookie. (property name: com.sun.identity.agents.config.attribute.cookie.encode) <br>Hot-swap: Yes",
    "propertyOrder" : 8500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "jbossWebAuthenticationAvailable" : {
    "title" : "WebAuthentication Available",
    "description" : "Enable agent to make programmatic authentication with the JBoss web container using WebAuthentication feature. (property name: com.sun.identity.agents.config.jboss.webauth.available) <br>Hot-swap: Yes",
    "propertyOrder" : 12300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "loginErrorUri" : {
    "title" : "Login Error URI",
    "description" : "List of absolute URIs corresponding to an application's web.xml form-error-page element. (property name: com.sun.identity.agents.config.login.error.uri) <br>Hot-swap: Yes <br> Example: <br> /BankApp/jsp/error.jsp",
    "propertyOrder" : 2900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "notEnforcedUris" : {
    "title" : "Not Enforced URIs",
    "description" : "List of URIs for which protection is not enforced by the Agent. (property name: com.sun.identity.agents.config.notenforced.uri) <br>Hot-swap: Yes <br> Examples: <br> /BankApp/public/* <br> /BankApp/images/*",
    "propertyOrder" : 7500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "fqdnCheck" : {

```

```

    "title" : "FQDN Check",
    "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 6400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "applicationLogoutHandlers" : {
    "title" : "Application Logout Handler",
    "description" : "An application-specific Map that identifies a handler to be used for logout
processing. (property name: com.sun.identity.agents.config.logout.application.handler) <br>Valid
key: the web application name. <br>Valid value: the application logout handler class name. <br>For
this property, a global value can be set to apply to all the applications that don't have their own
specific logout handler. <br>Hot-swap: Yes <br> Examples: <br>To set a global application logout
handler: leave Map Key field empty, and enter the global application logout handler class name
GlobalApplicationLogoutHandler in Corresponding Map Value field. <br>To set the logout handler for
application BankApp: enter BankApp in Map Key field, and enter the application logout handler class
name BankAppLogoutHandler in Corresponding Map Value field.",
    "propertyOrder" : 5900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "policyEvaluationApplication" : {
    "title" : "Application",
    "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.openam.agents.config.policy.evaluation.application) <br>Hot-swap: Yes",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "loginProbeTimeout" : {
    "title" : "Login URL Probe Timeout",
    "description" : "The connect timeout value in milliseconds, if also Login URL Probe is set to
true. (property name: com.sun.identity.agents.config.login.url.probe.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 4000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notEnforcedIpsCacheSize" : {
    "title" : "Not Enforced IP Cache Size",
    "description" : "Size of the cache to be used if Not Enforced IP Cache Flag is enabled.
(property name: com.sun.identity.agents.config.notenforced.ip.cache.size) <br>Hot-swap: Yes",
    "propertyOrder" : 8200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "alternativeAgentHostname" : {
    "title" : "Alternative Agent Host Name",

```

```

    "description" : "Host name identifying the Agent protected server to the client browsers if
different from the actual host name. (property name: com.sun.identity.agents.config.agent.host)
<br>Hot-swap: Yes",
    "propertyOrder" : 4100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoRedirectUri" : {
    "title" : "CDSSO Redirect URI",
    "description" : "An intermediate URI that is used by the Agent for processing CDSSO requests.
(property name: com.sun.identity.agents.config.cdsso.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "customVerificationHandlers" : {
    "title" : "Custom Verification Handler",
    "description" : "Application specific verification handler to validate the user credentials with
the local repository. (property name: com.sun.identity.agents.config.verification.handler) <br>Valid
key: the web application name. <br>Valid value: the verification handler class name. <br>Hot-swap:
Yes <br> Example: <br> To set verification handler for application BankApp: enter BankApp in Map Key
field, and enter verification handler class name BankVerificationHandler in Corresponding Map Value
field.",
    "propertyOrder" : 3400,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "postDataPreservation" : {
    "title" : "Post Data Preservation enabled",
    "description" : "Post Data Preservation functionality basically stores any POST
data before redirecting the user to the login screen and after successful login the agent
will generate a page that autosubmits the same POST to the original URL. (property name:
com.sun.identity.agents.config.postdata.preserve.enable)",
    "propertyOrder" : 13100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "localeLanguage" : {
    "title" : "Locale Language",
    "description" : "(property name: com.sun.identity.agents.config.locale.language) <br>Hot-swap:
No",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "privilegedAttributeType" : {
    "title" : "Privileged Attribute Type",

```

```

    "description" : "List of privileged attribute types that will be fetched for each user.
(property name: com.sun.identity.agents.config.privileged.attribute.type) <br>Hot-swap: Yes <br>
Example: <br> Group",
    "propertyOrder" : 9500,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"legacyRedirectUri" : {
    "title" : "Legacy User Agent Redirect URI",
    "description" : "An intermediate URI used by the Agent to redirect legacy user agent requests.
(property name: com.sun.identity.agents.config.legacy.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 6900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"policyClientResourceComparators" : {
    "title" : "Policy Client Resource Comparators",
    "description" : "Resource Comparators to be used for different service names. (property name:
com.sun.identity.policy.client.resourceComparators) <br>Hot-swap: No",
    "propertyOrder" : 11600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"cdssoDomainList" : {
    "title" : "CDSSO Domain List",
    "description" : "Domains for which cookies have to be set in a CDSSO scenario. (property name:
com.sun.identity.agents.config.cdsso.domain) <br>Hot-swap: Yes <br> Example: <br> .sun.com",
    "propertyOrder" : 5800,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"urlPolicyEnvJsessionParameters" : {
    "title" : "URL Policy Env jsession Parameters",
    "description" : "List of HTTP SESSION attributes whose names and values will be
set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.jsession.param) <br>Hot-swap: Yes <br> Examples: <br> name
<br> phonenumber",
    "propertyOrder" : 12000,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"shortenedPrivilegeAttributeValues" : {
    "title" : "Shortened privilege attribute values",
    "description" : "When using privileged attribute type, this setting will ensure that the
membership details will be stored in a shortened format and not in the default universal ID

```



```
format.<br><br>By default the agent maps identity memberships using their universal IDs (e.g.
id=admin,ou=group,dc=openam,dc=forgerock,dc=org), however this may not be always acceptable. Using
this setting the identity membership details will be mapped in a shortened format, only including the
group's/role's name (e.g. admin). Be aware that in case there are both roles and groups in the data
store, this setting will make them indistinguishable from each other, i.e. if there is a group and a
role with the same name it will not be possible to differentiate them.",
  "propertyOrder" : 13600,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"authServiceProtocol" : {
  "title" : "OpenAM Authentication Service Protocol",
  "description" : "Protocol to be used by the OpenAM authentication service. (property name:
com.ipplanet.am.server.protocol) <br>Hot-swap: No",
  "propertyOrder" : 10900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"cookieResetEnabled" : {
  "title" : "Cookie Reset",
  "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable) <br>Hot-swap: Yes",
  "propertyOrder" : 4600,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"localAuditRotationSize" : {
  "title" : "Local Audit Log Rotation Size",
  "description" : "Size limit when a local audit log file is rotated to a new file. (property
name: com.sun.identity.agents.config.local.log.size) <br>Hot-swap: Yes",
  "propertyOrder" : 1900,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"policyClientPollingInterval" : {
  "title" : "Policy Client Polling Interval",
  "description" : "Duration in minutes after which the cached entries are refreshed by remote
policy client. (property name: com.sun.identity.agents.polling.interval) <br>Hot-swap: No",
  "propertyOrder" : 11300,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"notEnforcedUrisCacheSize" : {
  "title" : "Not Enforced URIs Cache Size",
  "description" : "Size of the cache to be used if caching of not enforced URI list evaluation
results is enabled. (property name: com.sun.identity.agents.config.notenforced.uri.cache.size)
<br>Hot-swap: Yes",
  "propertyOrder" : 7800,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sessionAttributeMap" : {
  "title" : "Session Attribute Mapping",
```

```

    "description" : "Maps the session attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map
Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
    "propertyOrder" : 9000,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"ssoCacheEnabled" : {
    "title" : "SSO Cache Enable",
    "description" : "Specifies if the SSO Cache is active for the agent.
Cache is used through public APIs exposed by the agent SDK. (property name:
com.sun.identity.agents.config.amsso.cache.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 4500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"urlPolicyEnvGetParameters" : {
    "title" : "URL Policy Env GET Parameters",
    "description" : "List of HTTP GET request parameters whose names and values will be
set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.get.param) <br>Hot-swap: Yes <br> Examples: <br> name <br>
phoneNumber",
    "propertyOrder" : 11800,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"profileAttributeMap" : {
    "title" : "Profile Attribute Mapping",
    "description" : "Maps the profile attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.profile.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field,
and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate the value of profile
attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in
Corresponding Map Value field.",
    "propertyOrder" : 8800,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"responseAttributeMap" : {

```

```

    "title" : "Response Attribute Mapping",
    "description" : "Maps the policy response attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.response.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field,
and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
    "propertyOrder" : 9200,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"webServiceEndpoints" : {
    "title" : "Web Service End Points",
    "description" : "A list of Web Application end points that represent Web Services. (property
name: com.sun.identity.agents.config.webservice.endpoint) <br>Hot-swap: Yes",
    "propertyOrder" : 2100,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"invertNotEnforcedUris" : {
    "title" : "Invert Not Enforced URIs",
    "description" : "Inverts protection of URIs specified in Not Enforced URIs list. When set
to true, it indicates that the URIs specified should be enforced and all other URIs should be
not enforced by the Agent. (property name: com.sun.identity.agents.config.notenforced.uri.invert)
<br>Hot-swap: Yes",
    "propertyOrder" : 7600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"useInternalLogin" : {
    "title" : "Use Internal Login",
    "description" : "Set to false if want to customize Login Content File instead of default
internal content provided. (property name: com.sun.identity.agents.config.login.use.internal)
<br>Hot-swap: Yes",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"postDataStickySessionKeyValue" : {
    "title" : "PDP Stickysession key-value",
    "description" : "The provided key-value pair will be used for adding to
the URL or creating the cookie. <br>Example: <br>Set 'lb=server1' to append to
the querystring or to have 'lb' cookie with 'server1' value. (property name:
com.sun.identity.agents.config.postdata.preserve.stickysession.value)",
    "propertyOrder" : 13500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
}

```

```

    },
    "logoutIntrospection" : {
        "title" : "Logout Introspect Enabled",
        "description" : "Allows the Agent to search HTTP request body to locate logout parameter.
(property name: com.sun.identity.agents.config.logout.introspect.enabled) <br>Hot-swap: Yes",
        "propertyOrder" : 6200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "webServiceAuthorizationErrorContentFile" : {
        "title" : "Web Service Authorization Error Content File",
        "description" : "The name of file that contains content used by the
Agent to generate an authorization error fault for clients. (property name:
com.sun.identity.agents.config.webservice.autherror.content) <br>Hot-swap: Yes",
        "propertyOrder" : 2600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "policyClientClockSkew" : {
        "title" : "Policy Client Clock Skew",
        "description" : "Time in seconds which is allowed to accommodate the time difference
between the OpenAM server machine and the remote policy client machine. (property name:
com.sun.identity.policy.client.clockSkew) <br>Hot-swap: No",
        "propertyOrder" : 11700,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "customAuthenticationHandlers" : {
        "title" : "Custom Authentication Handler",
        "description" : "Application specific authentication handler to authenticate the logged on user
with the application server. (property name: com.sun.identity.agents.config.auth.handler) <br>Valid
key: the web application name. <br>Valid value: the authentication handler class name. <br>Hot-swap:
Yes <br>Example: <br>To set authentication handler for application BankApp: enter BankApp in Map
Key field, and enter authentication handler class name BankAuthHandler in Corresponding Map Value
field.",
        "propertyOrder" : 3200,
        "required" : true,
        "patternProperties" : {
            ".*" : {
                "type" : "string"
            }
        },
        "type" : "object",
        "exampleValue" : ""
    },
    "userMappingMode" : {
        "title" : "User Mapping Mode",
        "description" : "Specifies mechanism agent uses to determine user-ID. (property name:
com.sun.identity.agents.config.user.mapping.mode) <br>Hot-swap: Yes",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "debugLevel" : {
        "title" : "Agent Debug Level",

```

```

    "description" : "Specifies type of agent debug messages to log. (property name:
com.ipplanet.services.debug.level) <br>Hot-swap: Yes",
    "propertyOrder" : 10000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "notEnforcedUriCacheEnabled" : {
    "title" : "Not Enforced URIs Cache Enabled",
    "description" : "Enables the caching of the Not Enforced URIs list evaluation results. (property
name: com.sun.identity.agents.config.notenforced.uri.cache.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 7700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "postDataCacheTtl" : {
    "title" : "PDP entry TTL",
    "description" : "This value tells how long a given POST entry should be stored
in the local cache (in milliseconds), default value is 300000. (property name:
com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl)",
    "propertyOrder" : 13300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "ignorePathInfo" : {
    "title" : "Ignore Path Info in Request URL",
    "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info) <br>Hot-swap: Yes",
    "propertyOrder" : 18600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userDataCacheNotifications" : {
    "title" : "Enable Notification of User Data Caches",
    "description" : "Enable notifications for amsdk and IdRepo Caches. (property name:
com.sun.identity.idm.remote.notification.enabled) <br>Hot-swap: No",
    "propertyOrder" : 10500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cookieResetDomains" : {
    "title" : "Cookies Reset Domain Map",
    "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the domain of this cookie to be used when a reset event occurs. (property name:
com.sun.identity.agents.config.cookie.reset.domain) <br>Hot-swap: Yes",
    "propertyOrder" : 4800,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  }

```

```

    },
    "customLogoutHandlers" : {
        "title" : "Custom Logout Handler",
        "description" : "Application specific logout handler to log out a user with the application
server. (property name: com.sun.identity.agents.config.logout.handler) <br>Valid key: the web
application name. <br>Valid value: the logout handler class name. <br>Hot-swap: Yes <br> Example:
<br>To set logout handler for application BankApp: enter BankApp in Map Key field, and enter logout
handler class name BankLogoutHandler in Corresponding Map Value field.",
        "propertyOrder" : 3300,
        "required" : true,
        "patternProperties" : {
            ".*" : {
                "type" : "string"
            }
        },
        "type" : "object",
        "exampleValue" : ""
    },
    "encryptionProvider" : {
        "title" : "Encryption Provider",
        "description" : "Specifies the encryption provider implementation to be used by the Agent.
(property name: com.iplanet.security.encryptor) <br>Hot-swap: No",
        "propertyOrder" : 10400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "auditLogLocation" : {
        "title" : "Audit Log Location",
        "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition) <br>Hot-swap: Yes",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "policyEvaluationRealm" : {
        "title" : "Realm",
        "description" : "Which realm to start evaluating from. (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm) <br>Hot-swap: Yes",
        "propertyOrder" : 5400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "authServiceHost" : {
        "title" : "OpenAM Authentication Service Host Name",
        "description" : "Host name to be used by the OpenAM authentication service. (property name:
com.iplanet.am.server.host) <br>Hot-swap: No",
        "propertyOrder" : 11000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "portCheckEnabled" : {
        "title" : "Port Check Enable",
        "description" : "Indicates if port check functionality is enabled or disabled. (property name:
com.sun.identity.agents.config.port.check.enable) <br>Hot-swap: Yes",
        "propertyOrder" : 7200,

```

```

    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "repositoryLocation" : {
    "title" : "Location of Agent Configuration Repository",
    "description" : "Indicates agent's configuration located either on agent's host or centrally on
OpenAM server.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "filterMode" : {
    "title" : "Agent Filter Mode",
    "description" : "Specifies the mode of operation of the Filter. (property name:
com.sun.identity.agents.config.filter.mode) <br>Valid key: the web application name. <br>Valid
values: ALL, J2EE_POLICY, URL_POLICY, SSO_ONLY, NONE <br>For this property, a global value can be
set to apply to all the applications that don't have their own specific filter mode. <br>Hot-swap:
No <br>Examples: <br>To set ALL as the global filter mode: leave Map Key field empty, and enter ALL
in Corresponding Map Value field. <br>To set URL_POLICY as the filter mode for application BankApp:
enter BankApp in Map Key field, and enter URL_POLICY in Corresponding Map Value field.",
    "propertyOrder" : 500,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "applicationLogoutUri" : {
    "title" : "Application Logout URI",
    "description" : "An application-specific Map that identifies a request URI which indicates
a logout event. (property name: com.sun.identity.agents.config.logout.uri) <br>Valid key: the web
application name. <br>Valid value: the application logout URI. <br>For this property, a global value
can be set to apply to all the applications that don't have their own specific logout URI. <br>Hot-
swap: Yes <br>Examples: <br>To set a global application logout URI: leave Map Key field empty, and
enter the global application logout URI /logout.jsp in Corresponding Map Value field. <br>To set the
logout URI for application BankApp: enter BankApp in Map Key field, and enter the application logout
URI /BankApp/logout.jsp in Corresponding Map Value field.",
    "propertyOrder" : 6000,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "agentNotificationUrl" : {
    "title" : "Agent Notification URL",
    "description" : "URL used by agent to register notification listeners. (property name:
com.sun.identity.client.notification.url) <br>Hot-swap: No",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",

```

```

    "exampleValue" : ""
  },
  "defaultPrivilegedAttributes" : {
    "title" : "Default Privileged Attribute",
    "description" : "List of privileged attributes that will be granted to all users who have a
valid OpenAM session. (property name: com.sun.identity.agents.config.default.privileged.attribute)
<br>Hot-swap: Yes <br> Example: <br> AUTHENTICATED_USERS",
    "propertyOrder" : 9400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "fqdnMapping" : {
    "title" : "FQDN Virtual Host Map",
    "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN to
access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>Hot-
swap: Yes <br> Examples: <br> To map the partial hostname myserver to myserver.mydomain.com: enter
myserver in the Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map
a virtual server rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in
the Map Key field and rst.hostname.com in the Corresponding Map Value field.",
    "propertyOrder" : 6600,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "cdssoUrls" : {
    "title" : "CDSSO Servlet URL",
    "description" : "List of URLs of the available CDSSO controllers that may be used by the Agent
for CDSSO processing. (property name: com.sun.identity.agents.config.cdsso.cdcservlet.url) <br>Hot-
swap: Yes <br> Example: <br> http://host:port/opensso/cdcservlet",
    "propertyOrder" : 5200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "policyActionBooleanValues" : {
    "title" : "Policy Client Boolean Action Values",
    "description" : "Boolean action values for policy action names. (property name:
com.sun.identity.policy.client.booleanActionValues) <br>Hot-swap: No",
    "propertyOrder" : 11500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "policyNotifications" : {
    "title" : "Enable Policy Notifications",
    "description" : "Enable Notifications for remote policy client. (property name:
com.sun.identity.agents.notification.enabled) <br>Hot-swap: No",

```



```

    "propertyOrder" : 11200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "status" : {
    "title" : "Status",
    "description" : "Status of the agent configuration.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "privilegedAttributeMap" : {
    "title" : "Privileged Attribute Mapping",
    "description" : "Map if using Enable Privileged Attribute Mapping. (property name:
com.sun.identity.agents.config.privileged.attribute.mapping) <br>Hot-swap: Yes <br> Examples: <br>
To map UUID id=manager,ou=group,dc=openam,dc=forgerock,dc=org to the principal name am_manager_role
specified in webapp's deployment descriptor: enter id=manager,ou=group,dc=openam,dc=forgerock,dc=org
in Map Key field, and enter am_manager_role in Corresponding Map Value field. <br> To map UUID
id=employee,ou=group,dc=openam,dc=forgerock,dc=org to the principal name am_employee_role specified
in webapp's deployment descriptor: enter id=employee,ou=group,dc=openam,dc=forgerock,dc=org in Map
Key field, and enter am_employee_role in Corresponding Map Value field.",
    "propertyOrder" : 9900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "urlPolicyEnvPostParameters" : {
    "title" : "URL Policy Env POST Parameters",
    "description" : "List of HTTP POST request parameters whose names and values will
be set in the environment map for URL policy evaluation at OpenAM server. (property name:
com.sun.identity.agents.config.policy.env.post.param) <br>Hot-swap: Yes <br> Examples: <br> name <br>
phoneNumber",
    "propertyOrder" : 11900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "privilegedSessionAttribute" : {
    "title" : "Privileged Session Attribute",
    "description" : "List of session property names which hold privileged attributes for the
authenticated user. (property name: com.sun.identity.agents.config.privileged.session.attribute)
<br>Hot-swap: Yes <br> Example: <br> UserToken",
    "propertyOrder" : 9700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }

```

```

},
"responseAttributeFetchMode" : {
  "title" : "Response Attribute Fetch Mode",
  "description" : "The mode of fetching policy response attributes. (property name:
com.sun.identity.agents.config.response.attribute.fetch.mode) <br>Hot-swap: Yes",
  "propertyOrder" : 9100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"privilegedAttributesToLowerCase" : {
  "title" : "Privileged Attributes To Lower Case",
  "description" : "Maps the privileged attribute types to whether they should be converted to
lowercase. (property name: com.sun.identity.agents.config.privileged.attribute.tolowercase) <br>
Valid Keys: the privileged attribute types, such as Group, Role. <br>Valid value: true, false.
<br>Hot-swap: Yes <br> Example: <br> Enter Group in Map Key field, and enter false in Corresponding
Map Value field.",
  "propertyOrder" : 9600,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"policyClientCacheMode" : {
  "title" : "Policy Client Cache Mode",
  "description" : "Mode of caching to be used by remote policy client. (property name:
com.sun.identity.policy.client.cacheMode) <br>Hot-swap: No",
  "propertyOrder" : 11400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"webServiceProcessGetEnabled" : {
  "title" : "Web Service Process GET Enable",
  "description" : "Flag to indicates if the processing of HTTP GET requests for Web Service
endpoints is enabled. (property name: com.sun.identity.agents.config.webservice.process.get.enable)
<br>Hot-swap: Yes",
  "propertyOrder" : 2200,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"cdssoSecureCookies" : {
  "title" : "CDSSO Secure Enable",
  "description" : "The SSO Token cookie set by the agent in the different domains in CDSSO mode
will be marked secure. Only transmitted if the communications channel with host is a secure one.
(property name: com.sun.identity.agents.config.cdsso.secure.enable) <br>Hot-swap: Yes",
  "propertyOrder" : 5700,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"portCheckFile" : {
  "title" : "Port Check File",

```

```

    "description" : "Name or complete path of a file that has the necessary content needed to handle
requests that need port correction. (property name: com.sun.identity.agents.config.port.check.file)
<br>Hot-swap: Yes",
    "propertyOrder" : 7300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"privilegedAttributeMappingEnabled" : {
    "title" : "Enable Privileged Attribute Mapping",
    "description" : "Enable a mapping from the original value of an attribute to another value. To
satisfy container-specific restrictions on character set being used in certain configuration files.
(property name: com.sun.identity.agents.config.privileged.attribute.mapping.enable) <br>Hot-swap:
Yes",
    "propertyOrder" : 9800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"LegacyUserAgentSupport" : {
    "title" : "Legacy User Agent Support Enable",
    "description" : "Enables support for legacy user agents (browser). (property name:
com.sun.identity.agents.config.legacy.support.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 6700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"gotoParameterName" : {
    "title" : "Goto Parameter Name",
    "description" : "Property used only when CDSO is enabled. Default value should
be changed only when the login URL has a landing page specified <br> Example :
com.sun.identity.agents.config.cdsso.cdcservlet.url = http://host:port/opensso/cdcservlet?
goto=http://agent:port/landing.jsp <br> The parameter is used by the Agent to append the original
request URL to this cdcservlet URL. This parameter is consumed by the landing page to redirect to
the original URL. (property name: com.sun.identity.agents.config.redirect.param) <br>Hot-swap: Yes
<br> Example: com.sun.identity.agents.config.redirect.param = goto2<br> The complete URL sent for
authentication will be <br> http://host:port/opensso/cdcservlet?goto=http://agent:port/landing.jsp?
goto2=http://agent.port/original.jsp",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"cookieResetPaths" : {
    "title" : "Cookies Reset Path Map",
    "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the path of this cookie to be used when a reset event occurs. (property name:
com.sun.identity.agents.config.cookie.reset.path) <br>Hot-swap: Yes",
    "propertyOrder" : 4900,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
},

```

```

"clientPollingPeriod" : {
  "title" : "Client Polling Period",
  "description" : "Time in seconds after which the session client will request update of cached
session information from the server. (property name: com.iplanet.am.session.client.polling.period)
<br>Hot-swap: No",
  "propertyOrder" : 10300,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"missingPostDataPreservationEntryUri" : {
  "title" : "Missing PDP entry URI",
  "description" : "An application-specific URI Map that is used in case the referenced
PDP entry cannot be found in the local cache (due to ttl). In such cases it will redirect
to the specified URI, otherwise it will show a HTTP 403 Forbidden error. (property name:
com.sun.identity.agents.config.postdata.preservce.cache.noentry.url)<br>Examples: <br>To set a
redirect target for application BankApp: enter Bankapp in Map Key field and enter a redirect URI in
corresponding Map Value field.",
  "propertyOrder" : 13200,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"xssDetectionRedirectUri" : {
  "title" : "XSS detection redirect URI",
  "description" : "An application-specific Map that identifies a URI of the customized page if
XSS code has been detected. (property name: com.sun.identity.agents.config.xss.redirect.uri) <br>Hot-
swap: Yes <br>Examples: <br>To set a redirect target for application BankApp: enter BankApp in Map Key
field, and enter a redirect URI in Corresponding Map Value field.",
  "propertyOrder" : 12900,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"localeCountry" : {
  "title" : "Locale Country",
  "description" : "(property name: com.sun.identity.agents.config.locale.country) <br>Hot-swap:
No",
  "propertyOrder" : 1400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"amLoginUrl" : {
  "title" : "OpenAM Login URL",
  "description" : "OpenAM login page URL. (property name:
com.sun.identity.agents.config.login.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Login",
  "propertyOrder" : 3700,
  "required" : true,
  "items" : {

```

```

    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"customProperties" : {
  "title" : "Custom Properties",
  "description" : "Additional properties that allow users to augment the set of properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties) <br>Hot-swap: Yes <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br> custommap[key2]=custommap-value-2",
  "propertyOrder" : 12200,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"alternativeAgentProtocol" : {
  "title" : "Alternative Agent Protocol",
  "description" : "Protocol being used (http/https) by the client browsers to communicate with the Agent protected server if different from the actual protocol used by the server. (property name: com.sun.identity.agents.config.agent.protocol) <br>Hot-swap: Yes",
  "propertyOrder" : 4300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"cdssoRootUrl" : {
  "title" : "Agent Root URL for CDSO",
  "description" : "The agent root URL for CDSO. The valid value is in the following format: <br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https. The hostname represents the host name of the machine on which the agent resides. The port represents the port number on which the agent is installed. The slash following the port number is required.",
  "propertyOrder" : 22700,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"bypassPrincipallist" : {
  "title" : "Bypass Principal List",
  "description" : "List of principals that are bypassed by the Agent for authentication and search purposes. (property name: com.sun.identity.agents.config.bypass.principal) <br>Hot-swap: Yes <br> Examples: <br> guest <br> testuser",
  "propertyOrder" : 9300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"authServicePort" : {
  "title" : "OpenAM Authentication Service Port",

```

```

    "description" : "Port to be used by the OpenAM authentication service. (property name:
com.ipplanet.am.server.port) <br>Hot-swap: No",
    "propertyOrder" : 11100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notEnforcedIps" : {
    "title" : "Not Enforced Client IP List",
    "description" : "No authentication and authorization protection from agent are
required for the requests coming from these client IP addresses. (property name:
com.sun.identity.agents.config.load.interval) <br>Hot-swap: Yes <br> Examples: <br> 192.18.145.*
<br> 192.18.146.123",
    "propertyOrder" : 7900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "configurationReloadInterval" : {
    "title" : "Configuration Reload Interval",
    "description" : "Interval in seconds between configuration reloads. (property name:
com.sun.identity.agents.config.load.interval) <br>Hot-swap: Yes",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "logoutProbeTimeout" : {
    "title" : "Logout URL Probe Timeout",
    "description" : "The connect timeout value in milliseconds, if also Logout URL Probe is set to
true. (property name: com.sun.identity.agents.config.logout.url.probe.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 12700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "logoutRequestParameters" : {
    "title" : "Logout Request Parameter",
    "description" : "An application-specific Map that identifies a parameter
which when present in the HTTP request indicates a logout event. (property name:
com.sun.identity.agents.config.logout.request.param) <br>Valid key: the web application name.
<br>Valid value: the logout request parameter. <br>For this property, a global value can be set to
apply to all the applications that don't have their own specific logout request parameter. <br>Hot-
swap: Yes <br> Examples: <br>To set a global application logout request parameter: leave Map Key
field empty, and enter the global application logout request parameter logoutparam in Corresponding
Map Value field. <br> To set the logout request parameter for application BankApp: enter BankApp in
Map Key field, and enter the logout request parameter logoutparam in Corresponding Map Value field.",
    "propertyOrder" : 6100,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  }

```

```

    },
    "webServiceResponseProcessor" : {
        "title" : "Web Service Response Processor",
        "description" : "An implementation class of interface
com.sun.identity.agents.filter.IWebServiceResponseProcessor that can be used to process the web-
service responses. (property name: com.sun.identity.agents.config.webservice.responseprocessor)
<br>Hot-swap: Yes",
        "propertyOrder" : 2400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "cookieAttributeMultiValueSeparator" : {
        "title" : "Cookie Separator Character",
        "description" : "Character that will be used to separate multiple values
of the same attribute when it is being set as a cookie. (property name:
com.sun.identity.agents.config.attribute.cookie.separator) <br>Hot-swap: Yes",
        "propertyOrder" : 8300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "agentConfigChangeNotificationsEnabled" : {
        "title" : "Agent Configuration Change Notification",
        "description" : "Enable agent to receive notification messages from OpenAM server for
configuration changes. (property name: com.sun.identity.agents.config.change.notification.enable)
<br>Hot-swap: Yes",
        "propertyOrder" : 12100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "userTokenName" : {
        "title" : "User Token Name",
        "description" : "Session property name for user-ID of the authenticated user in session.
(property name: com.sun.identity.agents.config.user.token) <br>Hot-swap: Yes",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "loginFormUri" : {
        "title" : "Login Form URI",
        "description" : "List of absolute URIs corresponding to an application's web.xml form-login-page
element. (property name: com.sun.identity.agents.config.login.form) <br>Hot-swap: Yes <br> Example:
<br> /BankApp/jsp/login.jsp",
        "propertyOrder" : 2800,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "serviceDataCacheNotifications" : {
        "title" : "Enable Notification of Service Data Caches",
        "description" : "Enable the notifications for service management caches. (property name:
com.sun.identity.sm.notification.enabled) <br>Hot-swap: No",
        "propertyOrder" : 10700,

```

```

    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "possibleXssCodeElements" : {
    "title" : "Possible XSS code elements",
    "description" : "If one of these strings occurs in the request, the client is redirected to an
error page. (property name: com.sun.identity.agents.config.xss.code.elements) <br>Hot-swap: Yes",
    "propertyOrder" : 12800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "amLogoutUrl" : {
    "title" : "OpenAM Logout URL",
    "description" : "OpenAM logout page URL. (property name:
com.sun.identity.agents.config.logout.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Logout",
    "propertyOrder" : 12400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "remoteLogFilename" : {
    "title" : "Remote Log File Name",
    "description" : "Name of file stored on OpenAM server that contains agent audit messages.
(property name: com.sun.identity.agents.config.remote.logfile) <br>Hot-swap: Yes",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "customResponseHeader" : {
    "title" : "Custom Response Header",
    "description" : "Map specifies the custom headers that are set by the Agent on the client
browser. The key is the header name and the value represents the header value. (property name:
com.sun.identity.agents.config.response.header) <br>Hot-swap: Yes <br> Example: <br> To set the
custom header Cache-Control to value no-cache: enter Cache-Control in Map Key field, and enter no-
cache in Corresponding Map Value field.",
    "propertyOrder" : 7000,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "webServiceInternalErrorContentFile" : {
    "title" : "Web Service Internal Error Content File",

```



```

        "description" : "The name of file that contains content used by the
Agent to generate an internal error fault for clients. (property name:
com.sun.identity.agents.config.webservice.internalerror.content) <br>Hot-swap: Yes",
        "propertyOrder" : 2500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "webServiceAuthenticator" : {
        "title" : "Web Service Authenticator",
        "description" : "An implementation class of interface
com.sun.identity.agents.filter.IWebServiceAuthenticator that can be used to authenticate web-service
requests. (property name: com.sun.identity.agents.config.webservice.authenticator) <br>Hot-swap:
Yes",
        "propertyOrder" : 2300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "profileAttributeFetchMode" : {
        "title" : "Profile Attribute Fetch Mode",
        "description" : "The mode of fetching profile attributes. (property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode) <br>Hot-swap: Yes",
        "propertyOrder" : 8700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "auditAccessType" : {
        "title" : "Audit Access Types",
        "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype) <br>Hot-swap: Yes",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "amCookieName" : {
        "title" : "Cookie Name",
        "description" : "Name of the SSO Token cookie used between the OpenAM server and the Agent.
(property name: com.iplanet.am.cookie.name) <br>Hot-swap: No",
        "propertyOrder" : 10100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sessionAttributeFetchMode" : {
        "title" : "Session Attribute Fetch Mode",
        "description" : "The mode of fetching session attributes. (property name:
com.sun.identity.agents.config.session.attribute.fetch.mode) <br>Hot-swap: Yes",
        "propertyOrder" : 8900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "serviceDataCacheTime" : {
        "title" : "Service Data Cache Time",
        "description" : "Cache update time in minutes for service configuration data. If set to '0' no
updates happen. (property name: com.sun.identity.sm.cacheTime) <br>Hot-swap: No",

```

```

    "propertyOrder" : 10800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "localAuditLogRotation" : {
    "title" : "Rotate Local Audit Log",
    "description" : "Flag to indicate that audit log files should be rotated when reaching a certain
size. (property name: com.sun.identity.agents.config.local.log.rotate) <br>Hot-swap: Yes",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logoutEntryUri" : {
    "title" : "Logout Entry URI",
    "description" : "An application-specific Map that identifies a URI to be used as an entry point
after successful logout and subsequent successful authentication if applicable. (property name:
com.sun.identity.agents.config.logout.entry.uri) <br>Valid key: the web application name. <br>Valid
value: the logout entry URI. <br>For this property, a global value can be set to apply to all the
applications that don't have their own specific logout entry URI. <br>Hot-swap: Yes <br> Examples:
<br>To set a global application logout entry URI: leave Map Key field empty, and enter the global
application logout entry URI /welcome.html in Corresponding Map Value field. <br> To set the logout
entry URI for application BankApp: enter BankApp in Map Key field, and enter the logout entry URI /
BankApp/welcome.html in Corresponding Map Value field.",
    "propertyOrder" : 6300,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "cookieResetNames" : {
    "title" : "Cookies Reset Name List",
    "description" : "Cookie names that will be reset by the Agent if Cookie Reset is enabled.
(property name: com.sun.identity.agents.config.cdsso.cookie.reset.name) <br>Hot-swap: Yes",
    "propertyOrder" : 4700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userDataCachePollingTime" : {
    "title" : "User Data Cache Polling Time",
    "description" : "Cache update time in minutes for user management data. If set to '0' no updates
happen. (property name: com.ipplanet.am.sdk.remote.pollingTime) <br>Hot-swap: No",
    "propertyOrder" : 10600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "portCheckSetting" : {
    "title" : "Port Check Setting",

```

```

    "description" : "Map of port versus protocol entries with the key being the listening port
number and value being the listening protocol to be used by the Agent to identify requests with
invalid port numbers. (property name: com.sun.identity.agents.config.port.check.setting) <br>Hot-
swap: Yes <br> Example: <br> To map port 80 to protocol http: enter 80 in Map Key field, and enter
http in Corresponding Map Value field.",
    "propertyOrder" : 7400,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"probeLoginUrl" : {
    "title" : "Login URL Probe",
    "description" : "Specifies if agent will check the availability of these urls before redirecting
to them. (property name: com.sun.identity.agents.config.login.url.probe.enabled) <br>Hot-swap: Yes",
    "propertyOrder" : 3900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"cdsso" : {
    "title" : "Cross Domain SSO",
    "description" : "Enables Cross Domain Single SignOn. (property name:
com.sun.identity.agents.config.cdsso.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"redirectAttemptLimit" : {
    "title" : "Redirect Attempt Limit",
    "description" : "Number of successive single point redirects that a user can make using a
single browser session which will trigger the blocking of the user request. Set to 0 to disable this
feature. (property name: com.sun.identity.agents.config.redirect.attempt.limit) <br>Hot-swap: Yes",
    "propertyOrder" : 7100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"loginContentFile" : {
    "title" : "Login Content File Name",
    "description" : "Complete path and name of custom login content file. (property name:
com.sun.identity.agents.config.login.content.file) <br>Hot-swap: Yes",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"invertNotEnforcedIps" : {
    "title" : "Not Enforced IP Invert List",
    "description" : "Client IP Addresses to invert protection of IP addresses listed in the related
Not Enforced Client IP List. (property name: com.sun.identity.agents.config.notenforced.ip.invert)
<br>Hot-swap: Yes",
    "propertyOrder" : 8000,
    "required" : true,

```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "postDataStickySessionMode" : {
        "title" : "PDP Stickysession mode",
        "description" : "The PDP mechanism needs sticky loadbalancing, the URL mode will
append a querystring, while the Cookie mode will create a cookie. (property name:
com.sun.identity.agents.config.postdata.preserve.stickysession.mode)",
        "propertyOrder" : 13400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "userPrincipalFlag" : {
        "title" : "User Principal Flag",
        "description" : "Use principal instead of just the user-ID for authenticating the user.
(property name: com.sun.identity.agents.config.user.principal) <br>Hot-swap: Yes",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "webServiceEnabled" : {
        "title" : "Web Service Enable",
        "description" : "Flag specifies if Web Service processing is enabled. (property name:
com.sun.identity.agents.config.webservice.enable) <br>Hot-swap: Yes",
        "propertyOrder" : 2000,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "cdssoClockSkew" : {
        "title" : "CDSSO Clock Skew",
        "description" : "Time in seconds to be used by the Agent to determine the validity of the CDSSO
AuthnResponse assertion. (property name: com.sun.identity.agents.config.cdsso.clock.skew) <br>Hot-
swap: Yes",
        "propertyOrder" : 5300,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "notEnforcedUrisRefreshSessionIdleTime" : {
        "title" : "Refresh Session Idle Time",
        "description" : "Indicates if opensso session idle time should be refreshed or reset for not
enforced URIs. (property name: com.sun.identity.agents.config.notenforced.refresh.session.idletime)
<br>Hot-swap: Yes",
        "propertyOrder" : 8600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "fqdnDefault" : {
        "title" : "FQDN Default",
        "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default) <br>Hot-swap: Yes",
        "propertyOrder" : 6500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }

```

```

    },
    "alternativeAgentPort" : {
      "title" : "Alternative Agent Port Name",
      "description" : "Port number identifying the Agent protected server listening port
to the client browsers if different from the actual listening port. (property name:
com.sun.identity.agents.config.agent.port) <br>Hot-swap: Yes",
      "propertyOrder" : 4200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userAttributeName" : {
      "title" : "User Attribute Name",
      "description" : "Name of the attribute which contains the user-ID. (property name:
com.sun.identity.agents.config.user.attribute.name) <br>Hot-swap: Yes",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientIpHeader" : {
      "title" : "Client IP Address Header",
      "description" : "HTTP header name that holds the IP address of the client. (property name:
com.sun.identity.agents.config.client.ip.header) <br>Hot-swap: Yes",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "notEnforcedIpsCacheEnabled" : {
      "title" : "Not Enforced IP Cache Flag",
      "description" : "Enable caching of not-enforced IP list evaluation results. (property name:
com.sun.identity.agents.config.notenforced.ip.cache.enable) <br>Hot-swap: Yes",
      "propertyOrder" : 8100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cdssoTrustedIdProvider" : {
      "title" : "CDSSO Trusted ID Provider",
      "description" : "List of OpenAM Server/ID providers that should be trusted
by the agent, when evaluating the CDC Liberty Responses. (property name:
com.sun.identity.agents.config.cdsso.trusted.id.provider) <br>Hot-swap: Yes <br> Example: <br>
http://host:port/opensso/cdcservlet",
      "propertyOrder" : 5600,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "enableClientPolling" : {
      "title" : "Enable Client Polling",
      "description" : "Specifies if the session client must use polling for updating
session information and not depend upon server notifications. (property name:
com.iplanet.am.session.client.polling.enable) <br>Hot-swap: No",
      "propertyOrder" : 10200,
      "required" : true,

```

```

    "type" : "boolean",
    "exampleValue" : ""
  },
  "loginUrlPrioritized" : {
    "title" : "Login URL Prioritized",
    "description" : "Specifies if failover sequence for Login URLs or CDSSO URLs
should be prioritized as defined in the OpenAM Login URL list. (property name:
com.sun.identity.agents.config.login.url.prioritized) <br>Hot-swap: Yes",
    "propertyOrder" : 3800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "httpSessionBinding" : {
    "title" : "HTTP Session Binding",
    "description" : "If true will invalidate the http session when login has failed, user
has no SSO session, or principal user name does not match SSO user name. (property name:
com.sun.identity.agents.config.httpsession.binding) <br>Hot-swap: Yes",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }
}
}

```

## 1.65. Jdbc

### 1.65.1. Realm Operations

Resource path: `/realm-config/services/audit/JDBC`

Resource version: `1.0`

#### 1.65.1.1. create

Usage:

```
am> create Jdbc --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```

"properties" : {
  "jdbcBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 3,
    "properties" : {
      "bufferingEnabled" : {
        "title" : "Buffering Enabled",
        "description" : "Enables or disables audit event buffering.",
        "propertyOrder" : 4300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "bufferingMaxSize" : {
        "title" : "Buffer Size (number of events)",
        "description" : "Size of the queue where events are buffered before they are written to
the database.<br><br>This queue has to be big enough to store all incoming events that have not yet
been written to the database.<p>If the queue reaches capacity, the process will block until a write
occurs.",
        "propertyOrder" : 4400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "bufferingMaxBatchedEvents" : {
        "title" : "Max Batched Events",
        "description" : "Specifies the maximum number of batched statements the database can support
per connection.",
        "propertyOrder" : 4700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "bufferingWriteInterval" : {
        "title" : "Write Interval",
        "description" : "Specifies the interval (seconds) at which buffered events are written to
the database.",
        "propertyOrder" : 4500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "bufferingWriterThreads" : {
        "title" : "Writer Threads",
        "description" : "Specifies the number of threads used to write the buffered events.",
        "propertyOrder" : 4600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
      "topics" : {

```

```

        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 3200,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 3100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"jdbcDatabaseConfig" : {
    "type" : "object",
    "title" : "Database Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "databaseType" : {
            "title" : "Database Type",
            "description" : "Select the database to use for logging audit events.<br><br>Identifies the
database in use, for example MySQL, Oracle, or SQL.",
            "propertyOrder" : 3300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "minIdle" : {
            "title" : "Minimum Idle Connections",
            "description" : "Specifies the minimum number of idle connections in the connection pool.",
            "propertyOrder" : 4100,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "driverClassName" : {
            "title" : "JDBC Driver",
            "description" : "Fully qualified JDBC driver class name.",
            "propertyOrder" : 3500,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "maxLifetime" : {
            "title" : "Maximum Connection Time (seconds)",
            "description" : "Specifies the maximum time a JDBC connection can be open, in seconds.",
            "propertyOrder" : 4000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    },
    "idleTimeout" : {

```



```

        "title" : "Maximum Connection Idle Timeout (seconds)",
        "description" : "Specifies the maximum idle time before the connection is closed, in
seconds.",
        "propertyOrder" : 3900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "username" : {
        "title" : "Database Username",
        "description" : "Specifies the username to access the database server.",
        "propertyOrder" : 3600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "maxPoolSize" : {
        "title" : "Maximum Connections",
        "description" : "Specifies the maximum number of connections in the connection pool.",
        "propertyOrder" : 4200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "password" : {
        "title" : "Database Password",
        "description" : "Specifies the password to access the database server.",
        "propertyOrder" : 3700,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "jdbcUrl" : {
        "title" : "JDBC Database URL",
        "description" : "URL of the JDBC database.",
        "propertyOrder" : 3400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "connectionTimeout" : {
        "title" : "Connection Timeout (seconds)",
        "description" : "Specifies the maximum wait time before failing the connection, in
seconds.",
        "propertyOrder" : 3800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",

```

```
"description" : "The fully qualified class name of the factory  
responsible for creating the Audit Event Handler. The class must implement  
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",  
  "propertyOrder" : 4800,  
  "required" : true,  
  "type" : "string",  
  "exampleValue" : ""  
}  
}  
}  
}
```

### 1.65.1.2. delete

Usage:

```
am> delete Jdbc --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.65.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Jdbc --realm Realm --actionName getAllTypes
```

### 1.65.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Jdbc --realm Realm --actionName getCreatableTypes
```

### 1.65.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Jdbc --realm Realm --actionName nextdescendents
```

### 1.65.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Jdbc --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.65.1.7. read

Usage:

```
am> read Jdbc --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.65.1.8. update

Usage:

```
am> update Jdbc --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jdbcBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables audit event buffering.",
          "propertyOrder" : 4300,
          "required" : true,
```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "bufferingMaxSize" : {
        "title" : "Buffer Size (number of events)",
        "description" : "Size of the queue where events are buffered before they are written to
the database.<br><br>This queue has to be big enough to store all incoming events that have not yet
been written to the database.<p>If the queue reaches capacity, the process will block until a write
occurs.",
        "propertyOrder" : 4400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "bufferingMaxBatchedEvents" : {
        "title" : "Max Batched Events",
        "description" : "Specifies the maximum number of batched statements the database can support
per connection.",
        "propertyOrder" : 4700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "bufferingWriteInterval" : {
        "title" : "Write Interval",
        "description" : "Specifies the interval (seconds) at which buffered events are written to
the database.",
        "propertyOrder" : 4500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "bufferingWriterThreads" : {
        "title" : "Writer Threads",
        "description" : "Specifies the number of threads used to write the buffered events.",
        "propertyOrder" : 4600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 3200,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {

```

```

        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 3100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
},
"jdbcDatabaseConfig" : {
    "type" : "object",
    "title" : "Database Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "databaseType" : {
            "title" : "Database Type",
            "description" : "Select the database to use for logging audit events.<br><br>Identifies the
database in use, for example MySQL, Oracle, or SQL.",
            "propertyOrder" : 3300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "minIdle" : {
            "title" : "Minimum Idle Connections",
            "description" : "Specifies the minimum number of idle connections in the connection pool.",
            "propertyOrder" : 4100,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "driverClassName" : {
            "title" : "JDBC Driver",
            "description" : "Fully qualified JDBC driver class name.",
            "propertyOrder" : 3500,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "maxLifetime" : {
            "title" : "Maximum Connection Time (seconds)",
            "description" : "Specifies the maximum time a JDBC connection can be open, in seconds.",
            "propertyOrder" : 4000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "idleTimeout" : {
            "title" : "Maximum Connection Idle Timeout (seconds)",
            "description" : "Specifies the maximum idle time before the connection is closed, in
seconds.",
            "propertyOrder" : 3900,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "username" : {
            "title" : "Database Username",
            "description" : "Specifies the username to access the database server.",

```

```

        "propertyOrder" : 3600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "maxPoolSize" : {
        "title" : "Maximum Connections",
        "description" : "Specifies the maximum number of connections in the connection pool.",
        "propertyOrder" : 4200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "password" : {
        "title" : "Database Password",
        "description" : "Specifies the password to access the database server.",
        "propertyOrder" : 3700,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "jdbcUrl" : {
        "title" : "JDBC Database URL",
        "description" : "URL of the JDBC database.",
        "propertyOrder" : 3400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "connectionTimeout" : {
        "title" : "Connection Timeout (seconds)",
        "description" : "Specifies the maximum wait time before failing the connection, in
seconds.",
        "propertyOrder" : 3800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 4800,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
}
}
}

```

```
}
```

## 1.65.2. Global Operations

Resource path: `/global-config/services/audit/JDBC`

Resource version: `1.0`

### 1.65.2.1. create

Usage:

```
am> create Jdbc --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jdbcBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingWriteInterval" : {
          "title" : "Write Interval",
          "description" : "Specifies the interval (seconds) at which buffered events are written to
the database.",
          "propertyOrder" : 4500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingMaxBatchedEvents" : {
          "title" : "Max Batched Events",
          "description" : "Specifies the maximum number of batched statements the database can support
per connection.",
          "propertyOrder" : 4700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables audit event buffering.",
          "propertyOrder" : 4300,
```

```

        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "bufferingWriterThreads" : {
        "title" : "Writer Threads",
        "description" : "Specifies the number of threads used to write the buffered events.",
        "propertyOrder" : 4600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "bufferingMaxSize" : {
        "title" : "Buffer Size (number of events)",
        "description" : "Size of the queue where events are buffered before they are written to
the database.<br><br>This queue has to be big enough to store all incoming events that have not yet
been written to the database.<p>If the queue reaches capacity, the process will block until a write
occurs.",
        "propertyOrder" : 4400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"jdbcDatabaseConfig" : {
    "type" : "object",
    "title" : "Database Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "idleTimeout" : {
            "title" : "Maximum Connection Idle Timeout (seconds)",
            "description" : "Specifies the maximum idle time before the connection is closed, in
seconds.",
            "propertyOrder" : 3900,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "password" : {
            "title" : "Database Password",
            "description" : "Specifies the password to access the database server.",
            "propertyOrder" : 3700,
            "required" : true,
            "type" : "string",
            "format" : "password",
            "exampleValue" : ""
        },
        "maxLifetime" : {
            "title" : "Maximum Connection Time (seconds)",
            "description" : "Specifies the maximum time a JDBC connection can be open, in seconds.",
            "propertyOrder" : 4000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "driverClassName" : {
            "title" : "JDBC Driver",
            "description" : "Fully qualified JDBC driver class name.",

```



```

        "propertyOrder" : 3500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "databaseType" : {
        "title" : "Database Type",
        "description" : "Select the database to use for logging audit events.<br><br>Identifies the
database in use, for example MySQL, Oracle, or SQL.",
        "propertyOrder" : 3300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "minIdle" : {
        "title" : "Minimum Idle Connections",
        "description" : "Specifies the minimum number of idle connections in the connection pool.",
        "propertyOrder" : 4100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "connectionTimeout" : {
        "title" : "Connection Timeout (seconds)",
        "description" : "Specifies the maximum wait time before failing the connection, in
seconds.",
        "propertyOrder" : 3800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "maxPoolSize" : {
        "title" : "Maximum Connections",
        "description" : "Specifies the maximum number of connections in the connection pool.",
        "propertyOrder" : 4200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "jdbcUrl" : {
        "title" : "JDBC Database URL",
        "description" : "URL of the JDBC database.",
        "propertyOrder" : 3400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "username" : {
        "title" : "Database Username",
        "description" : "Specifies the username to access the database server.",
        "propertyOrder" : 3600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",

```

```

    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
      "handlerFactory" : {
        "title" : "Factory Class Name",
        "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
        "propertyOrder" : 4800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
      "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 3100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "topics" : {
        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 3200,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      }
    }
  }
}
}
}
}

```

### 1.65.2.2. delete

Usage:

```
am> delete Jdbc --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.65.2.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Jdbc --global --actionName getAllTypes
```

### 1.65.2.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Jdbc --global --actionName getCreatableTypes
```

### 1.65.2.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Jdbc --global --actionName nextdescendents
```

### 1.65.2.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Jdbc --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.65.2.7. read

Usage:

```
am> read Jdbc --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.65.2.8. update

Usage:

```
am> update Jdbc --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jdbcBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingWriteInterval" : {
          "title" : "Write Interval",
          "description" : "Specifies the interval (seconds) at which buffered events are written to
the database.",
          "propertyOrder" : 4500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingMaxBatchedEvents" : {
          "title" : "Max Batched Events",
          "description" : "Specifies the maximum number of batched statements the database can support
per connection.",
          "propertyOrder" : 4700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables audit event buffering.",
          "propertyOrder" : 4300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "bufferingWriterThreads" : {
          "title" : "Writer Threads",
          "description" : "Specifies the number of threads used to write the buffered events.",
          "propertyOrder" : 4600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    "bufferingMaxSize" : {
      "title" : "Buffer Size (number of events)",
      "description" : "Size of the queue where events are buffered before they are written to
the database.<br><br>This queue has to be big enough to store all incoming events that have not yet
been written to the database.<p>If the queue reaches capacity, the process will block until a write
occurs.",
      "propertyOrder" : 4400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "jdbcDatabaseConfig" : {
    "type" : "object",
    "title" : "Database Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "idleTimeout" : {
        "title" : "Maximum Connection Idle Timeout (seconds)",
        "description" : "Specifies the maximum idle time before the connection is closed, in
seconds.",
        "propertyOrder" : 3900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "password" : {
        "title" : "Database Password",
        "description" : "Specifies the password to access the database server.",
        "propertyOrder" : 3700,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
      },
      "maxLifetime" : {
        "title" : "Maximum Connection Time (seconds)",
        "description" : "Specifies the maximum time a JDBC connection can be open, in seconds.",
        "propertyOrder" : 4000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "driverClassName" : {
        "title" : "JDBC Driver",
        "description" : "Fully qualified JDBC driver class name.",
        "propertyOrder" : 3500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "databaseType" : {
        "title" : "Database Type",
        "description" : "Select the database to use for logging audit events.<br><br>Identifies the
database in use, for example MySQL, Oracle, or SQL.",
        "propertyOrder" : 3300,
        "required" : true,
        "type" : "string",

```

```

        "exampleValue" : ""
    },
    "minIdle" : {
        "title" : "Minimum Idle Connections",
        "description" : "Specifies the minimum number of idle connections in the connection pool.",
        "propertyOrder" : 4100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "connectionTimeout" : {
        "title" : "Connection Timeout (seconds)",
        "description" : "Specifies the maximum wait time before failing the connection, in
seconds.",
        "propertyOrder" : 3800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "maxPoolSize" : {
        "title" : "Maximum Connections",
        "description" : "Specifies the maximum number of connections in the connection pool.",
        "propertyOrder" : 4200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "jdbcUrl" : {
        "title" : "JDBC Database URL",
        "description" : "URL of the JDBC database.",
        "propertyOrder" : 3400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "username" : {
        "title" : "Database Username",
        "description" : "Specifies the username to access the database server.",
        "propertyOrder" : 3600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 4800,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}

```

```

    }
  },
  "commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
      "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 3100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "topics" : {
        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 3200,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      }
    }
  }
}
}
}
}

```

## 1.66. JdbcModule

### 1.66.1. Realm Operations

Resource path: `/realm-config/authentication/modules/jdbc`

Resource version: `1.0`

#### 1.66.1.1. create

Usage:

```
am> create JdbcModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "password" : {
      "title" : "Database Password",
      "description" : "The password used to authenticate to the database<br><br><i>NB </i>Only used
when connection type is JDBC",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "passwordTransformClass" : {
      "title" : "Class to Transform Password Syntax",
      "description" : "This class is used to transform the supplied credentials from the
database.<br><br>The default implementation for this property is <code>ClearTextTransform</
code> that performs no transformation. If the supplied credentials need to be transformed
before comparing with the password field retrieved from the database, a custom implementation
should be provided. Any custom implementation must implement the following interface
<code>com.sun.identity.authentication.modules.jdbc.JDBCPasswordSyntaxTransform</code>",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "passwordColumn" : {
      "title" : "Password Column Name",
      "description" : "The name of the column in the database containing the user
passwords<br><br>This property will be used to retrieve the correct column containing the password
from the results table returned by the database",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "connectionType" : {
      "title" : "Connection Type",
      "description" : "Controls how the authentication module will obtain the JDBC connection to
the database.<br><br>If the connection type is non-persistent JDBC connection then the JDBC driver
must be available to the OpenAM web-app. If the connection type is JNDI, the OpenAM web application
deployment descriptor <code>web.xml</code> must be updated to include the correct JNDI JDBC resource
information. The J2EE container must also be configured with the correct JNDI JDBC configuration.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jdbcDriver" : {
      "title" : "JDBC Driver",
      "description" : "The classname of the JDBC driver to use.<br><br>The fully qualified class name
of the JDBC driver to use to connect to the database. Only Oracle or MySQL drivers are supported.
JDBC drivers for other database may work, but the database will be treated as if it was Oracle.<br>
><br><i>NB </i>Only used when connection type is JDBC",
      "propertyOrder" : 300,

```



```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jdbcUrl" : {
    "title" : "JDBC URL",
    "description" : "The JDBC URL used to initialise the JDBC driver<br><br><i>NB </i>Only used when
connection type is JDBC",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "passwordStatement" : {
    "title" : "Prepared Statement",
    "description" : "The SQL statement used to search the database for user passwords<br><br>The
SQL statement used to search the database for the user password. A single property of the supplied
username is provided by the module. The result of the search should be a single row that contains the
password for the user under the specified column.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "username" : {
    "title" : "Database Username",
    "description" : "This username will be used to authenticate to the database<br><br><i>NB </
i>Only used when connection type is JDBC",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "connectionPoolJndiName" : {
    "title" : "Connection Pool JNDI Name",
    "description" : "The JNDI URL to the JDBC connection pool<br><br>The JNDI URL refers to the
JDBC connection pool created in the J2EE container for the authentication database.<br><br><i>NB </
i>Only used when connection type is JNDI",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
}

```

### 1.66.1.2. delete

Usage:

```
am> delete JdbcModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.66.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action JdbcModule --realm Realm --actionName getAllTypes
```

### 1.66.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action JdbcModule --realm Realm --actionName getCreatableTypes
```

### 1.66.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action JdbcModule --realm Realm --actionName nextdescendents
```

### 1.66.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query JdbcModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.66.1.7. read

Usage:

```
am> read JdbcModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.66.1.8. update

Usage:

```
am> update JdbcModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "password" : {
      "title" : "Database Password",
      "description" : "The password used to authenticate to the database<br><br><i>NB </i>Only used
when connection type is JDBC",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "passwordTransformClass" : {
      "title" : "Class to Transform Password Syntax",
      "description" : "This class is used to transform the supplied credentials from the
database.<br><br>The default implementation for this property is <code>ClearTextTransform</
code> that performs no transformation. If the supplied credentials need to be transformed
before comparing with the password field retrieved from the database, a custom implementation
should be provided. Any custom implementation must implement the following interface
<code>com.sun.identity.authentication.modules.jdbc.JDBCPasswordSyntaxTransform</code>",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "passwordColumn" : {
      "title" : "Password Column Name",
```

```

    "description" : "The name of the column in the database containing the user
passwords<br><br>This property will be used to retrieve the correct column containing the password
from the results table returned by the database",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "connectionType" : {
    "title" : "Connection Type",
    "description" : "Controls how the authentication module will obtain the JDBC connection to
the database.<br><br>If the connection type is non-persistent JDBC connection then the JDBC driver
must be available to the OpenAM web-app. If the connection type is JNDI, the OpenAM web application
deployment descriptor <code>web.xml</code> must be updated to include the correct JNDI JDBC resource
information. The J2EE container must also be configured with the correct JNDI JDBC configuration.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jdbcDriver" : {
    "title" : "JDBC Driver",
    "description" : "The classname of the JDBC driver to use.<br><br>The fully qualified class name
of the JDBC driver to use to connect to the database. Only Oracle or MySQL drivers are supported.
JDBC drivers for other database may work, but the database will be treated as if it was Oracle.<br>
><br><i>NB </i>Only used when connection type is JDBC",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jdbcUrl" : {
    "title" : "JDBC URL",
    "description" : "The JDBC URL used to initialise the JDBC driver<br><br><i>NB </i>Only used when
connection type is JDBC",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "passwordStatement" : {
    "title" : "Prepared Statement",
    "description" : "The SQL statement used to search the database for user passwords<br><br>The
SQL statement used to search the database for the user password. A single property of the supplied
username is provided by the module. The result of the search should be a single row that contains the
password for the user under the specified column.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",

```

```

    "exampleValue" : ""
  },
  "username" : {
    "title" : "Database Username",
    "description" : "This username will be used to authenticate to the database<br><br><i>NB </i>Only used when connection type is JDBC",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "connectionPoolJndiName" : {
    "title" : "Connection Pool JNDI Name",
    "description" : "The JNDI URL to the JDBC connection pool<br><br>The JNDI URL refers to the JDBC connection pool created in the J2EE container for the authentication database.<br><br><i>NB </i>Only used when connection type is JNDI",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
}

```

## 1.66.2. Global Operations

Resource path: `/global-config/authentication/modules/jdbc`

Resource version: `1.0`

### 1.66.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action JdbcModule --global --actionName getAllTypes
```

### 1.66.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action JdbcModule --global --actionName getCreatableTypes
```

### 1.66.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action JdbcModule --global --actionName nextdescendents
```

#### 1.66.2.4. read

Usage:

```
am> read JdbcModule --global
```

#### 1.66.2.5. update

Usage:

```
am> update JdbcModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "password" : {
          "title" : "Database Password",
          "description" : "The password used to authenticate to the database<br><br><i>NB </i>Only
used when connection type is JDBC",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "username" : {
          "title" : "Database Username",
          "description" : "This username will be used to authenticate to the database<br><br><i>NB </
i>Only used when connection type is JDBC",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

"connectionPoolJndiName" : {
  "title" : "Connection Pool JNDI Name",
  "description" : "The JNDI URL to the JDBC connection pool<br><br>The JNDI URL refers to the
JDBC connection pool created in the J2EE container for the authentication database.<br><br><i>NB </i>
Only used when connection type is JNDI",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"jdbcUrl" : {
  "title" : "JDBC URL",
  "description" : "The JDBC URL used to initialise the JDBC driver<br><br><i>NB </i>Only used
when connection type is JDBC",
  "propertyOrder" : 400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"passwordStatement" : {
  "title" : "Prepared Statement",
  "description" : "The SQL statement used to search the database for user passwords<br><br>The
SQL statement used to search the database for the user password. A single property of the supplied
username is provided by the module. The result of the search should be a single row that contains the
password for the user under the specified column.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"jdbcDriver" : {
  "title" : "JDBC Driver",
  "description" : "The classname of the JDBC driver to use.<br><br>The fully qualified
class name of the JDBC driver to use to connect to the database. Only Oracle or MySQL drivers are
supported. JDBC drivers for other database may work, but the database will be treated as if it was
Oracle.<br><br><i>NB </i>Only used when connection type is JDBC",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"passwordTransformClass" : {
  "title" : "Class to Transform Password Syntax",
  "description" : "This class is used to transform the supplied credentials from the
database.<br><br>The default implementation for this property is <code>ClearTextTransform</
code> that performs no transformation. If the supplied credentials need to be transformed
before comparing with the password field retrieved from the database, a custom implementation
should be provided. Any custom implementation must implement the following interface
<code>com.sun.identity.authentication.modules.jdbc.JDBCPasswordSyntaxTransform</code>",
  "propertyOrder" : 900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"connectionType" : {
  "title" : "Connection Type",
  "description" : "Controls how the authentication module will obtain the JDBC connection to
the database.<br><br>If the connection type is non-persistent JDBC connection then the JDBC driver
must be available to the OpenAM web-app. If the connection type is JNDI, the OpenAM web application

```

```
deployment descriptor <code>web.xml</code> must be updated to include the correct JNDI JDBC resource
information. The J2EE container must also be configured with the correct JNDI JDBC configuration.",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"passwordColumn" : {
  "title" : "Password Column Name",
  "description" : "The name of the column in the database containing the user
passwords<br><br>This property will be used to retrieve the correct column containing the password
from the results table returned by the database",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
},
"type" : "object",
"title" : "Realm Defaults"
}
}
```

## 1.67. Jms

### 1.67.1. Realm Operations

Resource path: `/realm-config/services/audit/JMS`

Resource version: `1.0`

#### 1.67.1.1. create

Usage:

```
am> create Jms --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jmsConfiguration" : {
```



```

    "type" : "object",
    "title" : "JMS Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "deliveryMode" : {
        "title" : "Delivery Mode",
        "description" : "Specifies whether JMS messages used to transmit audit events use persistent
or non-persistent delivery.<p><p>With persistent delivery, the JMS provider ensures that messages
are not lost in transit in case of a provider failure by logging messages to storage when they are
sent.<p>Specify the delivery mode as persistent if it is unacceptable for delivery of audit events
to be lost in JMS transit. If the possible loss of audit events is acceptable, choose non-persistent
delivery, which provides better performance.",
        "propertyOrder" : 6400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "jndiConnectionFactoryName" : {
        "title" : "JMS Connection Factory Name",
        "description" : "Specifies the JNDI lookup name for the connection factory exposed by your
JMS message broker. OpenAM performs a JNDI lookup on this name to locate your broker's connection
factory.<p><p>See the documentation for your JMS message broker for the required value.<p>The default
is the connection factory name for Apache ActiveMQ.",
        "propertyOrder" : 6800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "jndiContextProperties" : {
        "title" : "JNDI Context Properties",
        "description" : "Specifies JNDI properties that OpenAM uses to connect to the JMS message
broker to which OpenAM will publish audit events.<p><p>OpenAM acts as a JMS client, using a JMS
connection factory to connect to your JMS message broker. In order for OpenAM to connect to the
broker, the JNDI context properties must conform to those needed by the broker. See the documentation
for your JMS message broker for required values.<p>The default properties are example properties for
connecting to Apache ActiveMQ.",
        "propertyOrder" : 6600,
        "required" : true,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : ""
      },
      "jndiTopicName" : {
        "title" : "JMS Topic Name",
        "description" : "JNDI lookup name for the JMS topic",
        "propertyOrder" : 6700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "sessionMode" : {
        "title" : "Session Mode",
        "description" : "Specifies the JMS session acknowledgement mode: <code>AUTO</code>,
<code>CLIENT</code>, or <code>DUPS_OK</code>.<p><ul><li>Auto mode guarantees once-only delivery of
JMS messages used to transmit audit events.</li><li>Duplicates OK mode ensures that messages are

```

delivered at least once.

Client mode does not ensure delivery.

Use the default setting unless your JMS broker implementation requires otherwise. See your broker documentation for more information.

```

    "propertyOrder" : 6500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
},
"batchEvents" : {
  "type" : "object",
  "title" : "Batch Events",
  "propertyOrder" : 3,
  "properties" : {
    "batchEnabled" : {
      "title" : "Batch enabled",
      "description" : "Boolean for batch delivery of audit events.",
      "propertyOrder" : 6900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "insertTimeoutSec" : {
      "title" : "Insert Timeout",
      "description" : "Waiting period (seconds) for available capacity, when a new event enters
the queue.",
      "propertyOrder" : 7300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "pollTimeoutSec" : {
      "title" : "Polling Timeout",
      "description" : "Worker thread waiting period (seconds) for the next event, before going
idle.",
      "propertyOrder" : 7400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxBatchedEvents" : {
      "title" : "Max Batched",
      "description" : "Maximum number of events per batch.",
      "propertyOrder" : 7100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "batchThreadCount" : {
      "title" : "Thread Count",
      "description" : "Number of concurrent threads that pull events from the batch queue.",
      "propertyOrder" : 7200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "shutdownTimeoutSec" : {
      "title" : "Shutdown Timeout",

```

```

        "description" : "Application waiting period (seconds) for worker thread termination.",
        "propertyOrder" : 7500,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "batchCapacity" : {
        "title" : "Capacity",
        "description" : "Maximum event count in the batch queue; additional events are dropped.",
        "propertyOrder" : 7000,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 7600,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 6300,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 6200,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
}
}
}

```

```
}  
}
```

### 1.67.1.2. delete

Usage:

```
am> delete Jms --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.67.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Jms --realm Realm --actionName getAllTypes
```

### 1.67.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Jms --realm Realm --actionName getCreatableTypes
```

### 1.67.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Jms --realm Realm --actionName nextdescendents
```

### 1.67.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Jms --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.67.1.7. read

**Usage:**

```
am> read Jms --realm Realm --id id
```

**Parameters:****--id**

The unique identifier for the resource.

### 1.67.1.8. update

**Usage:**

```
am> update Jms --realm Realm --id id --body body
```

**Parameters:****--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jmsConfiguration" : {
      "type" : "object",
      "title" : "JMS Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "deliveryMode" : {
          "title" : "Delivery Mode",
          "description" : "Specifies whether JMS messages used to transmit audit events use persistent or non-persistent delivery.<p><p>With persistent delivery, the JMS provider ensures that messages are not lost in transit in case of a provider failure by logging messages to storage when they are sent.<p>Specify the delivery mode as persistent if it is unacceptable for delivery of audit events to be lost in JMS transit. If the possible loss of audit events is acceptable, choose non-persistent delivery, which provides better performance.",
          "propertyOrder" : 6400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiConnectionFactoryName" : {
          "title" : "JMS Connection Factory Name",
```

```

    "description" : "Specifies the JNDI lookup name for the connection factory exposed by your
JMS message broker. OpenAM performs a JNDI lookup on this name to locate your broker's connection
factory.<p><p>See the documentation for your JMS message broker for the required value.<p>The default
is the connection factory name for Apache ActiveMQ.",
    "propertyOrder" : 6800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
    "jndiContextProperties" : {
        "title" : "JNDI Context Properties",
        "description" : "Specifies JNDI properties that OpenAM uses to connect to the JMS message
broker to which OpenAM will publish audit events.<p><p>OpenAM acts as a JMS client, using a JMS
connection factory to connect to your JMS message broker. In order for OpenAM to connect to the
broker, the JNDI context properties must conform to those needed by the broker. See the documentation
for your JMS message broker for required values.<p>The default properties are example properties for
connecting to Apache ActiveMQ.",
        "propertyOrder" : 6600,
        "required" : true,
        "patternProperties" : {
            ".*" : {
                "type" : "string"
            }
        },
        "type" : "object",
        "exampleValue" : ""
    },
    "jndiTopicName" : {
        "title" : "JMS Topic Name",
        "description" : "JNDI lookup name for the JMS topic",
        "propertyOrder" : 6700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sessionMode" : {
        "title" : "Session Mode",
        "description" : "Specifies the JMS session acknowledgement mode: <code>AUTO</code>,
<code>CLIENT</code>, or <code>DUPS_OK</code>.<p><ul><li>Auto mode guarantees once-only delivery of
JMS messages used to transmit audit events.</li><li>Duplicates OK mode ensures that messages are
delivered at least once.</li><li>Client mode does not ensure delivery.</li></ul><p>Use the default
setting unless your JMS broker implementation requires otherwise. See your broker documentation for
more information.",
        "propertyOrder" : 6500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
    "batchEvents" : {
        "type" : "object",
        "title" : "Batch Events",
        "propertyOrder" : 3,
        "properties" : {
            "batchEnabled" : {
                "title" : "Batch enabled",
                "description" : "Boolean for batch delivery of audit events.",
                "propertyOrder" : 6900,

```

```

        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "insertTimeoutSec" : {
        "title" : "Insert Timeout",
        "description" : "Waiting period (seconds) for available capacity, when a new event enters
the queue.",
        "propertyOrder" : 7300,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "pollTimeoutSec" : {
        "title" : "Polling Timeout",
        "description" : "Worker thread waiting period (seconds) for the next event, before going
idle.",
        "propertyOrder" : 7400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "maxBatchedEvents" : {
        "title" : "Max Batched",
        "description" : "Maximum number of events per batch.",
        "propertyOrder" : 7100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "batchThreadCount" : {
        "title" : "Thread Count",
        "description" : "Number of concurrent threads that pull events from the batch queue.",
        "propertyOrder" : 7200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "shutdownTimeoutSec" : {
        "title" : "Shutdown Timeout",
        "description" : "Application waiting period (seconds) for worker thread termination.",
        "propertyOrder" : 7500,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "batchCapacity" : {
        "title" : "Capacity",
        "description" : "Maximum event count in the batch queue; additional events are dropped.",
        "propertyOrder" : 7000,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",

```

```

    "propertyOrder" : 1,
    "properties" : {
      "handlerFactory" : {
        "title" : "Factory Class Name",
        "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
        "propertyOrder" : 7600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 6300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}

```

## 1.67.2. Global Operations

Resource path: `/global-config/services/audit/JMS`

Resource version: `1.0`

### 1.67.2.1. create

Usage:

```
am> create Jms --global --id id --body body
```



Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "batchEvents" : {
      "type" : "object",
      "title" : "Batch Events",
      "propertyOrder" : 3,
      "properties" : {
        "batchEnabled" : {
          "title" : "Batch enabled",
          "description" : "Boolean for batch delivery of audit events.",
          "propertyOrder" : 6900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "maxBatchedEvents" : {
          "title" : "Max Batched",
          "description" : "Maximum number of events per batch.",
          "propertyOrder" : 7100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "pollTimeoutSec" : {
          "title" : "Polling Timeout",
          "description" : "Worker thread waiting period (seconds) for the next event, before going
idle.",
          "propertyOrder" : 7400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "insertTimeoutSec" : {
          "title" : "Insert Timeout",
          "description" : "Waiting period (seconds) for available capacity, when a new event enters
the queue.",
          "propertyOrder" : 7300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "batchCapacity" : {
          "title" : "Capacity",
          "description" : "Maximum event count in the batch queue; additional events are dropped.",
          "propertyOrder" : 7000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    },
    "batchThreadCount" : {
      "title" : "Thread Count",
      "description" : "Number of concurrent threads that pull events from the batch queue.",
      "propertyOrder" : 7200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "shutdownTimeoutSec" : {
      "title" : "Shutdown Timeout",
      "description" : "Application waiting period (seconds) for worker thread termination.",
      "propertyOrder" : 7500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
},
"jmsConfiguration" : {
  "type" : "object",
  "title" : "JMS Configuration",
  "propertyOrder" : 2,
  "properties" : {
    "jndiConnectionFactoryName" : {
      "title" : "JMS Connection Factory Name",
      "description" : "Specifies the JNDI lookup name for the connection factory exposed by your JMS message broker. OpenAM performs a JNDI lookup on this name to locate your broker's connection factory.<p><p>See the documentation for your JMS message broker for the required value.<p>The default is the connection factory name for Apache ActiveMQ.",
      "propertyOrder" : 6800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "jndiTopicName" : {
      "title" : "JMS Topic Name",
      "description" : "JNDI lookup name for the JMS topic",
      "propertyOrder" : 6700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "jndiContextProperties" : {
      "title" : "JNDI Context Properties",
      "description" : "Specifies JNDI properties that OpenAM uses to connect to the JMS message broker to which OpenAM will publish audit events.<p><p>OpenAM acts as a JMS client, using a JMS connection factory to connect to your JMS message broker. In order for OpenAM to connect to the broker, the JNDI context properties must conform to those needed by the broker. See the documentation for your JMS message broker for required values.<p>The default properties are example properties for connecting to Apache ActiveMQ.",
      "propertyOrder" : 6600,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      }
    },
    },
    "type" : "object",

```

```

        "exampleValue" : ""
    },
    "sessionMode" : {
        "title" : "Session Mode",
        "description" : "Specifies the JMS session acknowledgement mode: <code>AUTO</code>,
<code>CLIENT</code>, or <code>DUPS_OK</code>.<p><ul><li>Auto mode guarantees once-only delivery of
JMS messages used to transmit audit events.</li><li>Duplicates OK mode ensures that messages are
delivered at least once.</li><li>Client mode does not ensure delivery.</li></ul><p>Use the default
setting unless your JMS broker implementation requires otherwise. See your broker documentation for
more information.",
        "propertyOrder" : 6500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "deliveryMode" : {
        "title" : "Delivery Mode",
        "description" : "Specifies whether JMS messages used to transmit audit events use persistent
or non-persistent delivery.<p><p>With persistent delivery, the JMS provider ensures that messages
are not lost in transit in case of a provider failure by logging messages to storage when they are
sent.<p>Specify the delivery mode as persistent if it is unacceptable for delivery of audit events
to be lost in JMS transit. If the possible loss of audit events is acceptable, choose non-persistent
delivery, which provides better performance.",
        "propertyOrder" : 6400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 6300,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 6200,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",

```

```
    "propertyOrder" : 1,
    "properties" : {
      "handlerFactory" : {
        "title" : "Factory Class Name",
        "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
        "propertyOrder" : 7600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  }
}
```

### 1.67.2.2. delete

Usage:

```
am> delete Jms --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.67.2.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Jms --global --actionName getAllTypes
```

### 1.67.2.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Jms --global --actionName getCreatableTypes
```

### 1.67.2.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Jms --global --actionName nextdescendents
```

### 1.67.2.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Jms --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.67.2.7. read

Usage:

```
am> read Jms --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.67.2.8. update

Usage:

```
am> update Jms --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "batchEvents" : {
      "type" : "object",
      "title" : "Batch Events",
      "propertyOrder" : 3,
      "properties" : {
        "batchEnabled" : {
          "title" : "Batch enabled",
          "description" : "Boolean for batch delivery of audit events.",
          "propertyOrder" : 6900,
          "required" : true,
```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "maxBatchedEvents" : {
        "title" : "Max Batched",
        "description" : "Maximum number of events per batch.",
        "propertyOrder" : 7100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "pollTimeoutSec" : {
        "title" : "Polling Timeout",
        "description" : "Worker thread waiting period (seconds) for the next event, before going
idle.",
        "propertyOrder" : 7400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "insertTimeoutSec" : {
        "title" : "Insert Timeout",
        "description" : "Waiting period (seconds) for available capacity, when a new event enters
the queue.",
        "propertyOrder" : 7300,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "batchCapacity" : {
        "title" : "Capacity",
        "description" : "Maximum event count in the batch queue; additional events are dropped.",
        "propertyOrder" : 7000,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "batchThreadCount" : {
        "title" : "Thread Count",
        "description" : "Number of concurrent threads that pull events from the batch queue.",
        "propertyOrder" : 7200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "shutdownTimeoutSec" : {
        "title" : "Shutdown Timeout",
        "description" : "Application waiting period (seconds) for worker thread termination.",
        "propertyOrder" : 7500,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
}
},
"jmsConfiguration" : {
    "type" : "object",
    "title" : "JMS Configuration",
    "propertyOrder" : 2,

```

```

"properties" : {
  "jndiConnectionFactoryName" : {
    "title" : "JMS Connection Factory Name",
    "description" : "Specifies the JNDI lookup name for the connection factory exposed by your
JMS message broker. OpenAM performs a JNDI lookup on this name to locate your broker's connection
factory.<p><p>See the documentation for your JMS message broker for the required value.<p>The default
is the connection factory name for Apache ActiveMQ.",
    "propertyOrder" : 6800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jndiTopicName" : {
    "title" : "JMS Topic Name",
    "description" : "JNDI lookup name for the JMS topic",
    "propertyOrder" : 6700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jndiContextProperties" : {
    "title" : "JNDI Context Properties",
    "description" : "Specifies JNDI properties that OpenAM uses to connect to the JMS message
broker to which OpenAM will publish audit events.<p><p>OpenAM acts as a JMS client, using a JMS
connection factory to connect to your JMS message broker. In order for OpenAM to connect to the
broker, the JNDI context properties must conform to those needed by the broker. See the documentation
for your JMS message broker for required values.<p>The default properties are example properties for
connecting to Apache ActiveMQ.",
    "propertyOrder" : 6600,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "sessionMode" : {
    "title" : "Session Mode",
    "description" : "Specifies the JMS session acknowledgement mode: <code>AUTO</code>,
<code>CLIENT</code>, or <code>DUPS_OK</code>.<p><ul><li>Auto mode guarantees once-only delivery of
JMS messages used to transmit audit events.</li><li>Duplicates OK mode ensures that messages are
delivered at least once.</li><li>Client mode does not ensure delivery.</li></ul><p>Use the default
setting unless your JMS broker implementation requires otherwise. See your broker documentation for
more information.",
    "propertyOrder" : 6500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "deliveryMode" : {
    "title" : "Delivery Mode",
    "description" : "Specifies whether JMS messages used to transmit audit events use persistent
or non-persistent delivery.<p><p>With persistent delivery, the JMS provider ensures that messages
are not lost in transit in case of a provider failure by logging messages to storage when they are
sent.<p>Specify the delivery mode as persistent if it is unacceptable for delivery of audit events
to be lost in JMS transit. If the possible loss of audit events is acceptable, choose non-persistent
delivery, which provides better performance.",

```

```

        "propertyOrder" : 6400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 6300,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 6200,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement org.forgerock.openam.audit.AuditEventHandlerFactory.",
            "propertyOrder" : 7600,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
}
}
}
}

```



## 1.68. Json

### 1.68.1. Realm Operations

Resource path: `/realm-config/services/audit/JSON`

Resource version: `1.0`

#### 1.68.1.1. create

Usage:

```
am> create Json --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "jsonFileRotation" : {
```

```

    "type" : "object",
    "title" : "File Rotation",
    "propertyOrder" : 3,
    "properties" : {
      "rotationFilePrefix" : {
        "title" : "File Rotation Prefix",
        "description" : "Prefix to prepend to audit files when rotating audit files.",
        "propertyOrder" : 800,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationFileSuffix" : {
        "title" : "File Rotation Suffix",
        "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
        "propertyOrder" : 900,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationInterval" : {
        "title" : "Rotation Interval",
        "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationEnabled" : {
        "title" : "Rotation Enabled",
        "description" : "Enables and disables audit file rotation.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "rotationMaxFileSize" : {
        "title" : "Maximum File Size",
        "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationTimes" : {
        "title" : "Rotation Times",
        "description" : "Durations after midnight to trigger file rotation, in seconds.",
        "propertyOrder" : 1100,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      }
    }
  }
}

```

```

},
"jsonConfig" : {
  "type" : "object",
  "title" : "JSON Configuration",
  "propertyOrder" : 2,
  "properties" : {
    "rotationRetentionCheckInterval" : {
      "title" : "File Rotation Retention Check Interval",
      "description" : "Interval to check time-based file rotation policies, in seconds.",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "location" : {
      "title" : "Log Directory",
      "description" : "Directory in which to store audit log JSON files.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "elasticsearchCompatible" : {
      "title" : "ElasticSearch JSON Format Compatible",
      "description" : "JSON format should be transformed to be compatible with ElasticSearch
format restrictions.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
},
"commonHandlerPlugin" : {
  "type" : "object",
  "title" : "Audit Event Handler Factory",
  "propertyOrder" : 1,
  "properties" : {
    "handlerFactory" : {
      "title" : "Factory Class Name",
      "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
},
"jsonBuffering" : {
  "type" : "object",
  "title" : "Buffering",
  "propertyOrder" : 5,
  "properties" : {
    "bufferingWriteInterval" : {
      "title" : "Write interval",
      "description" : "Interval at which buffered events are written to a file, in milliseconds.",
      "propertyOrder" : 1600,

```

```

        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "bufferingMaxSize" : {
        "title" : "Batch Size",
        "description" : "Maximum number of audit log events that can be buffered.",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"jsonFileRetention" : {
    "type" : "object",
    "title" : "File Retention",
    "propertyOrder" : 4,
    "properties" : {
        "retentionMinFreeSpaceRequired" : {
            "title" : "Minimum Free Space Required",
            "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
            "title" : "Maximum Number of Historical Files",
            "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
            "propertyOrder" : 1200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
            "title" : "Maximum Disk Space",
            "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
}
}
}
}

```

### 1.68.1.2. delete

Usage:

```
am> delete Json --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.68.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Json --realm Realm --actionName getAllTypes
```

### 1.68.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Json --realm Realm --actionName getCreatableTypes
```

### 1.68.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Json --realm Realm --actionName nextdescendents
```

### 1.68.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Json --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.68.1.7. read

Usage:

```
am> read Json --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.68.1.8. update

Usage:

```
am> update Json --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "jsonFileRotation" : {
      "type" : "object",
      "title" : "File Rotation",
      "propertyOrder" : 3,
      "properties" : {
        "rotationFilePrefix" : {
          "title" : "File Rotation Prefix",
          "description" : "Prefix to prepend to audit files when rotating audit files.",
```

```

        "propertyOrder" : 800,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "rotationFileSuffix" : {
        "title" : "File Rotation Suffix",
        "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
        "propertyOrder" : 900,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "rotationInterval" : {
        "title" : "Rotation Interval",
        "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "rotationEnabled" : {
        "title" : "Rotation Enabled",
        "description" : "Enables and disables audit file rotation.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "rotationMaxFileSize" : {
        "title" : "Maximum File Size",
        "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "rotationTimes" : {
        "title" : "Rotation Times",
        "description" : "Durations after midnight to trigger file rotation, in seconds.",
        "propertyOrder" : 1100,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    }
}
},
"jsonConfig" : {
    "type" : "object",
    "title" : "JSON Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "rotationRetentionCheckInterval" : {

```

```

        "title" : "File Rotation Retention Check Interval",
        "description" : "Interval to check time-based file rotation policies, in seconds.",
        "propertyOrder" : 1800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "location" : {
        "title" : "Log Directory",
        "description" : "Directory in which to store audit log JSON files.",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "elasticsearchCompatible" : {
        "title" : "ElasticSearch JSON Format Compatible",
        "description" : "JSON format should be transformed to be compatible with ElasticSearch
format restrictions.",
        "propertyOrder" : 1700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 1900,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"jsonBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 5,
    "properties" : {
        "bufferingWriteInterval" : {
            "title" : "Write interval",
            "description" : "Interval at which buffered events are written to a file, in milliseconds.",
            "propertyOrder" : 1600,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "bufferingMaxSize" : {
            "title" : "Batch Size",
            "description" : "Maximum number of audit log events that can be buffered.",

```



```

        "propertyOrder" : 1500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"jsonFileRetention" : {
    "type" : "object",
    "title" : "File Retention",
    "propertyOrder" : 4,
    "properties" : {
        "retentionMinFreeSpaceRequired" : {
            "title" : "Minimum Free Space Required",
            "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
            "title" : "Maximum Number of Historical Files",
            "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
            "propertyOrder" : 1200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
            "title" : "Maximum Disk Space",
            "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
}
}
}

```

## 1.68.2. Global Operations

Resource path: `/global-config/services/audit/JSON`

Resource version: `1.0`

### 1.68.2.1. create

Usage:

```
am> create Json --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "rotationRetentionCheckInterval" : {
          "title" : "File Rotation Retention Check Interval",
          "description" : "Interval to check time-based file rotation policies, in seconds.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log JSON files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "elasticsearchCompatible" : {
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with ElasticSearch
format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "jsonBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 5,
      "properties" : {
        "bufferingMaxSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of audit log events that can be buffered.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    },
    "bufferingWriteInterval" : {
      "title" : "Write interval",
      "description" : "Interval at which buffered events are written to a file, in milliseconds.",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "jsonFileRetention" : {
    "type" : "object",
    "title" : "File Retention",
    "propertyOrder" : 4,
    "properties" : {
      "retentionMaxNumberOfHistoryFiles" : {
        "title" : "Maximum Number of Historical Files",
        "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
        "propertyOrder" : 1200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "retentionMinFreeSpaceRequired" : {
        "title" : "Minimum Free Space Required",
        "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "retentionMaxDiskSpaceToUse" : {
        "title" : "Maximum Disk Space",
        "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 1300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "jsonFileRotation" : {
    "type" : "object",
    "title" : "File Rotation",
    "propertyOrder" : 3,
    "properties" : {
      "rotationTimes" : {
        "title" : "Rotation Times",
        "description" : "Durations after midnight to trigger file rotation, in seconds.",
        "propertyOrder" : 1100,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",

```

```

    "exampleValue" : ""
  },
  "rotationMaxFileSize" : {
    "title" : "Maximum File Size",
    "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "rotationInterval" : {
    "title" : "Rotation Interval",
    "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "rotationEnabled" : {
    "title" : "Rotation Enabled",
    "description" : "Enables and disables audit file rotation.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "rotationFileSuffix" : {
    "title" : "File Rotation Suffix",
    "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
    "propertyOrder" : 900,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "rotationFilePrefix" : {
    "title" : "File Rotation Prefix",
    "description" : "Prefix to prepend to audit files when rotating audit files.",
    "propertyOrder" : 800,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  }
}
},
"commonHandlerPlugin" : {
  "type" : "object",
  "title" : "Audit Event Handler Factory",
  "propertyOrder" : 1,
  "properties" : {
    "handlerFactory" : {
      "title" : "Factory Class Name",
      "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
      "propertyOrder" : 1900,
      "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 400,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 300,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
}
}
}
}
}

```

### 1.68.2.2. delete

Usage:

```
am> delete Json --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.68.2.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Json --global --actionName getAllTypes
```

#### 1.68.2.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Json --global --actionName getCreatableTypes
```

#### 1.68.2.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Json --global --actionName nextdescendents
```

#### 1.68.2.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Json --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.68.2.7. read

Usage:

```
am> read Json --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.68.2.8. update

Usage:

```
am> update Json --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "rotationRetentionCheckInterval" : {
          "title" : "File Rotation Retention Check Interval",
          "description" : "Interval to check time-based file rotation policies, in seconds.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log JSON files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "elasticsearchCompatible" : {
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with ElasticSearch
format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "jsonBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 5,
      "properties" : {
        "bufferingMaxSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of audit log events that can be buffered.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingWriteInterval" : {
```

```

        "title" : "Write interval",
        "description" : "Interval at which buffered events are written to a file, in milliseconds.",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"jsonFileRetention" : {
    "type" : "object",
    "title" : "File Retention",
    "propertyOrder" : 4,
    "properties" : {
        "retentionMaxNumberOfHistoryFiles" : {
            "title" : "Maximum Number of Historical Files",
            "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
            "propertyOrder" : 1200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMinFreeSpaceRequired" : {
            "title" : "Minimum Free Space Required",
            "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
            "title" : "Maximum Disk Space",
            "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
            "propertyOrder" : 1300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"jsonFileRotation" : {
    "type" : "object",
    "title" : "File Rotation",
    "propertyOrder" : 3,
    "properties" : {
        "rotationTimes" : {
            "title" : "Rotation Times",
            "description" : "Durations after midnight to trigger file rotation, in seconds.",
            "propertyOrder" : 1100,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        }
    }
},

```



```

    "rotationMaxFileSize" : {
      "title" : "Maximum File Size",
      "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "rotationInterval" : {
      "title" : "Rotation Interval",
      "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "rotationEnabled" : {
      "title" : "Rotation Enabled",
      "description" : "Enables and disables audit file rotation.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "rotationFileSuffix" : {
      "title" : "File Rotation Suffix",
      "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
      "propertyOrder" : 900,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "rotationFilePrefix" : {
      "title" : "File Rotation Prefix",
      "description" : "Prefix to prepend to audit files when rotating audit files.",
      "propertyOrder" : 800,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
      "handlerFactory" : {
        "title" : "Factory Class Name",
        "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
        "propertyOrder" : 1900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  }
}

```

```

    }
  },
  "commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
      "topics" : {
        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 400,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  }
}
}
}
}

```

## 1.69. KbaQuestions

### 1.69.1. Realm Operations

KBA resource is responsible for delivering up configured security questions.

Resource path: `/selfservice/kba`

Resource version: `1.0`

#### 1.69.1.1. read

Read the configured security questions.

Usage:

```
am> read KbaQuestions --realm Realm
```

## 1.70. LdapModule

### 1.70.1. Realm Operations

Resource path: `/realm-config/authentication/modules/ldap`

Resource version: `1.0`

#### 1.70.1.1. create

Usage:

```
am> create LdapModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userProfileRetrievalAttribute" : {
      "title" : "Attribute Used to Retrieve User Profile",
      "description" : "The LDAP module will use this attribute to search of the profile of an authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user. Normally this will be the same attribute used to find the user account. The value will be the name of the user used for authentication.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "Enforced when the user is resetting their password as part of the authentication.<br><br>If the user needs to reset their password as part of the authentication process, the authentication module can enforce a minimum password length. This is separate from any password length controls from the underlying LDAP server. If the external LDAP server password policy is enforcing password length, set this value to 0 to avoid confusion.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "connectionHeartbeatTimeUnit" : {
      "title" : "LDAP Connection Heartbeat Time Unit",
      "description" : "Defines the time unit corresponding to the Heartbeat Interval setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
```

to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then it may take up to the interval period before the problem is detected. Use along with the Heartbeat Interval parameter to define the exact interval.",

```

    "propertyOrder" : 1800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributeMappings" : {
    "title" : "User Creation Attributes",
    "description" : "Controls the mapping of local attribute to external attribute for dynamic
profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
between the attribute/values retrieved from the users authenticated profile and the attribute/values
that will be provisioned into their matching account in the data store.<br><br>The format of this
property is: <br><br><code> local attr1|external attr1</code>",
    "propertyOrder" : 1300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "beheraPasswordPolicySupportEnabled" : {
    "title" : "LDAP Behera Password Policy Support",
    "description" : "Enables support for modern LDAP password policies<br><br>LDAP Behera Password
policies are supported by modern LDAP servers such as OpenDJ. If this functionality is disabled then
only the older Netscape VCHU password policy standard will be enforced.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "returnUserDN" : {
    "title" : "Return User DN to DataStore",
    "description" : "Controls whether the DN or the username is returned as the authentication
principal.",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userSearchAttributes" : {
    "title" : "Attributes Used to Search for a User to be Authenticated",
    "description" : "The attributes specified in this list form the LDAP search filter.<br><br>The
default value of uid will form the following search filter of <code>uid=<i>user</i></code>, if there
are multiple values such as uid and cn, the module will create a search filter as follows <code>(|
(uid=<i>user</i>)(cn=<i>user</i>))</code>",
    "propertyOrder" : 700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userBindPassword" : {
    "title" : "Bind User Password",
    "description" : "The password of the administration account.",

```

```

    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "secondaryLdapServer" : {
    "title" : "Secondary LDAP Server",
    "description" : "Use this list to set the secondary (failover) LDAP server used for authentication.<br><br>If the primary LDAP server fails, the LDAP authentication module will failover to the secondary server. A single entry must be in the format:<br><br><code>ldap_server:port</code><br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br><br><code>local server name | server:port</code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "trustAllServerCertificates" : {
    "title" : "Trust All Server Certificates",
    "description" : "Enables a <code>X509TrustManager</code> that trusts all certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP servers protected by self signed or invalid certificates (such as invalid hostname).<br><br><i>NB </i>Use this feature with care as it bypasses the normal certificate verification process",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "connectionHeartbeatInterval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then it may take up to the interval period before the problem is detected. Use along with the Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in disabling heartbeat requests.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "primaryLdapServer" : {
    "title" : "Primary LDAP Server",
    "description" : "Use this list to set the primary LDAP server used for authentication.<br><br>The LDAP authentication module will use this list as the primary server for authentication. A single entry must be in the format:<br><br><code>ldap_server:port</code><br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br><br><code>local server name | server:port</code><br><br>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },

```

```

    "type" : "array",
    "exampleValue" : ""
  },
  "userSearchStartDN" : {
    "title" : "DN to Start User Search",
    "description" : "The search for accounts to be authenticated start from this base DN <br><br>For a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different base DNS for the search The format is as follows:<br><br><code>local server name | search DN</code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "operationTimeout" : {
    "title" : "LDAP operations timeout",
    "description" : "Defines the timeout in seconds OpenAM should wait for a response of the Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or the JVM are applied. However this setting allows more granular control within OpenAM itself. A value of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS will apply.",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "openam-auth-ldap-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "searchScope" : {
    "title" : "Search Scope",
    "description" : "The level in the Directory Server that will be searched for a matching user profile.<br><br>This attribute controls how the directory is searched.<br><br><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the

```

```

single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
all levels below are searched</li></ul>",
  "propertyOrder" : 900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userSearchFilter" : {
  "title" : "User Search Filter",
  "description" : "This search filter will be appended to the standard user search
filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
For example: <code>(objectClass=person)</code>would result in the following user search filter:<br>
<br><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userBindDN" : {
  "title" : "Bind User DN",
  "description" : "The DN of an admin user used by the module to authentication to the LDAP
server<br><br>The LDAP module requires an administration account in order to perform functionality
such as password reset.<br><br><i>NB </i><code>cn=Directory Manager</code> should not be used in
production systems.",
  "propertyOrder" : 400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
}

```

### 1.70.1.2. delete

Usage:

```
am> delete LdapModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.70.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LdapModule --realm Realm --actionName getAllTypes
```

#### 1.70.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LdapModule --realm Realm --actionName getCreatableTypes
```

#### 1.70.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LdapModule --realm Realm --actionName nextdescendents
```

#### 1.70.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query LdapModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.70.1.7. read

Usage:

```
am> read LdapModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.70.1.8. update

Usage:

```
am> update LdapModule --realm Realm --id id --body body
```



Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userProfileRetrievalAttribute" : {
      "title" : "Attribute Used to Retrieve User Profile",
      "description" : "The LDAP module will use this attribute to search of the profile of an authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user. Normally this will be the same attribute used to find the user account. The value will be the name of the user used for authentication.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "Enforced when the user is resetting their password as part of the authentication.<br><br>If the user needs to reset their password as part of the authentication process, the authentication module can enforce a minimum password length. This is separate from any password length controls from the underlying LDAP server. If the external LDAP server password policy is enforcing password length, set this value to 0 to avoid confusion.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "connectionHeartbeatTimeUnit" : {
      "title" : "LDAP Connection Heartbeat Time Unit",
      "description" : "Defines the time unit corresponding to the Heartbeat Interval setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then it may take up to the interval period before the problem is detected. Use along with the Heartbeat Interval parameter to define the exact interval.",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "profileAttributeMappings" : {
      "title" : "User Creation Attributes",
      "description" : "Controls the mapping of local attribute to external attribute for dynamic profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping between the attribute/values retrieved from the users authenticated profile and the attribute/values that will be provisioned into their matching account in the data store.<br><br>The format of this property is: <br><br><code> local attr1|external attr1</code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      }
    }
  }
}
```

```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "beheraPasswordPolicySupportEnabled" : {
    "title" : "LDAP Behera Password Policy Support",
    "description" : "Enables support for modern LDAP password policies<br><br>LDAP Behera Password policies are supported by modern LDAP servers such as OpenDJ. If this functionality is disabled then only the older Netscape VCHU password policy standard will be enforced.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "returnUserDN" : {
    "title" : "Return User DN to DataStore",
    "description" : "Controls whether the DN or the username is returned as the authentication principal.",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userSearchAttributes" : {
    "title" : "Attributes Used to Search for a User to be Authenticated",
    "description" : "The attributes specified in this list form the LDAP search filter.<br><br>The default value of uid will form the following search filter of <code>uid=<i>user</i></code>, if there are multiple values such as uid and cn, the module will create a search filter as follows <code>(|uid=<i>user</i>)(cn=<i>user</i>)</code>",
    "propertyOrder" : 700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userBindPassword" : {
    "title" : "Bind User Password",
    "description" : "The password of the administration account.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "secondaryLdapServer" : {
    "title" : "Secondary LDAP Server",
    "description" : "Use this list to set the secondary (failover) LDAP server used for authentication.<br><br>If the primary LDAP server fails, the LDAP authentication module will failover to the secondary server. A single entry must be in the format:<br><br><code>ldap_server:port</code><br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br><br><code>local server name | server:port</code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },

```

```

    "type" : "array",
    "exampleValue" : ""
  },
  "trustAllServerCertificates" : {
    "title" : "Trust All Server Certificates",
    "description" : "Enables a X509TrustManager that trusts all
certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
servers protected by self signed or invalid certificates (such as invalid hostname).<br><br><i>NB
</i>Use this feature with care as it bypasses the normal certificate verification process",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "connectionHeartbeatInterval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "primaryLdapServer" : {
    "title" : "Primary LDAP Server",
    "description" : "Use this list to set the primary LDAP server used for authentication.
<br><br>The LDAP authentication module will use this list as the primary server for authentication. A
single entry must be in the format:<br><br><code>ldap_server:port</code><br><br>Multiple entries
allow associations between OpenAM servers and a LDAP server. The format is:<br><br><code>local
server name | server:port</code><br><br>The local server name is the full name of the server from
the list of servers and sites.",
    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userSearchStartDN" : {
    "title" : "DN to Start User Search",
    "description" : "The search for accounts to be authenticated start from this base DN <br><br>For
a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different
base DN's for the search The format is as follows:<br><br><code>local server name | search DN</
code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers
and sites.",
    "propertyOrder" : 300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "operationTimeout" : {

```

```

    "title" : "LDAP operations timeout",
    "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
will apply.",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"openam-auth-ldap-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default). ",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"searchScope" : {
    "title" : "Search Scope",
    "description" : "The level in the Directory Server that will be searched for a matching
user profile.<br><br>This attribute controls how the directory is searched.<br><br>
<ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
all levels below are searched</li></ul>",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"userSearchFilter" : {
    "title" : "User Search Filter",
    "description" : "This search filter will be appended to the standard user search
filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
For example: <code>(objectClass=person)</code>would result in the following user search filter:<br>
<code>(&(uid=<i>user</i>)(objectClass=person))</code>",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"userBindDN" : {
    "title" : "Bind User DN",

```

```

    "description" : "The DN of an admin user used by the module to authentication to the LDAP
server<br><br>The LDAP module requires an administration account in order to perform functionality
such as password reset.<br><br><i>NB </i><code>cn=Directory Manager</code> should not be used in
production systems.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

## 1.70.2. Global Operations

Resource path: `/global-config/authentication/modules/ldap`

Resource version: `1.0`

### 1.70.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LdapModule --global --actionName getAllTypes
```

### 1.70.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LdapModule --global --actionName getCreatableTypes
```

### 1.70.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LdapModule --global --actionName nextdescendents
```

### 1.70.2.4. read

Usage:

```
am> read LdapModule --global
```

## 1.70.2.5. update

Usage:

```
am> update LdapModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "userSearchAttributes" : {
          "title" : "Attributes Used to Search for a User to be Authenticated",
          "description" : "The attributes specified in this list form the LDAP search
filter.<br><br>The default value of uid will form the following search filter of <code>uid=<i>user</i></code>,
if there are multiple values such as uid and cn, the module will create a search filter as
follows <code>(|(uid=<i>user</i>)(cn=<i>user</i>))</code>",
          "propertyOrder" : 700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userSearchFilter" : {
          "title" : "User Search Filter",
          "description" : "This search filter will be appended to the standard user search
filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
For example: <code>(objectClass=person)</code>would result in the following user search filter:<br>
<code>(&(uid=<i>user</i>)(objectClass=person))</code>",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectionHeartbeatTimeUnit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "primaryLdapServer" : {
          "title" : "Primary LDAP Server",
          "description" : "Use this list to set the primary LDAP server used for authentication.
<br><br>The LDAP authentication module will use this list as the primary server for authentication. A
```

single entry must be in the format:  
`ldap_server:port`  
Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:  
`local server name | server:port`  
The local server name is the full name of the server from the list of servers and sites.",

```

    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "searchScope" : {
    "title" : "Search Scope",
    "description" : "The level in the Directory Server that will be searched for a
matching user profile.<br><br>This attribute controls how the directory is searched.<br><br>
<ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
all levels below are searched</li></ul>",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributeMappings" : {
    "title" : "User Creation Attributes",
    "description" : "Controls the mapping of local attribute to external attribute for dynamic
profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
between the attribute/values retrieved from the users authenticated profile and the attribute/values
that will be provisioned into their matching account in the data store.<br><br>The format of this
property is: <br><br><code> local attr|external attr</code>",
    "propertyOrder" : 1300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userProfileRetrievalAttribute" : {
    "title" : "Attribute Used to Retrieve User Profile",
    "description" : "The LDAP module will use this attribute to search of the profile of an
authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
Normally this will be the same attribute used to find the user account. The value will be the name of
the user used for authentication.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userBindPassword" : {
    "title" : "Bind User Password",
    "description" : "The password of the administration account.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
},

```

```

    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication
principal.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "Enforced when the user is resetting their password as part of the
authentication.<br><br>If the user needs to reset their password as part of the authentication
process, the authentication module can enforce a minimum password length. This is separate from any
password length controls from the underlying LDAP server. If the external LDAP server password policy
is enforcing password length, set this value to 0 to avoid confusion.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustAllServerCertificates" : {
      "title" : "Trust All Server Certificates",
      "description" : "Enables a <code>X509TrustManager</code> that trusts all
certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
servers protected by self signed or invalid certificates (such as invalid hostname).<br><br><i>NB
</i>Use this feature with care as it bypasses the normal certificate verification process",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "connectionHeartbeatInterval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "openam-auth-ldap-connection-mode" : {
      "title" : "LDAP Connection Mode",
      "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and

```



passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by using StartTLS extended operation.",

```

    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "beheraPasswordPolicySupportEnabled" : {
    "title" : "LDAP Behera Password Policy Support",
    "description" : "Enables support for modern LDAP password policies<br><br>LDAP Behera Password policies are supported by modern LDAP servers such as OpenDJ. If this functionality is disabled then only the older Netscape VCHU password policy standard will be enforced.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userBindDN" : {
    "title" : "Bind User DN",
    "description" : "The DN of an admin user used by the module to authentication to the LDAP server<br><br>The LDAP module requires an administration account in order to perform functionality such as password reset.<br><br><i>NB </i><code>cn=Directory Manager</code> should not be used in production systems.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userSearchStartDN" : {
    "title" : "DN to Start User Search",
    "description" : "The search for accounts to be authenticated start from this base DN<br><br>For a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different base DN's for the search The format is as follows:<br><br><code>local server name | search DN</code><br><br><i>NB </i><i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "operationTimeout" : {
    "title" : "LDAP operations timeout",
    "description" : "Defines the timeout in seconds OpenAM should wait for a response of the Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or the JVM are applied. However this setting allows more granular control within OpenAM itself. A value of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS will apply.",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "secondaryLdapServer" : {
    "title" : "Secondary LDAP Server",

```

```

    "description" : "Use this list to set the secondary (failover) LDAP server used for authentication.<br><br>If the primary LDAP server fails, the LDAP authentication module will failover to the secondary server. A single entry must be in the format:<br><br><code>ldap_server:port</code><br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br><br><code>local server name | server:port</code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.71. LegacyUserSelfService

### 1.71.1. Realm Operations

Resource path: `/realm-config/services/security`

Resource version: `1.0`

#### 1.71.1.1. create

Usage:

```
am> create LegacyUserSelfService --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```

{
  "type" : "object",
  "properties" : {
    "selfRegistrationTokenLifetime" : {
      "title" : "Self-Registration Token LifeTime (seconds)",
      "description" : "Maximum life time for the token allowing User Self-Registration using the REST API.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}

```

```

},
"selfRegistrationEnabled" : {
  "title" : "Self-Registration for Users",
  "description" : "If enabled, new users can sign up using a REST API client.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"forgotPasswordTokenLifetime" : {
  "title" : "Forgot Password Token Lifetime (seconds)",
  "description" : "Maximum life time for the token that allows a user to process a forgotten
password using the REST API.",
  "propertyOrder" : 600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"forgotPasswordConfirmationUrl" : {
  "title" : "Forgot Password Confirmation Email URL",
  "description" : "This page handles the HTTP GET request when the user clicks the link sent by
email in the confirmation request.",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"selfServiceEnabled" : {
  "title" : "Legacy Self-Service REST Endpoint",
  "description" : "Specify whether to enable the legacy self-service endpoint.<p>OpenAM supports
two User Self-Service components: the Legacy User Self-Service, which is based on a Java SDK and is
available in OpenAM versions prior to OpenAM 13, and a common REST-based/XUI-based User Self-Service
available in OpenAM 13 and later.<p>The Legacy User Self-Service will be deprecated in a future
release.",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"forgotPasswordEnabled" : {
  "title" : "Forgot Password for Users",
  "description" : "If enabled, users can assign themselves a new password using a REST API
client.",
  "propertyOrder" : 500,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"protectedUserAttributes" : {
  "title" : "Protected User Attributes",
  "description" : "A list of user profile attributes. Users modifying any of the attributes in
this list will be required to enter a password as confirmation before the change is accepted. This
option applies to XUI deployments only.",
  "propertyOrder" : 900,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",

```

```
    "exampleValue" : ""
  },
  "userRegisteredDestination" : {
    "title" : "Destination After Successful Self-Registration",
    "description" : "Specifies the behavior when self-registration has successfully completed.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "selfRegistrationConfirmationUrl" : {
    "title" : "Self-Registration Confirmation Email URL",
    "description" : "This page handles the HTTP GET request when the user clicks the link sent by email in the confirmation request.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
```

### 1.71.1.2. delete

Usage:

```
am> delete LegacyUserSelfService --realm Realm
```

### 1.71.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LegacyUserSelfService --realm Realm --actionName getAllTypes
```

### 1.71.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LegacyUserSelfService --realm Realm --actionName getCreatableTypes
```

### 1.71.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LegacyUserSelfService --realm Realm --actionName nextdescendents
```

### 1.71.1.6. read

Usage:

```
am> read LegacyUserSelfService --realm Realm
```

### 1.71.1.7. update

Usage:

```
am> update LegacyUserSelfService --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "selfRegistrationTokenLifetime" : {
      "title" : "Self-Registration Token LifeTime (seconds)",
      "description" : "Maximum life time for the token allowing User Self-Registration using the REST
API.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "selfRegistrationEnabled" : {
      "title" : "Self-Registration for Users",
      "description" : "If enabled, new users can sign up using a REST API client.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "forgotPasswordTokenLifetime" : {
      "title" : "Forgot Password Token Lifetime (seconds)",
      "description" : "Maximum life time for the token that allows a user to process a forgotten
password using the REST API.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "forgotPasswordConfirmationUrl" : {
      "title" : "Forgot Password Confirmation Email URL",
      "description" : "This page handles the HTTP GET request when the user clicks the link sent by
email in the confirmation request.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

```

    },
    "selfServiceEnabled" : {
      "title" : "Legacy Self-Service REST Endpoint",
      "description" : "Specify whether to enable the legacy self-service endpoint.<p>OpenAM supports two User Self-Service components: the Legacy User Self-Service, which is based on a Java SDK and is available in OpenAM versions prior to OpenAM 13, and a common REST-based/XUI-based User Self-Service available in OpenAM 13 and later.<p>The Legacy User Self-Service will be deprecated in a future release.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "forgotPasswordEnabled" : {
      "title" : "Forgot Password for Users",
      "description" : "If enabled, users can assign themselves a new password using a REST API client.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "protectedUserAttributes" : {
      "title" : "Protected User Attributes",
      "description" : "A list of user profile attributes. Users modifying any of the attributes in this list will be required to enter a password as confirmation before the change is accepted. This option applies to XUI deployments only.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userRegisteredDestination" : {
      "title" : "Destination After Successful Self-Registration",
      "description" : "Specifies the behavior when self-registration has successfully completed.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "selfRegistrationConfirmationUrl" : {
      "title" : "Self-Registration Confirmation Email URL",
      "description" : "This page handles the HTTP GET request when the user clicks the link sent by email in the confirmation request.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}

```

## 1.71.2. Global Operations

Resource path: `/global-config/services/security`

Resource version: `1.0`

### 1.71.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LegacyUserSelfService --global --actionName getAllTypes
```

### 1.71.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LegacyUserSelfService --global --actionName getCreatableTypes
```

### 1.71.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LegacyUserSelfService --global --actionName nextdescendents
```

### 1.71.2.4. read

Usage:

```
am> read LegacyUserSelfService --global
```

### 1.71.2.5. update

Usage:

```
am> update LegacyUserSelfService --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
```

```

"userRegisteredDestination" : {
  "title" : "Destination After Successful Self-Registration",
  "description" : "Specifies the behavior when self-registration has successfully completed.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"selfRegistrationEnabled" : {
  "title" : "Self-Registration for Users",
  "description" : "If enabled, new users can sign up using a REST API client.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"protectedUserAttributes" : {
  "title" : "Protected User Attributes",
  "description" : "A list of user profile attributes. Users modifying any of the attributes in
this list will be required to enter a password as confirmation before the change is accepted. This
option applies to XUI deployments only.",
  "propertyOrder" : 900,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"selfRegistrationTokenLifetime" : {
  "title" : "Self-Registration Token LifeTime (seconds)",
  "description" : "Maximum life time for the token allowing User Self-Registration using the
REST API.",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"forgotPasswordTokenLifetime" : {
  "title" : "Forgot Password Token Lifetime (seconds)",
  "description" : "Maximum life time for the token that allows a user to process a forgotten
password using the REST API.",
  "propertyOrder" : 600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"forgotPasswordConfirmationUrl" : {
  "title" : "Forgot Password Confirmation Email URL",
  "description" : "This page handles the HTTP GET request when the user clicks the link sent
by email in the confirmation request.",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"selfServiceEnabled" : {
  "title" : "Legacy Self-Service REST Endpoint",

```



```

    "description" : "Specify whether to enable the legacy self-service endpoint.<p>OpenAM
supports two User Self-Service components: the Legacy User Self-Service, which is based on a Java
SDK and is available in OpenAM versions prior to OpenAM 13, and a common REST-based/XUI-based User
Self-Service available in OpenAM 13 and later.<p>The Legacy User Self-Service will be deprecated in a
future release.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "forgotPasswordEnabled" : {
    "title" : "Forgot Password for Users",
    "description" : "If enabled, users can assign themselves a new password using a REST API
client.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "selfRegistrationConfirmationUrl" : {
    "title" : "Self-Registration Confirmation Email URL",
    "description" : "This page handles the HTTP GET request when the user clicks the link sent
by email in the confirmation request.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.72. Logging

### 1.72.1. Global Operations

Resource path: `/global-config/services/logging`

Resource version: `1.0`

#### 1.72.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Logging --global --actionName getAllTypes
```

### 1.72.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Logging --global --actionName getCreatableTypes
```

### 1.72.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Logging --global --actionName nextdescendents
```

### 1.72.1.4. read

Usage:

```
am> read Logging --global
```

### 1.72.1.5. update

Usage:

```
am> update Logging --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "database" : {
      "type" : "object",
      "title" : "Database",
      "propertyOrder" : 2,
      "properties" : {
        "password" : {
          "title" : "Database User Password",
          "description" : "When logging to a database, set this to the password used to connect to the database. If this attribute is incorrectly set, OpenAM performance suffers.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "maxRecords" : {
```

```

        "title" : "Maximum Number of Records",
        "description" : "The maximum number of records read from the logs via the Logging API",
        "propertyOrder" : 2500,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "user" : {
        "title" : "Database User Name",
        "description" : "When logging to a database, set this to the user name used to connect to
the database. If this attribute is incorrectly set, OpenAM performance suffers.",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "databaseFailureMemoryBufferSize" : {
        "title" : "DB Failure Memory Buffer Size",
        "description" : "Max number of log records held in memory if DB logging fails.<br><br>This
is the maximum number of log records that will be held in memory if the database is unavailable.
When the buffer is full, new log records cause the oldest record in the buffer to be cleared. OpenAM
monitoring records the number of log entries cleared when the database was unavailable.<br><br>If
the value of this property is less than that of the <i>Buffer Size</i> then the buffer size value
will take precedence. ",
        "propertyOrder" : 2800,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "driver" : {
        "title" : "Database Driver Name",
        "description" : "When logging to a database, set this to the class name of the JDBC driver
used to connect to the database.<br><br>The default is for Oracle. OpenAM also works with the MySQL
database driver.",
        "propertyOrder" : 1300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"general" : {
    "type" : "object",
    "title" : "General",
    "propertyOrder" : 0,
    "properties" : {
        "signingAlgorithm" : {
            "title" : "Secure Logging Signing Algorithm ",
            "description" : "Determines the algorithm used to digitally sign the log records.",
            "propertyOrder" : 2300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "verifyPeriod" : {
            "title" : "Log Verification Frequency",
            "description" : "The frequency (in seconds) that OpenAM verifies security of the log
files.<br><br>When secure logging is enabled, this is the period that OpenAM will check the integrity
of the log files.",

```

```

    "propertyOrder" : 2000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "resolveHostName" : {
    "title" : "Log Record Resolve Host Name",
    "description" : "Enable this to have OpenAM perform a DNS host lookup to populate the host
name field for log records.<br><br><i>Note:</i> Enabling this functionality will increase the load of
the logging system and the OpenAM host must have DNS configured. ",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "bufferTime" : {
    "title" : "Buffer Time",
    "description" : "The maximum time (in seconds) OpenAM will hold log records in memory before
flushing to the underlying repository.",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "signaturePeriod" : {
    "title" : "Log Signature Time",
    "description" : "The frequency (in seconds) that OpenAM will digitally sign the log
records.<br><br>When secure logging is enabled, this is the period that OpenAM will digitally
signed the contents of the log files. The log signatures form the basis of the log file integrity
checking.",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "jdkLoggingLevel" : {
    "title" : "Logging Level",
    "description" : "Control the level of JDK logging within OpenAM. ",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "certificateStore" : {
    "title" : "Logging Certificate Store Location",
    "description" : "The path to the Java keystore containing the logging system
certificate.<br><br>The secure logging system will use the certificate alias of <code>Logger</code>
to locate the certificate in the specified keystore.",
    "propertyOrder" : 2400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "filesPerKeystore" : {
    "title" : "Number of Files per Archive",
    "description" : "Controls the number of logs files that will be archived by the secure
logging system.",
    "propertyOrder" : 2600,
    "required" : true,

```

```

    "type" : "integer",
    "exampleValue" : ""
  },
  "buffering" : {
    "title" : "Time Buffering",
    "description" : "Enable or Disable log buffering<br><br>When enabled OpenAM holds all log
records in a memory buffer that it periodically flush to the repository. The period is set in the
<i>Buffer Time</i> property.",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "bufferSize" : {
    "title" : "Buffer Size",
    "description" : "The number of log records held in memory before the log records will be
flushed to the logfile or the database.",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "fields" : {
    "title" : "Configurable Log Fields",
    "description" : "Controls the fields that are logged by OpenAM.<br><br>This property is the
list of fields that are logged by default. Administrators can choose to limit the information logged
by OpenAM.",
    "propertyOrder" : 1900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "security" : {
    "title" : "Secure Logging",
    "description" : "Enable or Disable secure logging.<br><br>Enabling this setting will cause
OpenAM to digitally sign and verify the contents of the log files to help prevent and detect log file
tampering. A certificate must be configured for this functionality to be enabled. ",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "type" : {
    "title" : "Logging Type",
    "description" : "Specifies whether to log to a database, Syslog, or to the filing
system.<br><br>If you choose database then be sure to set the connection attributes correctly,
including the JDBC driver to use.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "status" : {
    "title" : "Log Status",
    "description" : "Enable the OpenAM logging system.<p><p>OpenAM supports two Audit Logging
Services: the legacy Logging Service, which is based on a Java SDK and is available in OpenAM

```

```
versions prior to OpenAM 13.5, and a new common REST-based Audit Logging Service available from
OpenAM 13.5.<p><p>The legacy Logging Service will be deprecated in a future release.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
},
"file" : {
  "type" : "object",
  "title" : "File",
  "propertyOrder" : 1,
  "properties" : {
    "suffix" : {
      "title" : "Logfile Rotation Suffix",
      "description" : "The name of the log files will be suffixed with the supplied
value.<br><br>This field defines the log file suffix. If no suffix is provided, then the following
default suffix format will be used: <code>-MM.dd.yy-kk.mm</code>. The suffix allows use of Date
and Time patterns defined in <a href='\"http://download.oracle.com/javase/6/docs/api/java/text/
SimpleDateFormat.html\"><code>SimpleDateFormat</code></a><p><p><i>Note:</i> This field is only used if
the time based rotation is enabled.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "rotationInterval" : {
      "title" : "Logfile Rotation Interval",
      "description" : "The rotation interval (in minutes).<br><br>The rotation interval determines
the frequency of when the log files will be rotated. If the value is <code>-1</code>, then time based
rotation is disabled and log file size based rotation is enabled.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "rotationEnabled" : {
      "title" : "Log Rotation",
      "description" : "Enable log rotation to cause new log files to be created when configured
thresholds are reached, such as <i>Maximum Log Size</i> or <i>Logfile Rotation Interval</i>.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "numberHistoryFiles" : {
      "title" : "Number of History Files",
      "description" : "Sets the number of history files for each log that OpenAM keeps, including
time-based histories.<p><p>The previously live file is moved and is included in the history count,
and a new log is created to serve as the live log file. Any log file in the history count that goes
over the number specified here will be deleted.<p><p>For time-based logs, a new set of logs will be
created when OpenAM is started because of the time-based file names that are used.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "prefix" : {
```

```

        "title" : "Logfile Rotation Prefix",
        "description" : "The name of the log files will be prefixed with the supplied
value.<br><br>This field defines the log file prefix. The prefix will be added to the name of all
logfiles.<br><br><i>Note:</i> Only used when time-based log rotation is enabled.",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "maxFileSize" : {
        "title" : "Maximum Log Size",
        "description" : "Maximum size of a log file, in bytes.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "location" : {
        "title" : "Log File Location",
        "description" : "The path to the location of the log files<br><br>This property controls
the location of the log files; the value of this property varies on whether File or DB logging is
in use:<p><ul><li>File: The full pathname to the directory containing the log files.</li><li>DB: The
JDBC URL to the database used to store the log file database.</li></ul>",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"syslog" : {
    "type" : "object",
    "title" : "Syslog",
    "propertyOrder" : 3,
    "properties" : {
        "host" : {
            "title" : "Syslog server host",
            "description" : "The URL or IP address of the syslog server, for example <code>http://
mysyslog.example.com</code>, or <code>localhost</code>.",
            "propertyOrder" : 1400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "facility" : {
            "title" : "Syslog facility",
            "description" : "Syslog uses the facility level to determine the type of program that is
logging the message.",
            "propertyOrder" : 1700,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "timeout" : {
            "title" : "Syslog connection timeout",
            "description" : "The amount of time to wait when attempting to connect to the syslog server
before reporting a failure, in seconds.",
            "propertyOrder" : 1800,
            "required" : true,

```

```
    "type" : "integer",
    "exampleValue" : ""
  },
  "port" : {
    "title" : "Syslog server port",
    "description" : "The port number the syslog server is configured to listen to.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "protocol" : {
    "title" : "Syslog transport protocol",
    "description" : "The protocol to use to connect to the syslog server.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
```

## 1.73. MembershipModule

### 1.73.1. Realm Operations

Resource path: `/realm-config/authentication/modules/membership`

Resource version: `1.0`

#### 1.73.1.1. create

Usage:

```
am> create MembershipModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```



```

"properties" : {
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "minimumPasswordLength" : {
    "title" : "Minimum Password Length",
    "description" : "The minimum length of the user password.<br><br>Setting this value to 0 disables this functionality.<br><br><i>NB </i>This feature is separate from any password policy in the underlying data store",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "defaultUserRoles" : {
    "title" : "Default User Roles",
    "description" : "The role DN's that will be assigned to the user.<br><br><i>NB </i>Roles are only supported in Sun Directory Server Enterprise Edition",
    "propertyOrder" : 200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "defaultUserStatus" : {
    "title" : "User Status After Registration",
    "description" : "Determines if the user account should be automatically active after registration completes.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
}

```

### 1.73.1.2. delete

#### Usage:

```
am> delete MembershipModule --realm Realm --id id
```

#### Parameters:

##### --id

The unique identifier for the resource.

### 1.73.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MembershipModule --realm Realm --actionName getAllTypes
```

### 1.73.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MembershipModule --realm Realm --actionName getCreatableTypes
```

### 1.73.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MembershipModule --realm Realm --actionName nextdescendents
```

### 1.73.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query MembershipModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.73.1.7. read

Usage:

```
am> read MembershipModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.73.1.8. update

Usage:

```
am> update MembershipModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "The minimum length of the user password.<br><br>Setting this value to 0 disables this functionality.<br><br><i>NB </i>This feature is separate from any password policy in the underlying data store",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "defaultUserRoles" : {
      "title" : "Default User Roles",
      "description" : "The role DN's that will be assigned to the user.<br><br><i>NB </i>Roles are only supported in Sun Directory Server Enterprise Edition",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaultUserStatus" : {
      "title" : "User Status After Registration",
      "description" : "Determines if the user account should be automatically active after registration completes.",
      "propertyOrder" : 300,
      "required" : true,

```

```
    "type" : "string",  
    "exampleValue" : ""  
  }  
}  
}
```

## 1.73.2. Global Operations

Resource path: `/global-config/authentication/modules/membership`

Resource version: `1.0`

### 1.73.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MembershipModule --global --actionName getAllTypes
```

### 1.73.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MembershipModule --global --actionName getCreatableTypes
```

### 1.73.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MembershipModule --global --actionName nextdescendents
```

### 1.73.2.4. read

Usage:

```
am> read MembershipModule --global
```

### 1.73.2.5. update

Usage:

```
am> update MembershipModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "minimumPasswordLength" : {
          "title" : "Minimum Password Length",
          "description" : "The minimum length of the user password.<br><br>Setting this value to 0 disables this functionality.<br><br><i>NB </i>This feature is separate from any password policy in the underlying data store",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "defaultUserRoles" : {
          "title" : "Default User Roles",
          "description" : "The role DN's that will be assigned to the user.<br><br><i>NB </i>Roles are only supported in Sun Directory Server Enterprise Edition",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultUserStatus" : {
          "title" : "User Status After Registration",
          "description" : "Determines if the user account should be automatically active after registration completes.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

```
}
```

## 1.74. Monitoring

### 1.74.1. Global Operations

Resource path: `/global-config/services/monitoring`

Resource version: `1.0`

#### 1.74.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Monitoring --global --actionName getAllTypes
```

#### 1.74.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Monitoring --global --actionName getCreatableTypes
```

#### 1.74.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Monitoring --global --actionName nextdescendents
```

#### 1.74.1.4. read

Usage:

```
am> read Monitoring --global
```

#### 1.74.1.5. update

Usage:

```
am> update Monitoring --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabled" : {
      "title" : "Monitoring Status",
      "description" : "Enable / Disable the monitoring system",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "sessionHistoryWindowSize" : {
      "title" : "Session monitoring history size",
      "description" : "Size of the window of most recent session operations to record to expose via monitoring system. Valid range is 100 - 1000000.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "authfilePath" : {
      "title" : "Monitoring HTTP interface authentication file path",
      "description" : "Path to the monitoring system authentication file<br><br>The <code>openam_mon_auth</code> file contains the username and password of the account used to protect the monitoring interfaces. The default username is <code>demo</code> with a password of <code>changeit</code>. Use the <code>ampassword</code> command to encrypt a new password.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "httpEnabled" : {
      "title" : "Monitoring HTTP interface status",
      "description" : "Enable / Disable the HTTP access to the monitoring system ",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "httpPort" : {
      "title" : "Monitoring HTTP Port",
      "description" : "Port number for the HTTP monitoring interface",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "snmpPort" : {
      "title" : "Monitoring SNMP Port",
      "description" : "Port number for the SNMP monitoring interface",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",

```

```

    "exampleValue" : ""
  },
  "rmiPort" : {
    "title" : "Monitoring RMI Port",
    "description" : "Port number for the JMX monitoring interface",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "snmpEnabled" : {
    "title" : "Monitoring SNMP interface status",
    "description" : "Enable / Disable the SNMP access to the monitoring system",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyHistoryWindowSize" : {
    "title" : "Policy evaluation monitoring history size",
    "description" : "Size of the window of most recent policy evaluations to record to expose via monitoring system. Valid range is 100 - 1000000.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "rmiEnabled" : {
    "title" : "Monitoring RMI interface status",
    "description" : "Enable / Disable the JMX access to the monitoring system",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }
}
}
}

```

## 1.75. MsisdnModule

### 1.75.1. Realm Operations

Resource path: `/realm-config/authentication/modules/msisdn`

Resource version: `1.0`

#### 1.75.1.1. create

Usage:

```
am> create MsisdnModule --realm Realm --id id --body body
```



Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "msisdnUserNamingAttribute" : {
      "title" : "LDAP Attribute Used to Retrieve User Profile",
      "description" : "The name of the attribute returned from the user profile matched against the supplied MSISDN number",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication principal.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapSslEnabled" : {
      "title" : "SSL/TLS for LDAP Access",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "msisdnRequestSearchLocations" : {
      "title" : "MSISDN Header Search Attribute",
      "description" : "Controls the elements that are searched by the authentication module ",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "msisdnParameterNames" : {
      "title" : "MSISDN Number Search Parameter Name",
      "description" : "Name of the HTTP cookie, header or query parameter containing the MSISDN number<br><br>The MSISDN authentication module will check the incoming HTTP cookie, header or query parameter of the request for the MSISDN number. The order of checking is as follows:<br><br><ol><li>Cookie</li><li>Header</li><li>Query</li></ol><br><br><i>NB </i>The <i>MSISDN Header Search Attribute</i> controls what elements of the request is searched",
      "propertyOrder" : 200,
      "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userProfileMsisdnAttribute" : {
    "title" : "Attribute To Use To Search LDAP",
    "description" : "The name of the attribute searched in the user profiles for the MSISDN number",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "baseSearchDN" : {
    "title" : "LDAP Start Search DN",
    "description" : "The start point in the LDAP server for the MSISDN search<br><br>When entering multiple entries, each entry must be prefixed with a local server name. Multiple entries allow different search Base DNs depending on the OpenAM server in use. The format is:<br><br><code>local server name | base dn</code><br><br>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "ldapUserBindPassword" : {
    "title" : "LDAP Server Authentication Password",
    "description" : "The password for the authentication user",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "ldapUserBindDN" : {
    "title" : "LDAP Server Authentication User ",
    "description" : "DN of the user used by the module to authenticate to the LDAP server<br><br>The MSISDN module authenticates to the LDAP server in order to search for a matching number. The DN entered here represents the account used for said authentication and must have read/search access to the LDAP server.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },

```

```

"ldapProviderUrl" : {
  "title" : "LDAP Server and Port ",
  "description" : "Use this list to set the LDAP server used to search for the MSISDN number.
<br><br>The MSISDN authentication module will use this list as the server that is searched for a
matching MSISDN number. A single entry must be in the format:<br><br><code>ldap_server:port</
code><br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The
format is:<br><br><code>local server name | server:port</code><br><br>The local server name is
the full name of the server from the list of servers and sites.",
  "propertyOrder" : 300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"trustedGatewayIPAddresses" : {
  "title" : "Trusted Gateway IP Address",
  "description" : "The list of IP address that are trusted to send MSISDN authentication
requests.<br><br>The client IP address of the authentication request is checked against this list, if
the client IP is not listed then the authentication module will fail.<br><br><i>NB </i>If the list
is empty then all hosts will be trusted.",
  "propertyOrder" : 100,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
}
}
}

```

### 1.75.1.2. delete

Usage:

```
am> delete MsisdnModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.75.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MsisdnModule --realm Realm --actionName getAllTypes
```

#### 1.75.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MsisdnModule --realm Realm --actionName getCreatableTypes
```

#### 1.75.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MsisdnModule --realm Realm --actionName nextdescendents
```

#### 1.75.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query MsisdnModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.75.1.7. read

Usage:

```
am> read MsisdnModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.75.1.8. update

Usage:

```
am> update MsisdnModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "msisdnUserNamingAttribute" : {
      "title" : "LDAP Attribute Used to Retrieve User Profile",
      "description" : "The name of the attribute returned from the user profile matched against the supplied MSISDN number",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication principal.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapSslEnabled" : {
      "title" : "SSL/TLS for LDAP Access",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "msisdnRequestSearchLocations" : {
      "title" : "MSISDN Header Search Attribute",
      "description" : "Controls the elements that are searched by the authentication module ",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "msisdnParameterNames" : {
      "title" : "MSISDN Number Search Parameter Name",
      "description" : "Name of the HTTP cookie, header or query parameter containing the MSISDN number<br><br>The MSISDN authentication module will check the incoming HTTP cookie, header or query parameter of the request for the MSISDN number. The order of checking is as follows:<br><br><ol><li>Cookie</li><li>Header</li><li>Query</li></ol><br><br><i>NB </i>The <i>MSISDN Header Search Attribute</i> controls what elements of the request is searched",
      "propertyOrder" : 200,
      "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userProfileMsisdnAttribute" : {
    "title" : "Attribute To Use To Search LDAP",
    "description" : "The name of the attribute searched in the user profiles for the MSISDN number",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "baseSearchDN" : {
    "title" : "LDAP Start Search DN",
    "description" : "The start point in the LDAP server for the MSISDN search<br><br>When entering multiple entries, each entry must be prefixed with a local server name. Multiple entries allow different search Base DNs depending on the OpenAM server in use. The format is:<br><br><code>local server name | base dn</code><br><br>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "ldapUserBindPassword" : {
    "title" : "LDAP Server Authentication Password",
    "description" : "The password for the authentication user",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "ldapUserBindDN" : {
    "title" : "LDAP Server Authentication User ",
    "description" : "DN of the user used by the module to authenticate to the LDAP server<br><br>The MSISDN module authenticates to the LDAP server in order to search for a matching number. The DN entered here represents the account used for said authentication and must have read/search access to the LDAP server.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
}

```

```

"ldapProviderUrl" : {
  "title" : "LDAP Server and Port ",
  "description" : "Use this list to set the LDAP server used to search for the MSISDN number.
<br><br>The MSISDN authentication module will use this list as the server that is searched for a
matching MSISDN number. A single entry must be in the format:<br><br><code>ldap_server:port</
code><br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The
format is:<br><br><code>local server name | server:port</code><br><br>The local server name is
the full name of the server from the list of servers and sites.",
  "propertyOrder" : 300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"trustedGatewayIPAddresses" : {
  "title" : "Trusted Gateway IP Address",
  "description" : "The list of IP address that are trusted to send MSISDN authentication
requests.<br><br>The client IP address of the authentication request is checked against this list, if
the client IP is not listed then the authentication module will fail.<br><br><i>NB </i>If the list
is empty then all hosts will be trusted.",
  "propertyOrder" : 100,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
}
}
}

```

## 1.75.2. Global Operations

Resource path: `/global-config/authentication/modules/msisdn`

Resource version: **1.0**

### 1.75.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MsisdnModule --global --actionName getAllTypes
```

### 1.75.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MsisdnModule --global --actionName getCreatableTypes
```

### 1.75.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MsisdnModule --global --actionName nextdescendents
```

### 1.75.2.4. read

Usage:

```
am> read MsisdnModule --global
```

### 1.75.2.5. update

Usage:

```
am> update MsisdnModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "trustedGatewayIPAddresses" : {
          "title" : "Trusted Gateway IP Address",
          "description" : "The list of IP address that are trusted to send MSISDN authentication requests.<br><br>The client IP address of the authentication request is checked against this list, if the client IP is not listed then the authentication module will fail.<br><br><i>NB</i>If the list is empty then all hosts will be trusted.",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "returnUserDN" : {
          "title" : "Return User DN to DataStore",
          "description" : "Controls whether the DN or the username is returned as the authentication principal.",
          "propertyOrder" : 1100,
          "required" : true,

```



```

    "type" : "boolean",
    "exampleValue" : ""
  },
  "msisdnUserNamingAttribute" : {
    "title" : "LDAP Attribute Used to Retrieve User Profile",
    "description" : "The name of the attribute returned from the user profile matched against
the supplied MSISDN number",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userProfileMsisdnAttribute" : {
    "title" : "Attribute To Use To Search LDAP",
    "description" : "The name of the attribute searched in the user profiles for the MSISDN
number",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "msisdnParameterNames" : {
    "title" : "MSISDN Number Search Parameter Name",
    "description" : "Name of the HTTP cookie, header or query parameter containing the MSISDN
number<br><br>The MSISDN authentication module will check the incoming HTTP cookie, header or
query parameter of the request for the MSISDN number. The order of checking is as follows:<br><br>
<ol><li>Cookie</li><li>Header</li><li>Query</li></ol><br><br><i>NB </i>The <i>MSISDN Header Search
Attribute</i> controls what elements of the request is searched",
    "propertyOrder" : 200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "ldapUserBindDN" : {
    "title" : "LDAP Server Authentication User ",
    "description" : "DN of the user used by the module to authenticate to the LDAP
server<br><br>The MSISDN module authenticates to the LDAP server in order to search for a matching
number. The DN entered here represents the account used for said authentication and must have read/
search access to the LDAP server.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "baseSearchDN" : {
    "title" : "LDAP Start Search DN",

```

```

    "description" : "The start point in the LDAP server for the MSISDN search<br><br>When
    entering multiple entries, each entry must be prefixed with a local server name. Multiple entries
    allow different search Base DN's depending on the OpenAM server in use. The format is:<br><br>
    <code>local server name | base dn</code><br><br>The local server name is the full name of the
    server from the list of servers and sites.",
    "propertyOrder" : 400,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"ldapUserBindPassword" : {
    "title" : "LDAP Server Authentication Password",
    "description" : "The password for the authentication user",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
},
"ldapSslEnabled" : {
    "title" : "SSL/TLS for LDAP Access",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"msisdNRequestSearchLocations" : {
    "title" : "MSISDN Header Search Attribute",
    "description" : "Controls the elements that are searched by the authentication module ",
    "propertyOrder" : 900,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"ldapProviderUrl" : {
    "title" : "LDAP Server and Port ",
    "description" : "Use this list to set the LDAP server used to search for the MSISDN number.
    <br><br>The MSISDN authentication module will use this list as the server that is searched for a
    matching MSISDN number. A single entry must be in the format:<br><br><code>ldap_server:port</code>
    <br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The
    format is:<br><br><code>local server name | server:port</code><br><br>The local server name is
    the full name of the server from the list of servers and sites.",
    "propertyOrder" : 300,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
}
},
"type" : "object",

```

```
    "title" : "Realm Defaults"  
  }  
}
```

## 1.76. MultiFederationProtocol

### 1.76.1. Global Operations

Resource path: `/global-config/services/federation/multi`

Resource version: `1.0`

#### 1.76.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MultiFederationProtocol --global --actionName getAllTypes
```

#### 1.76.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MultiFederationProtocol --global --actionName getCreatableTypes
```

#### 1.76.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MultiFederationProtocol --global --actionName nextdescendents
```

#### 1.76.1.4. read

Usage:

```
am> read MultiFederationProtocol --global
```

#### 1.76.1.5. update

Usage:

```
am> update MultiFederationProtocol --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "singleLogoutHandlerList" : {
      "title" : "Single Logout Handler List",
      "description" : "List of Logout handlers for each supported federation protocol<br><br>The multi-federation protocol engine supports Single Logout. Each federation protocol requires a different single logout handler. Logout handler must implement the <code>com.sun.identity.multiprotocol.SingleLogoutHandler</code> interface.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.77. Naming

### 1.77.1. Global Operations

Resource path: `/global-config/services/naming`

Resource version: `1.0`

#### 1.77.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Naming --global --actionName getAllTypes
```

#### 1.77.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Naming --global --actionName getCreatableTypes
```

### 1.77.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Naming --global --actionName nextdescendents
```

### 1.77.1.4. read

Usage:

```
am> read Naming --global
```

### 1.77.1.5. update

Usage:

```
am> update Naming --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "federationConfig" : {
      "type" : "object",
      "title" : "Federation Configuration",
      "propertyOrder" : 1,
      "properties" : {
        "samlAwareServletUrl" : {
          "title" : "SAML Web Profile/Artifact Service URL",
          "description" : "Specifies the SAML v1 endpoint.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "samlAssertionManagerUrl" : {
          "title" : "SAML Assertion Manager Service URL",
          "description" : "Specifies the SAML v1 assertion service endpoint.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "samlPostServletUrl" : {
```

```

        "title" : "SAML Web Profile/POST Service URL",
        "description" : "Specifies the SAML v1 Web Profile endpoint.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "jaxrpcUrl" : {
        "title" : "JAXRPC Endpoint URL",
        "description" : "Specifies the JAXRPC endpoint URL used by the remote IDM/SMS APIs.",
        "propertyOrder" : 1200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "samlSoapReceiverUrl" : {
        "title" : "SAML SOAP Service URL",
        "description" : "Specifies the SAML v1 SOAP service endpoint.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"generalConfig" : {
    "type" : "object",
    "title" : "General Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "sessionUrl" : {
            "title" : "Session Service URL",
            "description" : "Specifies the endpoint used by the session service.",
            "propertyOrder" : 200,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "authUrl" : {
            "title" : "Authentication Service URL",
            "description" : "Specifies the endpoint used by the authentication service.",
            "propertyOrder" : 500,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "policyUrl" : {
            "title" : "Policy Service URL",
            "description" : "Specifies the endpoint used by the policy service.",
            "propertyOrder" : 400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "loggingUrl" : {
            "title" : "Logging Service URL",
            "description" : "Specifies the endpoint used by the logging service.",
            "propertyOrder" : 300,
            "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "profileUrl" : {
        "title" : "Profile Service URL",
        "description" : "Specifies the endpoint used by the profile service.<p><p>This attribute is
deprecated.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"endpointConfig" : {
    "type" : "object",
    "title" : "Endpoint Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "federationAssertionManagerUrl" : {
            "title" : "Federation Assertion Manager Service URL",
            "description" : "Specifies the ID-FF assertion manager endpoint.",
            "propertyOrder" : 1000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "idsvcsRestUrl" : {
            "title" : "Identity REST Services Endpoint URL",
            "description" : "Specifies the endpoint for the Identity REST services.",
            "propertyOrder" : 1400,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "securityTokenManagerUrl" : {
            "title" : "Security Token Manager URL",
            "description" : "Specifies the security token manager endpoint.",
            "propertyOrder" : 1100,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "jaxwsUrl" : {
            "title" : "Identity Web Services Endpoint URL",
            "description" : "Specifies the endpoint for the Identity WSDL services.",
            "propertyOrder" : 1300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "stsMexUrl" : {
            "title" : "Security Token Service MEX Endpoint URL",
            "description" : "Specifies the STS MEX endpoint.",
            "propertyOrder" : 1600,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},

```

```
"stsUrl" : {  
  "title" : "Security Token Service Endpoint URL",  
  "description" : "Specifies the STS endpoint.",  
  "propertyOrder" : 1500,  
  "required" : true,  
  "type" : "string",  
  "exampleValue" : ""  
}  
}  
}  
}
```

## 1.78. OAuth2ClientAgentGroups

### 1.78.1. Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/OAuth2Client`

Resource version: **1.0**

#### 1.78.1.1. create

Usage:

```
am> create OAuth2ClientAgentGroups --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "type" : "object",  
  "properties" : {  
    "redirectionUris" : {  
      "title" : "Redirection URIs",  
      "description" : "Redirection URIs (optional for confidential clients). Complete URIs or URIs  
consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust  
that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify  
the URI that the user should be redirected to following approval. May not contain a fragment (#).",  
      "propertyOrder" : 23200,  
      "required" : true,  
      "items" : {  
        "type" : "string"
```



```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "idTokenEncryptionAlgorithm" : {
    "title" : "ID Token Encryption Algorithm",
    "description" : "Algorithm the ID Token for this client must be encrypted with.",
    "propertyOrder" : 24700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userinfoSignedResponseAlg" : {
    "title" : "User info signed response algorithm",
    "description" : "JWS algorithm for signing UserInfo Responses. If this is specified, the response will be JWT <a href='\"https://tools.ietf.org/html/rfc7519\"'>JWT</a> serialized, and signed using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8 encoded JSON object using the application/json content-type.",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authorizationCodeLifetime" : {
    "title" : "Authorization Code Lifetime (seconds)",
    "description" : "The time in seconds an authorization code is valid for. <i>NB</i> If this field is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.",
    "propertyOrder" : 25800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "descriptions" : {
    "title" : "Display description",
    "description" : "A description of the client or other information that may be relevant to the resource owner when considering approval.<br><br>The description may be entered as a single string or as pipe separated strings for locale and localized name; e.g. \\\"en|The company intranet is requesting the following access permission\\\". Locale strings are in the format <code>language + \\\"_\\\" + country + \\\"_\\\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted, the description is displayed to all users having undefined locales. e.g. \\\"The company intranet is requesting the following access permission\\\".",
    "propertyOrder" : 23600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "updateAccessToken" : {
    "title" : "Access Token",
    "description" : "The access token used to update the client.",
    "propertyOrder" : 25100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userinfoResponseFormat" : {
    "title" : "User info response format.",

```

```

    "description" : "The user info endpoint offers different output format. See http://openid.net/
specs/openid-connect-core-1_0.html#UserInfoResponse",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "tokenEndpointAuthSigningAlgorithm" : {
    "title" : "Token Endpoint Authentication Signing Algorithm",
    "description" : "The JWS algorithm that MUST be used for signing the JWT used to authenticate
the Client at the Token Endpoint for the private_key_jwt and client_secret_jwt authentication methods.
All Token Requests using these authentication methods from this Client MUST be rejected, if the JWT
is not signed with this algorithm.",
    "propertyOrder" : 24130,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "idTokenSignedResponseAlg" : {
    "title" : "ID Token Signing Algorithm",
    "description" : "Algorithm the ID Token for this client must be signed with.",
    "propertyOrder" : 24500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "accessTokenLifetime" : {
    "title" : "Access Token Lifetime (seconds)",
    "description" : "The time in seconds an access token is valid for. <i>NB</i> If this field is
set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.",
    "propertyOrder" : 26000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "postLogoutRedirectUri" : {
    "title" : "Post Logout Redirect URIs",
    "description" : "URIs that can be redirected to after the client logout process.",
    "propertyOrder" : 25000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "mixUpMitigation" : {
    "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
    "description" : "Enables OAuth 2.0 mix-up mitigation on the authorization server
side.<br><br>Enable this setting only if this OAuth 2.0 client supports the <a href=\"https://
tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01\">OAuth 2.0 Mix-Up Mitigation draft</a>,
otherwise OpenAM will fail to validate access token requests received from this client.",
    "propertyOrder" : 26300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "idTokenPublicEncryptionKey" : {
    "title" : "Client ID Token Public Encryption Key",

```

```

    "description" : "A Base64 encoded public key for encrypting ID Tokens.",
    "propertyOrder" : 24900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "status" : {
    "title" : "Status",
    "description" : "Status of the agent configuration.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "defaultMaxAge" : {
    "title" : "Default Max Age",
    "description" : "Minimum value 1. Sets the maximum length of time in seconds a session may be active after the authorization service has succeeded before the user must actively re-authenticate.",
    "propertyOrder" : 25500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "jwksCacheTimeout" : {
    "title" : "JWKS URI content cache timeout in ms",
    "description" : "To avoid loading the JWKS URI content for every token encryption, the JWKS content is cached. This timeout defines the maximum of time the JWKS URI content can be cached before being refreshed.",
    "propertyOrder" : 24110,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "idTokenEncryptionEnabled" : {
    "title" : "Enable ID Token Encryption",
    "description" : "Select to enable ID token encryption.",
    "propertyOrder" : 24600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userinfoEncryptedResponseEncryptionAlgorithm" : {
    "title" : "User info encrypted response encryption algorithm",
    "description" : "JWE enc algorithm for encrypting UserInfo Responses. If userinfo encrypted response algorithm is specified, the default for this value is A128CBC-HS256. When user info encrypted response encryption is included, user info encrypted response algorithm MUST also be provided.<br>OpenAM supports the following token encryption algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jwtTokenLifetime" : {
    "title" : "OpenID Connect JWT Token Lifetime (seconds)",
    "description" : "The time in seconds a JWT is valid for. <i>NB</i> If this field is set to zero, JWT Token Lifetime of the OAuth2 Provider is used instead of.",

```

```

    "propertyOrder" : 26100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "clientName" : {
    "title" : "Client Name",
    "description" : "This value is a readable name for this client.",
    "propertyOrder" : 25300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "scopes" : {
    "title" : "Scope(s)",
    "description" : "Scope(s). Scopes are strings that are presented to the user for approval
and included in tokens so that the protected resource may make decisions about what to give access
to.<br><br>Scopes may be entered as simple strings or pipe separated strings representing the
internal scope name, locale, and localized description; e.g. \"read|en|Permission to view email
messages in your account\". Locale strings are in the format <code>language + \"_\" + country + \"_\"
\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description
is displayed to all users having undefined locales. e.g. \"read|Permission to view email messages in
your account\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g.
specifying \"read|\" would allow the scope \"read\" to be used by the client, but would not display
it to the user when it was requested.",
    "propertyOrder" : 23300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "refreshTokenLifetime" : {
    "title" : "Refresh Token Lifetime (seconds)",
    "description" : "The time in seconds a refresh token is valid for. <i>NB</i> If this field is
set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set to
-1, the token will never expire.",
    "propertyOrder" : 25900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "defaultMaxAgeEnabled" : {
    "title" : "Default Max Age Enabled",
    "description" : "Whether or not the default max age is enforced.",
    "propertyOrder" : 25600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "idTokenEncryptionMethod" : {
    "title" : "ID Token Encryption Method",
    "description" : "Encryption method the ID Token for this client must be encrypted with.",
    "propertyOrder" : 24800,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "jwkSet" : {
    "title" : "Json Web Key",
    "description" : "Raw JSON Web Key value containing the client's public keys.",
    "propertyOrder" : 24200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userinfoEncryptedResponseAlg" : {
    "title" : "User info encrypted response algorithm",
    "description" : "JWE algorithm for encrypting UserInfo Responses. If both signing and encryption
are requested, the response will be signed then encrypted, with the result being a Nested JWT. The
default, if omitted, is that no encryption is performed.",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientType" : {
    "title" : "Client type",
    "description" : "Type of OAuth 2.0 client. Confidential clients can keep their password secret,
and are typically web apps or other server-based clients. Public clients run the risk of exposing
their password to a host or user agent, such as rich browser applications or desktop clients.",
    "propertyOrder" : 23100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "publicKeyLocation" : {
    "title" : "Public key selector",
    "description" : "Select the public key for this client to come from either the jwks_uri, manual
jwks or X509 field.",
    "propertyOrder" : 25700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "responseTypes" : {
    "title" : "Response Types",
    "description" : "Response types this client will support and use.",
    "propertyOrder" : 23800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "jwkStoreCacheMissCacheTime" : {
    "title" : "JWKS URI content cache miss cache time",
    "description" : "To avoid loading the JWKS URI content for every token signature verification,
especially when the kid is not in the jwks content already cached, the JWKS content will be cache for
a minimum period of time. This cache miss cache time defines the minimum of time the JWKS URI content
is cache.",
    "propertyOrder" : 24120,
    "required" : true,

```

```

    "type" : "integer",
    "exampleValue" : ""
  },
  "clientSessionUri" : {
    "title" : "Client Session URI",
    "description" : "This is the URI that will be used to check messages sent to the session
management endpoints. This URI must match the origin of the message",
    "propertyOrder" : 25200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jwksUri" : {
    "title" : "Json Web Key URI",
    "description" : "The uri that contains the client's public keys in Json Web Key format.",
    "propertyOrder" : 24100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "isConsentImplied" : {
    "title" : "Implied consent",
    "description" : "When enabled, the resource owner will not be asked for consent during
authorization flows. The OAuth2 Provider must be configured to allow clients to skip consent.",
    "propertyOrder" : 26200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "claims" : {
    "title" : "Claim(s)",
    "description" : "List of claim name translations, which will override those specified for
the AS. Claims are values that are presented to the user to inform them what data is being made
available to the Client.<br><br>Claims may be entered as simple strings or pipe separated strings
representing the internal claim name, locale, and localized description; e.g. \"name|en|Your full
name|. Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>,
e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all
users having undefined locales. e.g. \"name|Your full name|. <i>NB</i> If the description is also
omitted, nothing is displayed to all users, e.g. specifying \"name|\" would allow the claim \"name\"
to be used by the client, but would not display it to the user when it was requested.<p>If a value is
not given here, the value will be computed from the OAuth 2 Provider settings.</p>",
    "propertyOrder" : 23400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "contacts" : {
    "title" : "Contacts",
    "description" : "Email addresses of users who can administrate this client.",
    "propertyOrder" : 23900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }

```

```

},
"name" : {
  "title" : "Display name",
  "description" : "A client name that may be relevant to the resource owner when considering approval.<br><br>The name may be entered as a single string or as pipe separated strings for locale and localized name; e.g. \"en|The ExampleCo Intranet\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted, the name is displayed to all users having undefined locales. e.g. \"The ExampleCo Intranet\".",
  "propertyOrder" : 23500,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"userpassword" : {
  "title" : "Client password",
  "description" : "Client password. Used when the client authenticates to OpenAM.",
  "propertyOrder" : 23000,
  "required" : true,
  "type" : "string",
  "format" : "password",
  "exampleValue" : ""
},
"subjectType" : {
  "title" : "Subject Type",
  "description" : "The subject type added to responses for this client.",
  "propertyOrder" : 24400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"clientJwtPublicKey" : {
  "title" : "Client JWT Bearer Public Key",
  "description" : "A Base64 encoded X509 certificate, containing the public key, represented as a UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.",
  "propertyOrder" : 25400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"tokenEndpointAuthMethod" : {
  "title" : "Token Endpoint Authentication Method",
  "description" : "The authentication method with which a client authenticates to the authorization server at the token endpoint. The authentication method applies to OIDC requests with the openid scope.",
  "propertyOrder" : 24000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sectorIdentifierUri" : {
  "title" : "Sector Identifier URI",
  "description" : "The Host component of this URL is used in the computation of pairwise Subject Identifiers.",
  "propertyOrder" : 24300,
  "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "defaultScopes" : {
    "title" : "Default Scope(s)",
    "description" : "Default Scope(s). Scopes automatically given to tokens.<br><br>Default Scopes
may be entered as simple strings or pipe separated strings representing the internal scope name,
locale, and localized description; e.g. \"read|en|Permission to view email messages in your account
\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g.
en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all users
having undefined locales. e.g. \"read|Permission to view email messages in your account\". <i>NB</i>
If the description is also omitted, nothing is displayed to all users, e.g. specifying \"read|\"
would allow the scope \"read\" to be used by the client, but would not display it to the user when it
was requested.",
    "propertyOrder" : 23700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }
}
}

```

### 1.78.1.2. delete

Usage:

```
am> delete OAuth2ClientAgentGroups --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.78.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2ClientAgentGroups --realm Realm --actionName getAllTypes
```

### 1.78.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:



```
am> action OAuth2ClientAgentGroups --realm Realm --actionName getCreatableTypes
```

### 1.78.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2ClientAgentGroups --realm Realm --actionName nextdescendents
```

### 1.78.1.6. query

Querying the agent groups of a specific type

Usage:

```
am> query OAuth2ClientAgentGroups --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.78.1.7. read

Usage:

```
am> read OAuth2ClientAgentGroups --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.78.1.8. update

Usage:

```
am> update OAuth2ClientAgentGroups --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "redirectionUri" : {
      "title" : "Redirection URIs",
      "description" : "Redirection URIs (optional for confidential clients). Complete URIs or URIs consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify the URI that the user should be redirected to following approval. May not contain a fragment (#).",
      "propertyOrder" : 23200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "idTokenEncryptionAlgorithm" : {
      "title" : "ID Token Encryption Algorithm",
      "description" : "Algorithm the ID Token for this client must be encrypted with.",
      "propertyOrder" : 24700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userInfoSignedResponseAlg" : {
      "title" : "User info signed response algorithm",
      "description" : "JWS algorithm for signing UserInfo Responses. If this is specified, the response will be JWT <a href='\"https://tools.ietf.org/html/rfc7519\"'>JWT</a> serialized, and signed using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8 encoded JSON object using the application/json content-type.",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authorizationCodeLifetime" : {
      "title" : "Authorization Code Lifetime (seconds)",
      "description" : "The time in seconds an authorization code is valid for. <i>NB</i> If this field is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.",
      "propertyOrder" : 25800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "descriptions" : {
      "title" : "Display description",
      "description" : "A description of the client or other information that may be relevant to the resource owner when considering approval.<br><br>The description may be entered as a single string or as pipe separated strings for locale and localized name; e.g. \\\"en|The company intranet is requesting the following access permission\\\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted, the description is displayed to all users having undefined locales. e.g. \\\"The company intranet is requesting the following access permission\\\".",
      "propertyOrder" : 23600,

```

```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "updateAccessToken" : {
    "title" : "Access Token",
    "description" : "The access token used to update the client.",
    "propertyOrder" : 25100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userinfoResponseFormat" : {
    "title" : "User info response format.",
    "description" : "The user info endpoint offers different output format. See http://openid.net/specs/openid-connect-core-1\_0.html#UserInfoResponse",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "tokenEndpointAuthSigningAlgorithm" : {
    "title" : "Token Endpoint Authentication Signing Algorithm",
    "description" : "The JWS algorithm that MUST be used for signing the JWT used to authenticate the Client at the Token Endpoint for the private_key_jwt and client_secret_jwt authentication methods. All Token Requests using these authentication methods from this Client MUST be rejected, if the JWT is not signed with this algorithm.",
    "propertyOrder" : 24130,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "idTokenSignedResponseAlg" : {
    "title" : "ID Token Signing Algorithm",
    "description" : "Algorithm the ID Token for this client must be signed with.",
    "propertyOrder" : 24500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "accessTokenLifetime" : {
    "title" : "Access Token Lifetime (seconds)",
    "description" : "The time in seconds an access token is valid for. <i>NB</i> If this field is set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.",
    "propertyOrder" : 26000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "postLogoutRedirectUri" : {
    "title" : "Post Logout Redirect URIs",
    "description" : "URIs that can be redirected to after the client logout process.",
    "propertyOrder" : 25000,
    "required" : true,
    "items" : {
      "type" : "string"
    }
  }

```

```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "mixUpMitigation" : {
    "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
    "description" : "Enables OAuth 2.0 mix-up mitigation on the authorization server
side.<br><br>Enable this setting only if this OAuth 2.0 client supports the <a href=\"https://
tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01\">OAuth 2.0 Mix-Up Mitigation draft</a>,
otherwise OpenAM will fail to validate access token requests received from this client.",
    "propertyOrder" : 26300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "idTokenPublicEncryptionKey" : {
    "title" : "Client ID Token Public Encryption Key",
    "description" : "A Base64 encoded public key for encrypting ID Tokens.",
    "propertyOrder" : 24900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "status" : {
    "title" : "Status",
    "description" : "Status of the agent configuration.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "defaultMaxAge" : {
    "title" : "Default Max Age",
    "description" : "Minimum value 1. Sets the maximum length of time in seconds a session may be
active after the authorization service has succeeded before the user must actively re-authenticate.",
    "propertyOrder" : 25500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "jwksCacheTimeout" : {
    "title" : "JWKS URI content cache timeout in ms",
    "description" : "To avoid loading the JWKS URI content for every token encryption, the JWKS
content is cached. This timeout defines the maximum of time the JWKS URI content can be cached before
being refreshed.",
    "propertyOrder" : 24110,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "idTokenEncryptionEnabled" : {
    "title" : "Enable ID Token Encryption",
    "description" : "Select to enable ID token encryption.",
    "propertyOrder" : 24600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userinfoEncryptedResponseEncryptionAlgorithm" : {

```

```

    "title" : "User info encrypted response encryption algorithm",
    "description" : "JWE enc algorithm for encrypting UserInfo Responses. If userinfo encrypted
response algorithm is specified, the default for this value is A128CBC-HS256. When user info
encrypted response encryption is included, user info encrypted response algorithm MUST also be
provided.<br><br>OpenAM supports the following token encryption algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jwtTokenLifetime" : {
    "title" : "OpenID Connect JWT Token Lifetime (seconds)",
    "description" : "The time in seconds a JWT is valid for. <i>NB</i> If this field is set to zero,
JWT Token Lifetime of the OAuth2 Provider is used instead of.",
    "propertyOrder" : 26100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "clientName" : {
    "title" : "Client Name",
    "description" : "This value is a readable name for this client.",
    "propertyOrder" : 25300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "scopes" : {
    "title" : "Scope(s)",
    "description" : "Scope(s). Scopes are strings that are presented to the user for approval
and included in tokens so that the protected resource may make decisions about what to give access
to.<br><br>Scopes may be entered as simple strings or pipe separated strings representing the
internal scope name, locale, and localized description; e.g. \"read|en|Permission to view email
messages in your account\". Locale strings are in the format <code>language + \"_\" + country + \"_\"
+ variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description
is displayed to all users having undefined locales. e.g. \"read|Permission to view email messages in
your account\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g.
specifying \"read|\" would allow the scope \"read\" to be used by the client, but would not display
it to the user when it was requested.",
    "propertyOrder" : 23300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "refreshTokenLifetime" : {
    "title" : "Refresh Token Lifetime (seconds)",
    "description" : "The time in seconds a refresh token is valid for. <i>NB</i> If this field is
set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set to
-1, the token will never expire.",
    "propertyOrder" : 25900,

```

```

    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "defaultMaxAgeEnabled" : {
    "title" : "Default Max Age Enabled",
    "description" : "Whether or not the default max age is enforced.",
    "propertyOrder" : 25600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "idTokenEncryptionMethod" : {
    "title" : "ID Token Encryption Method",
    "description" : "Encryption method the ID Token for this client must be encrypted with.",
    "propertyOrder" : 24800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jwkSet" : {
    "title" : "Json Web Key",
    "description" : "Raw JSON Web Key value containing the client's public keys.",
    "propertyOrder" : 24200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userinfoEncryptedResponseAlg" : {
    "title" : "User info encrypted response algorithm",
    "description" : "JWE algorithm for encrypting UserInfo Responses. If both signing and encryption are requested, the response will be signed then encrypted, with the result being a Nested JWT. The default, if omitted, is that no encryption is performed.",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientType" : {
    "title" : "Client type",
    "description" : "Type of OAuth 2.0 client. Confidential clients can keep their password secret, and are typically web apps or other server-based clients. Public clients run the risk of exposing their password to a host or user agent, such as rich browser applications or desktop clients.",
    "propertyOrder" : 23100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "publicKeyLocation" : {
    "title" : "Public key selector",
    "description" : "Select the public key for this client to come from either the jwks_uri, manual jwks or X509 field.",
    "propertyOrder" : 25700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "responseTypes" : {
    "title" : "Response Types",

```

```

    "description" : "Response types this client will support and use.",
    "propertyOrder" : 23800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "jwkStoreCacheMissCacheTime" : {
    "title" : "JWKS URI content cache miss cache time",
    "description" : "To avoid loading the JWKS URI content for every token signature verification, especially when the kid is not in the jwks content already cached, the JWKS content will be cache for a minimum period of time. This cache miss cache time defines the minimum of time the JWKS URI content is cache.",
    "propertyOrder" : 24120,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "clientSessionUri" : {
    "title" : "Client Session URI",
    "description" : "This is the URI that will be used to check messages sent to the session management endpoints. This URI must match the origin of the message",
    "propertyOrder" : 25200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jwksUri" : {
    "title" : "Json Web Key URI",
    "description" : "The uri that contains the client's public keys in Json Web Key format.",
    "propertyOrder" : 24100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "isConsentImplied" : {
    "title" : "Implied consent",
    "description" : "When enabled, the resource owner will not be asked for consent during authorization flows. The OAuth2 Provider must be configured to allow clients to skip consent.",
    "propertyOrder" : 26200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "claims" : {
    "title" : "Claim(s)",
    "description" : "List of claim name translations, which will override those specified for the AS. Claims are values that are presented to the user to inform them what data is being made available to the Client.<br><br>Claims may be entered as simple strings or pipe separated strings representing the internal claim name, locale, and localized description; e.g. \"name|en|Your full name\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all users having undefined locales. e.g. \"name|Your full name\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g. specifying \"name|\" would allow the claim \"name\" to be used by the client, but would not display it to the user when it was requested.<p>If a value is not given here, the value will be computed from the OAuth 2 Provider settings.</p>\",
    "propertyOrder" : 23400,

```

```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "contacts" : {
    "title" : "Contacts",
    "description" : "Email addresses of users who can administrate this client.",
    "propertyOrder" : 23900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "name" : {
    "title" : "Display name",
    "description" : "A client name that may be relevant to the resource owner when considering approval.<br><br>The name may be entered as a single string or as pipe separated strings for locale and localized name; e.g. \n|The ExampleCo Intranet|. Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted, the name is displayed to all users having undefined locales. e.g. \n|The ExampleCo Intranet|.\"",
    "propertyOrder" : 23500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Client password",
    "description" : "Client password. Used when the client authenticates to OpenAM.",
    "propertyOrder" : 23000,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "subjectType" : {
    "title" : "Subject Type",
    "description" : "The subject type added to responses for this client.",
    "propertyOrder" : 24400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientJwtPublicKey" : {
    "title" : "Client JWT Bearer Public Key",
    "description" : "A Base64 encoded X509 certificate, containing the public key, represented as a UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.",
    "propertyOrder" : 25400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}

```



```

    },
    "tokenEndpointAuthMethod" : {
      "title" : "Token Endpoint Authentication Method",
      "description" : "The authentication method with which a client authenticates to the
authorization server at the token endpoint. The authentication method applies to OIDC requests with
the openid scope.",
      "propertyOrder" : 24000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sectorIdentifierUri" : {
      "title" : "Sector Identifier URI",
      "description" : "The Host component of this URL is used in the computation of pairwise Subject
Identifiers.",
      "propertyOrder" : 24300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "defaultScopes" : {
      "title" : "Default Scope(s)",
      "description" : "Default Scope(s). Scopes automatically given to tokens.<br><br>Default Scopes
may be entered as simple strings or pipe separated strings representing the internal scope name,
locale, and localized description; e.g. \"read|en|Permission to view email messages in your account
\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g.
en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all users
having undefined locales. e.g. \"read|Permission to view email messages in your account\". <i>NB</
i> If the description is also omitted, nothing is displayed to all users, e.g. specifying \"read|\"
would allow the scope \"read\" to be used by the client, but would not display it to the user when it
was requested.",
      "propertyOrder" : 23700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}

```

## 1.79. OAuth2Clients

### 1.79.1. Realm Operations

Agents handler that is responsible for managing agents

Resource path: </realm-config/agents/OAuth2Client>

Resource version: [1.0](#)

### 1.79.1.1. create

Usage:

```
am> create OAuth2Clients --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "updateAccessToken" : {
      "title" : "Access Token",
      "description" : "The access token used to update the client.",
      "propertyOrder" : 25100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwtTokenLifetime" : {
      "title" : "OpenID Connect JWT Token Lifetime (seconds)",
      "description" : "The time in seconds a JWT is valid for. <i>NB</i> If this field is set to zero,
      JWT Token Lifetime of the OAuth2 Provider is used instead of.",
      "propertyOrder" : 26100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "idTokenEncryptionEnabled" : {
      "title" : "Enable ID Token Encryption",
      "description" : "Select to enable ID token encryption.",
      "propertyOrder" : 24600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userinfoResponseFormat" : {
      "title" : "User info response format.",
      "description" : "The user info endpoint offers different output format. See http://openid.net/
      specs/openid-connect-core-1_0.html#UserInfoResponse",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userinfoSignedResponseAlg" : {
      "title" : "User info signed response algorithm",
      "description" : "JWS algorithm for signing UserInfo Responses. If this is specified, the
      response will be JWT <a href='\"https://tools.ietf.org/html/rfc7519\">JWT</a> serialized, and signed
```

```

using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8
encoded JSON object using the application/json content-type.",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"defaultMaxAgeEnabled" : {
  "title" : "Default Max Age Enabled",
  "description" : "Whether or not the default max age is enforced.",
  "propertyOrder" : 25600,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"jwksCacheTimeout" : {
  "title" : "JWKS URI content cache timeout in ms",
  "description" : "To avoid loading the JWKS URI content for every token encryption, the JWKS
content is cached. This timeout defines the maximum of time the JWKS URI content can be cached before
being refreshed.",
  "propertyOrder" : 24110,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"accessTokenLifetime" : {
  "title" : "Access Token Lifetime (seconds)",
  "description" : "The time in seconds an access token is valid for. <i>NB</i> If this field is
set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.",
  "propertyOrder" : 26000,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"responseTypes" : {
  "title" : "Response Types",
  "description" : "Response types this client will support and use.",
  "propertyOrder" : 23800,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"clientSessionUri" : {
  "title" : "Client Session URI",
  "description" : "This is the URI that will be used to check messages sent to the session
management endpoints. This URI must match the origin of the message",
  "propertyOrder" : 25200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"claims" : {
  "title" : "Claim(s)",
  "description" : "List of claim name translations, which will override those specified for
the AS. Claims are values that are presented to the user to inform them what data is being made
available to the Client.<br><br>Claims may be entered as simple strings or pipe separated strings

```

representing the internal claim name, locale, and localized description; e.g. `\name|en|Your full name\`. Locale strings are in the format `<code>language + \"_\" + country + \"_\" + variant</code>`, e.g. `en`, `en_GB`, `en_US_WIN`. If the locale and pipe is omitted, the description is displayed to all users having undefined locales. e.g. `\name|Your full name\`. *<i>NB</i>* If the description is also omitted, nothing is displayed to all users, e.g. specifying `\name|` would allow the claim `\name\` to be used by the client, but would not display it to the user when it was requested.*<p>*If a value is not given here, the value will be computed from the OAuth 2 Provider settings.*</p>*

```

    "propertyOrder" : 23400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "redirectionUris" : {
    "title" : "Redirection URIs",
    "description" : "Redirection URIs (optional for confidential clients). Complete URIs or URIs
consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust
that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify
the URI that the user should be redirected to following approval. May not contain a fragment (#).",
    "propertyOrder" : 23200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Client password",
    "description" : "Client password. Used when the client authenticates to OpenAM.",
    "propertyOrder" : 23000,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "authorizationCodeLifetime" : {
    "title" : "Authorization Code Lifetime (seconds)",
    "description" : "The time in seconds an authorization code is valid for. <i>NB</i> If this field
is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.",
    "propertyOrder" : 25800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "subjectType" : {
    "title" : "Subject Type",
    "description" : "The subject type added to responses for this client.",
    "propertyOrder" : 24400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientJwtPublicKey" : {
    "title" : "Client JWT Bearer Public Key",
    "description" : "A Base64 encoded X509 certificate, containing the public key, represented as a
UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.",

```

```

    "propertyOrder" : 25400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "postLogoutRedirectUri" : {
    "title" : "Post Logout Redirect URIs",
    "description" : "URIs that can be redirected to after the client logout process.",
    "propertyOrder" : 25000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "clientName" : {
    "title" : "Client Name",
    "description" : "This value is a readable name for this client.",
    "propertyOrder" : 25300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "refreshTokenLifetime" : {
    "title" : "Refresh Token Lifetime (seconds)",
    "description" : "The time in seconds a refresh token is valid for. <i>NB</i> If this field is
set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set to
-1, the token will never expire.",
    "propertyOrder" : 25900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "publicKeyLocation" : {
    "title" : "Public key selector",
    "description" : "Select the public key for this client to come from either the jwks_uri, manual
jwks or X509 field.",
    "propertyOrder" : 25700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "defaultScopes" : {
    "title" : "Default Scope(s)",
    "description" : "Default Scope(s). Scopes automatically given to tokens.<br><br>Default Scopes
may be entered as simple strings or pipe separated strings representing the internal scope name,
locale, and localized description; e.g. \"read|en|Permission to view email messages in your account
\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g.
en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all users
having undefined locales. e.g. \"read|Permission to view email messages in your account\". <i>NB</i>
If the description is also omitted, nothing is displayed to all users, e.g. specifying \"read|\"
would allow the scope \"read\" to be used by the client, but would not display it to the user when it
was requested.",
    "propertyOrder" : 23700,
    "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "idTokenSignedResponseAlg" : {
    "title" : "ID Token Signing Algorithm",
    "description" : "Algorithm the ID Token for this client must be signed with.",
    "propertyOrder" : 24500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "scopes" : {
    "title" : "Scope(s)",
    "description" : "Scope(s). Scopes are strings that are presented to the user for approval
and included in tokens so that the protected resource may make decisions about what to give access
to.<br><br>Scopes may be entered as simple strings or pipe separated strings representing the
internal scope name, locale, and localized description; e.g. \"read|en|Permission to view email
messages in your account\". Locale strings are in the format <code>language + \"_\" + country + \"_\"
+ variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description
is displayed to all users having undefined locales. e.g. \"read|Permission to view email messages in
your account\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g.
specifying \"read|\" would allow the scope \"read\" to be used by the client, but would not display
it to the user when it was requested.",
    "propertyOrder" : 23300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "tokenEndpointAuthSigningAlgorithm" : {
    "title" : "Token Endpoint Authentication Signing Algorithm",
    "description" : "The JWS algorithm that MUST be used for signing the JWT used to authenticate
the Client at the Token Endpoint for the private_key_jwt and client_secret_jwt authentication methods.
All Token Requests using these authentication methods from this Client MUST be rejected, if the JWT
is not signed with this algorithm.",
    "propertyOrder" : 24130,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "idTokenEncryptionAlgorithm" : {
    "title" : "ID Token Encryption Algorithm",
    "description" : "Algorithm the ID Token for this client must be encrypted with.",
    "propertyOrder" : 24700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "descriptions" : {
    "title" : "Display description",
    "description" : "A description of the client or other information that may be relevant to the
resource owner when considering approval.<br><br>The description may be entered as a single string or
as pipe separated strings for locale and localized name; e.g. \"en|The company intranet is requesting
the following access permission\". Locale strings are in the format <code>language + \"_\" + country

```

```
+ \"\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted, the description is
displayed to all users having undefined locales. e.g. \"The company intranet is requesting the
following access permission\".",
  "propertyOrder" : 23600,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"clientType" : {
  "title" : "Client type",
  "description" : "Type of OAuth 2.0 client. Confidential clients can keep their password secret,
and are typically web apps or other server-based clients. Public clients run the risk of exposing
their password to a host or user agent, such as rich browser applications or desktop clients.",
  "propertyOrder" : 23100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"mixUpMitigation" : {
  "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
  "description" : "Enables OAuth 2.0 mix-up mitigation on the authorization server
side.<br><br>Enable this setting only if this OAuth 2.0 client supports the <a href=\"https://
tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01\">OAuth 2.0 Mix-Up Mitigation draft</a>,
otherwise OpenAM will fail to validate access token requests received from this client.",
  "propertyOrder" : 26300,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"contacts" : {
  "title" : "Contacts",
  "description" : "Email addresses of users who can administrate this client.",
  "propertyOrder" : 23900,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"idTokenEncryptionMethod" : {
  "title" : "ID Token Encryption Method",
  "description" : "Encryption method the ID Token for this client must be encrypted with.",
  "propertyOrder" : 24800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"jwkSet" : {
  "title" : "Json Web Key",
  "description" : "Raw JSON Web Key value containing the client's public keys.",
  "propertyOrder" : 24200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
},
```

```

    "isConsentImplied" : {
      "title" : "Implied consent",
      "description" : "When enabled, the resource owner will not be asked for consent during
authorization flows. The OAuth2 Provider must be configured to allow clients to skip consent.",
      "propertyOrder" : 26200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userinfoEncryptedResponseEncryptionAlgorithm" : {
      "title" : "User info encrypted response encryption algorithm",
      "description" : "JWE enc algorithm for encrypting UserInfo Responses. If userinfo encrypted
response algorithm is specified, the default for this value is A128CBC-HS256. When user info
encrypted response encryption is included, user info encrypted response algorithm MUST also be
provided.<br><br>OpenAM supports the following token encryption algorithms:<ul><li><code>A128GCM</code></li>
<code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sectorIdentifierUri" : {
      "title" : "Sector Identifier URI",
      "description" : "The Host component of this URL is used in the computation of pairwise Subject
Identifiers.",
      "propertyOrder" : 24300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "defaultMaxAge" : {
      "title" : "Default Max Age",
      "description" : "Minimum value 1. Sets the maximum length of time in seconds a session may be
active after the authorization service has succeeded before the user must actively re-authenticate.",
      "propertyOrder" : 25500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKS URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every token signature verification,
especially when the kid is not in the jwks content already cached, the JWKS content will be cache for
a minimum period of time. This cache miss cache time defines the minimum of time the JWKS URI content
is cache.",
      "propertyOrder" : 24120,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The uri that contains the client's public keys in Json Web Key format.",
      "propertyOrder" : 24100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }

```



```

    },
    "name" : {
      "title" : "Display name",
      "description" : "A client name that may be relevant to the resource owner when considering approval.<br><br>The name may be entered as a single string or as pipe separated strings for locale and localized name; e.g. \"en|The ExampleCo Intranet\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted, the name is displayed to all users having undefined locales. e.g. \"The ExampleCo Intranet\".",
      "propertyOrder" : 23500,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "idTokenPublicEncryptionKey" : {
      "title" : "Client ID Token Public Encryption Key",
      "description" : "A Base64 encoded public key for encrypting ID Tokens.",
      "propertyOrder" : 24900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userinfoEncryptedResponseAlg" : {
      "title" : "User info encrypted response algorithm",
      "description" : "JWE algorithm for encrypting UserInfo Responses. If both signing and encryption are requested, the response will be signed then encrypted, with the result being a Nested JWT. The default, if omitted, is that no encryption is performed.",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpointAuthMethod" : {
      "title" : "Token Endpoint Authentication Method",
      "description" : "The authentication method with which a client authenticates to the authorization server at the token endpoint. The authentication method applies to OIDC requests with the openid scope.",
      "propertyOrder" : 24000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}

```

### 1.79.1.2. delete

Usage:

```
am> delete OAuth2Clients --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.79.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Clients --realm Realm --actionName getAllTypes
```

### 1.79.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Clients --realm Realm --actionName getCreatableTypes
```

### 1.79.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Clients --realm Realm --actionName nextdescendents
```

### 1.79.1.6. query

Querying the agents of a specific type

Usage:

```
am> query OAuth2Clients --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.79.1.7. read

Usage:

```
am> read OAuth2Clients --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.79.1.8. update

Usage:

```
am> update OAuth2Clients --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "updateAccessToken" : {
      "title" : "Access Token",
      "description" : "The access token used to update the client.",
      "propertyOrder" : 25100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwtTokenLifetime" : {
      "title" : "OpenID Connect JWT Token Lifetime (seconds)",
      "description" : "The time in seconds a JWT is valid for. <i>NB</i> If this field is set to zero, JWT Token Lifetime of the OAuth2 Provider is used instead of.",
      "propertyOrder" : 26100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "idTokenEncryptionEnabled" : {
      "title" : "Enable ID Token Encryption",
      "description" : "Select to enable ID token encryption.",
      "propertyOrder" : 24600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
}
```

```

"userinfoResponseFormat" : {
  "title" : "User info response format.",
  "description" : "The user info endpoint offers different output format. See http://openid.net/specs/openid-connect-core-1_0.html#UserInfoResponse",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userinfoSignedResponseAlg" : {
  "title" : "User info signed response algorithm",
  "description" : "JWS algorithm for signing UserInfo Responses. If this is specified, the response will be JWT <a href='\"https://tools.ietf.org/html/rfc7519\">JWT</a> serialized, and signed using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8 encoded JSON object using the application/json content-type.",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"defaultMaxAgeEnabled" : {
  "title" : "Default Max Age Enabled",
  "description" : "Whether or not the default max age is enforced.",
  "propertyOrder" : 25600,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"jwksCacheTimeout" : {
  "title" : "JWKS URI content cache timeout in ms",
  "description" : "To avoid loading the JWKS URI content for every token encryption, the JWKS content is cached. This timeout defines the maximum of time the JWKS URI content can be cached before being refreshed.",
  "propertyOrder" : 24110,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"accessTokenLifetime" : {
  "title" : "Access Token Lifetime (seconds)",
  "description" : "The time in seconds an access token is valid for. <i>NB</i> If this field is set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.",
  "propertyOrder" : 26000,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"responseTypes" : {
  "title" : "Response Types",
  "description" : "Response types this client will support and use.",
  "propertyOrder" : 23800,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"clientSessionUri" : {

```

```

    "title" : "Client Session URI",
    "description" : "This is the URI that will be used to check messages sent to the session
management endpoints. This URI must match the origin of the message",
    "propertyOrder" : 25200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "claims" : {
    "title" : "Claim(s)",
    "description" : "List of claim name translations, which will override those specified for
the AS. Claims are values that are presented to the user to inform them what data is being made
available to the Client.<br><br>Claims may be entered as simple strings or pipe separated strings
representing the internal claim name, locale, and localized description; e.g. \"name|en|Your full
name\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>,
e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all
users having undefined locales. e.g. \"name|Your full name\". <i>NB</i> If the description is also
omitted, nothing is displayed to all users, e.g. specifying \"name|\" would allow the claim \"name\"
to be used by the client, but would not display it to the user when it was requested.<p>If a value is
not given here, the value will be computed from the OAuth 2 Provider settings.</p>",
    "propertyOrder" : 23400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "redirectionUris" : {
    "title" : "Redirection URIs",
    "description" : "Redirection URIs (optional for confidential clients). Complete URIs or URIs
consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust
that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify
the URI that the user should be redirected to following approval. May not contain a fragment (#).",
    "propertyOrder" : 23200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Client password",
    "description" : "Client password. Used when the client authenticates to OpenAM.",
    "propertyOrder" : 23000,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "authorizationCodeLifetime" : {
    "title" : "Authorization Code Lifetime (seconds)",
    "description" : "The time in seconds an authorization code is valid for. <i>NB</i> If this field
is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.",
    "propertyOrder" : 25800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }
}

```

```

},
"subjectType" : {
  "title" : "Subject Type",
  "description" : "The subject type added to responses for this client.",
  "propertyOrder" : 24400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"clientJwtPublicKey" : {
  "title" : "Client JWT Bearer Public Key",
  "description" : "A Base64 encoded X509 certificate, containing the public key, represented as a
UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.",
  "propertyOrder" : 25400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"postLogoutRedirectUri" : {
  "title" : "Post Logout Redirect URIs",
  "description" : "URIs that can be redirected to after the client logout process.",
  "propertyOrder" : 25000,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"clientName" : {
  "title" : "Client Name",
  "description" : "This value is a readable name for this client.",
  "propertyOrder" : 25300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"refreshTokenLifetime" : {
  "title" : "Refresh Token Lifetime (seconds)",
  "description" : "The time in seconds a refresh token is valid for. <i>NB</i> If this field is
set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set to
-1, the token will never expire.",
  "propertyOrder" : 25900,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"publicKeyLocation" : {
  "title" : "Public key selector",
  "description" : "Select the public key for this client to come from either the jwks_uri, manual
jwks or X509 field.",
  "propertyOrder" : 25700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
},

```

```

"defaultScopes" : {
  "title" : "Default Scope(s)",
  "description" : "Default Scope(s). Scopes automatically given to tokens.<br><br>Default Scopes
may be entered as simple strings or pipe separated strings representing the internal scope name,
locale, and localized description; e.g. \"read|en|Permission to view email messages in your account
\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g.
en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all users
having undefined locales. e.g. \"read|Permission to view email messages in your account\". <i>NB</i>
i> If the description is also omitted, nothing is displayed to all users, e.g. specifying \"read|\"
would allow the scope \"read\" to be used by the client, but would not display it to the user when it
was requested.",
  "propertyOrder" : 23700,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"idTokenSignedResponseAlg" : {
  "title" : "ID Token Signing Algorithm",
  "description" : "Algorithm the ID Token for this client must be signed with.",
  "propertyOrder" : 24500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"scopes" : {
  "title" : "Scope(s)",
  "description" : "Scope(s). Scopes are strings that are presented to the user for approval
and included in tokens so that the protected resource may make decisions about what to give access
to.<br><br>Scopes may be entered as simple strings or pipe separated strings representing the
internal scope name, locale, and localized description; e.g. \"read|en|Permission to view email
messages in your account\". Locale strings are in the format <code>language + \"_\" + country + \"_\"
\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description
is displayed to all users having undefined locales. e.g. \"read|Permission to view email messages in
your account\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g.
specifying \"read|\" would allow the scope \"read\" to be used by the client, but would not display
it to the user when it was requested.",
  "propertyOrder" : 23300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"tokenEndpointAuthSigningAlgorithm" : {
  "title" : "Token Endpoint Authentication Signing Algorithm",
  "description" : "The JWS algorithm that MUST be used for signing the JWT used to authenticate
the Client at the Token Endpoint for the private_key_jwt and client_secret_jwt authentication methods.
All Token Requests using these authentication methods from this Client MUST be rejected, if the JWT
is not signed with this algorithm.",
  "propertyOrder" : 24130,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"idTokenEncryptionAlgorithm" : {

```

```

    "title" : "ID Token Encryption Algorithm",
    "description" : "Algorithm the ID Token for this client must be encrypted with.",
    "propertyOrder" : 24700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "descriptions" : {
    "title" : "Display description",
    "description" : "A description of the client or other information that may be relevant to the resource owner when considering approval.<br><br>The description may be entered as a single string or as pipe separated strings for locale and localized name; e.g. \"en|The company intranet is requesting the following access permission\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted, the description is displayed to all users having undefined locales. e.g. \"The company intranet is requesting the following access permission\".",
    "propertyOrder" : 23600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "clientType" : {
    "title" : "Client type",
    "description" : "Type of OAuth 2.0 client. Confidential clients can keep their password secret, and are typically web apps or other server-based clients. Public clients run the risk of exposing their password to a host or user agent, such as rich browser applications or desktop clients.",
    "propertyOrder" : 23100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "mixUpMitigation" : {
    "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
    "description" : "Enables OAuth 2.0 mix-up mitigation on the authorization server side.<br><br>Enable this setting only if this OAuth 2.0 client supports the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to validate access token requests received from this client.",
    "propertyOrder" : 26300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "contacts" : {
    "title" : "Contacts",
    "description" : "Email addresses of users who can administrate this client.",
    "propertyOrder" : 23900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "idTokenEncryptionMethod" : {
    "title" : "ID Token Encryption Method",
    "description" : "Encryption method the ID Token for this client must be encrypted with.",

```



```

    "propertyOrder" : 24800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "jwkSet" : {
    "title" : "Json Web Key",
    "description" : "Raw JSON Web Key value containing the client's public keys.",
    "propertyOrder" : 24200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "isConsentImplied" : {
    "title" : "Implied consent",
    "description" : "When enabled, the resource owner will not be asked for consent during authorization flows. The OAuth2 Provider must be configured to allow clients to skip consent.",
    "propertyOrder" : 26200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userinfoEncryptedResponseEncryptionAlgorithm" : {
    "title" : "User info encrypted response encryption algorithm",
    "description" : "JWE enc algorithm for encrypting UserInfo Responses. If userinfo encrypted response algorithm is specified, the default for this value is A128CBC-HS256. When user info encrypted response encryption is included, user info encrypted response algorithm MUST also be provided.<br><br>OpenAM supports the following token encryption algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
    "propertyOrder" : null,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sectorIdentifierUri" : {
    "title" : "Sector Identifier URI",
    "description" : "The Host component of this URL is used in the computation of pairwise Subject Identifiers.",
    "propertyOrder" : 24300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "defaultMaxAge" : {
    "title" : "Default Max Age",
    "description" : "Minimum value 1. Sets the maximum length of time in seconds a session may be active after the authorization service has succeeded before the user must actively re-authenticate.",
    "propertyOrder" : 25500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "jwkStoreCacheMissCacheTime" : {
    "title" : "JWKS URI content cache miss cache time",
    "description" : "To avoid loading the JWKS URI content for every token signature verification, especially when the kid is not in the jwks content already cached, the JWKS content will be cache for

```

```

a minimum period of time. This cache miss cache time defines the minimum of time the JWKS URI content
is cache.",
  "propertyOrder" : 24120,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"jwksUri" : {
  "title" : "Json Web Key URI",
  "description" : "The uri that contains the client's public keys in Json Web Key format.",
  "propertyOrder" : 24100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"name" : {
  "title" : "Display name",
  "description" : "A client name that may be relevant to the resource owner when considering
approval.<br><br>The name may be entered as a single string or as pipe separated strings for
locale and localized name; e.g. \"en|The ExampleCo Intranet\". Locale strings are in the format
<code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale
is omitted, the name is displayed to all users having undefined locales. e.g. \"The ExampleCo
Intranet\".",
  "propertyOrder" : 23500,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"idTokenPublicKey" : {
  "title" : "Client ID Token Public Encryption Key",
  "description" : "A Base64 encoded public key for encrypting ID Tokens.",
  "propertyOrder" : 24900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userinfoEncryptedResponseAlg" : {
  "title" : "User info encrypted response algorithm",
  "description" : "JWE algorithm for encrypting UserInfo Responses. If both signing and encryption
are requested, the response will be signed then encrypted, with the result being a Nested JWT. The
default, if omitted, is that no encryption is performed.",
  "propertyOrder" : null,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"tokenEndpointAuthMethod" : {
  "title" : "Token Endpoint Authentication Method",
  "description" : "The authentication method with which a client authenticates to the
authorization server at the token endpoint. The authentication method applies to OIDC requests with
the openid scope.",
  "propertyOrder" : 24000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},

```

```

    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}

```

## 1.80. OAuth2Module

### 1.80.1. Realm Operations

Resource path: `/realm-config/authentication/modules/oauth2`

Resource version: `1.0`

#### 1.80.1.1. create

Usage:

```
am> create OAuth2Module --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```

{
  "type" : "object",
  "properties" : {
    "saveAttributesInSession" : {
      "title" : "Save attributes in the session",
      "description" : "If this option is enabled, the attributes configured in the attribute mapper
will be saved into the OpenAM session",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "accessTokenEndpointUrl" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",

```

```

    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "anonymousUserName" : {
    "title" : "Anonymous User",
    "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that will
represent the anonymous user. This user account must already exist in the realm.",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "scope" : {
    "title" : "Scope",
    "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
client application requires. The list depends on the permissions that the resource owner grants to
the client application.<br><br> Some authorization servers use non-standard separators for scopes.
For example, Facebook takes a comma-separated list.<br><br> Default: <code>email, read_stream</
code> (Facebook example)",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "mailGatewayClass" : {
    "title" : "Mail Server Gateway implementation class",
    "description" : "The class used by the module to send email.<br><br>This class is used by the
module to send email. A custom implementation can be provided.<br><br>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpHostPort" : {
    "title" : "SMTP port",
    "description" : "The TCP port that will be used by the SMTP gateway",
    "propertyOrder" : 2400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "oauth2LogoutServiceUrl" : {
    "title" : "OAuth 2.0 Provider logout service",
    "description" : "The URL of the OAuth Identity Providers Logout service<br><br>OAuth 2.0
Identity Providers can have a logout service. If this logout functionality is required then the URL
of the Logout endpoint should configured here.",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "attributeMapperConfiguration" : {
    "title" : "Attribute Mapper Configuration",
    "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the

```

```

local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</code>
",
  "propertyOrder" : 1300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"authenticationEndpointUrl" : {
  "title" : "Authentication Endpoint URL",
  "description" : "OAuth authentication endpoint URL<br/><br/>This is the URL endpoint for OAuth authentication provided by the OAuth Identity Provider",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"smtpUsername" : {
  "title" : "SMTP User Name",
  "description" : "If the SMTP Service requires authentication, configure the user name here",
  "propertyOrder" : 2500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"smtpPassword" : {
  "title" : "SMTP User Password",
  "description" : "The Password of the SMTP User Name",
  "propertyOrder" : 2600,
  "required" : true,
  "type" : "string",
  "format" : "password",
  "exampleValue" : ""
},
"openidConnectContextType" : {
  "title" : "OpenID Connect validation configuration type",
  "description" : "Required when the 'openid' scope is included. Please select either 1. the issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
  "propertyOrder" : 3000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"clientId" : {
  "title" : "Client Id",
  "description" : "OAuth client_id parameter<br/><br/>For more information on the OAuth client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=\"_blank\">RFC 6749</a>, section 2.3.1",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"mixUpMitigation" : {
  "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
  "description" : "Enables OAuth 2.0 mix-up mitigation<br/><br/>The authorization server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-

```

```
mitigation-01#section-3.1\>OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
  "propertyOrder" : 3300,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"accessTokenParameterName" : {
  "title" : "OAuth2 Access Token Profile Service Parameter name",
  "description" : "The name of the parameter that will contain the access token value when
accessing the profile service",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"openidConnectContextValue" : {
  "title" : "OpenID Connect validation configuration value",
  "description" : "Required when the 'openid' scope is included. The discovery url, or jwk
url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url
entered, entry must be in valid url format, <br>e.g. https://accounts.google.com/.well-known/openid-
configuration<br><i>NB </i>If client_secret entered, entry is ignored and the value of the Client
Secret is used.",
  "propertyOrder" : 3100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"userProfileServiceUrl" : {
  "title" : "User Profile Service URL",
  "description" : "User profile information URL<br><br>This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider<br><i>NB </i>This URL should return
JSON objects in response",
  "propertyOrder" : 500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"authenticationLevel" : {
  "title" : "Authentication Level",
  "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
  "propertyOrder" : 2900,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"oauth2EmailAttribute" : {
  "title" : "Email attribute in OAuth2 Response",
  "description" : "Attribute from the OAuth2 response used to send activation code
emails.<br><br>The attribute in the response from the profile service in the OAuth 2.0 Provider that
contains the email address of the authenticated user. This address will be used to send an email with
an activation code when the accounts are allowed to be created dynamically.",
  "propertyOrder" : 1500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
```

```

},
"smtpSslEnabled" : {
  "title" : "SMTP SSL Enabled",
  "description" : "Tick this option if the SMTP Server provides SSL",
  "propertyOrder" : 2700,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"smtpHostName" : {
  "title" : "SMTP host",
  "description" : "The mail host that will be used by the Email Gateway implementation",
  "propertyOrder" : 2300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"accountMapperConfiguration" : {
  "title" : "Account Mapper Configuration",
  "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute configuration that will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
  "propertyOrder" : 1100,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"promptForPassword" : {
  "title" : "Prompt for password setting and activation code",
  "description" : "Users must set a password and complete the activation flow during dynamic profile creation.<br><br>If this is enabled, the user must set a password before the system creates an account dynamically and an activation code will be sent to the user's email address. The account will be created only if the password and activation code are properly set. <br />If this is disabled, the account will be created transparently without prompting the user.",
  "propertyOrder" : 1700,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"clientSecret" : {
  "title" : "Client Secret",
  "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=\"_blank\">RFC 6749</a>, section 2.3.1",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "string",
  "format" : "password",
  "exampleValue" : ""
},
"attributeMappingClasses" : {
  "title" : "Attribute Mapper",
  "description" : "Name of the class that implements the attribute mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom attribute mapper can be provided.<br><br>A custom attribute mapper must implement the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>"
}

```

```

interface.<br/>Provided implementations
are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
    "propertyOrder" : 1200,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"createAccount" : {
    "title" : "Create account if it does not exist",
    "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an account
will be created dynamically.<br><br>If this is enabled, the account mapper could create the account
dynamically if there is no account mapped. Before creating the account, a dialog prompting for
a password and asking for an activation code can be shown if the parameter \"Prompt for password
setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3 alternative
options exist:<br><br><ol><li>The accounts need to have a user profile in the OpenAM User Data
Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in the
Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"openidConnectIssuer" : {
    "title" : "Token Issuer",
    "description" : "Required when the 'openid' scope is included. Value must match the iss field in
issued ID Token<br>>e.g. accounts.google.com<br><br>The issuer value MUST be provided when OAuth 2.0
Mix-Up Mitigation is enabled.",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"logoutBehaviour" : {
    "title" : "Logout options",
    "description" : "Controls how Logout options will be presented to the user.<br><br>The OAuth
module has the following logout options for the user:<br><br><ul><li>Prompt: Prompt the user to
logout from the OAuth 2.0 Provider</li><li>Logout: Logout from the OAuth 2.0 Provider and do not
prompt</li><li>Do not logout: Do not logout the user from the OAuth 2.0 Provider and do not prompt</
li></ul>",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"accountProviderClass" : {
    "title" : "Account Provider",
    "description" : "Name of the class implementing the account provider.<br><br>This class
is used by the module to find the account from the attributes mapped by the Account Mapper
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
interface.<br>String constructor parameters can be provided by appending <code>|</code> separated
values.",
    "propertyOrder" : 900,

```



```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ssoProxyUrl" : {
    "title" : "Proxy URL",
    "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be changed
from the default, if an external server is performing the GET to POST proxying. The default is
<code>/openam/oauth2c/OAuthProxy.jsp</code>",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "mapToAnonymousUser" : {
    "title" : "Map to anonymous user",
    "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated users<br><br>If
selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the anonymous user
configured in the next parameter.<br>If not selected the users authenticated will be mapped by the
parameters configured in the account mapper.<br><br><i>NB </i>If <i>Create account if it does not
exist</i> is enabled, that parameter takes precedence.",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "accountMapperClass" : {
    "title" : "Account Mapper",
    "description" : "Name of the class implementing the attribute mapping for the account
search.<br><br>This class is used by the module to map from the account information
received from the OAuth Identity Provider into OpenAM.<br><br>The class must implement
the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
interface.<br>Provided implementations
are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpFromAddress" : {
    "title" : "SMTP From address",
    "description" : "The email address on behalf of whom the messages will be sent",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
}

```

## 1.80.1.2. delete

Usage:

```
am> delete OAuth2Module --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.80.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Module --realm Realm --actionName getAllTypes
```

### 1.80.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Module --realm Realm --actionName getCreatableTypes
```

### 1.80.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Module --realm Realm --actionName nextdescendents
```

### 1.80.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query OAuth2Module --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.80.1.7. read

Usage:

```
am> read OAuth2Module --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.80.1.8. update

Usage:

```
am> update OAuth2Module --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "saveAttributesInSession" : {
      "title" : "Save attributes in the session",
      "description" : "If this option is enabled, the attributes configured in the attribute mapper
will be saved into the OpenAM session",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "accessTokenEndpointUrl" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "anonymousUserName" : {
      "title" : "Anonymous User",
      "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that will
represent the anonymous user. This user account must already exist in the realm.",
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scope" : {
      "title" : "Scope",
```

```

    "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
client application requires. The list depends on the permissions that the resource owner grants to
the client application.<br><br>Some authorization servers use non-standard separators for scopes.
For example, Facebook takes a comma-separated list.<br><br>Default: <code>email, read_stream</
code> (Facebook example)",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "mailGatewayClass" : {
    "title" : "Mail Server Gateway implementation class",
    "description" : "The class used by the module to send email.<br><br>This class is used by the
module to send email. A custom implementation can be provided.<br><br>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpHostPort" : {
    "title" : "SMTP port",
    "description" : "The TCP port that will be used by the SMTP gateway",
    "propertyOrder" : 2400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "oauth2LogoutServiceUrl" : {
    "title" : "OAuth 2.0 Provider logout service",
    "description" : "The URL of the OAuth Identity Providers Logout service<br><br>OAuth 2.0
Identity Providers can have a logout service. If this logout functionality is required then the URL
of the Logout endpoint should configured here.",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "attributeMapperConfiguration" : {
    "title" : "Attribute Mapper Configuration",
    "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
local user data store in the OpenAM.<br><br>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
    "propertyOrder" : 1300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "authenticationEndpointUrl" : {
    "title" : "Authentication Endpoint URL",
    "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider",
    "propertyOrder" : 300,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "smtpUsername" : {
    "title" : "SMTP User Name",
    "description" : "If the SMTP Service requires authentication, configure the user name here",
    "propertyOrder" : 2500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpPassword" : {
    "title" : "SMTP User Password",
    "description" : "The Password of the SMTP User Name",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "openidConnectContextType" : {
    "title" : "OpenID Connect validation configuration type",
    "description" : "Required when the 'openid' scope is included. Please select either 1. the issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientId" : {
    "title" : "Client Id",
    "description" : "OAuth client_id parameter<br><br>For more information on the OAuth client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=\"_blank\">RFC 6749</a>, section 2.3.1",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "mixUpMitigation" : {
    "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
    "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
    "propertyOrder" : 3300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "accessTokenParameterName" : {
    "title" : "OAuth2 Access Token Profile Service Parameter name",
    "description" : "The name of the parameter that will contain the access token value when accessing the profile service",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }

```

```

    },
    "openidConnectContextValue" : {
      "title" : "OpenID Connect validation configuration value",
      "description" : "Required when the 'openid' scope is included. The discovery url, or jwk url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url entered, entry must be in valid url format, <br><br>e.g. https://accounts.google.com/.well-known/openid-configuration<br><i>NB </i>If client_secret entered, entry is ignored and the value of the Client Secret is used.",
      "propertyOrder" : 3100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "userProfileServiceUrl" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL<br><br>This URL endpoint provides user profile information and is provided by the OAuth Identity Provider<br><br><i>NB </i>This URL should return JSON objects in response",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 2900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    },
    "oauth2EmailAttribute" : {
      "title" : "Email attribute in OAuth2 Response",
      "description" : "Attribute from the OAuth2 response used to send activation code emails.<br><br>The attribute in the response from the profile service in the OAuth 2.0 Provider that contains the email address of the authenticated user. This address will be used to send an email with an activation code when the accounts are allowed to be created dynamically.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "smtpSslEnabled" : {
      "title" : "SMTP SSL Enabled",
      "description" : "Tick this option if the SMTP Server provides SSL",
      "propertyOrder" : 2700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "smtpHostName" : {
      "title" : "SMTP host",
      "description" : "The mail host that will be used by the Email Gateway implementation",
      "propertyOrder" : 2300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }

```

```

    },
    "accountMapperConfiguration" : {
      "title" : "Account Mapper Configuration",
      "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute configuration
that will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local
data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
      "propertyOrder" : 1100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "promptForPassword" : {
      "title" : "Prompt for password setting and activation code",
      "description" : "Users must set a password and complete the activation flow during dynamic
profile creation.<br><br>If this is enabled, the user must set a password before the system creates
an account dynamically and an activation code will be sent to the user's email address. The account
will be created only if the password and activation code are properly set. <br />If this is disabled,
the account will be created transparently without prompting the user.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "attributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute mapping<br><br>This
class maps the OAuth properties into OpenAM properties. A custom attribute
mapper can be provided.<br><br>A custom attribute mapper must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
interface.<br><br>Provided implementations
are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
      "propertyOrder" : 1200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "createAccount" : {
      "title" : "Create account if it does not exist",

```

```

    "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an account
will be created dynamically.<br><br>If this is enabled, the account mapper could create the account
dynamically if there is no account mapped. Before creating the account, a dialog prompting for
a password and asking for an activation code can be shown if the parameter \"Prompt for password
setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3 alternative
options exist:<br><br><ol><li>The accounts need to have a user profile in the OpenAM User Data
Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in the
Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "openidConnectIssuer" : {
    "title" : "Token Issuer",
    "description" : "Required when the 'openid' scope is included. Value must match the iss field in
issued ID Token<br>e.g. accounts.google.com<br><br>The issuer value MUST be provided when OAuth 2.0
Mix-Up Mitigation is enabled.",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "logoutBehaviour" : {
    "title" : "Logout options",
    "description" : "Controls how Logout options will be presented to the user.<br><br>The OAuth
module has the following logout options for the user:<br><br><ul><li>Prompt: Prompt the user to
logout from the OAuth 2.0 Provider</li><li>Logout: Logout from the OAuth 2.0 Provider and do not
prompt</li><li>Do not logout: Do not logout the user from the OAuth 2.0 Provider and do not prompt</
li></ul>",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "accountProviderClass" : {
    "title" : "Account Provider",
    "description" : "Name of the class implementing the account provider.<br><br>This class
is used by the module to find the account from the attributes mapped by the Account Mapper
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
interface.<br>String constructor parameters can be provided by appending <code>|</code> separated
values.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ssoProxyUrl" : {
    "title" : "Proxy URL",
    "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be changed
from the default, if an external server is performing the GET to POST proxying. The default is
<code>/openam/oauth2c/OAuthProxy.jsp</code>",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "mapToAnonymousUser" : {

```



```

        "title" : "Map to anonymous user",
        "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated users<br><br>If
selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the anonymous user
configured in the next parameter.<br>If not selected the users authenticated will be mapped by the
parameters configured in the account mapper.<br><br><i>NB </i>If <i>Create account if it does not
exist</i> is enabled, that parameter takes precedence.",
        "propertyOrder" : 1800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "accountMapperClass" : {
        "title" : "Account Mapper",
        "description" : "Name of the class implementing the attribute mapping for the account
search.<br><br>This class is used by the module to map from the account information
received from the OAuth Identity Provider into OpenAM.<br><br>The class must implement
the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
interface.<br>Provided implementations
are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "smtpFromAddress" : {
        "title" : "SMTP From address",
        "description" : "The email address on behalf of whom the messages will be sent",
        "propertyOrder" : 2800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

## 1.80.2. Global Operations

Resource path: `/global-config/authentication/modules/oauth2`

Resource version: `1.0`

### 1.80.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Module --global --actionName getAllTypes
```

### 1.80.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Module --global --actionName getCreatableTypes
```

### 1.80.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Module --global --actionName nextdescendents
```

### 1.80.2.4. read

Usage:

```
am> read OAuth2Module --global
```

### 1.80.2.5. update

Usage:

```
am> update OAuth2Module --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationEndpointUrl" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpHostName" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 2300,
          "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "scope" : {
    "title" : "Scope",
    "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
client application requires. The list depends on the permissions that the resource owner grants to
the client application.<br><br> Some authorization servers use non-standard separators for scopes.
For example, Facebook takes a comma-separated list.<br><br> Default: <code>email, read_stream</
code> (Facebook example)",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpUsername" : {
    "title" : "SMTP User Name",
    "description" : "If the SMTP Service requires authentication, configure the user name here",
    "propertyOrder" : 2500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "anonymousUserName" : {
    "title" : "Anonymous User",
    "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
will represent the anonymous user. This user account must already exist in the realm.",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "clientSecret" : {
    "title" : "Client Secret",
    "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "smtpHostPort" : {
    "title" : "SMTP port",
    "description" : "The TCP port that will be used by the SMTP gateway",
    "propertyOrder" : 2400,
    "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "saveAttributesInSession" : {
        "title" : "Save attributes in the session",
        "description" : "If this option is enabled, the attributes configured in the attribute
mapper will be saved into the OpenAM session",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "createAccount" : {
        "title" : "Create account if it does not exist",
        "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
account will be created dynamically.<br><br>If this is enabled, the account mapper could create
the account dynamically if there is no account mapped. Before creating the account, a dialog
prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
alternative options exist:<br><br><ol><li>The accounts need to have a user profile in the OpenAM
User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "attributeMappingClasses" : {
        "title" : "Attribute Mapper",
        "description" : "Name of the class that implements the attribute
mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
attribute mapper can be provided.<br><br>A custom attribute mapper must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
interface.<br>Provided implementations
are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
        "propertyOrder" : 1200,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "mixUpMitigation" : {
        "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
        "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
        "propertyOrder" : 3300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    },

```

```

"openidConnectIssuer" : {
  "title" : "Token Issuer",
  "description" : "Required when the 'openid' scope is included. Value must match the iss
field in issued ID Token<br/>e.g. accounts.google.com<br/><br>The issuer value MUST be provided when
OAuth 2.0 Mix-Up Mitigation is enabled.",
  "propertyOrder" : 3200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"clientId" : {
  "title" : "Client Id",
  "description" : "OAuth client_id parameter<br/><br>For more information on the OAuth
client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"accessTokenEndpointUrl" : {
  "title" : "Access Token Endpoint URL",
  "description" : "OAuth access token endpoint URL<br/><br>This is the URL endpoint for
access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
  "propertyOrder" : 400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"oauth2EmailAttribute" : {
  "title" : "Email attribute in OAuth2 Response",
  "description" : "Attribute from the OAuth2 response used to send activation code
emails.<br/><br>The attribute in the response from the profile service in the OAuth 2.0 Provider that
contains the email address of the authenticated user. This address will be used to send an email with
an activation code when the accounts are allowed to be created dynamically.",
  "propertyOrder" : 1500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"ssoProxyUrl" : {
  "title" : "Proxy URL",
  "description" : "The URL to the OpenAM OAuth proxy JSP<br/><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"accessTokenParameterName" : {
  "title" : "OAuth2 Access Token Profile Service Parameter name",
  "description" : "The name of the parameter that will contain the access token value when
accessing the profile service",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}

```

```

    },
    "smtpPassword" : {
      "title" : "SMTP User Password",
      "description" : "The Password of the SMTP User Name",
      "propertyOrder" : 2600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "openidConnectContextType" : {
      "title" : "OpenID Connect validation configuration type",
      "description" : "Required when the 'openid' scope is included. Please select either 1. the issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
      "propertyOrder" : 3000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mailGatewayClass" : {
      "title" : "Mail Server Gateway implementation class",
      "description" : "The class used by the module to send email.<br><br>This class is used by the module to send email. A custom implementation can be provided.<br><br>The custom implementation must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
      "propertyOrder" : 2200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "accountProviderClass" : {
      "title" : "Account Provider",
      "description" : "Name of the class implementing the account provider.<br><br>This class is used by the module to find the account from the attributes mapped by the Account Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.<br><br>String constructor parameters can be provided by appending <code>|</code> separated values.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "promptForPassword" : {
      "title" : "Prompt for password setting and activation code",
      "description" : "Users must set a password and complete the activation flow during dynamic profile creation.<br><br>If this is enabled, the user must set a password before the system creates an account dynamically and an activation code will be sent to the user's email address. The account will be created only if the password and activation code are properly set. <br />If this is disabled, the account will be created transparently without prompting the user.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "accountMapperConfiguration" : {
      "title" : "Account Mapper Configuration",
      "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute configuration that will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",

```

```

    "propertyOrder" : 1100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userProfileServiceUrl" : {
    "title" : "User Profile Service URL",
    "description" : "User profile information URL<br><br>This URL endpoint provides user profile information and is provided by the OAuth Identity Provider<br><br><i>NB </i>This URL should return JSON objects in response",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "mapToAnonymousUser" : {
    "title" : "Map to anonymous user",
    "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the anonymous user configured in the next parameter.<br>If not selected the users authenticated will be mapped by the parameters configured in the account mapper.<br><br><i>NB </i>If <i>Create account if it does not exist</i> is enabled, that parameter takes precedence.",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logoutBehaviour" : {
    "title" : "Logout options",
    "description" : "Controls how Logout options will be presented to the user.<br><br>The OAuth module has the following logout options for the user:<br><br><ul><li>Prompt: Prompt the user to logout from the OAuth 2.0 Provider</li><li>Logout: Logout from the OAuth 2.0 Provider and do not prompt</li><li>Do not logout: Do not logout the user from the OAuth 2.0 Provider and do not prompt</li></ul>",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "oauth2LogoutServiceUrl" : {
    "title" : "OAuth 2.0 Provider logout service",
    "description" : "The URL of the OAuth Identity Providers Logout service<br><br>OAuth 2.0 Identity Providers can have a logout service. If this logout functionality is required then the URL of the Logout endpoint should be configured here.",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "smtpSslEnabled" : {
    "title" : "SMTP SSL Enabled",
    "description" : "Tick this option if the SMTP Server provides SSL",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }

```

```

    },
    "smtpFromAddress" : {
      "title" : "SMTP From address",
      "description" : "The email address on behalf of whom the messages will be sent",
      "propertyOrder" : 2800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "attributeMapperConfiguration" : {
      "title" : "Attribute Mapper Configuration",
      "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data store in the OpenAM.<br><br>Example: <code>OAuth2.0_attribute=local_attribute</code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "openidConnectContextValue" : {
      "title" : "OpenID Connect validation configuration value",
      "description" : "Required when the 'openid' scope is included. The discovery url, or jwk url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url entered, entry must be in valid url format, <br>>e.g. https://accounts.google.com/.well-known/openid-configuration<br><i>NB </i>If client_secret entered, entry is ignored and the value of the Client Secret is used.",
      "propertyOrder" : 3100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "accountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the account search.<br><br>This class is used by the module to map from the account information received from the OAuth Identity Provider into OpenAM.<br><br>The class must implement the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.<br><br>Provided implementations are:<ul><li><code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</code></li><li><code>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code> (can only be used when using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</code> separated values.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "type" : "object",
  "title" : "Realm Defaults"
}
}
}

```



## 1.81. OAuth2Provider

### 1.81.1. Realm Operations

Resource path: `/realm-config/services/oauth-oidc`

Resource version: `1.0`

#### 1.81.1.1. create

Usage:

```
am> create OAuth2Provider --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "deviceCodeConfig" : {
      "type" : "object",
      "title" : "Device Flow",
      "propertyOrder" : 4,
      "properties" : {
        "devicePollInterval" : {
          "title" : "Device Polling Interval",
          "description" : "The polling frequency for devices waiting for tokens when using the device
code flow.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "deviceCodeLifetime" : {
          "title" : "Device Code Lifetime (seconds)",
          "description" : "The lifetime of the device code, in seconds.",
          "propertyOrder" : 390,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "verificationUrl" : {
          "title" : "Verification URL",
          "description" : "The URL that the user will be instructed to visit to complete their OAuth
2.0 login and consent when using the device code flow.",
          "propertyOrder" : 370,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    "completionUrl" : {
      "title" : "Device Completion URL",
      "description" : "The URL that the user will be sent to on completion of their OAuth 2.0
login and consent when using the device code flow.",
      "propertyOrder" : 380,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "coreOAuth2Config" : {
    "type" : "object",
    "title" : "Core",
    "propertyOrder" : 0,
    "properties" : {
      "codeLifetime" : {
        "title" : "Authorization Code Lifetime (seconds)",
        "description" : "The time an authorization code is valid for, in seconds.",
        "propertyOrder" : 10,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "issueRefreshTokenOnRefreshedToken" : {
        "title" : "Issue Refresh Tokens on Refreshing Access Tokens",
        "description" : "Whether to issue a refresh token when refreshing an access token.",
        "propertyOrder" : 50,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "refreshTokenLifetime" : {
        "title" : "Refresh Token Lifetime (seconds)",
        "description" : "The time in seconds a refresh token is valid for. If this field is set to
<code>-1</code>, the token will never expire.",
        "propertyOrder" : 20,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "savedConsentAttribute" : {
        "title" : "Saved Consent Attribute Name",
        "description" : "Name of a multi-valued attribute on resource owner profiles where OpenAM
can save authorization consent decisions.<p><p>When the resource owner chooses to save the decision
to authorize access for a client application, then OpenAM updates the resource owner's profile to
avoid having to prompt the resource owner to grant authorization when the client issues subsequent
authorization requests.",
        "propertyOrder" : 110,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "issueRefreshToken" : {
        "title" : "Issue Refresh Tokens",
        "description" : "Whether to issue a refresh token when returning an access token.",
        "propertyOrder" : 40,
        "required" : true,
        "type" : "boolean",

```

```

        "exampleValue" : ""
    },
    "statelessTokensEnabled" : {
        "title" : "Use Stateless Access & Refresh Tokens",
        "description" : "When enabled, OpenAM issues access and refresh tokens that can be inspected
by resource servers.",
        "propertyOrder" : 3,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "accessTokenLifetime" : {
        "title" : "Access Token Lifetime (seconds)",
        "description" : "The time an access token is valid for, in seconds.",
        "propertyOrder" : 30,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
}
},
"coreOIDCConfig" : {
    "type" : "object",
    "title" : "OpenID Connect",
    "propertyOrder" : 2,
    "properties" : {
        "supportedClaims" : {
            "title" : "Supported Claims",
            "description" : "Set of claims supported by the OpenID Connect <code>/oauth2/userinfo</code>
endpoint, with translations.<br><br>Claims may be entered as simple strings or pipe separated
strings representing the internal claim name, locale, and localized description.<p><p>For example:
<code>name|en|Your full name.</code>.<p>Locale strings are in the format: <code>language +
\"_\" + country + \"_\" + variant</code>, for example <code>en</code>, <code>en_GB</code>, or
<code>en_US_WIN</code>. If the locale and pipe is omitted, the description is displayed to all users
that have undefined locales.<p><p>If the description is also omitted, nothing is displayed on the
consent page for the claim. For example specifying <code>family_name</code> would allow the claim
<code>family_name</code> to be used by the client, but would not display it to the user on the
consent page when requested.",
            "propertyOrder" : 190,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "oidcClaimsScript" : {
            "title" : "OIDC Claims Script",
            "description" : "The script that is run when issuing an ID token or making a request to the
<i>/userinfo</i> endpoint during OpenID requests.<p><p>The script gathers the scopes and populates
claims, and has access to the access token, the user's identity and, if available, the user's
session.",
            "propertyOrder" : 80,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "supportedIDTokenEncryptionMethods" : {
            "title" : "ID Token Encryption Methods supported",

```

```

    "description" : "Encryption methods supported to encrypt OpenID Connect ID tokens
in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES
in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
<code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
    "propertyOrder" : 180,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"supportedIDTokenSigningAlgorithms" : {
    "title" : "ID Token Signing Algorithms supported",
    "description" : "Algorithms supported to sign OpenID Connect <code>id_tokens</
code>.<p><p>OpenAM supports algorithms listed in JSON Web Algorithms (JWA): <a href=\"http://
tools.ietf.org/html/draft-ietf-jose-json-web-algorithms#section-3.1\">\"alg\" (Algorithm) Header
Parameter Values for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</
code> - HMAC with SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code>
- ECDSA with SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with
SHA-384 and NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and
NIST standard P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</
li></ul>",
    "propertyOrder" : 160,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"jwtTokenLifetime" : {
    "title" : "OpenID Connect JWT Token Lifetime (seconds)",
    "description" : "The amount of time the JWT will be valid for, in seconds.",
    "propertyOrder" : 210,
    "required" : false,
    "type" : "integer",
    "exampleValue" : ""
},
"supportedIDTokenEncryptionAlgorithms" : {
    "title" : "ID Token Encryption Algorithms supported",
    "description" : "Encryption algorithms supported to encrypt OpenID Connect ID tokens
in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</
li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</
li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
with 192-bit key derived from the client secret.</li></ul>",
    "propertyOrder" : 170,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
}

```

```

    }
  },
  "advanced0Auth2Config" : {
    "type" : "object",
    "title" : "Advanced",
    "propertyOrder" : 1,
    "properties" : {
      "supportedScopes" : {
        "title" : "Supported Scopes",
        "description" : "The set of supported scopes, with translations.<br><br><p>Scopes may be entered as simple strings or pipe-separated strings representing the internal scope name, locale, and localized description.</p><p>For example: <code>read|en|Permission to view email messages in your account</code></p><p>Locale strings are in the format: <code>language_country_variant</code>, for example <code>en</code>, <code>en_GB</code>, or <code>en_US_WIN</code>.</p><p>If the locale and pipe is omitted, the description is displayed to all users that have undefined locales.</p><p>If the description is also omitted, nothing is displayed on the consent page for the scope. For example specifying <code>read|</code> would allow the scope read to be used by the client, but would not display it to the user on the consent page when requested.</p>",
        "propertyOrder" : 130,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "scopeImplementationClass" : {
        "title" : "Scope Implementation Class",
        "description" : "The class that contains the required scope implementation, must implement the <code>org.forgerock.oauth2.core.ScopeValidator</code> interface.",
        "propertyOrder" : 70,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "defaultScopes" : {
        "title" : "Default Client Scopes",
        "description" : "List of scopes a client will be granted if they request registration without specifying which scopes they want. Default scopes are NOT auto-granted to clients created through the OpenAM console.",
        "propertyOrder" : 200,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "keypairName" : {
        "title" : "Token Signing RSA public/private key pair",
        "description" : "The public/private key pair used by RS256.<br><br>The public/private key pair will be retrieved from the keystore referenced by the property <code>com.sun.identity.saml.xmlsig.keystore</code>.",
        "propertyOrder" : 240,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },

```

```

"moduleMessageEnabledInPasswordGrant" : {
  "title" : "Enable auth module messages for Password Credentials Grant",
  "description" : "If enabled, authentication module failure messages are used to create
Resource Owner Password Credentials Grant failure messages. If disabled, a standard authentication
failed message is used.<br><br>The Password Grant Type requires the <code>grant_type=password</code>
parameter.",
  "propertyOrder" : 440,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"createdTimestampAttribute" : {
  "title" : "Created Timestamp attribute name",
  "description" : "The identity Data Store attribute used to return created timestamp
values.",
  "propertyOrder" : 350,
  "required" : false,
  "type" : "string",
  "exampleValue" : ""
},
"customLoginUrlTemplate" : {
  "title" : "Custom Login URL Template",
  "description" : "Custom URL for handling login, to override the default OpenAM login
page.<br><br>Supports Freemarker syntax, with the following variables:<table><tr><th>Variable</
th><th>Description</th></tr><tr><td><code>gotoUrl</code></td><td><p>The URL to redirect to after
login.</p></td></tr><tr><td><code>acrValues</code></td><td><p>The Authentication Context Class
Reference (acr) values for the authorization request.</p></td></tr><tr><td><code>realm</code></
td><td><p>The OpenAM realm the authorization request was made on.</p></td></tr><tr><td><code>module</
code></td><td><p>The name of the OpenAM authentication module requested to perform resource
owner authentication.</p></td></tr><tr><td><code>service</code></td><td><p>The name of the
OpenAM authentication chain requested to perform resource owner authentication.</p></td></
tr><tr><td><code>locale</code></td><td><p>A space-separated list of locales, ordered by preference.</
p></td></tr></table>The following example template redirects users to a non-OpenAM front end to handle
login, which will then redirect back to the <code>/oauth2/authorize</code> endpoint with any required
parameters:<p> <code>http://mylogin.com/login?goto=${goto}&#x2F;if acrValues??&#x2F;if
${acrValues}&#x2F;if realm??&#x2F;if module??&#x2F;if service??&#x2F;if locale??&#x2F;if
module??&#x2F;if service??&#x2F;if locale??&#x2F;if locale=${locale}&#x2F;if</code>",
  "propertyOrder" : 60,
  "required" : false,
  "type" : "string",
  "exampleValue" : ""
},
"hashSalt" : {
  "title" : "Subject identifier hash salt",
  "description" : "If <i>pairwise</i> subject types are supported, it is <em>STRONGLY
RECOMMENDED</em> to change this value. It is used in the salting of hashes for returning
specific <code>sub</code> claims to individuals using the same <code>request_uri</code> or
<code>sector_identifier_uri</code>.",
  "propertyOrder" : 260,
  "required" : false,
  "type" : "string",
  "exampleValue" : "changeme"
},
"modifiedTimestampAttribute" : {
  "title" : "Modified Timestamp attribute name",
  "description" : "The identity Data Store attribute used to return modified timestamp
values.",
  "propertyOrder" : 340,

```

```

    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "tokenSigningECDSAKeyAlias" : {
    "title" : "Token Signing ECDSA public/private key pair alias",
    "description" : "The list of public/private key pairs used for the elliptic curve algorithms (ES256/ES384/ES512). Add an entry to specify an alias for a specific elliptic curve algorithm, for example <code>ES256|es256Alias</code>.<br><br>Each of the public/private key pairs will be retrieved from the keystore referenced by the property <code>com.sun.identity.saml.xmlsig.keystore</code>.",
    "propertyOrder" : 241,
    "required" : false,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "supportedSubjectTypes" : {
    "title" : "Subject Types supported",
    "description" : "List of subject types supported. Valid values are:<ul><li><code>public</code> - Each client receives the same subject (<code>sub</code>) value.</li><li><code>pairwise</code> - Each client receives a different subject (<code>sub</code>) value, to prevent correlation between clients.</li></ul>",
    "propertyOrder" : 150,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "clientsCanSkipConsent" : {
    "title" : "Allow clients to skip consent",
    "description" : "If enabled, clients may be configured so that the resource owner will not be asked for consent during authorization flows.",
    "propertyOrder" : 420,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "tokenCompressionEnabled" : {
    "title" : "Stateless Token Compression",
    "description" : "Whether stateless access and refresh tokens should be compressed.",
    "propertyOrder" : 223,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "authenticationAttributes" : {
    "title" : "User Profile Attribute(s) the Resource Owner is Authenticated On",
    "description" : "Names of profile attributes that resource owners use to log in. You can add others to the default, for example <code>mail</code>.",
    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",

```

```

    "exampleValue" : ""
  },
  "responseTypeClasses" : {
    "title" : "Response Type Plugins",
    "description" : "List of plugins that handle the valid <code>response_type</code>
values.<br><br>OAuth 2.0 clients pass response types as parameters to the OAuth 2.0 Authorization
endpoint (<code>/oauth2/authorize</code>) to indicate which grant type is requested from the
provider. For example, the client passes <code>code</code> when requesting an authorization code,
and <code>token</code> when requesting an access token.<p><p>Values in this list take the form
<code>response-type|plugin-class-name</code>.",
    "propertyOrder" : 90,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "tokenSigningAlgorithm" : {
    "title" : "OAuth2 Token Signing Algorithm",
    "description" : "Algorithm used to sign stateless OAuth 2.0 tokens in order to detect
tampering.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA):
<a href=\"http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms#section-3.1\">"alg
\" (Algorithm) Header Parameter Values for JWS</a>:<ul><li><code>HS256</code> - HMAC with
SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</li><li><code>HS512</code> - HMAC
with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and NIST standard P-256 elliptic
curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard P-384 elliptic
curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.</
li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
    "propertyOrder" : 220,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "displayNameAttribute" : {
    "title" : "User Display Name attribute",
    "description" : "The profile attribute that contains the name to be displayed for the user
on the consent page.",
    "propertyOrder" : 120,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "tokenSigningHmacSharedSecret" : {
    "title" : "Token Signing HMAC Shared Secret",
    "description" : "Base64-encoded key used by HS256, HS384 and HS512.",
    "propertyOrder" : 230,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "codeVerifierEnforced" : {
    "title" : "Code verifier parameter required",
    "description" : "If enabled, requests using the authorization code grant require a
<code>code_challenge</code> attribute.<br><br>For more information, read the <a href=\"https://
tools.ietf.org/html/draft-ietf-oauth-spop-12\">draft specification for this feature</a>.",
    "propertyOrder" : 270,
    "required" : true,
    "type" : "boolean",

```



```

        "exampleValue" : ""
    }
}
},
"advancedOIDCConfig" : {
    "type" : "object",
    "title" : "Advanced OpenID Connect",
    "propertyOrder" : 3,
    "properties" : {
        "loaMapping" : {
            "title" : "OpenID Connect acr_values to Auth Chain Mapping",
            "description" : "Maps OpenID Connect ACR values to authentication chains. See the <a href=
\\http://openid.net/specs/openid-connect-core-1_0.html#AuthRequest\\\" target=\\\"_blank\\\">acr_values
parameter</a> in the OpenID Connect authentication request specification for more details.",
            "propertyOrder" : 310,
            "required" : false,
            "patternProperties" : {
                ".*" : { }
            },
            "type" : "object",
            "exampleValue" : ""
        },
        "allowDynamicRegistration" : {
            "title" : "Allow Open Dynamic Client Registration",
            "description" : "Allow clients to register without an access token. If enabled, you should
consider adding some form of rate limiting. See <a href=\\\"http://openid.net/specs/openid-connect-
registration-1_0.html#ClientRegistration\\\" target=\\\"_blank\\\">Client Registration</a> in the OpenID
Connect specification for details.",
            "propertyOrder" : 280,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "storeOpsTokens" : {
            "title" : "Store Ops Tokens",
            "description" : "Whether OpenAM will store the <i>ops</i> tokens corresponding to OpenID
Connect sessions in the CTS store. Note that session management related endpoints will not work when
this setting is disabled.",
            "propertyOrder" : 410,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "jwksURI" : {
            "title" : "Remote JSON Web Key URL",
            "description" : "The Remote URL where the providers JSON Web Key can be retrieved.<p><p>If
this setting is not configured, then OpenAM provides a local URL to access the public key of the
private key used to sign ID tokens.",
            "propertyOrder" : 140,
            "required" : false,
            "type" : "string",
            "exampleValue" : ""
        },
        "amrMappings" : {
            "title" : "OpenID Connect id_token amr values to Auth Module mappings",
            "description" : "Specify <code>amr</code> values to be returned in the OpenID Connect
<code>id_token</code>. Once authentication has completed, the authentication modules that were used
from the authentication service will be mapped to the <code>amr</code> values. If you do not require
<code>amr</code> values, or are not providing OpenID Connect tokens, leave this field blank.",

```

```

    "propertyOrder" : 330,
    "required" : false,
    "patternProperties" : {
      ".*" : { }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "claimsParameterSupported" : {
    "title" : "Enable \"claims_parameter_supported\"",
    "description" : "If enabled, clients will be able to request individual claims using the
<code>claims</code> request parameter, as per <a href='\"http://openid.net/specs/openid-connect-
core-1_0.html#ClaimsParameter\"' target='\"_blank\"'>section 5.5 of the OpenID Connect specification</
a>.",
    "propertyOrder" : 250,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "alwaysAddClaimsToToken" : {
    "title" : "Always return claims in ID Tokens",
    "description" : "If enabled, include scope-derived claims in the <code>id_token</code>,
even if an access token is also returned that could provide access to get the claims from the
<code>userinfo</code> endpoint.<br><br>If not enabled, if an access token is requested the client
must use it to access the <code>userinfo</code> endpoint for scope-derived claims, as they will not
be included in the ID token.",
    "propertyOrder" : 360,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "defaultACR" : {
    "title" : "OpenID Connect default acr claim",
    "description" : "Default value to use as the <code>acr</code> claim in an OpenID Connect ID
Token when using the default authentication chain.",
    "propertyOrder" : 320,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "idTokenInfoClientAuthenticationEnabled" : {
    "title" : "Idtokeninfo endpoint requires client authentication",
    "description" : "When enabled, the <code>/oauth2/idtokeninfo</code> endpoint requires
client authentication if the signing algorithm is set to <code>HS256</code>, <code>HS384</code>, or
<code>HS512</code>.",
    "propertyOrder" : 225,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "generateRegistrationAccessTokens" : {
    "title" : "Generate Registration Access Tokens",
    "description" : "Whether to generate Registration Access Tokens for clients that register
via open dynamic client registration. Such tokens allow the client to access the <a href='\"http://
openid.net/specs/openid-connect-registration-1_0.html#ClientConfigurationEndpoint\"' target='\"_blank
\">Client Configuration Endpoint</a> as per the OpenID Connect specification. This setting has no
effect if open dynamic client registration is disabled.",
    "propertyOrder" : 290,
    "required" : true,

```

```
        "type" : "boolean",  
        "exampleValue" : ""  
      }  
    }  
  }  
}
```

### 1.81.1.2. delete

Usage:

```
am> delete OAuth2Provider --realm Realm
```

### 1.81.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Provider --realm Realm --actionName getAllTypes
```

### 1.81.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Provider --realm Realm --actionName getCreatableTypes
```

### 1.81.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Provider --realm Realm --actionName nextdescendents
```

### 1.81.1.6. read

Usage:

```
am> read OAuth2Provider --realm Realm
```

### 1.81.1.7. update

Usage:

```
am> update OAuth2Provider --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "deviceCodeConfig" : {
      "type" : "object",
      "title" : "Device Flow",
      "propertyOrder" : 4,
      "properties" : {
        "devicePollInterval" : {
          "title" : "Device Polling Interval",
          "description" : "The polling frequency for devices waiting for tokens when using the device
code flow.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "deviceCodeLifetime" : {
          "title" : "Device Code Lifetime (seconds)",
          "description" : "The lifetime of the device code, in seconds.",
          "propertyOrder" : 390,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "verificationUrl" : {
          "title" : "Verification URL",
          "description" : "The URL that the user will be instructed to visit to complete their OAuth
2.0 login and consent when using the device code flow.",
          "propertyOrder" : 370,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "completionUrl" : {
          "title" : "Device Completion URL",
          "description" : "The URL that the user will be sent to on completion of their OAuth 2.0
login and consent when using the device code flow.",
          "propertyOrder" : 380,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "coreOAuth2Config" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "codeLifetime" : {
```

```

    "title" : "Authorization Code Lifetime (seconds)",
    "description" : "The time an authorization code is valid for, in seconds.",
    "propertyOrder" : 10,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "issueRefreshTokenOnRefreshedToken" : {
    "title" : "Issue Refresh Tokens on Refreshing Access Tokens",
    "description" : "Whether to issue a refresh token when refreshing an access token.",
    "propertyOrder" : 50,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "refreshTokenLifetime" : {
    "title" : "Refresh Token Lifetime (seconds)",
    "description" : "The time in seconds a refresh token is valid for. If this field is set to
<code>-1</code>, the token will never expire.",
    "propertyOrder" : 20,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "savedConsentAttribute" : {
    "title" : "Saved Consent Attribute Name",
    "description" : "Name of a multi-valued attribute on resource owner profiles where OpenAM
can save authorization consent decisions.<p><p>When the resource owner chooses to save the decision
to authorize access for a client application, then OpenAM updates the resource owner's profile to
avoid having to prompt the resource owner to grant authorization when the client issues subsequent
authorization requests.",
    "propertyOrder" : 110,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "issueRefreshToken" : {
    "title" : "Issue Refresh Tokens",
    "description" : "Whether to issue a refresh token when returning an access token.",
    "propertyOrder" : 40,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "statelessTokensEnabled" : {
    "title" : "Use Stateless Access & Refresh Tokens",
    "description" : "When enabled, OpenAM issues access and refresh tokens that can be inspected
by resource servers.",
    "propertyOrder" : 3,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "accessTokenLifetime" : {
    "title" : "Access Token Lifetime (seconds)",
    "description" : "The time an access token is valid for, in seconds.",
    "propertyOrder" : 30,
    "required" : true,
    "type" : "integer",

```

```

        "exampleValue" : ""
    }
},
"coreOIDCConfig" : {
    "type" : "object",
    "title" : "OpenID Connect",
    "propertyOrder" : 2,
    "properties" : {
        "supportedClaims" : {
            "title" : "Supported Claims",
            "description" : "Set of claims supported by the OpenID Connect <code>/oauth2/userinfo</code> endpoint, with translations.<br><br>Claims may be entered as simple strings or pipe separated strings representing the internal claim name, locale, and localized description.<p><p>For example: <code>name|en|Your full name.</code>.<p>Locale strings are in the format: <code>language + \"_\" + country + \"_\" + variant</code>, for example <code>en</code>, <code>en_GB</code>, or <code>en_US_WIN</code>. If the locale and pipe is omitted, the description is displayed to all users that have undefined locales.<p><p>If the description is also omitted, nothing is displayed on the consent page for the claim. For example specifying <code>family_name|</code> would allow the claim <code>family_name</code> to be used by the client, but would not display it to the user on the consent page when requested.",
            "propertyOrder" : 190,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "oidcClaimsScript" : {
            "title" : "OIDC Claims Script",
            "description" : "The script that is run when issuing an ID token or making a request to the <i>userinfo</i> endpoint during OpenID requests.<p><p>The script gathers the scopes and populates claims, and has access to the access token, the user's identity and, if available, the user's session.",
            "propertyOrder" : 80,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "supportedIDTokenEncryptionMethods" : {
            "title" : "ID Token Encryption Methods supported",
            "description" : "Encryption methods supported to encrypt OpenID Connect ID tokens in order to hide its contents.<br><br>OpenAM supports the following ID token encryption algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
            "propertyOrder" : 180,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "supportedIDTokenSigningAlgorithms" : {
            "title" : "ID Token Signing Algorithms supported",

```

```

    "description" : "Algorithms supported to sign OpenID Connect <code>id_tokens</code>.",
    "propertyOrder" : 160,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "jwtTokenLifetime" : {
    "title" : "OpenID Connect JWT Token Lifetime (seconds)",
    "description" : "The amount of time the JWT will be valid for, in seconds.",
    "propertyOrder" : 210,
    "required" : false,
    "type" : "integer",
    "exampleValue" : ""
  },
  "supportedIDTokenEncryptionAlgorithms" : {
    "title" : "ID Token Encryption Algorithms supported",
    "description" : "Encryption algorithms supported to encrypt OpenID Connect ID tokens
in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
with 192-bit key derived from the client secret.</li></ul>",
    "propertyOrder" : 170,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }
},
"advancedOAuth2Config" : {
  "type" : "object",
  "title" : "Advanced",
  "propertyOrder" : 1,
  "properties" : {
    "supportedScopes" : {
      "title" : "Supported Scopes",
      "description" : "The set of supported scopes, with translations.<br><br><p>Scopes may be
entered as simple strings or pipe-separated strings representing the internal scope name, locale,
and localized description.</p><p>For example: <code>read|en|Permission to view email messages in
your account</code></p><p>Locale strings are in the format: <code>language_country_variant</code>,
for example <code>en</code>, <code>en_GB</code>, or <code>en_US_WIN</code>.</p><p>If the locale and
pipe is omitted, the description is displayed to all users that have undefined locales.</p><p>If

```

the description is also omitted, nothing is displayed on the consent page for the scope. For example specifying `read|` would allow the scope read to be used by the client, but would not display it to the user on the consent page when requested.

```

    "propertyOrder" : 130,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "scopeImplementationClass" : {
    "title" : "Scope Implementation Class",
    "description" : "The class that contains the required scope implementation, must implement
the <code>org.forgerock.oauth2.core.ScopeValidator</code> interface.",
    "propertyOrder" : 70,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "defaultScopes" : {
    "title" : "Default Client Scopes",
    "description" : "List of scopes a client will be granted if they request registration
without specifying which scopes they want. Default scopes are NOT auto-granted to clients created
through the OpenAM console.",
    "propertyOrder" : 200,
    "required" : false,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "keypairName" : {
    "title" : "Token Signing RSA public/private key pair",
    "description" : "The public/private key pair used by RS256.<br><br>The
public/private key pair will be retrieved from the keystore referenced by the property
<code>com.sun.identity.saml.xmlsig.keystore</code>.",
    "propertyOrder" : 240,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "moduleMessageEnabledInPasswordGrant" : {
    "title" : "Enable auth module messages for Password Credentials Grant",
    "description" : "If enabled, authentication module failure messages are used to create
Resource Owner Password Credentials Grant failure messages. If disabled, a standard authentication
failed message is used.<br><br>The Password Grant Type requires the <code>grant_type=password</code>
parameter.",
    "propertyOrder" : 440,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "createdTimestampAttribute" : {
    "title" : "Created Timestamp attribute name",
    "description" : "The identity Data Store attribute used to return created timestamp
values.",
    "propertyOrder" : 350,

```



```

    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "customLoginUrlTemplate" : {
    "title" : "Custom Login URL Template",
    "description" : "Custom URL for handling login, to override the default OpenAM login page.<br><br>Supports Freemarker syntax, with the following variables:<table><tr><th>Variable</th><th>Description</th></tr><tr><td><code>gotoUrl</code></td><td><p>The URL to redirect to after login.</p></td></tr><tr><td><code>acrValues</code></td><td><p>The Authentication Context Class Reference (acr) values for the authorization request.</p></td></tr><tr><td><code>realm</code></td><td><p>The OpenAM realm the authorization request was made on.</p></td></tr><tr><td><code>module</code></td><td><p>The name of the OpenAM authentication module requested to perform resource owner authentication.</p></td></tr><tr><td><code>service</code></td><td><p>The name of the OpenAM authentication chain requested to perform resource owner authentication.</p></td></tr><tr><td><code>locale</code></td><td><p>A space-separated list of locales, ordered by preference.</p></td></tr></table>The following example template redirects users to a non-OpenAM front end to handle login, which will then redirect back to the <code>/oauth2/authorize</code> endpoint with any required parameters:<p> <code>http://mylogin.com/login?goto=${goto}&#x26;acrValues??&#x26;acr_values=${acrValues}&#x26;realm??&#x26;realm=${realm}&#x26;module??&#x26;module=${module}&#x26;service??&#x26;service=${service}&#x26;locale??&#x26;locale=${locale}&#x26;".
    "propertyOrder" : 60,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "hashSalt" : {
    "title" : "Subject identifier hash salt",
    "description" : "If <i>pairwise</i> subject types are supported, it is <em>STRONGLY RECOMMENDED</em> to change this value. It is used in the salting of hashes for returning specific <code>sub</code> claims to individuals using the same <code>request_uri</code> or <code>sector_identifier_uri</code>.",
    "propertyOrder" : 260,
    "required" : false,
    "type" : "string",
    "exampleValue" : "changeme"
  },
  "modifiedTimestampAttribute" : {
    "title" : "Modified Timestamp attribute name",
    "description" : "The identity Data Store attribute used to return modified timestamp values.",
    "propertyOrder" : 340,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "tokenSigningECDSAKeyAlias" : {
    "title" : "Token Signing ECDSA public/private key pair alias",
    "description" : "The list of public/private key pairs used for the elliptic curve algorithms (ES256/ES384/ES512). Add an entry to specify an alias for a specific elliptic curve algorithm, for example <code>ES256|es256Alias</code>.<br><br>Each of the public/private key pairs will be retrieved from the keystore referenced by the property <code>com.sun.identity.saml.xmlsig.keystore</code>.",
    "propertyOrder" : 241,
    "required" : false,
    "items" : {
      "type" : "string"
    },
    "type" : "array",

```

```

    "exampleValue" : ""
  },
  "supportedSubjectTypes" : {
    "title" : "Subject Types supported",
    "description" : "List of subject types supported. Valid values are:<ul><li><code>public</code></li><li><code>pairwise</code></li><li><code>pairwise</code></li><li><code>pairwise</code></li></ul> - Each client receives the same subject (<code>sub</code>) value.</li><li><code>pairwise</code></li><li><code>pairwise</code></li><li><code>pairwise</code></li></ul> - Each client receives a different subject (<code>sub</code>) value, to prevent correlation between clients.</li><li><code>pairwise</code></li><li><code>pairwise</code></li><li><code>pairwise</code></li></ul>",
    "propertyOrder" : 150,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "clientsCanSkipConsent" : {
    "title" : "Allow clients to skip consent",
    "description" : "If enabled, clients may be configured so that the resource owner will not be asked for consent during authorization flows.",
    "propertyOrder" : 420,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "tokenCompressionEnabled" : {
    "title" : "Stateless Token Compression",
    "description" : "Whether stateless access and refresh tokens should be compressed.",
    "propertyOrder" : 223,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "authenticationAttributes" : {
    "title" : "User Profile Attribute(s) the Resource Owner is Authenticated On",
    "description" : "Names of profile attributes that resource owners use to log in. You can add others to the default, for example <code>mail</code>.",
    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "responseTypeClasses" : {
    "title" : "Response Type Plugins",
    "description" : "List of plugins that handle the valid <code>response_type</code> values.<br><br>OAuth 2.0 clients pass response types as parameters to the OAuth 2.0 Authorization endpoint (<code>/oauth2/authorize</code>) to indicate which grant type is requested from the provider. For example, the client passes <code>code</code> when requesting an authorization code, and <code>token</code> when requesting an access token.<p><p>Values in this list take the form <code>response-type|plugin-class-name</code>.",
    "propertyOrder" : 90,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",

```

```

    "exampleValue" : ""
  },
  "tokenSigningAlgorithm" : {
    "title" : "OAuth2 Token Signing Algorithm",
    "description" : "Algorithm used to sign stateless OAuth 2.0 tokens in order to detect
tampering.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA):
<a href='\"http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms#section-3.1\"'>\"alg
\" (Algorithm) Header Parameter Values for JWS</a>:<ul><li><code>HS256</code> - HMAC with
SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</li><li><code>HS512</code> - HMAC
with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and NIST standard P-256 elliptic
curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard P-384 elliptic
curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.</
li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
    "propertyOrder" : 220,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "displayNameAttribute" : {
    "title" : "User Display Name attribute",
    "description" : "The profile attribute that contains the name to be displayed for the user
on the consent page.",
    "propertyOrder" : 120,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "tokenSigningHmacSharedSecret" : {
    "title" : "Token Signing HMAC Shared Secret",
    "description" : "Base64-encoded key used by HS256, HS384 and HS512.",
    "propertyOrder" : 230,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "codeVerifierEnforced" : {
    "title" : "Code verifier parameter required",
    "description" : "If enabled, requests using the authorization code grant require a
<code>code_challenge</code> attribute.<br><br>For more information, read the <a href='\"https://
tools.ietf.org/html/draft-ietf-oauth-spop-12\"'>draft specification for this feature</a>.",
    "propertyOrder" : 270,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }
}
},
"advancedOIDCConfig" : {
  "type" : "object",
  "title" : "Advanced OpenID Connect",
  "propertyOrder" : 3,
  "properties" : {
    "loaMapping" : {
      "title" : "OpenID Connect acr_values to Auth Chain Mapping",
      "description" : "Maps OpenID Connect ACR values to authentication chains. See the <a href='\"
http://openid.net/specs/openid-connect-core-1_0.html#AuthRequest\"' target='\"_blank\"'>acr_values
parameter</a> in the OpenID Connect authentication request specification for more details.",
      "propertyOrder" : 310,
      "required" : false,

```

```

    "patternProperties" : {
      ".*" : { }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "allowDynamicRegistration" : {
    "title" : "Allow Open Dynamic Client Registration",
    "description" : "Allow clients to register without an access token. If enabled, you should consider adding some form of rate limiting. See <a href=\"http://openid.net/specs/openid-connect-registration-1_0.html#ClientRegistration\" target=\"_blank\">Client Registration</a> in the OpenID Connect specification for details.",
    "propertyOrder" : 280,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "storeOpsTokens" : {
    "title" : "Store Ops Tokens",
    "description" : "Whether OpenAM will store the <i>ops</i> tokens corresponding to OpenID Connect sessions in the CTS store. Note that session management related endpoints will not work when this setting is disabled.",
    "propertyOrder" : 410,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "jksURI" : {
    "title" : "Remote JSON Web Key URL",
    "description" : "The Remote URL where the providers JSON Web Key can be retrieved.<p><p>If this setting is not configured, then OpenAM provides a local URL to access the public key of the private key used to sign ID tokens.",
    "propertyOrder" : 140,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "amrMappings" : {
    "title" : "OpenID Connect id_token amr values to Auth Module mappings",
    "description" : "Specify <code>amr</code> values to be returned in the OpenID Connect <code>id_token</code>. Once authentication has completed, the authentication modules that were used from the authentication service will be mapped to the <code>amr</code> values. If you do not require <code>amr</code> values, or are not providing OpenID Connect tokens, leave this field blank.",
    "propertyOrder" : 330,
    "required" : false,
    "patternProperties" : {
      ".*" : { }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "claimsParameterSupported" : {
    "title" : "Enable \"claims_parameter_supported\"",
    "description" : "If enabled, clients will be able to request individual claims using the <code>claims</code> request parameter, as per <a href=\"http://openid.net/specs/openid-connect-core-1_0.html#ClaimsParameter\" target=\"_blank\">section 5.5 of the OpenID Connect specification</a>.",
    "propertyOrder" : 250,
    "required" : true,

```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "alwaysAddClaimsToToken" : {
        "title" : "Always return claims in ID Tokens",
        "description" : "If enabled, include scope-derived claims in the <code>id_token</code>,
even if an access token is also returned that could provide access to get the claims from the
<code>userinfo</code> endpoint.<br><br>If not enabled, if an access token is requested the client
must use it to access the <code>userinfo</code> endpoint for scope-derived claims, as they will not
be included in the ID token.",
        "propertyOrder" : 360,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "defaultACR" : {
        "title" : "OpenID Connect default acr claim",
        "description" : "Default value to use as the <code>acr</code> claim in an OpenID Connect ID
Token when using the default authentication chain.",
        "propertyOrder" : 320,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "idTokenInfoClientAuthenticationEnabled" : {
        "title" : "Idtokeninfo endpoint requires client authentication",
        "description" : "When enabled, the <code>/oauth2/idtokeninfo</code> endpoint requires
client authentication if the signing algorithm is set to <code>HS256</code>, <code>HS384</code>, or
<code>HS512</code>.",
        "propertyOrder" : 225,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "generateRegistrationAccessTokens" : {
        "title" : "Generate Registration Access Tokens",
        "description" : "Whether to generate Registration Access Tokens for clients that register
via open dynamic client registration. Such tokens allow the client to access the <a href=\"http://
openid.net/specs/openid-connect-registration-1_0.html#ClientConfigurationEndpoint\" target=\"_blank
\">Client Configuration Endpoint</a> as per the OpenID Connect specification. This setting has no
effect if open dynamic client registration is disabled.",
        "propertyOrder" : 290,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    }
    }
}
}
}
}

```

## 1.81.2. Global Operations

Resource path: `/global-config/services/oauth-oidc`

Resource version: 1.0

### 1.81.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Provider --global --actionName getAllTypes
```

### 1.81.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Provider --global --actionName getCreatableTypes
```

### 1.81.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Provider --global --actionName nextdescendents
```

### 1.81.2.4. read

Usage:

```
am> read OAuth2Provider --global
```

### 1.81.2.5. update

Usage:

```
am> update OAuth2Provider --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "blacklistCacheSize" : {
      "title" : "Token Blacklist Cache Size",
      "description" : "Number of blacklisted tokens to cache in memory to speed up blacklist checks
and reduce load on the CTS.",
      "propertyOrder" : 0,
      "required" : true,
      "type" : "integer",
```

```

    "exampleValue" : ""
  },
  "blacklistPurgeDelay" : {
    "title" : "Blacklist Purge Delay (minutes)",
    "description" : "Length of time to blacklist tokens beyond their expiry time.<br><br>Allows additional time to account for clock skew to ensure that a token has expired before it is removed from the blacklist.",
    "propertyOrder" : 2,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "idTokenAuthenticitySecret" : {
    "title" : "HMAC ID Token Authenticity Secret",
    "description" : "A secret to use when signing a claim in HMAC-signed ID tokens so that authenticity can be assured when they are presented back to OpenAM.",
    "propertyOrder" : 3,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "agentIdTokenSigningKeyAlias" : {
    "title" : "ID Token Signing Key Alias for Agent Clients",
    "description" : "The alias for the RSA key that should be used signing ID tokens for Agent OAuth2 Clients",
    "propertyOrder" : 4,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "blacklistPollInterval" : {
    "title" : "Blacklist Poll Interval (seconds)",
    "description" : "How frequently to poll for token blacklist changes from other servers, in seconds.<br><br>How often each server will poll the CTS for token blacklist changes from other servers. This is used to maintain a highly compressed view of the overall current token blacklist improving performance. A lower number will reduce the delay for blacklisted tokens to propagate to all servers at the cost of increased CTS load. Set to 0 to disable this feature completely.",
    "propertyOrder" : 1,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "defaults" : {
    "properties" : {
      "advancedOAuth2Config" : {
        "type" : "object",
        "title" : "Advanced",
        "propertyOrder" : 1,
        "properties" : {
          "moduleMessageEnabledInPasswordGrant" : {
            "title" : "Enable auth module messages for Password Credentials Grant",
            "description" : "If enabled, authentication module failure messages are used to create Resource Owner Password Credentials Grant failure messages. If disabled, a standard authentication failed message is used.<br><br>The Password Grant Type requires the <code>grant_type=password</code> parameter.",
            "propertyOrder" : 440,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
          }
        }
      }
    }
  }
}

```

```

    },
    "scopeImplementationClass" : {
      "title" : "Scope Implementation Class",
      "description" : "The class that contains the required scope implementation, must
implement the <code>org.forgerock.oauth2.core.ScopeValidator</code> interface.",
      "propertyOrder" : 70,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "supportedScopes" : {
      "title" : "Supported Scopes",
      "description" : "The set of supported scopes, with translations.<br><br><p>Scopes may
be entered as simple strings or pipe-separated strings representing the internal scope name, locale,
and localized description.</p><p>For example: <code>read|en|Permission to view email messages in
your account</code></p><p>Locale strings are in the format: <code>language_country_variant</code>,
for example <code>en</code>, <code>en_GB</code>, or <code>en_US_WIN</code>.</p><p>If the locale and
pipe is omitted, the description is displayed to all users that have undefined locales.</p><p>If
the description is also omitted, nothing is displayed on the consent page for the scope. For example
specifying <code>read</code> would allow the scope read to be used by the client, but would not
display it to the user on the consent page when requested.</p>",
      "propertyOrder" : 130,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "supportedSubjectTypes" : {
      "title" : "Subject Types supported",
      "description" : "List of subject types supported. Valid values
are:<ul><li><code>public</code> - Each client receives the same subject (<code>sub</code>) value.</li>
<li><code>pairwise</code> - Each client receives a different subject (<code>sub</code>) value, to
prevent correlation between clients.</li></ul>",
      "propertyOrder" : 150,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "customLoginUrlTemplate" : {
      "title" : "Custom Login URL Template",
      "description" : "Custom URL for handling login, to override the default OpenAM login
page.<br><br>Supports Freemarker syntax, with the following variables:<table><tr><th>Variable</th>
<th>Description</th></tr><tr><td><code>gotoUrl</code></td><td><p>The URL to redirect to after
login.</p></td></tr><tr><td><code>acrValues</code></td><td><p>The Authentication Context Class
Reference (acr) values for the authorization request.</p></td></tr><tr><td><code>realm</code></td>
<td><p>The OpenAM realm the authorization request was made on.</p></td></tr><tr><td><code>module</code>
</td><td><p>The name of the OpenAM authentication module requested to perform resource
owner authentication.</p></td></tr><tr><td><code>service</code></td><td><p>The name of the
OpenAM authentication chain requested to perform resource owner authentication.</p></td></tr>
<tr><td><code>locale</code></td><td><p>A space-separated list of locales, ordered by preference.</p>
</td></tr></table>The following example template redirects users to a non-OpenAM front end to handle
login, which will then redirect back to the <code>/oauth2/authorize</code> endpoint with any required
parameters:<p> <code>http://mylogin.com/login?goto=${goto}&#x26;acr_values=
${acrValues}&#x26;realm=${realm}&#x26;if=<code>http://mylogin.com/login?goto=${goto}&#x26;acr_values=
${acrValues}&#x26;realm=${realm}&#x26;if

```



```

module??&module=${module}&#x2F;if&#x2F;if service??&service=
${service}&#x2F;if&#x2F;if locale??&locale=${locale}&#x2F;if&#x2F;if</code>,
    "propertyOrder" : 60,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
},
"modifiedTimestampAttribute" : {
    "title" : "Modified Timestamp attribute name",
    "description" : "The identity Data Store attribute used to return modified timestamp
values.",
    "propertyOrder" : 340,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
},
"keypairName" : {
    "title" : "Token Signing RSA public/private key pair",
    "description" : "The public/private key pair used by RS256.<br><br>The
public/private key pair will be retrieved from the keystore referenced by the property
<code>com.sun.identity.saml.xmlsig.keystore</code>.",
    "propertyOrder" : 240,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
},
"codeVerifierEnforced" : {
    "title" : "Code verifier parameter required",
    "description" : "If enabled, requests using the authorization code grant require a
<code>code_challenge</code> attribute.<br><br>For more information, read the <a href=\\\"https://
tools.ietf.org/html/draft-ietf-oauth-spop-12\\\">draft specification for this feature</a>.",
    "propertyOrder" : 270,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"tokenCompressionEnabled" : {
    "title" : "Stateless Token Compression",
    "description" : "Whether stateless access and refresh tokens should be compressed.",
    "propertyOrder" : 223,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"tokenSigningAlgorithm" : {
    "title" : "OAuth2 Token Signing Algorithm",
    "description" : "Algorithm used to sign stateless OAuth 2.0 tokens in order to
detect tampering.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms
(JWA): <a href=\\\"http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms#section-3.1\\\">
\\\"alg\\\" (Algorithm) Header Parameter Values for JWS</a>:<ul><li><code>HS256</code> - HMAC
with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</li><li><code>HS512</code> -
HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and NIST standard P-256
elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard P-384 elliptic
curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.</
li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
    "propertyOrder" : 220,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
}

```

```

    },
    "clientsCanSkipConsent" : {
      "title" : "Allow clients to skip consent",
      "description" : "If enabled, clients may be configured so that the resource owner will
not be asked for consent during authorization flows.",
      "propertyOrder" : 420,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "displayNameAttribute" : {
      "title" : "User Display Name attribute",
      "description" : "The profile attribute that contains the name to be displayed for the
user on the consent page.",
      "propertyOrder" : 120,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationAttributes" : {
      "title" : "User Profile Attribute(s) the Resource Owner is Authenticated On",
      "description" : "Names of profile attributes that resource owners use to log in. You can
add others to the default, for example <code>mail</code>.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "createdTimestampAttribute" : {
      "title" : "Created Timestamp attribute name",
      "description" : "The identity Data Store attribute used to return created timestamp
values.",
      "propertyOrder" : 350,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "hashSalt" : {
      "title" : "Subject identifier hash salt",
      "description" : "If <i>pairwise</i> subject types are supported, it is <em>STRONGLY
RECOMMENDED</em> to change this value. It is used in the salting of hashes for returning
specific <code>sub</code> claims to individuals using the same <code>request_uri</code> or
<code>sector_identifier_uri</code>.",
      "propertyOrder" : 260,
      "required" : false,
      "type" : "string",
      "exampleValue" : "changeme"
    },
    "defaultScopes" : {
      "title" : "Default Client Scopes",
      "description" : "List of scopes a client will be granted if they request registration
without specifying which scopes they want. Default scopes are NOT auto-granted to clients created
through the OpenAM console.",
      "propertyOrder" : 200,
      "required" : false,
      "items" : {

```

```

        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "tokenSigningECDSAKeyAlias" : {
      "title" : "Token Signing ECDSA public/private key pair alias",
      "description" : "The list of public/private key pairs used for the elliptic
curve algorithms (ES256/ES384/ES512). Add an entry to specify an alias for a specific
elliptic curve algorithm, for example <code>ES256|es256Alias</code>.<br><br>Each of the
public/private key pairs will be retrieved from the keystore referenced by the property
<code>com.sun.identity.saml.xmlsig.keystore</code>.",
      "propertyOrder" : 241,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "responseTypeClasses" : {
      "title" : "Response Type Plugins",
      "description" : "List of plugins that handle the valid <code>response_type</code>
values.<br><br>OAuth 2.0 clients pass response types as parameters to the OAuth 2.0 Authorization
endpoint (<code>/oauth2/authorize</code>) to indicate which grant type is requested from the
provider. For example, the client passes <code>code</code> when requesting an authorization code,
and <code>token</code> when requesting an access token.<p><p>Values in this list take the form
<code>response_type|plugin-class-name</code>.",
      "propertyOrder" : 90,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "tokenSigningHmacSharedSecret" : {
      "title" : "Token Signing HMAC Shared Secret",
      "description" : "Base64-encoded key used by HS256, HS384 and HS512.",
      "propertyOrder" : 230,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
},
"advancedOIDCConfig" : {
  "type" : "object",
  "title" : "Advanced OpenID Connect",
  "propertyOrder" : 3,
  "properties" : {
    "claimsParameterSupported" : {
      "title" : "Enable \"claims_parameter_supported\"",
      "description" : "If enabled, clients will be able to request individual claims using
the <code>claims</code> request parameter, as per <a href=\"http://openid.net/specs/openid-connect-
core-1_0.html#ClaimsParameter\" target=\"_blank\">section 5.5 of the OpenID Connect specification</
a>.",
      "propertyOrder" : 250,
      "required" : true,

```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "storeOpsTokens" : {
        "title" : "Store Ops Tokens",
        "description" : "Whether OpenAM will store the <i>ops</i> tokens corresponding to OpenID
Connect sessions in the CTS store. Note that session management related endpoints will not work when
this setting is disabled.",
        "propertyOrder" : 410,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "loaMapping" : {
        "title" : "OpenID Connect acr_values to Auth Chain Mapping",
        "description" : "Maps OpenID Connect ACR values to authentication chains. See the

```

```

must use it to access the <code>userinfo</code> endpoint for scope-derived claims, as they will not
be included in the ID token.",
  "propertyOrder" : 360,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"allowDynamicRegistration" : {
  "title" : "Allow Open Dynamic Client Registration",
  "description" : "Allow clients to register without an access token. If enabled, you
should consider adding some form of rate limiting. See <a href='\"http://openid.net/specs/openid-
connect-registration-1_0.html#ClientRegistration\"' target='\"_blank\">Client Registration</a> in the
OpenID Connect specification for details.",
  "propertyOrder" : 280,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"idTokenInfoClientAuthenticationEnabled" : {
  "title" : "Idtokeninfo endpoint requires client authentication",
  "description" : "When enabled, the <code>/oauth2/idthtokeninfo</code> endpoint requires
client authentication if the signing algorithm is set to <code>HS256</code>, <code>HS384</code>, or
<code>HS512</code>.",
  "propertyOrder" : 225,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"jwksURI" : {
  "title" : "Remote JSON Web Key URL",
  "description" : "The Remote URL where the providers JSON Web Key can be
retrieved.<p><p>If this setting is not configured, then OpenAM provides a local URL to access the
public key of the private key used to sign ID tokens.",
  "propertyOrder" : 140,
  "required" : false,
  "type" : "string",
  "exampleValue" : ""
},
"defaultACR" : {
  "title" : "OpenID Connect default acr claim",
  "description" : "Default value to use as the <code>acr</code> claim in an OpenID Connect
ID Token when using the default authentication chain.",
  "propertyOrder" : 320,
  "required" : false,
  "type" : "string",
  "exampleValue" : ""
}
}
},
"coreOIDCConfig" : {
  "type" : "object",
  "title" : "OpenID Connect",
  "propertyOrder" : 2,
  "properties" : {
    "supportedIDTokenEncryptionMethods" : {
      "title" : "ID Token Encryption Methods supported",
      "description" : "Encryption methods supported to encrypt OpenID Connect ID
tokens in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES

```

```

in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
<code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
  "propertyOrder" : 180,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"supportedIDTokenEncryptionAlgorithms" : {
  "title" : "ID Token Encryption Algorithms supported",
  "description" : "Encryption algorithms supported to encrypt OpenID Connect ID
tokens in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</
li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</
li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
with 192-bit key derived from the client secret.</li></ul>",
  "propertyOrder" : 170,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"supportedIDTokenSigningAlgorithms" : {
  "title" : "ID Token Signing Algorithms supported",
  "description" : "Algorithms supported to sign OpenID Connect <code>id_tokens</
code>.<p><p>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"http://
tools.ietf.org/html/draft-ietf-jose-json-web-algorithms#section-3.1\">\"alg\" (Algorithm) Header
Parameter Values for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</
code> - HMAC with SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code>
- ECDSA with SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with
SHA-384 and NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and
NIST standard P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</
li></ul>",
  "propertyOrder" : 160,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"supportedClaims" : {
  "title" : "Supported Claims",
  "description" : "Set of claims supported by the OpenID Connect <code>/oauth2/
userinfo</code> endpoint, with translations.<br><br>Claims may be entered as simple strings or pipe
separated strings representing the internal claim name, locale, and localized description.<p><p>For
example: <code>name|en|Your full name.</code>.<p>Locale strings are in the format: <code>language
+ \"_\" + country + \"_\" + variant</code>, for example <code>en</code>, <code>en_GB</code>, or
<code>en_US_WIN</code>. If the locale and pipe is omitted, the description is displayed to all users
that have undefined locales.<p><p>If the description is also omitted, nothing is displayed on the
consent page for the claim. For example specifying <code>family_name|</code> would allow the claim

```

```

<code>family_name</code> to be used by the client, but would not display it to the user on the
consent page when requested.",
  "propertyOrder" : 190,
  "required" : false,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"jwtTokenLifetime" : {
  "title" : "OpenID Connect JWT Token Lifetime (seconds)",
  "description" : "The amount of time the JWT will be valid for, in seconds.",
  "propertyOrder" : 210,
  "required" : false,
  "type" : "integer",
  "exampleValue" : ""
},
"oidcClaimsScript" : {
  "title" : "OIDC Claims Script",
  "description" : "The script that is run when issuing an ID token or making a request
to the <i>userinfo</i> endpoint during OpenID requests.<p><p>The script gathers the scopes and
populates claims, and has access to the access token, the user's identity and, if available, the
user's session.",
  "propertyOrder" : 80,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
},
"deviceCodeConfig" : {
  "type" : "object",
  "title" : "Device Flow",
  "propertyOrder" : 4,
  "properties" : {
    "deviceCodeLifetime" : {
      "title" : "Device Code Lifetime (seconds)",
      "description" : "The lifetime of the device code, in seconds.",
      "propertyOrder" : 390,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "verificationUrl" : {
      "title" : "Verification URL",
      "description" : "The URL that the user will be instructed to visit to complete their
OAuth 2.0 login and consent when using the device code flow.",
      "propertyOrder" : 370,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "devicePollInterval" : {
      "title" : "Device Polling Interval",
      "description" : "The polling frequency for devices waiting for tokens when using the
device code flow.",
      "propertyOrder" : 400,
      "required" : true,

```

```

        "type" : "integer",
        "exampleValue" : ""
    },
    "completionUrl" : {
        "title" : "Device Completion URL",
        "description" : "The URL that the user will be sent to on completion of their OAuth 2.0
login and consent when using the device code flow.",
        "propertyOrder" : 380,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    }
},
"coreOAuth2Config" : {
    "type" : "object",
    "title" : "Core",
    "propertyOrder" : 0,
    "properties" : {
        "refreshTokenLifetime" : {
            "title" : "Refresh Token Lifetime (seconds)",
            "description" : "The time in seconds a refresh token is valid for. If this field is set
to <code>-1</code>, the token will never expire.",
            "propertyOrder" : 20,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "statelessTokensEnabled" : {
            "title" : "Use Stateless Access & Refresh Tokens",
            "description" : "When enabled, OpenAM issues access and refresh tokens that can be
inspected by resource servers.",
            "propertyOrder" : 3,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "savedConsentAttribute" : {
            "title" : "Saved Consent Attribute Name",
            "description" : "Name of a multi-valued attribute on resource owner profiles where
OpenAM can save authorization consent decisions.<p><p>When the resource owner chooses to save the
decision to authorize access for a client application, then OpenAM updates the resource owner's
profile to avoid having to prompt the resource owner to grant authorization when the client issues
subsequent authorization requests.",
            "propertyOrder" : 110,
            "required" : false,
            "type" : "string",
            "exampleValue" : ""
        },
        "codeLifetime" : {
            "title" : "Authorization Code Lifetime (seconds)",
            "description" : "The time an authorization code is valid for, in seconds.",
            "propertyOrder" : 10,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "issueRefreshToken" : {
            "title" : "Issue Refresh Tokens",

```



```

        "description" : "Whether to issue a refresh token when returning an access token.",
        "propertyOrder" : 40,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "issueRefreshTokenOnRefreshedToken" : {
        "title" : "Issue Refresh Tokens on Refreshing Access Tokens",
        "description" : "Whether to issue a refresh token when refreshing an access token.",
        "propertyOrder" : 50,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "accessTokenLifetime" : {
        "title" : "Access Token Lifetime (seconds)",
        "description" : "The time an access token is valid for, in seconds.",
        "propertyOrder" : 30,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
    }
    },
    "type" : "object",
    "title" : "Realm Defaults"
}
}
}

```

## 1.82. OAuth2UserApplications

### 1.82.1. Realm Operations

This endpoint exposes a list of all the applications (clients) that the user authorized using OAuth 2.0. Access for those applications can then be revoked on a per-client basis.

Resource path: `/users/{user}/oauth2/applications`

Resource version: `1.0`

#### 1.82.1.1. delete

Delete the tokens for the specified client ID.

Usage:

```
am> delete OAuth2UserApplications --realm Realm --id id --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--user**

This endpoint exposes a list of all the applications (clients) that the user authorized using OAuth 2.0. Access for those applications can then be revoked on a per-client basis.

### 1.82.1.2. query

Get a list of the applications that have been granted OAuth 2.0 access. Only `\_queryFilter=true` is supported.

Usage:

```
am> query OAuth2UserApplications --realm Realm --filter filter --user user
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

**--user**

This endpoint exposes a list of all the applications (clients) that the user authorized using OAuth 2.0. Access for those applications can then be revoked on a per-client basis.

## 1.83. OathModule

### 1.83.1. Realm Operations

Resource path: `/realm-config/authentication/modules/oath`

Resource version: `1.0`

#### 1.83.1.1. create

Usage:

```
am> create OathModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "lastLoginTimeAttribute" : {
      "title" : "Last Login Time Attribute",
      "description" : "Attribute to store the time of the users last login. This is required if TOTP is chosen as the OATH algorithm.<br><br>This attribute stores the last time a user logged in to prevent time based attacks. The value is stored as a number (Unix Time).",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "secretKeyAttribute" : {
      "title" : "Secret Key Attribute Name",
      "description" : "The name of the attribute in the user profile to store the user secret key.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every few seconds as specified by the time step interval.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "hotpWindowSize" : {
      "title" : "HOTP Window Size",
      "description" : "The size of the window to resynchronize with the client.<br><br>This sets the window that the OTP device and the server counter can be out of sync. For example, if the window size is 100 and the servers last successful login was at counter value 2, then the server will accept a OTP from the OTP device that is from device counter 3 to 102.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "passwordLength" : {
      "title" : "One Time Password Length ",
      "description" : "The length of the generated OTP in digits. Must be 6 digits or longer.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "hotpCounterAttribute" : {
      "title" : "Counter Attribute Name",
      "description" : "The name of the attribute in the user profile to store the user counter. This is required if HOTP is chosen as the OATH algorithm.",
      "propertyOrder" : 700,
```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "stepsInWindow" : {
    "title" : "TOTP Time Steps",
    "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This is the number of time step intervals to check the received OTP against both forward in time and back in time. For example, with 2 time steps and a time step interval of 30 seconds the server will allow a clock drift between client and server of 89 seconds. (2-30 second steps and 29 seconds for the interval that the OTP arrived in)",
    "propertyOrder" : 1100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "forgerock-oath-sharedsecret-implementation-class" : {
    "title" : "The Shared Secret Provider Class",
    "description" : "The fully qualified class name for the Shared Secret Provider extension.<br><br>The class that is used to process the user profile attribute used to store the user secret key.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "addChecksum" : {
    "title" : "Add Checksum Digit",
    "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in addition to the actual password length. You should only set this if your device supports it.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "minimumSecretKeyLength" : {
    "title" : "Minimum Secret Key Length",
    "description" : "Number of hexadecimal characters allowed for the Secret Key.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "forgerock-oath-observed-clock-drift-attribute-name" : {
    "title" : "Clock Drift Attribute Name",
    "description" : "The name of the attribute in the user profile to store the clock drift. If left empty then clock drift checking is disabled.<br><br>The name of the attribute used to store the last observed clock drift which is used to indicated when a manual resynchronisation is required.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "timeStepSize" : {
    "title" : "TOTP Time Step Interval",
    "description" : "The TOTP time step in seconds that the OTP device uses to generate the OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30

```

```
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
  "propertyOrder" : 1000,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"forgerock-oath-maximum-clock-drift" : {
  "title" : "Maximum Allowed Clock Drift",
  "description" : "Number of time steps a client is allowed to get out of sync with the server
before manual resynchronisation is required. This should be greater than the TOTP Time Steps
value.<br><br>As this checks the time drift over multiple requests it needs to be greater than the
value specified in TOTP Time Steps.",
  "propertyOrder" : 1500,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"authenticationLevel" : {
  "title" : "Authentication Level",
  "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"truncationOffset" : {
  "title" : "Truncation Offset",
  "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used
by the HOTP algorithm that not all devices support. This should be left default unless you know your
device uses a offset.",
  "propertyOrder" : 900,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
}
}
}
```

### 1.83.1.2. delete

Usage:

```
am> delete OathModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.83.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OathModule --realm Realm --actionName getAllTypes
```

### 1.83.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OathModule --realm Realm --actionName getCreatableTypes
```

### 1.83.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OathModule --realm Realm --actionName nextdescendents
```

### 1.83.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query OathModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.83.1.7. read

Usage:

```
am> read OathModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.83.1.8. update

Usage:

```
am> update OathModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "lastLoginTimeAttribute" : {
      "title" : "Last Login Time Attribute",
      "description" : "Attribute to store the time of the users last login. This is required if TOTP
is chosen as the OATH algorithm.<br><br>This attribute stores the last time a user logged in to
prevent time based attacks. The value is stored as a number (Unix Time).",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "secretKeyAttribute" : {
      "title" : "Secret Key Attribute Name",
      "description" : "The name of the attribute in the user profile to store the user secret key.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a
counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every
few seconds as specified by the time step interval.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "hotpWindowSize" : {
      "title" : "HOTP Window Size",
      "description" : "The size of the window to resynchronize with the client.<br><br>This sets the
window that the OTP device and the server counter can be out of sync. For example, if the window size
is 100 and the servers last successful login was at counter value 2, then the server will accept a
OTP from the OTP device that is from device counter 3 to 102.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
}
```

```

"passwordLength" : {
  "title" : "One Time Password Length ",
  "description" : "The length of the generated OTP in digits. Must be 6 digits or longer.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"hotpCounterAttribute" : {
  "title" : "Counter Attribute Name",
  "description" : "The name of the attribute in the user profile to store the user counter. This
is required if HOTP is chosen as the OATH algorithm.",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"stepsInWindow" : {
  "title" : "TOTP Time Steps",
  "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This
is the number of time step intervals to check the received OTP against both forward in time and back
in time. For example, with 2 time steps and a time step interval of 30 seconds the server will allow
a clock drift between client and server of 89 seconds. (2-30 second steps and 29 seconds for the
interval that the OTP arrived in)",
  "propertyOrder" : 1100,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"forgerock-oath-sharedsecret-implementation-class" : {
  "title" : "The Shared Secret Provider Class",
  "description" : "The fully qualified class name for the Shared Secret Provider
extension.<br><br>The class that is used to process the user profile attribute used to store the user
secret key.",
  "propertyOrder" : 1300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"addChecksum" : {
  "title" : "Add Checksum Digit",
  "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
addition to the actual password length. You should only set this if your device supports it.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"minimumSecretKeyLength" : {
  "title" : "Minimum Secret Key Length",
  "description" : "Number of hexadecimal characters allowed for the Secret Key.",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"forgerock-oath-observed-clock-drift-attribute-name" : {
  "title" : "Clock Drift Attribute Name",

```



```

        "description" : "The name of the attribute in the user profile to store the clock drift. If left
empty then clock drift checking is disabled.<br><br>The name of the attribute used to store the last
observed clock drift which is used to indicated when a manual resynchronisation is required.",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "timeStepSize" : {
        "title" : "TOTP Time Step Interval",
        "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "forgerock-oath-maximum-clock-drift" : {
        "title" : "Maximum Allowed Clock Drift",
        "description" : "Number of time steps a client is allowed to get out of sync with the server
before manual resynchronisation is required. This should be greater than the TOTP Time Steps
value.<br><br>As this checks the time drift over multiple requests it needs to be greater than the
value specified in TOTP Time Steps.",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "authenticationLevel" : {
        "title" : "Authentication Level",
        "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "truncationOffset" : {
        "title" : "Truncation Offset",
        "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used
by the HOTP algorithm that not all devices support. This should be left default unless you know your
device uses a offset.",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
}
}
}

```

## 1.83.2. Global Operations

Resource path: </global-config/authentication/modules/oath>

Resource version: 1.0

### 1.83.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OathModule --global --actionName getAllTypes
```

### 1.83.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OathModule --global --actionName getCreatableTypes
```

### 1.83.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OathModule --global --actionName nextdescendents
```

### 1.83.2.4. read

Usage:

```
am> read OathModule --global
```

### 1.83.2.5. update

Usage:

```
am> update OathModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "oathAlgorithm" : {
          "title" : "OATH Algorithm to Use",
```

```

    "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every few seconds as specified by the time step interval.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "forgerock-oath-maximum-clock-drift" : {
    "title" : "Maximum Allowed Clock Drift",
    "description" : "Number of time steps a client is allowed to get out of sync with the server before manual resynchronisation is required. This should be greater than the TOTP Time Steps value.<br><br>As this checks the time drift over multiple requests it needs to be greater than the value specified in TOTP Time Steps.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "stepsInWindow" : {
    "title" : "TOTP Time Steps",
    "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This is the number of time step intervals to check the received OTP against both forward in time and back in time. For example, with 2 time steps and a time step interval of 30 seconds the server will allow a clock drift between client and server of 89 seconds. (2-30 second steps and 29 seconds for the interval that the OTP arrived in)",
    "propertyOrder" : 1100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "hotpWindowSize" : {
    "title" : "HOTP Window Size",
    "description" : "The size of the window to resynchronize with the client.<br><br>This sets the window that the OTP device and the server counter can be out of sync. For example, if the window size is 100 and the servers last successful login was at counter value 2, then the server will accept a OTP from the OTP device that is from device counter 3 to 102.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "lastLoginTimeAttribute" : {
    "title" : "Last Login Time Attribute",
    "description" : "Attribute to store the time of the users last login. This is required if TOTP is chosen as the OATH algorithm.<br><br>This attribute stores the last time a user logged in to prevent time based attacks. The value is stored as a number (Unix Time).",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "secretKeyAttribute" : {
    "title" : "Secret Key Attribute Name",
    "description" : "The name of the attribute in the user profile to store the user secret key.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",

```

```

    "exampleValue" : ""
  },
  "addChecksum" : {
    "title" : "Add Checksum Digit",
    "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
addition to the actual password length. You should only set this if your device supports it.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "forgerock-oath-observed-clock-drift-attribute-name" : {
    "title" : "Clock Drift Attribute Name",
    "description" : "The name of the attribute in the user profile to store the clock drift. If
left empty then clock drift checking is disabled.<br><br>The name of the attribute used to store the
last observed clock drift which is used to indicated when a manual resynchronisation is required.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "passwordLength" : {
    "title" : "One Time Password Length ",
    "description" : "The length of the generated OTP in digits. Must be 6 digits or longer.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "truncationOffset" : {
    "title" : "Truncation Offset",
    "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option
used by the HOTP algorithm that not all devices support. This should be left default unless you know
your device uses a offset.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "timeStepSize" : {
    "title" : "TOTP Time Step Interval",
    "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "integer",

```

```

        "exampleValue" : ""
    },
    "minimumSecretKeyLength" : {
        "title" : "Minimum Secret Key Length",
        "description" : "Number of hexadecimal characters allowed for the Secret Key.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "hotpCounterAttribute" : {
        "title" : "Counter Attribute Name",
        "description" : "The name of the attribute in the user profile to store the user counter.
This is required if HOTP is chosen as the OATH algorithm.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "forgerock-oath-sharedsecret-implementation-class" : {
        "title" : "The Shared Secret Provider Class",
        "description" : "The fully qualified class name for the Shared Secret Provider
extension.<br><br>The class that is used to process the user profile attribute used to store the user
secret key.",
        "propertyOrder" : 1300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.84. OathUserDevices

### 1.84.1. Realm Operations

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

Resource path: `/users/{user}/devices/2fa/oath`

Resource version: `1.0`

#### 1.84.1.1. checkOathDevice

Checks if the user's Authenticator OATH module is 'skippable' and returns the result as a boolean

Usage:

```
am> action OathUserDevices --realm Realm --body body --user user --actionName checkOathDevice
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Oath user device check action request schema",
  "type" : "object",
  "title" : "Oath user device check action request schema"
}
```

**--user**

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

### 1.84.1.2. delete

Delete Oath user device

Usage:

```
am> delete OathUserDevices --realm Realm --id id --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--user**

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

### 1.84.1.3. query

Query the user's device profile

Usage:

```
am> query OathUserDevices --realm Realm --filter filter --user user
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

**--user**

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

#### 1.84.1.4. resetOathDevice

Sets the user's 'skippable' selection of Authenticator OATH module to default (NOT\_SET) and deletes their profiles attribute

Usage:

```
am> action OathUserDevices --realm Realm --body body --user user --actionName resetOathDevice
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Oath user device reset action request schema",
  "type" : "object",
  "title" : "Oath user device reset action request schema"
}
```

**--user**

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

#### 1.84.1.5. skipOathDevice

Sets the user's ability to skip an Authenticator OATH module

Usage:

```
am> action OathUserDevices --realm Realm --body body --user user --actionName skipOathDevice
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Oath user device skip action request schema",
  "type" : "object",
  "title" : "Oath user device skip action request schema",
  "properties" : {
    "value" : {
      "type" : "boolean",
      "title" : "Skip OATH module response value",
      "description" : "True if the OATH device is set to skipped"
    }
  },
  "required" : [ "value" ]
}
```

**--user**

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

## 1.85. OpenDj

### 1.85.1. Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForOpenDS`

Resource version: `1.0`

#### 1.85.1.1. create

Usage:

```
am> create OpenDj --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunIdRepoClass" : {
      "title" : "LDAPv3 Repository Plug-in Class Name",
      "description" : "",
      "propertyOrder" : 1700,
      "required" : true,

```



```

    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-objectclass" : {
    "title" : "LDAP User Object Class",
    "description" : "",
    "propertyOrder" : 2300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-isactive" : {
    "title" : "Attribute Name of User Status",
    "description" : "",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authpw" : {
    "title" : "LDAP Bind Password",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-interval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the
    directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
    request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
    error) then it may take up to the interval period before the problem is detected. Use along with the
    Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
    disabling heartbeat requests.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "com.ipplanet.am.ldap.connection.delay.between.retries" : {
    "title" : "The Delay Time Between Retries",
    "description" : "In milliseconds.",
    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-time-limit" : {
    "title" : "Search Timeout",
    "description" : "In seconds.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }

```

```

},
"sun-idrepo-ldapv3-config-users-search-filter" : {
  "title" : "LDAP Users Search Filter",
  "description" : "",
  "propertyOrder" : 2200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-groups-search-filter" : {
  "title" : "LDAP Groups Search Filter",
  "description" : "",
  "propertyOrder" : 3000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-users-search-attribute" : {
  "title" : "LDAP Users Search Attribute",
  "description" : "",
  "propertyOrder" : 2100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-groups-search-attribute" : {
  "title" : "LDAP Groups Search Attribute",
  "description" : "",
  "propertyOrder" : 2900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-value" : {
  "title" : "LDAP Groups Container Value",
  "description" : "",
  "propertyOrder" : 3200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-people-container-name" : {
  "title" : "LDAP People Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 5000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-people-container-value" : {
  "title" : "LDAP People Container Value",
  "description" : "",
  "propertyOrder" : 5100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-psearch-filter" : {
  "title" : "Persistent Search Filter",

```

```

    "description" : "",
    "propertyOrder" : 5600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-attributes" : {
    "title" : "LDAP User Attributes",
    "description" : "",
    "propertyOrder" : 2400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-size" : {
    "title" : "DN Cache Size",
    "description" : "In DN items, only used when DN Cache is enabled.",
    "propertyOrder" : 6000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-attr" : {
    "title" : "Knowledge Based Authentication Attribute Name",
    "description" : "",
    "propertyOrder" : 5300,

```

```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-max-result" : {
    "title" : "Maximum Results Returned from Search",
    "description" : "",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {

```

```

    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-enabled" : {
    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository  

    implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during  

    authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying  

    LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP  

    store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberurl" : {
    "title" : "Attribute Name of Group Member URL",
    "description" : "",
    "propertyOrder" : 3700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-naming-attr" : {
    "title" : "Authentication Naming Attribute",
    "description" : "",
    "propertyOrder" : 5200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",
    "description" : "",
    "propertyOrder" : 3400,
    "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-active" : {
    "title" : "User Status Active Value",
    "description" : "",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-timeunit" : {
    "title" : "LDAP Connection Heartbeat Time Unit",
    "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
    "propertyOrder" : 700,

```

```
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-name" : {
    "title" : "LDAP Groups Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoSupportedOperations" : {
    "title" : "LDAPv3 Plug-in Supported Types and Operations",
    "description" : "",
    "propertyOrder" : 1900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }
}
```

### 1.85.1.2. delete

Usage:

```
am> delete OpenDJ --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.85.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OpenDJ --realm Realm --actionName getAllTypes
```

### 1.85.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OpenDJ --realm Realm --actionName getCreatableTypes
```

### 1.85.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OpenDJ --realm Realm --actionName nextdescendents
```

### 1.85.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query OpenDJ --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.85.1.7. read

Usage:

```
am> read OpenDJ --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.85.1.8. update

Usage:

```
am> update OpenDJ --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.



--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunIdRepoClass" : {
      "title" : "LDAPv3 Repository Plug-in Class Name",
      "description" : "",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-user-objectclass" : {
      "title" : "LDAP User Object Class",
      "description" : "",
      "propertyOrder" : 2300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-isactive" : {
      "title" : "Attribute Name of User Status",
      "description" : "",
      "propertyOrder" : 2600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-authpw" : {
      "title" : "LDAP Bind Password",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "openam-idrepo-ldapv3-heartbeat-interval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
        directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
        request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
        error) then it may take up to the interval period before the problem is detected. Use along with the
        Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
        disabling heartbeat requests.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "com.ipplanet.am.ldap.connection.delay.between.retries" : {
      "title" : "The Delay Time Between Retries",
      "description" : "In milliseconds.",

```

```

    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-time-limit" : {
    "title" : "Search Timeout",
    "description" : "In seconds.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-filter" : {
    "title" : "LDAP Users Search Filter",
    "description" : "",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-filter" : {
    "title" : "LDAP Groups Search Filter",
    "description" : "",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-attribute" : {
    "title" : "LDAP Groups Search Attribute",
    "description" : "",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-value" : {
    "title" : "LDAP Groups Container Value",
    "description" : "",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-name" : {
    "title" : "LDAP People Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "string",

```

```

    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-value" : {
    "title" : "LDAP People Container Value",
    "description" : "",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-filter" : {
    "title" : "Persistent Search Filter",
    "description" : "",
    "propertyOrder" : 5600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-attributes" : {
    "title" : "LDAP User Attributes",
    "description" : "",
    "propertyOrder" : 2400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-size" : {
    "title" : "DN Cache Size",
    "description" : "In DN items, only used when DN Cache is enabled.",
    "propertyOrder" : 6000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",

```

```

    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-attr" : {
    "title" : "Knowledge Based Authentication Attribute Name",
    "description" : "",
    "propertyOrder" : 5300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-max-result" : {
    "title" : "Maximum Results Returned from Search",
    "description" : "",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-enabled" : {
    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository  
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during  
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying  
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP  
store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberurl" : {
    "title" : "Attribute Name of Group Member URL",
    "description" : "",
    "propertyOrder" : 3700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-naming-attr" : {

```

```

    "title" : "Authentication Naming Attribute",
    "description" : "",
    "propertyOrder" : 5200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",
    "description" : "",
    "propertyOrder" : 3400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-active" : {
    "title" : "User Status Active Value",
    "description" : "",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br>If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br>If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-timeunit" : {
    "title" : "LDAP Connection Heartbeat Time Unit",
    "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then

```

```

it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
  "propertyOrder" : 1400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-authid" : {
  "title" : "LDAP Bind DN",
  "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-name" : {
  "title" : "LDAP Groups Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 3100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sunIdRepoSupportedOperations" : {
  "title" : "LDAPv3 Plug-in Supported Types and Operations",
  "description" : "",
  "propertyOrder" : 1900,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
}
}
}

```

## 1.86. OpenIdConnectModule

### 1.86.1. Realm Operations

Resource path: `/realm-config/authentication/modules/openidconnect`

Resource version: `1.0`

#### 1.86.1.1. create

Usage:

```
am> create OpenIdConnectModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "audienceName" : {
      "title" : "Audience name",
      "description" : "A case sensitive string<br><br>The audience name for this OpenID Conenct module. This will be used to check that the ID token received is intended for this module as an audience.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idTokenHeaderName" : {
      "title" : "Name of header referencing the ID Token",
      "description" : "",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idTokenIssuer" : {
      "title" : "Name of OpenID Connect ID Token Issuer",
      "description" : "Value must match the iss field in issued ID Token",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "cryptoContextType" : {
      "title" : "OpenID Connect validation configuration type",
      "description" : "Please select either 1. the issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "principalMapperClass" : {
      "title" : "Principal mapper class",
      "description" : "Class which implements mapping of jwt state to a Principal in the local identity repository<br><br>Any custom implementation must implement the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
```



```

    "title" : "Client Secret",
    "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
    "propertyOrder" : 301,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
},
"cryptoContextValue" : {
    "title" : "OpenID Connect validation configuration value",
    "description" : "The discovery url, or jwk url, or the client_secret, corresponding to the
selection above.<br><br>If discovery or jwk url entered, entry must be in valid url format, <br>e.g.
https://accounts.google.com/.well-known/openid-configuration<br><i>NB </i>If client_secret entered,
entry is ignored and the value of the Client Secret is used.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"acceptedAuthorizedParties" : {
    "title" : "List of accepted authorized parties",
    "description" : "A list of case sensitive strings which can be either string or URI
values<br><br>A list of authorized parties which this module will accept ID tokens from. This will be
checked against the authorized party claim of the ID token.",
    "propertyOrder" : 800,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"accountProviderClass" : {
    "title" : "Account provider class",
    "description" : "Name of the class implementing the account provider.<br><br>This class
is used by the module to find the account from the attributes mapped by the Account Mapper
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"jwtToLdapAttributeMappings" : {
    "title" : "Mapping of jwt attributes to local LDAP attributes",
    "description" : "Format: jwt_attribute=local_ldap_attribute<br><br>Mappings allow jwt entries to
drive principal lookup. This entry determines how to translate between local LDAP attributes and the
entries in the jwt. See <a href=\"http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims
\" target=\"_blank\">OpenID Connect Core 1.0 Specification</a> section 5.4 on how to request the
inclusion of additional attributes in issued ID Tokens.",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
}
}

```

```
}  
}
```

### 1.86.1.2. delete

Usage:

```
am> delete OpenIdConnectModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.86.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OpenIdConnectModule --realm Realm --actionName getAllTypes
```

### 1.86.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OpenIdConnectModule --realm Realm --actionName getCreatableTypes
```

### 1.86.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OpenIdConnectModule --realm Realm --actionName nextdescendents
```

### 1.86.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query OpenIdConnectModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

**1.86.1.7. read**

Usage:

```
am> read OpenIdConnectModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

**1.86.1.8. update**

Usage:

```
am> update OpenIdConnectModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "audienceName" : {
      "title" : "Audience name",
      "description" : "A case sensitive string<br><br>The audience name for this OpenID Conenct module. This will be used to check that the ID token received is intended for this module as an audience.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idTokenHeaderName" : {
      "title" : "Name of header referencing the ID Token",
      "description" : "",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idTokenIssuer" : {
      "title" : "Name of OpenID Connect ID Token Issuer",
```

```

    "description" : "Value must match the iss field in issued ID Token",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cryptoContextType" : {
    "title" : "OpenID Connect validation configuration type",
    "description" : "Please select either 1. the issuer discovery url, 2. the issuer jwk url, or 3.
the client_secret.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "principalMapperClass" : {
    "title" : "Principal mapper class",
    "description" : "Class which implements mapping of jwt state to a Principal in
the local identity repository<br><br>Any custom implementation must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientSecret" : {
    "title" : "Client Secret",
    "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
    "propertyOrder" : 301,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "cryptoContextValue" : {
    "title" : "OpenID Connect validation configuration value",
    "description" : "The discovery url, or jwk url, or the client_secret, corresponding to the
selection above.<br><br>If discovery or jwk url entered, entry must be in valid url format, <br>>e.g.
https://accounts.google.com/.well-known/openid-configuration<br></i>NB </i>If client_secret entered,
entry is ignored and the value of the Client Secret is used.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "acceptedAuthorizedParties" : {
    "title" : "List of accepted authorized parties",
    "description" : "A list of case sensitive strings which can be either string or URI
values<br><br>A list of authorized parties which this module will accept ID tokens from. This will be
checked against the authorized party claim of the ID token.",
    "propertyOrder" : 800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }

```

```

    },
    "accountProviderClass" : {
      "title" : "Account provider class",
      "description" : "Name of the class implementing the account provider.<br><br>This class
is used by the module to find the account from the attributes mapped by the Account Mapper
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwtToLdapAttributeMappings" : {
      "title" : "Mapping of jwt attributes to local LDAP attributes",
      "description" : "Format: jwt_attribute=local_ldap_attribute<br><br>Mappings allow jwt entries to
drive principal lookup. This entry determines how to translate between local LDAP attributes and the
entries in the jwt. See <a href=\"http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims
\" target=\"_blank\">OpenID Connect Core 1.0 Specification</a> section 5.4 on how to request the
inclusion of additional attributes in issued ID Tokens.",
      "propertyOrder" : 600,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}

```

## 1.86.2. Global Operations

Resource path: `/global-config/authentication/modules/openidconnect`

Resource version: `1.0`

### 1.86.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OpenIdConnectModule --global --actionName getAllTypes
```

### 1.86.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OpenIdConnectModule --global --actionName getCreatableTypes
```

### 1.86.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OpenIdConnectModule --global --actionName nextdescendents
```

### 1.86.2.4. read

Usage:

```
am> read OpenIdConnectModule --global
```

### 1.86.2.5. update

Usage:

```
am> update OpenIdConnectModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "principalMapperClass" : {
          "title" : "Principal mapper class",
          "description" : "Class which implements mapping of jwt state to a Principal
in the local identity repository<br><br>Any custom implementation must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account provider class",
          "description" : "Name of the class implementing the account provider.<br><br>This
class is used by the module to find the account from the attributes mapped by the Account Mapper
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "acceptedAuthorizedParties" : {
          "title" : "List of accepted authorized parties",
```

```

    "description" : "A list of case sensitive strings which can be either string or URI
values<br><br>A list of authorized parties which this module will accept ID tokens from. This will be
checked against the authorized party claim of the ID token.",
    "propertyOrder" : 800,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"idTokenHeaderName" : {
    "title" : "Name of header referencing the ID Token",
    "description" : "",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"cryptoContextType" : {
    "title" : "OpenID Connect validation configuration type",
    "description" : "Please select either 1. the issuer discovery url, 2. the issuer jwk url, or
3. the client_secret.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"clientSecret" : {
    "title" : "Client Secret",
    "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
    "propertyOrder" : 301,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
},
"jwtToLdapAttributeMappings" : {
    "title" : "Mapping of jwt attributes to local LDAP attributes",
    "description" : "Format: jwt_attribute=local_ldap_attribute<br><br>Mappings allow jwt
entries to drive principal lookup. This entry determines how to translate between local LDAP
attributes and the entries in the jwt. See <a href=\"http://openid.net/specs/openid-connect-
core-1_0.html#ScopeClaims\" target=\"_blank\">OpenID Connect Core 1.0 Specification</a> section 5.4 on
how to request the inclusion of additional attributes in issued ID Tokens.",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"cryptoContextValue" : {
    "title" : "OpenID Connect validation configuration value",
    "description" : "The discovery url, or jwk url, or the client_secret, corresponding to the
selection above.<br><br>If discovery or jwk url entered, entry must be in valid url format, <br>e.g.

```

```
https://accounts.google.com/.well-known/openid-configuration<br/><i>NB </i>If client_secret entered,
entry is ignored and the value of the Client Secret is used.",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"audienceName" : {
  "title" : "Audience name",
  "description" : "A case sensitive string<br/><br>The audience name for this OpenID Conenct
module. This will be used to check that the ID token received is intended for this module as an
audience.",
  "propertyOrder" : 700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"idTokenIssuer" : {
  "title" : "Name of OpenID Connect ID Token Issuer",
  "description" : "Value must match the iss field in issued ID Token",
  "propertyOrder" : 500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
},
"type" : "object",
"title" : "Realm Defaults"
}
}
```

## 1.87. PendingUmaRequests

### 1.87.1. Realm Operations

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

Resource path: `/users/{user}/uma/pendingrequests`

Resource version: `1.0`

#### 1.87.1.1. approve

Approve the pending request and grant access to the requesting user.

Usage:

```
am> action PendingUmaRequests --realm Realm --id id --body body --user user --actionName approve
```



Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Approve action request schema.",
  "type" : "object",
  "title" : "Approve action request schema",
  "properties" : {
    "scopes" : {
      "type" : "array",
      "title" : "Approve request scopes",
      "description" : "The list of the scopes the requesting user gets access to.",
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "scopes" ]
}
```

**--user**

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

### 1.87.1.2. approveAll

Approve every pending requests and grant access to the requesting user.

Usage:

```
am> action PendingUmaRequests --realm Realm --body body --user user --actionName approveAll
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Approve action request schema.",
  "type" : "object",
  "title" : "Approve action request schema",
  "properties" : {
    "scopes" : {
      "type" : "array",
      "title" : "Approve request scopes",
      "description" : "The list of the scopes the requesting user gets access to.",
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "scopes" ]
}
```

**--user**

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

### 1.87.1.3. query

Query the collection of pending requests.

Usage:

```
am> query PendingUmaRequests --realm Realm --filter filter --user user
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

**--user**

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

### 1.87.1.4. read

Read pending request

Usage:

```
am> read PendingUmaRequests --realm Realm --id id --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--user**

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

## 1.88. PersistentCookieModule

### 1.88.1. Realm Operations

Resource path: `/realm-config/authentication/modules/persistentcookie`

Resource version: `1.0`

#### 1.88.1.1. create

Usage:

```
am> create PersistentCookieModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "useHttpOnlyCookie" : {
      "title" : "Use HTTP only cookie",
      "description" : "Sets the persistent cookie as \"HttpOnly\"",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "enforceClientIP" : {
      "title" : "Enforce Client IP",
      "description" : "Enforces that the persistent cookie can only be used from the same client IP to which the cookie was issued.",
      "propertyOrder" : 300,
      "required" : true,

```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "useSecureCookie" : {
        "title" : "Use secure cookie",
        "description" : "Sets the persistent cookie as \"Secure\"",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "hmacKey" : {
        "title" : "HMAC Signing Key",
        "description" : "Base64-encoded 256-bit key to use for HMAC signing of the cookie.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "maxLife" : {
        "title" : "Max Life",
        "description" : "The maximum length of time the persistent cookie is valid for, in hours.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "idleTimeout" : {
        "title" : "Idle Timeout",
        "description" : "The maximum idle time between requests before the cookie is invalidated, in
hours.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
}
}

```

### 1.88.1.2. delete

Usage:

```
am> delete PersistentCookieModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.88.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PersistentCookieModule --realm Realm --actionName getAllTypes
```

#### 1.88.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PersistentCookieModule --realm Realm --actionName getCreatableTypes
```

#### 1.88.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PersistentCookieModule --realm Realm --actionName nextdescendents
```

#### 1.88.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query PersistentCookieModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.88.1.7. read

Usage:

```
am> read PersistentCookieModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.88.1.8. update

Usage:

```
am> update PersistentCookieModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "useHttpOnlyCookie" : {
      "title" : "Use HTTP only cookie",
      "description" : "Sets the persistent cookie as \"HttpOnly\"",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "enforceClientIP" : {
      "title" : "Enforce Client IP",
      "description" : "Enforces that the persistent cookie can only be used from the same client IP to
which the cookie was issued.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "useSecureCookie" : {
      "title" : "Use secure cookie",
      "description" : "Sets the persistent cookie as \"Secure\"",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "hmacKey" : {
      "title" : "HMAC Signing Key",
      "description" : "Base64-encoded 256-bit key to use for HMAC signing of the cookie.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "maxLife" : {
      "title" : "Max Life",
      "description" : "The maximum length of time the persistent cookie is valid for, in hours.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "idleTimeout" : {
      "title" : "Idle Timeout",
```

```
    "description" : "The maximum idle time between requests before the cookie is invalidated, in  
    hours.",  
    "propertyOrder" : 100,  
    "required" : true,  
    "type" : "integer",  
    "exampleValue" : ""  
  }  
}
```

## 1.88.2. Global Operations

Resource path: `/global-config/authentication/modules/persistentcookie`

Resource version: `1.0`

### 1.88.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PersistentCookieModule --global --actionName getAllTypes
```

### 1.88.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PersistentCookieModule --global --actionName getCreatableTypes
```

### 1.88.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PersistentCookieModule --global --actionName nextdescendents
```

### 1.88.2.4. read

Usage:

```
am> read PersistentCookieModule --global
```

### 1.88.2.5. update

## Usage:

```
am> update PersistentCookieModule --global --body body
```

## Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "idleTimeout" : {
          "title" : "Idle Timeout",
          "description" : "The maximum idle time between requests before the cookie is invalidated, in
hours.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxLife" : {
          "title" : "Max Life",
          "description" : "The maximum length of time the persistent cookie is valid for, in hours.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "enforceClientIP" : {
          "title" : "Enforce Client IP",
          "description" : "Enforces that the persistent cookie can only be used from the same client
IP to which the cookie was issued.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "useSecureCookie" : {
          "title" : "Use secure cookie",
          "description" : "Sets the persistent cookie as \"Secure\"",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "useHttpOnlyCookie" : {
          "title" : "Use HTTP only cookie",
          "description" : "Sets the persistent cookie as \"HttpOnly\"",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "hmacKey" : {
          "title" : "HMAC Signing Key",
```



```
    "description" : "Base64-encoded 256-bit key to use for HMAC signing of the cookie.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
```

## 1.89. Platform

### 1.89.1. Global Operations

Resource path: `/global-config/services/platform`

Resource version: `1.0`

#### 1.89.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Platform --global --actionName getAllTypes
```

#### 1.89.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Platform --global --actionName getCreatableTypes
```

#### 1.89.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Platform --global --actionName nextdescendents
```

#### 1.89.1.4. read

Usage:

```
am> read Platform --global
```

## 1.89.1.5. update

Usage:

```
am> update Platform --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cookieDomains" : {
      "title" : "Cookie Domains",
      "description" : "Set the list of domains into which OpenAM writes cookies.<br><br>If you set multiple cookie domains, OpenAM still only sets the cookie in the domain the client uses to access OpenAM. If this property is left blank, then the fully qualified domain name of the server is used to set the cookie domain, meaning that a host cookie rather than a domain cookie is set.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "locale" : {
      "title" : "Platform Locale",
      "description" : "Set the fallback locale used when the user locale cannot be determined.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.90. Policies

### 1.90.1. Realm Operations

The Policy resource with copy and move support endpoint is responsible for managing policies. It supports all the operations that previous version of Policy resource endpoint supports - create, read, update, delete, query, evalute and evaluateTree action - with two new actions move and copy for copying and moving policies between realms

Resource path: `/policies`

Resource version: `2.1`

### 1.90.1.1. copy

Copy a list of policies

Usage:

```
am> action Policies --realm Realm --body body --actionName copy
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Policy copy action schema",
  "type" : "object",
  "title" : "Policy copy action schema",
  "properties" : {
    "from" : {
      "title" : "Copy/move from",
      "description" : "Policy copy/move origin parameters",
      "type" : "object",
      "properties" : {
        "application" : {
          "title" : "Application",
          "description" : "The policy set in which the input policies are located",
          "type" : "string"
        }
      },
      "required" : [ "application" ]
    },
    "to" : {
      "type" : "object",
      "title" : "Copy/Move To",
      "description" : "Policy copy/move destination parameters",
      "properties" : {
        "application" : {
          "title" : "Application",
          "description" : "The policy set in which to place the output policy. Required when copying or moving a policy to a different policy set.",
          "type" : "string"
        },
        "realm" : {
          "title" : "Realm",
          "description" : "The realm in which to place the output policy. If not specified, OpenAM copies or moves the policy within the realm identified in the URL. Required when copying or moving a policy to a different realm.",
          "type" : "string"
        },
        "namePostfix" : {
          "title" : "Name postfix",
          "description" : "A value appended to output policy names in order to prevent name clashes",

```

```

        "type" : "string"
      }
    },
    "required" : [ "namePostfix" ]
  },
  "resourceTypeMapping" : {
    "title" : "Resource type mapping",
    "description" : "One or more resource types mappings, where the left side of the mapping
specifies the UUID of a resource type used by the input policies and the right side of the mapping
specifies the UUID of a resource type used by the output policies. The two resource types should have
the same resource patterns",
    "type" : "object",
    "additionalProperties" : {
      "type" : "string"
    }
  }
},
"required" : [ "from", "to" ]
}

```

### 1.90.1.2. create

Create new policy

Usage:

```
am> create Policies --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```

{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Json schema for the policy resource",
  "title" : "Policy Resource Schema",
  "type" : "object",
  "properties" : {
    "name" : {
      "title" : "Name",
      "description" : "String matching the name of the application",
      "type" : "string"
    },
    "active" : {
      "title" : "Active flag",
      "description" : "Boolean indicating whether OpenAM considers the policy active for evaluation
purposes, defaults to false",
      "type" : "boolean"
    },
    "description" : {
      "title" : "Description",
      "description" : "String describing the policy",

```

```

    "type" : "string"
  },
  "applicationName" : {
    "title" : "Application name",
    "description" : "String containing the application name, such as \"iPlanetAMWebAgentService\",
or \"mypolicyset\"",
    "type" : "string"
  },
  "actionValues" : {
    "title" : "Action values",
    "description" : "Set of string action names, each set to a boolean indicating whether the action
is allowed. Chosen from the available actions provided by the associated Managing Resource Types
resource type",
    "type" : "object",
    "additionalProperties" : {
      "type" : "boolean"
    }
  },
  "resources" : {
    "title" : "Resources",
    "description" : "List of the resource name pattern strings to which the policy applies. Must
conform to the pattern templates provided by the associated Managing Resource Types resource type",
    "type" : "array",
    "items" : {
      "type" : "string"
    }
  },
  "subject" : {
    "title" : "Subject",
    "description" : "Specifies the subject conditions to which the policy applies, where subjects
can be combined by using the built-in types \"AND\", \"OR\", and \"NOT\", and where subject
implementations are pluggable",
    "type" : "object"
  },
  "condition" : {
    "title" : "Condition",
    "description" : "Specifies environment conditions, where conditions can be combined by using the
built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
    "type" : "object",
    "properties" : {
      "type" : {
        "type" : "string"
      },
      "conditions" : {
        "type" : "array",
        "title" : "Condition",
        "description" : "Specifies environment conditions, where conditions can be combined by using
the built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
        "items" : {
          "type" : "object"
        }
      }
    }
  },
  "resourceTypeUuid" : {
    "title" : "Resource Type UUID",
    "description" : "The UUIDs of the resource type associated with the policy",
    "type" : "string"
  },

```

```
"resourceAttributes" : {
  "title" : "Resource Attributes",
  "description" : "List of attributes to return with decisions. These attributes are known as
response attributes",
  "type" : "array",
  "items" : {
    "type" : "object"
  }
},
"lastModifiedBy" : {
  "title" : "Last Modified By",
  "description" : "A string containing the universal identifier DN of the subject that most
recently updated the policy",
  "type" : "string"
},
"lastModifiedDate" : {
  "title" : "Last Modified date",
  "description" : "An integer containing the last modified date and time, in number of seconds",
  "type" : "string"
},
"createdBy" : {
  "title" : "Created By",
  "description" : "A string containing the universal identifier DN of the subject that created the
policy",
  "type" : "string"
},
"creationDate" : {
  "title" : "Creation Date",
  "description" : "An integer containing the creation date and time, in number of seconds",
  "type" : "string"
}
}
```

### 1.90.1.3. delete

Delete policy

Usage:

```
am> delete Policies --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.90.1.4. evaluate

Request policy decisions for specific resources

Usage:

```
am> action Policies --realm Realm --body body --actionName evaluate
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Evaluate action schema",
  "title" : "Evaluate action schema",
  "type" : "object",
  "properties" : {
    "resources" : {
      "type" : "array",
      "title" : "Resources",
      "description" : "Specifies the list of resources for which to return decisions",
      "items" : {
        "type" : "string"
      }
    },
    "application" : {
      "title" : "Application",
      "description" : "Holds the name of the application, and defaults to \"iPlanetAMWebAgentService\" if not specified",
      "type" : "string"
    },
    "subject" : {
      "title" : "Subject",
      "description" : "Holds an object that represents the subject. You can specify one or more of the following keys. If you specify multiple keys, the subject can have multiple associated principals, and you can use subject conditions corresponding to any type in the request",
      "type" : "object",
      "properties" : {
        "ssoToken" : {
          "title" : "SSOToken",
          "description" : "The value is the SSO token ID string for the subject",
          "type" : "string"
        },
        "jwt" : {
          "title" : "JWT",
          "description" : "The value is a JWT string",
          "type" : "string"
        },
        "claims" : {
          "title" : "Claims",
          "description" : "The value is an object (map) of JWT claims to their values.",
          "type" : "object",
          "additionalProperties" : {
            "type" : "string"
          }
        }
      }
    },
    "environment" : {
      "title" : "Environment",
      "description" : "Holds a map of keys to lists of values",
      "type" : "object",
      "additionalProperties" : {
        "type" : "array",

```

```
    "items" : {
      "type" : "string"
    }
  },
  "required" : [ "resources", "application" ]
}
```

### 1.90.1.5. evaluateTree

Request policy decisions for a tree of resources

Usage:

```
am> action Policies --realm Realm --body body --actionName evaluateTree
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Evaluate tree action schema",
  "title" : "Evaluate tree action schema",
  "type" : "object",
  "properties" : {
    "resource" : {
      "title" : "Resource",
      "description" : "Specifies the root resource for the decisions to return",
      "type" : "string"
    },
    "application" : {
      "title" : "Application",
      "description" : "Holds the name of the application, and defaults to \"iPlanetAMWebAgentService\" if not specified",
      "type" : "string"
    },
    "subject" : {
      "title" : "Subject",
      "description" : "Holds an object that represents the subject. You can specify one or more of the following keys. If you specify multiple keys, the subject can have multiple associated principals, and you can use subject conditions corresponding to any type in the request",
      "type" : "object",
      "properties" : {
        "ssoToken" : {
          "title" : "SSOToken",
          "description" : "The value is the SSO token ID string for the subject",
          "type" : "string"
        },
        "jwt" : {
          "title" : "JWT",
          "description" : "The value is a JWT string",
          "type" : "string"
        }
      }
    }
  }
}
```



```

    },
    "claims" : {
      "title" : "Claims",
      "description" : "The value is an object (map) of JWT claims to their values.",
      "type" : "object",
      "additionalProperties" : {
        "type" : "string"
      }
    }
  },
  "environment" : {
    "title" : "Environment",
    "description" : "Holds a map of keys to lists of values",
    "type" : "object",
    "additionalProperties" : {
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    }
  }
},
"required" : [ "resources", "application" ]
}

```

### 1.90.1.6. move

Move a list of policies

Usage:

```
am> action Policies --realm Realm --body body --actionName move
```

Parameters:

#### --body

The resource in JSON format, described by the following JSON schema:

```

{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Policy copy action schema",
  "type" : "object",
  "title" : "Policy copy action schema",
  "properties" : {
    "from" : {
      "title" : "Copy/move from",
      "description" : "Policy copy/move origin parameters",
      "type" : "object",
      "properties" : {
        "application" : {
          "title" : "Application",
          "description" : "The policy set in which the input policies are located",
          "type" : "string"
        }
      }
    }
  }
},

```

```

    "required" : [ "application" ]
  },
  "to" : {
    "type" : "object",
    "title" : "Copy/Move To",
    "description" : "Policy copy/move destination parameters",
    "properties" : {
      "application" : {
        "title" : "Application",
        "description" : "The policy set in which to place the output policy. Required when copying
or moving a policy to a different policy set.",
        "type" : "string"
      },
      "realm" : {
        "title" : "Realm",
        "description" : "The realm in which to place the output policy. If not specified, OpenAM
copies or moves the policy within the realm identified in the URL. Required when copying or moving a
policy to a different realm.",
        "type" : "string"
      },
      "namePostfix" : {
        "title" : "Name postfix",
        "description" : "A value appended to output policy names in order to prevent name clashes",
        "type" : "string"
      }
    }
  },
  "required" : [ "namePostfix" ]
},
"resourceTypeMapping" : {
  "title" : "Resource type mapping",
  "description" : "One or more resource types mappings, where the left side of the mapping
specifies the UUID of a resource type used by the input policies and the right side of the mapping
specifies the UUID of a resource type used by the output policies. The two resource types should have
the same resource patterns",
  "type" : "object",
  "additionalProperties" : {
    "type" : "string"
  }
}
},
"required" : [ "from", "to" ]
}

```

### 1.90.1.7. query

Query the stored policies

Usage:

```
am> query Policies --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

### 1.90.1.8. read

Read policy

Usage:

```
am> read Policies --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.90.1.9. update

Update an existing policy

Usage:

```
am> update Policies --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Json schema for the policy resource",
  "title" : "Policy Resource Schema",
  "type" : "object",
  "properties" : {
    "name" : {
      "title" : "Name",
      "description" : "String matching the name of the application",
      "type" : "string"
    },
    "active" : {
      "title" : "Active flag",
      "description" : "Boolean indicating whether OpenAM considers the policy active for evaluation purposes, defaults to false",
      "type" : "boolean"
    },
    "description" : {
      "title" : "Description",
      "description" : "String describing the policy",
      "type" : "string"
    },
    "applicationName" : {
      "title" : "Application name",
      "description" : "String containing the application name, such as \"iPlanetAMWebAgentService\", or \"mypolicyset\"",

```

```

    "type" : "string"
  },
  "actionValues" : {
    "title" : "Action values",
    "description" : "Set of string action names, each set to a boolean indicating whether the action
is allowed. Chosen from the available actions provided by the associated Managing Resource Types
resource type",
    "type" : "object",
    "additionalProperties" : {
      "type" : "boolean"
    }
  },
  "resources" : {
    "title" : "Resources",
    "description" : "List of the resource name pattern strings to which the policy applies. Must
conform to the pattern templates provided by the associated Managing Resource Types resource type",
    "type" : "array",
    "items" : {
      "type" : "string"
    }
  },
  "subject" : {
    "title" : "Subject",
    "description" : "Specifies the subject conditions to which the policy applies, where subjects
can be combined by using the built-in types \"AND\", \"OR\", and \"NOT\", and where subject
implementations are pluggable",
    "type" : "object"
  },
  "condition" : {
    "title" : "Condition",
    "description" : "Specifies environment conditions, where conditions can be combined by using the
built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
    "type" : "object",
    "properties" : {
      "type" : {
        "type" : "string"
      },
      "conditions" : {
        "type" : "array",
        "title" : "Condition",
        "description" : "Specifies environment conditions, where conditions can be combined by using
the built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
        "items" : {
          "type" : "object"
        }
      }
    }
  },
  "resourceTypeUuid" : {
    "title" : "Resource Type UUID",
    "description" : "The UUIDs of the resource type associated with the policy",
    "type" : "string"
  },
  "resourceAttributes" : {
    "title" : "Resource Attributes",
    "description" : "List of attributes to return with decisions. These attributes are known as
response attributes",
    "type" : "array",
    "items" : {

```

```
    "type" : "object"
  }
},
"lastModifiedBy" : {
  "title" : "Last Modified By",
  "description" : "A string containing the universal identifier DN of the subject that most recently updated the policy",
  "type" : "string"
},
"lastModifiedDate" : {
  "title" : "Last Modified date",
  "description" : "An integer containing the last modified date and time, in number of seconds",
  "type" : "string"
},
"createdBy" : {
  "title" : "Created By",
  "description" : "A string containing the universal identifier DN of the subject that created the policy",
  "type" : "string"
},
"creationDate" : {
  "title" : "Creation Date",
  "description" : "An integer containing the creation date and time, in number of seconds",
  "type" : "string"
}
}
```

## 1.91. PolicyAgents

### 1.91.1. Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/2.2_Agent`

Resource version: `1.0`

#### 1.91.1.1. create

Usage:

```
am> create PolicyAgents --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cdssoRootUrl" : {
      "title" : "Agent Key Value(s)",
      "description" : "Set the agent properties with a key/value pair. This property is used
by OpenAM to receive agent requests for credential assertions about users. Currently, only
one property is valid and all other properties will be ignored. Use the following format: <br>
agentRootURL=protocol://hostname:port/ <br> The entry must be precise and agentRootURL is case
sensitive.",
      "propertyOrder" : 22500,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "description" : {
      "title" : "Description",
      "description" : "",
      "propertyOrder" : 22400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

### 1.91.1.2. delete

Usage:

```
am> delete PolicyAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.91.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PolicyAgents --realm Realm --actionName getAllTypes
```

### 1.91.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PolicyAgents --realm Realm --actionName getCreatableTypes
```

### 1.91.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PolicyAgents --realm Realm --actionName nextdescendents
```

### 1.91.1.6. query

Querying the agents of a specific type

Usage:

```
am> query PolicyAgents --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.91.1.7. read

Usage:

```
am> read PolicyAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.91.1.8. update

Usage:

```
am> update PolicyAgents --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cdssoRootUrl" : {
      "title" : "Agent Key Value(s)",
      "description" : "Set the agent properties with a key/value pair. This property is used
by OpenAM to receive agent requests for credential assertions about users. Currently, only
one property is valid and all other properties will be ignored. Use the following format: <br>
agentRootURL=protocol://hostname:port/ <br> The entry must be precise and agentRootURL is case
sensitive.",
      "propertyOrder" : 22500,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "description" : {
      "title" : "Description",
      "description" : "",
      "propertyOrder" : 22400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",

```



```
    "propertyOrder" : 100,  
    "required" : true,  
    "type" : "string",  
    "format" : "password",  
    "exampleValue" : ""  
  }  
}  
}
```

## 1.92. PolicyConfiguration

### 1.92.1. Realm Operations

Resource path: `/realm-config/services/policyconfiguration`

Resource version: `1.0`

#### 1.92.1.1. create

Usage:

```
am> create PolicyConfiguration --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "type" : "object",  
  "properties" : {  
    "bindDn" : {  
      "title" : "LDAP Bind DN",  
      "description" : "Bind DN to connect to the directory server for policy information.",  
      "propertyOrder" : 700,  
      "required" : true,  
      "type" : "string",  
      "exampleValue" : ""  
    },  
    "connectionPoolMinimumSize" : {  
      "title" : "LDAP Connection Pool Minimum Size",  
      "description" : "Minimum number of connections in the pool.",  
      "propertyOrder" : 1700,  
      "required" : true,  
      "type" : "integer",  
      "exampleValue" : ""  
    },  
    "rolesSearchScope" : {  
      "title" : "OpenAM Roles Search Scope",  
      "description" : "Search scope to find OpenAM roles entries.",  
      "propertyOrder" : 1200,  
      "required" : true,  
      "type" : "string",  
      "exampleValue" : ""  
    }  
  }  
}
```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "usersSearchAttribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "Naming attribute for user entries.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ldapServer" : {
    "title" : "Primary LDAP Server",
    "description" : "Configuration directory server host:port that OpenAM searches for policy
information.<p><p>Format: <code>local server name | host name:port</code><p><p>Multiple entries must
be prefixed by local server name.",
    "propertyOrder" : 400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userAliasEnabled" : {
    "title" : "User Alias",
    "description" : "If enabled, OpenAM can evaluate policy for remote users aliased to local
users.",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "connectionPoolMaximumSize" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "Maximum number of connections in the pool.",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "usersBaseDn" : {
    "title" : "LDAP Users Base DN",
    "description" : "Base DN for LDAP Users subject searches.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "bindPassword" : {
    "title" : "LDAP Bind Password",
    "description" : "Bind password to connect to the directory server for policy information.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
},

```

```

"rolesBaseDn" : {
  "title" : "OpenAM Roles Base DN",
  "description" : "Base DN for OpenAM Roles searches.",
  "propertyOrder" : 600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"realmSearchFilter" : {
  "title" : "LDAP Organization Search Filter",
  "description" : "Search filter to match organization entries.",
  "propertyOrder" : 900,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sslEnabled" : {
  "title" : "LDAP SSL/TLS",
  "description" : "If enabled, OpenAM connects securely to the directory server. This requires
that you install the directory server certificate.",
  "propertyOrder" : 1600,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"usersSearchFilter" : {
  "title" : "LDAP Users Search Filter",
  "description" : "Search filter to match user entries.",
  "propertyOrder" : 1000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"usersSearchScope" : {
  "title" : "LDAP Users Search Scope",
  "description" : "Search scope to find user entries.",
  "propertyOrder" : 1100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"searchTimeout" : {
  "title" : "Search Timeout",
  "description" : "Time after which OpenAM returns an error for an incomplete search, in
seconds.",
  "propertyOrder" : 1500,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"maximumSearchResults" : {
  "title" : "Maximum Results Returned from Search",
  "description" : "Search limit for LDAP searches.",
  "propertyOrder" : 1400,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"subjectsResultTTL" : {

```

```
    "title" : "Subjects Result Time to Live",
    "description" : "Maximum time that OpenAM caches a subject result for evaluating policy
requests, in minutes. A value of <code>0</code> prevents OpenAM from caching subject evaluations for
policy decisions.",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }
}
```

### 1.92.1.2. delete

Usage:

```
am> delete PolicyConfiguration --realm Realm
```

### 1.92.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PolicyConfiguration --realm Realm --actionName getAllTypes
```

### 1.92.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PolicyConfiguration --realm Realm --actionName getCreatableTypes
```

### 1.92.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PolicyConfiguration --realm Realm --actionName nextdescendents
```

### 1.92.1.6. read

Usage:

```
am> read PolicyConfiguration --realm Realm
```

## 1.92.1.7. update

Usage:

```
am> update PolicyConfiguration --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "bindDn" : {
      "title" : "LDAP Bind DN",
      "description" : "Bind DN to connect to the directory server for policy information.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "connectionPoolMinimumSize" : {
      "title" : "LDAP Connection Pool Minimum Size",
      "description" : "Minimum number of connections in the pool.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "rolesSearchScope" : {
      "title" : "OpenAM Roles Search Scope",
      "description" : "Search scope to find OpenAM roles entries.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "usersSearchAttribute" : {
      "title" : "LDAP Users Search Attribute",
      "description" : "Naming attribute for user entries.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ldapServer" : {
      "title" : "Primary LDAP Server",
      "description" : "Configuration directory server host:port that OpenAM searches for policy information.<p><p>Format: <code>local server name | host name:port</code><p><p>Multiple entries must be prefixed by local server name.",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",

```

```

    "exampleValue" : ""
  },
  "userAliasEnabled" : {
    "title" : "User Alias",
    "description" : "If enabled, OpenAM can evaluate policy for remote users aliased to local users.",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "connectionPoolMaximumSize" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "Maximum number of connections in the pool.",
    "propertyOrder" : 1800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "usersBaseDn" : {
    "title" : "LDAP Users Base DN",
    "description" : "Base DN for LDAP Users subject searches.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "bindPassword" : {
    "title" : "LDAP Bind Password",
    "description" : "Bind password to connect to the directory server for policy information.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "rolesBaseDn" : {
    "title" : "OpenAM Roles Base DN",
    "description" : "Base DN for OpenAM Roles searches.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "realmSearchFilter" : {
    "title" : "LDAP Organization Search Filter",
    "description" : "Search filter to match organization entries.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sslEnabled" : {
    "title" : "LDAP SSL/TLS",
    "description" : "If enabled, OpenAM connects securely to the directory server. This requires that you install the directory server certificate.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "usersSearchFilter" : {
    "title" : "LDAP Users Search Filter",
    "description" : "Search filter to match user entries.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "usersSearchScope" : {
    "title" : "LDAP Users Search Scope",
    "description" : "Search scope to find user entries.",
    "propertyOrder" : 1100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "searchTimeout" : {
    "title" : "Search Timeout",
    "description" : "Time after which OpenAM returns an error for an incomplete search, in
seconds.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "maximumSearchResults" : {
    "title" : "Maximum Results Returned from Search",
    "description" : "Search limit for LDAP searches.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "subjectsResultTTL" : {
    "title" : "Subjects Result Time to Live",
    "description" : "Maximum time that OpenAM caches a subject result for evaluating policy
requests, in minutes. A value of <code>0</code> prevents OpenAM from caching subject evaluations for
policy decisions.",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }
}
}

```

## 1.92.2. Global Operations

Resource path: </global-config/services/policyconfiguration>

Resource version: [1.0](#)

### 1.92.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PolicyConfiguration --global --actionName getAllTypes
```

### 1.92.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PolicyConfiguration --global --actionName getCreatableTypes
```

### 1.92.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PolicyConfiguration --global --actionName nextdescendents
```

### 1.92.2.4. read

Usage:

```
am> read PolicyConfiguration --global
```

### 1.92.2.5. update

Usage:

```
am> update PolicyConfiguration --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "resourceComparators" : {
      "title" : "Resource Comparator",
      "description" : "OpenAM uses resource comparators to match resources specified in policy rules.
When setting comparators on the command line, separate fields with <code>|</code> characters.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
```



```

    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"realmAliasReferrals" : {
  "title" : "Realm Alias Referrals",
  "description" : "If yes, then OpenAM allows creation of policies for HTTP and HTTPS resources
whose FQDN matches the DNS alias for the realm even when no referral policy exists.",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"continueEvaluationOnDeny" : {
  "title" : "Continue Evaluation on Deny Decision",
  "description" : "If no, then OpenAM stops evaluating policy as soon as it reaches a deny
decision.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"defaults" : {
  "properties" : {
    "usersSearchFilter" : {
      "title" : "LDAP Users Search Filter",
      "description" : "Search filter to match user entries.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "rolesBaseDn" : {
      "title" : "OpenAM Roles Base DN",
      "description" : "Base DN for OpenAM Roles searches.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ldapServer" : {
      "title" : "Primary LDAP Server",
      "description" : "Configuration directory server host:port that OpenAM searches for policy
information.<p><p>Format: <code>local server name | host name:port</code><p><p>Multiple entries must
be prefixed by local server name.",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "connectionPoolMinimumSize" : {
      "title" : "LDAP Connection Pool Minimum Size",
      "description" : "Minimum number of connections in the pool.",
      "propertyOrder" : 1700,
      "required" : true,

```

```

    "type" : "integer",
    "exampleValue" : ""
  },
  "realmSearchFilter" : {
    "title" : "LDAP Organization Search Filter",
    "description" : "Search filter to match organization entries.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "usersSearchAttribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "Naming attribute for user entries.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "subjectsResultTTL" : {
    "title" : "Subjects Result Time to Live",
    "description" : "Maximum time that OpenAM caches a subject result for evaluating policy
requests, in minutes. A value of <code>0</code> prevents OpenAM from caching subject evaluations for
policy decisions.",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "searchTimeout" : {
    "title" : "Search Timeout",
    "description" : "Time after which OpenAM returns an error for an incomplete search, in
seconds.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "userAliasEnabled" : {
    "title" : "User Alias",
    "description" : "If enabled, OpenAM can evaluate policy for remote users aliased to local
users.",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "bindPassword" : {
    "title" : "LDAP Bind Password",
    "description" : "Bind password to connect to the directory server for policy information.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "usersBaseDn" : {
    "title" : "LDAP Users Base DN",
    "description" : "Base DN for LDAP Users subject searches.",

```

```

        "propertyOrder" : 500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "rolesSearchScope" : {
        "title" : "OpenAM Roles Search Scope",
        "description" : "Search scope to find OpenAM roles entries.",
        "propertyOrder" : 1200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "connectionPoolMaximumSize" : {
        "title" : "LDAP Connection Pool Maximum Size",
        "description" : "Maximum number of connections in the pool.",
        "propertyOrder" : 1800,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "sslEnabled" : {
        "title" : "LDAP SSL/TLS",
        "description" : "If enabled, OpenAM connects securely to the directory server. This requires
that you install the directory server certificate.",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "maximumSearchResults" : {
        "title" : "Maximum Results Returned from Search",
        "description" : "Search limit for LDAP searches.",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "usersSearchScope" : {
        "title" : "LDAP Users Search Scope",
        "description" : "Search scope to find user entries.",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "bindDn" : {
        "title" : "LDAP Bind DN",
        "description" : "Bind DN to connect to the directory server for policy information.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"type" : "object",
"title" : "Realm Defaults"
}
}

```

```
}
```

## 1.93. PushAuthenticationUserDevices

### 1.93.1. Realm Operations

The push authentication user devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

Resource path: `/users/{user}/devices/push`

Resource version: `1.0`

#### 1.93.1.1. delete

Delete push user authentication device

Usage:

```
am> delete PushAuthenticationUserDevices --realm Realm --id id --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--user**

The push authentication user devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

#### 1.93.1.2. query

Query the user's device profile

Usage:

```
am> query PushAuthenticationUserDevices --realm Realm --filter filter --user user
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: `[*]`

**--user**

The push authentication user devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

### 1.93.1.3. resetPushDevice

Query the user's device profile

Usage:

```
am> action PushAuthenticationUserDevices --realm Realm --user user --actionName resetPushDevice
```

Parameters:

#### --user

The push authentication user devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

## 1.94. PushNotification

### 1.94.1. Realm Operations

Resource path: `/realm-config/services/pushNotification`

Resource version: `1.0`

#### 1.94.1.1. create

Usage:

```
am> create PushNotification --realm Realm --body body
```

Parameters:

#### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accessKey" : {
      "title" : "SNS Access Key ID",
      "description" : "Amazon Simple Notification Service Access Key ID. For more information, see https://aws.amazon.com/developers/access-keys/.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "AKIAIOSFODNN7EXAMPLE"
    },
    "mdConcurrency" : {
      "title" : "Response Cache Concurrency",
```

```

    "description" : "Level of concurrency to use when accessing the message dispatcher cache. Defaults to 16, and must be greater than 0. Choose a value to accommodate as many threads as will ever concurrently access the message dispatcher cache.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "mdDuration" : {
    "title" : "Response Cache Duration",
    "description" : "The minimum lifetime to keep unanswered message records in the message dispatcher cache, in seconds. To keep unanswered message records indefinitely, set this property to 0. Should be tuned so that it is applicable to the use case of this service. For example, the ForgeRock Authenticator (Push) authentication module has a default timeout of 120 seconds.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "mdCacheSize" : {
    "title" : "Response Cache Size",
    "description" : "Maximum size of the message dispatcher cache, in number of records. If set to 0 the cache can grow indefinitely. If the number of records that need to be stored exceeds this maximum, then older items in the cache will be removed to make space.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "delegateFactory" : {
    "title" : "Message Transport Delegate Factory",
    "description" : "The fully qualified class name of the factory responsible for creating the PushNotificationDelegate. The class must implement org.forgerock.openam.services.push.PushNotificationDelegate.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "googleEndpoint" : {
    "title" : "SNS Endpoint for GCM",
    "description" : "The Simple Notification Service endpoint in Amazon Resource Name format, used to send push messages over Google Cloud Messaging (GCM).",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/GCM/production"
  },
  "region" : {
    "title" : "SNS Client Region",
    "description" : "Region of your registered Amazon Simple Notification Service client. For more information, see https://docs.aws.amazon.com/general/latest/gr/rande.html.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "secret" : {

```

```
    "title" : "SNS Access Key Secret",
    "description" : "Amazon Simple Notification Service Access Key Secret. For more information, see
    <a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/access-
    keys/</a>.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
  },
  "appleEndpoint" : {
    "title" : "SNS Endpoint for APNS",
    "description" : "The Simple Notification Service endpoint in Amazon Resource Name format, used
    to send push messages to the Apple Push Notification Service (APNS).",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/APNS/production"
  }
}
```

#### 1.94.1.2. delete

Usage:

```
am> delete PushNotification --realm Realm
```

#### 1.94.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PushNotification --realm Realm --actionName getAllTypes
```

#### 1.94.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PushNotification --realm Realm --actionName getCreatableTypes
```

#### 1.94.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PushNotification --realm Realm --actionName nextdescendents
```

## 1.94.1.6. read

Usage:

```
am> read PushNotification --realm Realm
```

## 1.94.1.7. update

Usage:

```
am> update PushNotification --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accessKey" : {
      "title" : "SNS Access Key ID",
      "description" : "Amazon Simple Notification Service Access Key ID. For more information, see
<a href='\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/access-
keys/</a>.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "AKIAIOSFODNN7EXAMPLE"
    },
    "mdConcurrency" : {
      "title" : "Response Cache Concurrency",
      "description" : "Level of concurrency to use when accessing the message dispatcher cache.
Defaults to <code>16</code>, and must be greater than <code>0</code>. Choose a value to accommodate
as many threads as will ever concurrently access the message dispatcher cache.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "mdDuration" : {
      "title" : "Response Cache Duration",
      "description" : "The minimum lifetime to keep unanswered message records in the message
dispatcher cache, in seconds. To keep unanswered message records indefinitely, set this property to
<code>0</code>.Should be tuned so that it is applicable to the use case of this service. For example,
the ForgeRock Authenticator (Push) authentication module has a default timeout of 120 seconds.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "mdCacheSize" : {
      "title" : "Response Cache Size",
```



```

        "description" : "Maximum size of the message dispatcher cache, in number of records. If set
to <code>0</code> the cache can grow indefinitely. If the number of records that need to be stored
exceeds this maximum, then older items in the cache will be removed to make space.",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "delegateFactory" : {
        "title" : "Message Transport Delegate Factory",
        "description" : "The fully qualified class name of the factory
responsible for creating the PushNotificationDelegate. The class must implement
<code>org.forgerock.openam.services.push.PushNotificationDelegate</code>.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "googleEndpoint" : {
        "title" : "SNS Endpoint for GCM",
        "description" : "The Simple Notification Service endpoint in Amazon Resource Name format, used
to send push messages over Google Cloud Messaging (GCM).",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "string",
        "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/GCM/production"
    },
    "region" : {
        "title" : "SNS Client Region",
        "description" : "Region of your registered Amazon Simple Notification Service client. For
more information, see <a href=\"https://docs.aws.amazon.com/general/latest/gr/rande.html\">https://
docs.aws.amazon.com/general/latest/gr/rande.html</a>.",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "secret" : {
        "title" : "SNS Access Key Secret",
        "description" : "Amazon Simple Notification Service Access Key Secret. For more information, see
<a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/access-
keys/</a>.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
    },
    "appleEndpoint" : {
        "title" : "SNS Endpoint for APNS",
        "description" : "The Simple Notification Service endpoint in Amazon Resource Name format, used
to send push messages to the Apple Push Notification Service (APNS).",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "string",
        "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/APNS/production"
    }
}
}
}

```

## 1.94.2. Global Operations

Resource path: `/global-config/services/pushNotification`

Resource version: `1.0`

### 1.94.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PushNotification --global --actionName getAllTypes
```

### 1.94.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PushNotification --global --actionName getCreatableTypes
```

### 1.94.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PushNotification --global --actionName nextdescendents
```

### 1.94.2.4. read

Usage:

```
am> read PushNotification --global
```

### 1.94.2.5. update

Usage:

```
am> update PushNotification --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "accessKey" : {
          "title" : "SNS Access Key ID",
          "description" : "Amazon Simple Notification Service Access Key ID. For more information, see
https://aws.amazon.com/developers/access-
keys/.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "AKIAIOSFODNN7EXAMPLE"
        },
        "mdCacheSize" : {
          "title" : "Response Cache Size",
          "description" : "Maximum size of the message dispatcher cache, in number of records. If set
to <code>0</code> the cache can grow indefinitely. If the number of records that need to be stored
exceeds this maximum, then older items in the cache will be removed to make space.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "mdConcurrency" : {
          "title" : "Response Cache Concurrency",
          "description" : "Level of concurrency to use when accessing the message dispatcher cache.
Defaults to <code>16</code>, and must be greater than <code>0</code>. Choose a value to accommodate
as many threads as will ever concurrently access the message dispatcher cache.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "appleEndpoint" : {
          "title" : "SNS Endpoint for APNS",
          "description" : "The Simple Notification Service endpoint in Amazon Resource Name format,
used to send push messages to the Apple Push Notification Service (APNS).",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/APNS/production"
        },
        "mdDuration" : {
          "title" : "Response Cache Duration",
          "description" : "The minimum lifetime to keep unanswered message records in the message
dispatcher cache, in seconds. To keep unanswered message records indefinitely, set this property to
<code>0</code>. Should be tuned so that it is applicable to the use case of this service. For example,
the ForgeRock Authenticator (Push) authentication module has a default timeout of 120 seconds.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    "region" : {
      "title" : "SNS Client Region",
      "description" : "Region of your registered Amazon Simple Notification Service client. For
more information, see <a href=\"https://docs.aws.amazon.com/general/latest/gr/rande.html\">https://
docs.aws.amazon.com/general/latest/gr/rande.html</a>.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "googleEndpoint" : {
      "title" : "SNS Endpoint for GCM",
      "description" : "The Simple Notification Service endpoint in Amazon Resource Name format,
used to send push messages over Google Cloud Messaging (GCM).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/GCM/production"
    },
    "delegateFactory" : {
      "title" : "Message Transport Delegate Factory",
      "description" : "The fully qualified class name of the factory
responsible for creating the PushNotificationDelegate. The class must implement
<code>org.forgerock.openam.services.push.PushNotificationDelegate</code>.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "secret" : {
      "title" : "SNS Access Key Secret",
      "description" : "Amazon Simple Notification Service Access Key Secret. For more information,
see <a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/
access-keys/</a>.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
    }
  },
  "type" : "object",
  "title" : "Realm Defaults"
}
}
}

```

## 1.95. PushNotificationResponse

### 1.95.1. Realm Operations

Push Authentication depends on the secure verification of information sent from the server to the client, and from the client to the server. This allows the server to verify that the notification was received by the original device, and for the device to verify that only the server sent out the original

request. This endpoint provides the place for the device to return responses to the server to requests received either by QR code or by push notification.

Resource path: `/push/sns/message`

Resource version: `1.0`

### 1.95.1.1. authenticate

Message sent from device to server in response to a request for authentication sent to the device via Push notification. This message is generally sent from the ForgeRock Authenticator app.

Usage:

```
am> action PushNotificationResponse --realm Realm --body body --actionName authenticate
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "messageId" : {
      "type" : "string",
      "title" : "Message ID",
      "description" : "Unique message identifier"
    },
    "jwt" : {
      "type" : "string",
      "title" : "JWT",
      "description" : "Signed JWT containing claims:\n* `response`: Response to challenge (Base64 encoding of the HmacSHA256 hashing of the decoded shared secret and the decoded challenge)\n* `deny`: Indication that this auth attempt should be shut down (boolean)"
    }
  },
  "required" : [ "messageId", "jwt" ]
}
```

### 1.95.1.2. register

Message sent from device to server in response to a registration message received on the device via a QR code. This message is generally sent from the ForgeRock Authenticator app.

Usage:

```
am> action PushNotificationResponse --realm Realm --body body --actionName register
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "messageId" : {
      "type" : "string",
      "title" : "Message ID",
      "description" : "Unique message identifier"
    },
    "jwt" : {
      "type" : "string",
      "title" : "JWT",
      "description" : "Signed JWT containing claims:\n* `response`: Response to challenge (Base64 encoding of the HmacSHA256 hashing of the decoded shared secret and the decoded challenge)\n* `mechanismUid`: The device-specific identifier for the just-registered mechanism (string)\n* `deviceId`: The registration token used by GCM or APNS (string)\n* `deviceType`: `android` or `ios` (string)\n* `communicationType`: `gcm` or `apns` (string)"
    }
  },
  "required" : [ "messageId", "jwt" ]
}
```

## 1.96. RadiusClient

### 1.96.1. Global Operations

Resource path: `/global-config/services/RadiusServerService/radiusClient`

Resource version: `1.0`

#### 1.96.1.1. create

Usage:

```
am> create RadiusClient --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientSecret" : {
      "title" : "Client Secret",
```

```

    "description" : "This secret shared between server and client for encryption of the user
password.<br><br>This secret must be conveyed to the RADIUS client and entered into its configuration
before the User-Password field of incoming Access-Request packets can be decrypted to validate the
password for the represented by that packet. A default value is generated for you but you can enter a
custom value if desired.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"clientPacketsLogged" : {
    "title" : "Log Packet Contents for this Client",
    "description" : "Indicates if full packet contents should be dumped to the log.<br><br>When
troubleshooting issues with RADIUS it is helpful to know what was received in a given packet.
Enabling this feature will cause packet contents to be logged in a human consumable format. The only
caveat is that the USER_PASSWORD field will be obfuscated by replacing with asterisks. This should
only be enabled for troubleshooting as it adds significant content to logs and slows processing.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"handlerClass" : {
    "title" : "Handler Class",
    "description" : "The fully qualified name of a class to handle incoming
RADIUS Access-Requests for this client.<br><br>This class must implement the
<code>com.sun.identity.authentication.modules.radius.server.spi.AccessRequestHandler</code> interface
to handle incoming Access-Request packets and provide a suitable response. An instance of this class
is created when configuration is first loaded to validate the class and then once for each new
request. The configuration properties will only be passed for the request handling instances and not
when validating the class.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"clientIpAddress" : {
    "title" : "Client IP Address",
    "description" : "The IP Address of the client.<br><br><a href=\"http://tools.ietf.org/html/
rfc2865#section-5.4\" target=\"_blank\">Section 5.4 of the RADIUS Authentication Specification,
RFC 2865</a>, indicates that the source IP address of the Access-Request packet <em>MUST</em> be
used to identify a configured client and hence determine the shared secret to use for decrypting
the User-Password field.<p><p>This property should hold the source IP address of the client. This
should match the value obtained from Java's <code>InetAddress.getAddress().toString()</code>
function.<p><p>To verify the value, send an Access-Request packet to OpenAM's RADIUS port and watch
for a message stating: <code>\"No Defined RADIUS Client matches IP address '127.0.0.1'. Dropping
request.\"</code>. The value used in this property should match the IP address returned in the single
quotes.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"handlerConfig" : {
    "title" : "Handler Class Configuration Properties",
    "description" : "Properties needed by the handler class for its configuration.<br><br>These
properties are provided to the handler via its <code>init</code> method prior to the call to handle
the request packet. If these values are changed the next handler instance created for an incoming
request will receive the updated values. Each entry assumes that the first '<code>=</code>' character

```

```
incurred separates a key from its value. All entries are placed in a properties file handed to each handler instance.",
  "propertyOrder" : 900,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
}
}
```

### 1.96.1.2. delete

Usage:

```
am> delete RadiusClient --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.96.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RadiusClient --global --actionName getAllTypes
```

### 1.96.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RadiusClient --global --actionName getCreatableTypes
```

### 1.96.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RadiusClient --global --actionName nextdescendents
```



### 1.96.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query RadiusClient --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.96.1.7. read

Usage:

```
am> read RadiusClient --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.96.1.8. update

Usage:

```
am> update RadiusClient --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "This secret shared between server and client for encryption of the user password.<br><br>This secret must be conveyed to the RADIUS client and entered into its configuration before the User-Password field of incoming Access-Request packets can be decrypted to validate the password for the represented by that packet. A default value is generated for you but you can enter a custom value if desired.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
```

```

    "exampleValue" : ""
  },
  "clientPacketsLogged" : {
    "title" : "Log Packet Contents for this Client",
    "description" : "Indicates if full packet contents should be dumped to the log.<br><br>When troubleshooting issues with RADIUS it is helpful to know what was received in a given packet. Enabling this feature will cause packet contents to be logged in a human consumable format. The only caveat is that the USER_PASSWORD field will be obfuscated by replacing with asterisks. This should only be enabled for troubleshooting as it adds significant content to logs and slows processing.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "handlerClass" : {
    "title" : "Handler Class",
    "description" : "The fully qualified name of a class to handle incoming RADIUS Access-Requests for this client.<br><br>This class must implement the <code>com.sun.identity.authentication.modules.radius.server.spi.AccessRequestHandler</code> interface to handle incoming Access-Request packets and provide a suitable response. An instance of this class is created when configuration is first loaded to validate the class and then once for each new request. The configuration properties will only be passed for the request handling instances and not when validating the class.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientIpAddress" : {
    "title" : "Client IP Address",
    "description" : "The IP Address of the client.<br><br><a href=\"http://tools.ietf.org/html/rfc2865#section-5.4\" target=\"_blank\">Section 5.4 of the RADIUS Authentication Specification, RFC 2865</a>, indicates that the source IP address of the Access-Request packet <em>MUST</em> be used to identify a configured client and hence determine the shared secret to use for decrypting the User-Password field.<p><p>This property should hold the source IP address of the client. This should match the value obtained from Java's <code>InetSocketAddress.getAddress().toString()</code> function.<p><p>To verify the value, send an Access-Request packet to OpenAM's RADIUS port and watch for a message stating: <code>\"No Defined RADIUS Client matches IP address '127.0.0.1'. Dropping request.\"</code>. The value used in this property should match the IP address returned in the single quotes.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "handlerConfig" : {
    "title" : "Handler Class Configuration Properties",
    "description" : "Properties needed by the handler class for its configuration.<br><br>These properties are provided to the handler via its <code>init</code> method prior to the call to handle the request packet. If these values are changed the next handler instance created for an incoming request will receive the updated values. Each entry assumes that the first '<code>=</code>' character incurred separates a key from its value. All entries are placed in a properties file handed to each handler instance.",
    "propertyOrder" : 900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",

```

```
    "exampleValue" : ""
  }
}
```

## 1.97. RadiusModule

### 1.97.1. Realm Operations

Resource path: `/realm-config/authentication/modules/radius`

Resource version: `1.0`

#### 1.97.1.1. create

Usage:

```
am> create RadiusModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverTimeout" : {
      "title" : "Timeout",
      "description" : "Amount of time in seconds to wait for the RADIUS server response.<br><br>This sets the <code>SO_TIMEOUT</code> timeout on the packet. ",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "secondaryRadiusServers" : {
      "title" : "Secondary Radius Servers",
      "description" : "A list of secondary Radius servers that will be used for authentication, in case the primary servers are unavailable.<br><br>The module will use secondary servers for authentication if all primary servers are unavailable. A single entry must be in the format:<br><code>radius_server:port</code><br><br>Multiple entries allow associations between OpenAM servers and a Radius server. The format is:<br><code>local server name | radius_server:port</code><br><br><i>NB</i> The local server name is the full name of the server from the list of servers and sites.",
      "propertyOrder" : 200,
      "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sharedSecret" : {
    "title" : "Shared Secret",
    "description" : "The secret shared between the RADIUS server and the authentication module.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "primaryRadiusServers" : {
    "title" : "Primary Radius Servers",
    "description" : "A list of primary Radius servers that will be used for authentication<br><br>The module will use these servers in preference to the secondary servers. A single entry must be in the format:<br><br><code>radius_server:port</code><br><br>Multiple entries allow associations between OpenAM servers and a Radius server. The format is:<br><br><code>local server name | radius_server:port</code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "serverPortNumber" : {
    "title" : "Port Number",
    "description" : "Port number on which the RADIUS server is listening.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "healthCheckInterval" : {
    "title" : "Health check interval",
    "description" : "The interval between checks to unavailable RADIUS servers, in minutes.<br><br>Determines how often OpenAM checks an offline server's status. The check will send an invalid authentication request to the RADIUS server. Offline servers will not be used until the healthcheck was successful. Primary servers that become available will be used in preference to secondary servers.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "integer",

```

```
    "exampleValue" : ""  
  }  
}
```

### 1.97.1.2. delete

Usage:

```
am> delete RadiusModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.97.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RadiusModule --realm Realm --actionName getAllTypes
```

### 1.97.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RadiusModule --realm Realm --actionName getCreatableTypes
```

### 1.97.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RadiusModule --realm Realm --actionName nextdescendents
```

### 1.97.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query RadiusModule --realm Realm --filter filter
```

Parameters:

## --filter

A CREST formatted query filter, where "true" will query all.

## 1.97.1.7. read

Usage:

```
am> read RadiusModule --realm Realm --id id
```

Parameters:

### --id

The unique identifier for the resource.

## 1.97.1.8. update

Usage:

```
am> update RadiusModule --realm Realm --id id --body body
```

Parameters:

### --id

The unique identifier for the resource.

### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverTimeout" : {
      "title" : "Timeout",
      "description" : "Amount of time in seconds to wait for the RADIUS server response.<br><br>This sets the <code>SO_TIMEOUT</code> timeout on the packet. ",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "secondaryRadiusServers" : {
      "title" : "Secondary Radius Servers",
      "description" : "A list of secondary Radius servers that will be used for authentication, in case the primary servers are unavailable.<br><br>The module will use secondary servers for authentication if all primary servers are unavailable. A single entry must be in the format:<br><br><code>radius_server:port</code><br><br>Multiple entries allow associations between OpenAM servers and a Radius server. The format is:<br><br><code>local server name | radius_server:port</code><br><br><i>NB</i> The local server name is the full name of the server from the list of servers and sites.",
      "propertyOrder" : 200,
      "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sharedSecret" : {
    "title" : "Shared Secret",
    "description" : "The secret shared between the RADIUS server and the authentication module.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "primaryRadiusServers" : {
    "title" : "Primary Radius Servers",
    "description" : "A list of primary Radius servers that will be used for authentication<br><br>The module will use these servers in preference to the secondary servers. A single entry must be in the format:<br><br><code>radius_server:port</code><br><br>Multiple entries allow associations between OpenAM servers and a Radius server. The format is:<br><br><code>local server name | radius_server:port</code><br><br><i>NB </i>The local server name is the full name of the server from the list of servers and sites.",
    "propertyOrder" : 100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "serverPortNumber" : {
    "title" : "Port Number",
    "description" : "Port number on which the RADIUS server is listening.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "healthCheckInterval" : {
    "title" : "Health check interval",
    "description" : "The interval between checks to unavailable RADIUS servers, in minutes.<br><br>Determines how often OpenAM checks an offline server's status. The check will send an invalid authentication request to the RADIUS server. Offline servers will not be used until the healthcheck was successful. Primary servers that become available will be used in preference to secondary servers.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "integer",

```

```
    "exampleValue" : ""  
  }  
}
```

## 1.97.2. Global Operations

Resource path: `/global-config/authentication/modules/radius`

Resource version: `1.0`

### 1.97.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RadiusModule --global --actionName getAllTypes
```

### 1.97.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RadiusModule --global --actionName getCreatableTypes
```

### 1.97.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RadiusModule --global --actionName nextdescendents
```

### 1.97.2.4. read

Usage:

```
am> read RadiusModule --global
```

### 1.97.2.5. update



## Usage:

```
am> update RadiusModule --global --body body
```

## Parameters:

### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "serverPortNumber" : {
          "title" : "Port Number",
          "description" : "Port number on which the RADIUS server is listening.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sharedSecret" : {
          "title" : "Shared Secret",
          "description" : "The secret shared between the RADIUS server and the authentication
module.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "secondaryRadiusServers" : {
          "title" : "Secondary Radius Servers",
          "description" : "A list of secondary Radius servers that will be used for authentication,
in case the primary servers are unavailable.<br><br>The module will use secondary servers for
authentication if all primary servers are unavailable. A single entry must be in the format:<br><br>
<code>radius_server:port</code><br><br>Multiple entries allow associations between OpenAM servers
and a Radius server. The format is:<br><br><code>local server name | radius_server:port</code><br>
<br><i>NB </i>The local server name is the full name of the server from the list of servers and
sites.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    },
    "serverTimeout" : {
      "title" : "Timeout",
      "description" : "Amount of time in seconds to wait for the RADIUS server
response.<br><br>This sets the <code>SO_TIMEOUT</code> timeout on the packet. ",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "healthCheckInterval" : {
      "title" : "Health check interval",
      "description" : "The interval between checks to unavailable RADIUS servers, in minutes.
<br><br>Determines how often OpenAM checks an offline server's status. The check will send an invalid
authentication request to the RADIUS server. Offline servers will not be used until the healthcheck
was successful. Primary servers that become available will be used in preference to secondary
servers.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "primaryRadiusServers" : {
      "title" : "Primary Radius Servers",
      "description" : "A list of primary Radius servers that will be used for
authentication<br><br>The module will use these servers in preference to the secondary servers.
A single entry must be in the format:<br><br><code>radius_server:port</code><br><br>Multiple
entries allow associations between OpenAM servers and a Radius server. The format is:<br><br>
><code>local server name | radius_server:port</code><br><br><i>NB </i>The local server name is the
full name of the server from the list of servers and sites.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "type" : "object",
  "title" : "Realm Defaults"
}
}
}

```

## 1.98. RadiusServer

### 1.98.1. Global Operations

Resource path: </global-config/services/RadiusServerService>

Resource version: 1.0

### 1.98.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RadiusServer --global --actionName getAllTypes
```

### 1.98.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RadiusServer --global --actionName getCreatableTypes
```

### 1.98.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RadiusServer --global --actionName nextdescendents
```

### 1.98.1.4. read

Usage:

```
am> read RadiusServer --global
```

### 1.98.1.5. update

Usage:

```
am> update RadiusServer --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "radiusListenerEnabled" : {
      "title" : "Enabled",
      "description" : "Enables the OpenAM RADIUS server to listen for requests on the listener port
and to handle the requests.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
```

```

    "exampleValue" : ""
  },
  "radiusThreadPoolKeepaliveSeconds" : {
    "title" : "Thread Pool Keep-Alive Seconds",
    "description" : "If the pool currently has more than Thread Pool Core Size threads, excess threads will be terminated if they have been idle for more than the Keep-Alive Seconds. Specify a value from 1 to 3600.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "radiusThreadPoolMaxSize" : {
    "title" : "Thread Pool Max Size",
    "description" : "Maximum number of threads allowed in the pool. See also \"Thread Pool Core Size\".",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "radiusThreadPoolCoreSize" : {
    "title" : "Thread Pool Core Size",
    "description" : "When a RADIUS request is received and fewer than corePoolSize threads are running, a new thread is created to handle the request, even if other worker threads are idle. If there are more than \"Thread Pool Core Size\" but less than \"Thread Pool Max Size\" threads running, a new thread will be created only if the queue is full. By setting \"Thread Pool Core Size\" and \"Thread Pool Max Size\" to the same value, you create a fixed-size thread pool. Specify a value from 1 to 100.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "radiusServerPort" : {
    "title" : "Listener Port",
    "description" : "The UDP port on which each OpenAM server will listen for RADIUS Access-Request packets<br>According to the RADIUS Authentication Specification, 1812. Specify a value from 1024 to 65535. All client requests are handled through the same port.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "radiusThreadPoolQueueSize" : {
    "title" : "Thread Pool Queue Size",
    "description" : "The number of requests that can be queued for the pool before further requests will be silently dropped. See also \"Thread Pool Core Size\" and \"Thread Pool Max Size\". Specify a value from 1 to 1000.",
    "propertyOrder" : 1100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }
}
}

```

# 1.99. Realms

## 1.99.1. Global Operations

The endpoint for Realm operations

Resource path: `/global-config/realms`

Resource version: `1.0`

### 1.99.1.1. create

Create a Realm

Usage:

```
am> create Realms --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Represents a Realm Resource",
  "type" : "object",
  "title" : "Realm",
  "properties" : {
    "name" : {
      "type" : "string",
      "title" : "Name",
      "description" : "The name of the Realm"
    },
    "active" : {
      "type" : "boolean",
      "title" : "Active",
      "description" : "True if the Realm is active"
    },
    "parentPath" : {
      "type" : "string",
      "title" : "Parent",
      "description" : "The path of the Realm's parent Realm"
    },
    "aliases" : {
      "type" : "array",
      "title" : "Aliases",
      "description" : "Aliases which can be used reference to the Realm",
      "items" : {
        "type" : "string"
      }
    }
  }
},
```

```
"required" : [ "name", "active", "parentPath", "aliases" ]  
}
```

### 1.99.1.2. delete

Delete a Realm

Usage:

```
am> delete Realms --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.99.1.3. query

Usage:

```
am> query Realms --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.99.1.4. read

Read a Realm

Usage:

```
am> read Realms --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.99.1.5. update

Update a Realm

Usage:

```
am> update Realms --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Represents a Realm Resource",
  "type" : "object",
  "title" : "Realm",
  "properties" : {
    "name" : {
      "type" : "string",
      "title" : "Name",
      "description" : "The name of the Realm"
    },
    "active" : {
      "type" : "boolean",
      "title" : "Active",
      "description" : "True if the Realm is active"
    },
    "parentPath" : {
      "type" : "string",
      "title" : "Parent",
      "description" : "The path of the Realm's parent Realm"
    },
    "aliases" : {
      "type" : "array",
      "title" : "Aliases",
      "description" : "Aliases which can be used reference to the Realm",
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "name", "active", "parentPath", "aliases" ]
}
```

## 1.100. Records

### 1.100.1. Realm Operations

Service for creating records.

Resource path: [/records](#)

Resource version: [1.0](#)

## 1.100.1.1. start

Starts recording.

Usage:

```
am> action Records --realm Realm --body body --actionName start
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "The properties of a Record, which can be serialized from json.",
  "type" : "object",
  "title" : "Record properties",
  "properties" : {
    "issueID" : {
      "description" : "A case number is a good choice for the issueID value.",
      "title" : "Issue ID",
      "type" : "integer",
      "format" : "int64"
    },
    "referenceID" : {
      "description" : "A second identifier to segregate multiple recording events for the same issue.",
      "title" : "Reference ID",
      "type" : "string"
    },
    "description" : {
      "description" : "A textual description of the recording event.",
      "title" : "Description",
      "type" : "string"
    },
    "threadDumpDelayInSeconds" : {
      "description" : "Object used to specify an interval at which thread dumps are taken. The initial thread dump is taken at the start of the recording event; subsequent thread dumps are taken at multiples of the delay interval.",
      "title" : "Thread dump delay in seconds",
      "type" : "integer",
      "format" : "int64"
    },
    "configExportPassword" : {
      "description" : "A key required to import the exported configuration.",
      "title" : "Config export password",
      "type" : "string"
    },
    "debugLevel" : {
      "description" : "The debug level to set for the recording event.",
      "title" : "Debug level",
      "type" : "string",
      "enum" : [ "OFF", "ERROR", "WARNING", "MESSAGE", "ON" ]
    },
    "autoStopTimeInMS" : {
      "description" : "Used to specify an event that automatically ends a recording period. For time-based termination, specify a time object; for termination based on uncompressed file size, specify a
```



```

fileSize object. If you specify both time and fileSize objects, the event that occurs first causes
recording to stop.",
  "title" : "Auto stop time in milliseconds",
  "type" : "integer",
  "format" : "int64"
},
"configExportSharePasswordEnabled" : {
  "description" : "Whether to show the password value in the ssoadm start-recording, ssoadm get-
recording-status, ssoadm stop-recording output and in the info.json file.",
  "title" : "Config export share password enabled",
  "type" : "boolean"
},
"autoStopFileSizeInKB" : {
  "description" : "Configures a recording period to terminate after the aggregate size of
uncompressed debug logs has reached this size.",
  "title" : "Auto stop file size in KB",
  "type" : "integer",
  "format" : "int64"
},
"threadDumpEnabled" : {
  "description" : "Whether to dump threads during the recording event.",
  "title" : "Thread dump enabled",
  "type" : "boolean"
},
"configExportEnabled" : {
  "description" : "Whether to export the OpenAM configuration upon completion of the recording
event.",
  "title" : "Config export enabled",
  "type" : "boolean"
},
"autoStopEnabled" : {
  "description" : "Whether auto stop is enabled.",
  "title" : "Auto stop enabled",
  "type" : "boolean"
},
"autoStopTimeEnabled" : {
  "description" : "Whether time is specified for the auto stop.",
  "title" : "Auto stop time enabled",
  "type" : "boolean"
},
"autoStopFileSizeEnabled" : {
  "description" : "Whether file size is enabled for the auto stop.",
  "title" : "Auto stop file size enabled",
  "type" : "boolean"
},
"zipEnabled" : {
  "description" : "Whether to compress the output directory into a zip file when recording has
stopped.",
  "title" : "Zip enabled",
  "type" : "boolean"
}
}
}

```

### 1.100.1.2. status

Returns status of recording.

Usage:

```
am> action Records --realm Realm --actionName status
```

### 1.100.1.3. stop

Stops recording.

Usage:

```
am> action Records --realm Realm --actionName stop
```

## 1.101. ResourceSets

### 1.101.1. Realm Operations

Resource set resource provider is responsible for managing Resource Sets belonging to a user. Available operations are update, query, read, revoke all action.

Resource path: `/users/{user}/oauth2/resources/sets`

Resource version: `1.0`

#### 1.101.1.1. query

Query the collection of the user's Resource Set.

Usage:

```
am> query ResourceSets --realm Realm --filter filter --user user
```

Parameters:

#### **--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: `[*]`

#### **--user**

Resource set resource provider is responsible for managing Resource Sets belonging to a user. Available operations are update, query, read, revoke all action.

#### 1.101.1.2. read

Read Resource Set from the collection by id.

Usage:

```
am> read ResourceSets --realm Realm --id id --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--user**

Resource set resource provider is responsible for managing Resource Sets belonging to a user. Available operations are update, query, read, revoke all action.

### 1.101.1.3. update

Update a Resource Set record.

Usage:

```
am> update ResourceSets --realm Realm --id id --body body --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Describes the structure of the OpenAM representation of a user's OAuth Resource Set. For further information see [insert link to the RSR standard], and documentation about UMA in OpenAM.",
  "type" : "object",
  "title" : "Resource Set resource schema",
  "properties" : {
    "scopes" : {
      "type" : "array",
      "title" : "Scopes",
      "description" : "List of Resource Set scopes.",
      "items" : {
        "type" : "string"
      }
    },
    "_id" : {
      "type" : "string",
      "title" : "Resource set id",
      "description" : "Unique identifier of the Resource Set."
    },
    "resourceServer" : {
      "type" : "string",
      "title" : "Resource server",
      "description" : "The resources server name."
    },
    "labels" : {
      "type" : "array",
```

```
    "title" : "Resource labels",
    "description" : "Labels of the resource.",
    "items" : {
      "type" : "string"
    }
  },
  "name" : {
    "type" : "string",
    "title" : "Resource name",
    "description" : "Name of the resource."
  },
  "icon_uri" : {
    "type" : "string",
    "title" : "Icon uri",
    "description" : "Resource icon uri."
  },
  "resourceOwnerId" : {
    "type" : "string",
    "title" : "Resource owner",
    "description" : "Name of the resource owner."
  },
  "type" : {
    "type" : "string",
    "title" : "Resource type",
    "description" : "Type of the resources."
  }
}
```

--user

Resource set resource provider is responsible for managing Resource Sets belonging to a user. Available operations are update, query, read, revoke all action.

## 1.102. ResourceTypes

### 1.102.1. Realm Operations

The Resource Types resource is responsible for managing resource types, which define a template for the resources that Managing Policies policies apply to, and the actions associated with those resources. Available operations are Query, Read, Create, Update, Delete

Resource path: [/resourcetypes](#)

Resource version: [1.0](#)

#### 1.102.1.1. create

Create new resource type

Usage:

```
am> create ResourceTypes --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Resource Types Resource schema",
  "type" : "object",
  "title" : "Resource Types Resource schema",
  "properties" : {
    "uuid" : {
      "title" : "UUID",
      "description" : "Unique identifier of the record",
      "type" : "string"
    },
    "name" : {
      "title" : "Name",
      "description" : "Resource type name",
      "type" : "string"
    },
    "description" : {
      "title" : "Description",
      "description" : "Resource type description",
      "type" : "string"
    },
    "patterns" : {
      "title" : "Patterns",
      "description" : "Resource type patterns",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    },
    "actions" : {
      "title" : "Actions",
      "description" : "Resource type actions",
      "type" : "object",
      "additionalProperties" : {
        "type" : "boolean"
      }
    },
    "createdBy" : {
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject created the resource type",
      "type" : "string"
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",

```

```
    "type" : "number"
  },
  "lastModifiedBy" : {
    "title" : "Last modifier",
    "description" : "A string containing the universal identifier DN of the subject that most
recently updated the resource type. If the resource type has not been modified since it was created,
this property will have the same value as createdBy",
    "type" : "string"
  },
  "lastModifiedDate" : {
    "title" : "Last modification date",
    "description" : "A string containing the last modified date and time, in ISO 8601 format. If the
resource typ has not been modified since it was created, this property will have the same value as
creationDate",
    "type" : "number"
  }
}
```

### 1.102.1.2. delete

Delete resource type

Usage:

```
am> delete ResourceTypes --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.102.1.3. query

Query the collection of resource types

Usage:

```
am> query ResourceTypes --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

### 1.102.1.4. read

Read from the resource types collection by unique identifier

Usage:

```
am> read ResourceTypes --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.102.1.5. update

Update an existing resource type

Usage:

```
am> update ResourceTypes --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Resource Types Resource schema",
  "type" : "object",
  "title" : "Resource Types Resource schema",
  "properties" : {
    "uuid" : {
      "title" : "UUID",
      "description" : "Unique identifier of the record",
      "type" : "string"
    },
    "name" : {
      "title" : "Name",
      "description" : "Resource type name",
      "type" : "string"
    },
    "description" : {
      "title" : "Description",
      "description" : "Resource type description",
      "type" : "string"
    },
    "patterns" : {
      "title" : "Patterns",
      "description" : "Resource type patterns",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    }
  }
},
```

```
"actions" : {
  "title" : "Actions",
  "description" : "Resource type actions",
  "type" : "object",
  "additionalProperties" : {
    "type" : "boolean"
  }
},
"createdBy" : {
  "title" : "Created by",
  "description" : "A string containing the universal identifier DN of the subject created the resource type",
  "type" : "string"
},
"creationDate" : {
  "title" : "Creation date",
  "description" : "An integer containing the creation date and time, in ISO 8601 format",
  "type" : "number"
},
"lastModifiedBy" : {
  "title" : "Last modifier",
  "description" : "A string containing the universal identifier DN of the subject that most recently updated the resource type. If the resource type has not been modified since it was created, this property will have the same value as createdBy",
  "type" : "string"
},
"lastModifiedDate" : {
  "title" : "Last modification date",
  "description" : "A string containing the last modified date and time, in ISO 8601 format. If the resource typ has not been modified since it was created, this property will have the same value as creationDate",
  "type" : "number"
}
}
```

## 1.103. RestApis

### 1.103.1. Global Operations

Resource path: `/global-config/services/rest`

Resource version: `1.0`

#### 1.103.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RestApis --global --actionName getAllTypes
```



### 1.103.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RestApis --global --actionName getCreatableTypes
```

### 1.103.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RestApis --global --actionName nextdescendents
```

### 1.103.1.4. read

Usage:

```
am> read RestApis --global
```

### 1.103.1.5. update

Usage:

```
am> update RestApis --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "descriptionsState" : {
      "title" : "API Descriptions",
      "description" : "Whether API Explorer and API Docs are enabled in OpenAM and how the
documentation for them is generated. Dynamic generation includes descriptions from any custom
services and authentication modules you may have added. Static generation only includes services
and authentication modules that were present when OpenAM was built. Note that dynamic documentation
generation may not work in some application containers.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "defaultVersion" : {
      "title" : "Default Resource Version",
```

```

        "description" : "The API resource version to use when the REST request does not specify an
explicit version. Choose from:<br><br><ul><li><code>Latest</code>. If an explicit version is not
specified, the latest resource version of an API is used.</li><li><code>Oldest</code>. If an explicit
version is not specified, the oldest supported resource version of an API is used. Note that since
APIs may be deprecated and fall out of support, the oldest <i>supported</i> version may not be the
first version.</li><li><code>None</code>. If an explicit version is not specified, the request will
not be handled and an error status is returned.</li></ul>",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "warningHeader" : {
        "title" : "Warning Header",
        "description" : "Whether to include a warning header in the response to a request which fails to
include the <code>Accept-API-Version</code> header.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "defaultProtocolVersion" : {
        "title" : "Default Protocol Version",
        "description" : "The API protocol version to use when a REST request does not specify an
explicit version. Choose from:<br><br><ul><li><code>Oldest</code>. If an explicit version is not
specified, the oldest protocol version is used.</li><li><code>Latest</code>. If an explicit version
is not specified, the latest protocol version is used.</li><li><code>None</code>. If an explicit
version is not specified, the request will not be handled and an error status is returned.</li></
ul>",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

## 1.104. SaeModule

### 1.104.1. Realm Operations

Resource path: `/realm-config/authentication/modules/sae`

Resource version: `1.0`

#### 1.104.1.1. create

Usage:

```
am> create SaeModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

### 1.104.1.2. delete

Usage:

```
am> delete SaeModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.104.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SaeModule --realm Realm --actionName getAllTypes
```

### 1.104.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SaeModule --realm Realm --actionName getCreatableTypes
```

### 1.104.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SaeModule --realm Realm --actionName nextdescendents
```

### 1.104.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query SaeModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.104.1.7. read

Usage:

```
am> read SaeModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.104.1.8. update

Usage:

```
am> update SaeModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

## 1.104.2. Global Operations

Resource path: `/global-config/authentication/modules/sae`

Resource version: `1.0`

### 1.104.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SaeModule --global --actionName getAllTypes
```

### 1.104.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SaeModule --global --actionName getCreatableTypes
```

### 1.104.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SaeModule --global --actionName nextdescendents
```

### 1.104.2.4. read

Usage:

```
am> read SaeModule --global
```

## 1.104.2.5. update

Usage:

```
am> update SaeModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

## 1.105. Saml2Entity

### 1.105.1. Realm Operations

Resource path: </realm-config/federation/entityproviders/saml2>

Resource version: [1.0](#)

#### 1.105.1.1. create

Usage:

```
am> create Saml2Entity --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

### 1.105.1.2. delete

Usage:

```
am> delete Saml2Entity --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.105.1.3. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Saml2Entity --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.105.1.4. read

Usage:

```
am> read Saml2Entity --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.105.1.5. update

Usage:

```
am> update Saml2Entity --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```



## 1.106. Saml2Module

### 1.106.1. Realm Operations

Resource path: `/realm-config/authentication/modules/authSaml`

Resource version: `1.0`

#### 1.106.1.1. create

Usage:

```
am> create Saml2Module --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "isPassive" : {
      "title" : "Passive Authentication",
      "description" : "Use this parameter to indicate whether the identity provider should
authenticate passively (true) or not (false).",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "nameIdFormat" : {
      "title" : "NameID Format",
      "description" : "(Optional) Use this parameter to specify a SAML Name
Identifier format identifier such as <pre>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</pre> <pre>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</pre>
<pre>urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified</pre>",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,

```

```

    "type" : "integer",
    "exampleValue" : ""
  },
  "authComparison" : {
    "title" : "Comparison Type",
    "description" : "(Optional) Use this parameter to specify a comparison method to evaluate the
    requested context classes or statements. OpenAM accepts the following values: <pre>better</pre>,
    <pre>exact</pre>, <pre>maximum</pre>, and <pre>minimum</pre>.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sloEnabled" : {
    "title" : "Single Logout Enabled",
    "description" : "Enable to attempt logout of the user's
    IdP session at the point of session logout. Required the
    <pre>org.forgerock.openam.authentication.modules.saml2.SAML2PostAuthenticationPlugin</pre> to be
    active on the chain that includes this SAML2 module.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "allowCreate" : {
    "title" : "Allow IdP to Create NameID",
    "description" : "Use this parameter to indicate whether the identity provider can create a new
    identifier for the principal if none exists (true) or not (false).",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "reqBinding" : {
    "title" : "Request Binding",
    "description" : "Use this parameter to indicate what binding the SP should use when
    communicating with the IdP.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sloRelay" : {
    "title" : "Single Logout URL",
    "description" : "If Single Logout is enabled, this is the URL to which the user should be
    forwarded after successful IdP logout. This must be a fully-qualified URL (start with http...), or
    the redirect will not function.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "forceAuthn" : {
    "title" : "Force IdP Authentication",
    "description" : "Use this parameter to indicate whether the identity provider should force
    authentication (true) or can reuse existing security contexts (false).",
    "propertyOrder" : 1100,
    "required" : true,
    "type" : "string",

```

```

    "exampleValue" : ""
  },
  "authnContextClassRef" : {
    "title" : "Authentication Context Class Reference",
    "description" : "(Optional) Use this parameter to specify authentication context class
references. Separate multiple values with pipe characters (|).",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "entityName" : {
    "title" : "IdP Entity ID",
    "description" : "The entity name of the SAML2 IdP Service to use for this module (must be
configured).",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "loginChain" : {
    "title" : "Linking Authentication Chain",
    "description" : "The authentication chain that will be executed when a user is required to be
authenticated locally to match their user account with that of a remotely authenticated assertion.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "metaAlias" : {
    "title" : "SP MetaAlias",
    "description" : "MetaAlias for Service Provider. The format of this parameter is <pre>/
realm_name/SP</pre>",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "binding" : {
    "title" : "Response Binding",
    "description" : "Use this parameter to indicate what binding the IdP should use when
communicating with this SP.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authnContextDeclRef" : {
    "title" : "Authentication Context Declaration Reference",
    "description" : "(Optional) Use this parameter to specify authentication context declaration
references. Separate multiple values with pipe characters (|).",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}
}

```

### 1.106.1.2. delete

Usage:

```
am> delete Saml2Module --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.106.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Saml2Module --realm Realm --actionName getAllTypes
```

### 1.106.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Saml2Module --realm Realm --actionName getCreatableTypes
```

### 1.106.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Saml2Module --realm Realm --actionName nextdescendents
```

### 1.106.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Saml2Module --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

## 1.106.1.7. read

Usage:

```
am> read Saml2Module --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.106.1.8. update

Usage:

```
am> update Saml2Module --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "isPassive" : {
      "title" : "Passive Authentication",
      "description" : "Use this parameter to indicate whether the identity provider should
authenticate passively (true) or not (false).",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "nameIdFormat" : {
      "title" : "NameID Format",
      "description" : "(Optional) Use this parameter to specify a SAML Name
Identifier format identifier such as <pre>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</pre> <pre>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</pre>
<pre>urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified</pre>",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
```

```

    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "authComparison" : {
    "title" : "Comparison Type",
    "description" : "(Optional) Use this parameter to specify a comparison method to evaluate the
requested context classes or statements. OpenAM accepts the following values: <pre>better</pre>,
<pre>exact</pre>, <pre>maximum</pre>, and <pre>minimum</pre>.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sloEnabled" : {
    "title" : "Single Logout Enabled",
    "description" : "Enable to attempt logout of the user's
IdP session at the point of session logout. Required the
<pre>org.forgerock.openam.authentication.modules.saml2.SAML2PostAuthenticationPlugin</pre> to be
active on the chain that includes this SAML2 module.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "allowCreate" : {
    "title" : "Allow IdP to Create NameID",
    "description" : "Use this parameter to indicate whether the identity provider can create a new
identifier for the principal if none exists (true) or not (false).",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "reqBinding" : {
    "title" : "Request Binding",
    "description" : "Use this parameter to indicate what binding the SP should use when
communicating with the IdP.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sloRelay" : {
    "title" : "Single Logout URL",
    "description" : "If Single Logout is enabled, this is the URL to which the user should be
forwarded after successful IdP logout. This must be a fully-qualified URL (start with http...), or
the redirect will not function.",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "forceAuthn" : {
    "title" : "Force IdP Authentication",
    "description" : "Use this parameter to indicate whether the identity provider should force
authentication (true) or can reuse existing security contexts (false).",
    "propertyOrder" : 1100,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authnContextClassRef" : {
    "title" : "Authentication Context Class Reference",
    "description" : "(Optional) Use this parameter to specify authentication context class
references. Separate multiple values with pipe characters (|).",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "entityName" : {
    "title" : "IdP Entity ID",
    "description" : "The entity name of the SAML2 IdP Service to use for this module (must be
configured).",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "loginChain" : {
    "title" : "Linking Authentication Chain",
    "description" : "The authentication chain that will be executed when a user is required to be
authenticated locally to match their user account with that of a remotely authenticated assertion.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "metaAlias" : {
    "title" : "SP MetaAlias",
    "description" : "MetaAlias for Service Provider. The format of this parameter is <pre>/
realm_name/SP</pre>",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "binding" : {
    "title" : "Response Binding",
    "description" : "Use this parameter to indicate what binding the IdP should use when
communicating with this SP.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authnContextDeclRef" : {
    "title" : "Authentication Context Declaration Reference",
    "description" : "(Optional) Use this parameter to specify authentication context declaration
references. Separate multiple values with pipe characters (|).",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}

```

```
}
```

## 1.106.2. Global Operations

Resource path: `/global-config/authentication/modules/authSaml`

Resource version: `1.0`

### 1.106.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Saml2Module --global --actionName getAllTypes
```

### 1.106.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Saml2Module --global --actionName getCreatableTypes
```

### 1.106.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Saml2Module --global --actionName nextdescendents
```

### 1.106.2.4. read

Usage:

```
am> read Saml2Module --global
```

### 1.106.2.5. update

Usage:

```
am> update Saml2Module --global --body body
```



Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "isPassive" : {
          "title" : "Passive Authentication",
          "description" : "Use this parameter to indicate whether the identity provider should
authenticate passively (true) or not (false).",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authnContextDeclRef" : {
          "title" : "Authentication Context Declaration Reference",
          "description" : "(Optional) Use this parameter to specify authentication context declaration
references. Separate multiple values with pipe characters (|).",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "forceAuthn" : {
          "title" : "Force IdP Authentication",
          "description" : "Use this parameter to indicate whether the identity provider should force
authentication (true) or can reuse existing security contexts (false).",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "reqBinding" : {
          "title" : "Request Binding",
          "description" : "Use this parameter to indicate what binding the SP should use when
communicating with the IdP.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sloRelay" : {
          "title" : "Single Logout URL",
          "description" : "If Single Logout is enabled, this is the URL to which the user should be
forwarded after successful IdP logout. This must be a fully-qualified URL (start with http...), or
the redirect will not function.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "entityName" : {
          "title" : "IdP Entity ID",

```

```

    "description" : "The entity name of the SAML2 IdP Service to use for this module (must be
configured).",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authnContextClassRef" : {
    "title" : "Authentication Context Class Reference",
    "description" : "(Optional) Use this parameter to specify authentication context class
references. Separate multiple values with pipe characters (|).",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "nameIdFormat" : {
    "title" : "NameID Format",
    "description" : "(Optional) Use this parameter to specify a SAML Name
Identifier format identifier such as <pre>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</pre> <pre>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</pre>
<pre>urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified</pre>",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sloEnabled" : {
    "title" : "Single Logout Enabled",
    "description" : "Enable to attempt logout of the
user's IdP session at the point of session logout. Required the
<pre>org.forgerock.openam.authentication.modules.saml2.SAML2PostAuthenticationPlugin</pre> to be
active on the chain that includes this SAML2 module.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "binding" : {
    "title" : "Response Binding",
    "description" : "Use this parameter to indicate what binding the IdP should use when
communicating with this SP.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authComparison" : {
    "title" : "Comparison Type",
    "description" : "(Optional) Use this parameter to specify a comparison method to evaluate
the requested context classes or statements. OpenAM accepts the following values: <pre>better</pre>,
<pre>exact</pre>, <pre>maximum</pre>, and <pre>minimum</pre>.",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",

```

```

    "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "metaAlias" : {
    "title" : "SP MetaAlias",
    "description" : "MetaAlias for Service Provider. The format of this parameter is <pre>/realm_name/SP</pre>",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "allowCreate" : {
    "title" : "Allow IdP to Create NameID",
    "description" : "Use this parameter to indicate whether the identity provider can create a new identifier for the principal if none exists (true) or not (false).",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "loginChain" : {
    "title" : "Linking Authentication Chain",
    "description" : "The authentication chain that will be executed when a user is required to be authenticated locally to match their user account with that of a remotely authenticated assertion.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.107. SamlV2ServiceConfiguration

### 1.107.1. Realm Operations

Resource path: </realm-config/services/saml2>

Resource version: [1.0](#)

### 1.107.1.1. create

Usage:

```
am> create SamlV2ServiceConfiguration --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "metadataSigningKey" : {
      "title" : "Metadata signing key alias",
      "description" : "Specify the private key alias to be used to sign the given entity's metadata
when requesting signed metadata, either by using exportmetadata.jsp or the <code>ssoadm</code>
command.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadataSigningKeyPass" : {
      "title" : "Metadata signing key password",
      "description" : "Specify the password used to retrieve the signing key from the keystore.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

### 1.107.1.2. delete

Usage:

```
am> delete SamlV2ServiceConfiguration --realm Realm
```

### 1.107.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --realm Realm --actionName getAllTypes
```

#### 1.107.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --realm Realm --actionName getCreatableTypes
```

#### 1.107.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --realm Realm --actionName nextdescendents
```

#### 1.107.1.6. read

Usage:

```
am> read SamlV2ServiceConfiguration --realm Realm
```

#### 1.107.1.7. update

Usage:

```
am> update SamlV2ServiceConfiguration --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "metadataSigningKey" : {
      "title" : "Metadata signing key alias",
      "description" : "Specify the private key alias to be used to sign the given entity's metadata
when requesting signed metadata, either by using exportmetadata.jsp or the <code>ssoadm</code>
command.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadataSigningKeyPass" : {
      "title" : "Metadata signing key password",
      "description" : "Specify the password used to retrieve the signing key from the keystore.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

## 1.107.2. Global Operations

Resource path: `/global-config/services/saml2`

Resource version: `1.0`

### 1.107.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --global --actionName getAllTypes
```

### 1.107.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --global --actionName getCreatableTypes
```

### 1.107.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --global --actionName nextdescendents
```

## 1.107.2.4. read

Usage:

```
am> read SamlV2ServiceConfiguration --global
```

## 1.107.2.5. update

Usage:

```
am> update SamlV2ServiceConfiguration --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "idpDiscoveryCookieType" : {
      "title" : "Cookie type for IdP Discovery Service",
      "description" : "Specifies the cookie type to use.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idpDiscoveryUrlSchema" : {
      "title" : "URL scheme for IdP Discovery Service",
      "description" : "Specifies the URL scheme to use.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "caCertValidation" : {
      "title" : "CA Certificate Validation",
      "description" : "If enabled, then validate CA certificates.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "encryptedKeyInKeyInfo" : {
      "title" : "Include xenc:EncryptedKey inside ds:KeyInfo Element",
      "description" : "Specify whether to include the <code>xenc:EncryptedKey</code> property inside the <code>ds:KeyInfo</code> element.",
      "propertyOrder" : 800,
      "required" : true,
```

```

    "type" : "boolean",
    "exampleValue" : ""
  },
  "signingCertValidation" : {
    "title" : "XML Signing Certificate Validation",
    "description" : "If enabled, then validate certificates used to sign documents.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "failOverEnabled" : {
    "title" : "Enable SAML v2.0 failover",
    "description" : "If enabled, OpenAM can failover SAML v2.0 requests to another instance.",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "idpDiscoveryCookieDomain" : {
    "title" : "Cookie domain for IdP Discovery Service",
    "description" : "Specifies the cookie domain for the IDP discovery service.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "xmlSigningClass" : {
    "title" : "XML Signing SPI implementation class",
    "description" : "Used by the SAML2 engine to <em>sign</em> documents.",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "xmlEncryptionClass" : {
    "title" : "XML Encryption SPI implementation class",
    "description" : "Used by the SAML2 engine to <em>encrypt</em> and <em>decrypt</em> documents.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "nameIDInfoAttribute" : {
    "title" : "Attribute name for Name ID information",
    "description" : "User entry attribute to store name identifier information.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "bufferLength" : {
    "title" : "Buffer length (in bytes) to decompress request",
    "description" : "Specify the size of the buffer used for decompressing requests, in bytes.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
},

```



```

"nameIDInfoKeyAttribute" : {
  "title" : "Attribute name for Name ID information key",
  "description" : "User entry attribute to store the name identifier key.",
  "propertyOrder" : 300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"cacheCleanupInterval" : {
  "title" : "Cache cleanup interval (in seconds)",
  "description" : "Time between cache cleanup operations, in seconds.",
  "propertyOrder" : 100,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"defaults" : {
  "properties" : {
    "metadataSigningKey" : {
      "title" : "Metadata signing key alias",
      "description" : "Specify the private key alias to be used to sign the given entity's
metadata when requesting signed metadata, either by using exportmetadata.jsp or the <code>ssoadm</
code> command.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadataSigningKeyPass" : {
      "title" : "Metadata signing key password",
      "description" : "Specify the password used to retrieve the signing key from the keystore.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  },
  "type" : "object",
  "title" : "Realm Defaults"
}
}
}

```

## 1.108. SamlV2SoapBinding

### 1.108.1. Global Operations

Resource path: </global-config/services/federation/saml2soapbinding>

Resource version: 1.0

### 1.108.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SamlV2SoapBinding --global --actionName getAllTypes
```

### 1.108.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SamlV2SoapBinding --global --actionName getCreatableTypes
```

### 1.108.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SamlV2SoapBinding --global --actionName nextdescendents
```

### 1.108.1.4. read

Usage:

```
am> read SamlV2SoapBinding --global
```

### 1.108.1.5. update

Usage:

```
am> update SamlV2SoapBinding --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "requestHandlers" : {
      "title" : "Request Handler List",
      "description" : "List of handlers to deal with SAML v2.0 requests bound to SOAP. <p><p>The required format is: <code>key=<em>Meta Alias</em>|class=<em>Handler Class</em></code> <p><p>Set the <em>key</em> property for a request handler to the meta alias, and the <em>class</em> property to the name of the class that implements the handler.<p><p> For example: <code>key=/pdp|class=com.sun.identity.xacml.plugins.XACMLAuthzDecisionQueryHandler</code>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.109. ScriptStore

### 1.109.1. Realm Operations

Resource path: `/realm-config/services/scripts`

Resource version: `1.0`

#### 1.109.1.1. create

Usage:

```
am> create ScriptStore --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "context" : {
      "title" : "Script type",
```

```

    "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
AUTHENTICATION_SERVER_SIDE : Server-side Authentication AUTHENTICATION_CLIENT_SIDE : Client-side
Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "script" : {
    "title" : "Script",
    "description" : "The source code of the script. The source code is in UTF-8 format and encoded
into Base64",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "createdBy" : {
    "title" : "Created by",
    "description" : "A string containing the universal identifier DN of the subject that created the
script",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "description" : {
    "title" : "Script description",
    "description" : "An optional text string to help identify the script",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lastModifiedBy" : {
    "title" : "Last modifier",
    "description" : "A string containing the universal identifier DN of the subject that most
recently updated the script. If the script has not been modified since it was created, this property
will have the same value as createdBy",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lastModifiedDate" : {
    "title" : "Last modification date",
    "description" : "A string containing the last modified date and time, in ISO 8601 format. If
the script has not been modified since it was created, this property will have the same value as
creationDate",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "creationDate" : {
    "title" : "Creation date",
    "description" : "An integer containing the creation date and time, in ISO 8601 format",
    "propertyOrder" : 1000,
    "required" : true,

```

```
    "type" : "string",
    "exampleValue" : ""
  },
  "name" : {
    "title" : "Script name",
    "description" : "The name provided for the script",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "language" : {
    "title" : "Script language",
    "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
```

### 1.109.1.2. delete

Usage:

```
am> delete ScriptStore --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.109.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptStore --realm Realm --actionName getAllTypes
```

### 1.109.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptStore --realm Realm --actionName getCreatableTypes
```

### 1.109.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptStore --realm Realm --actionName nextdescendents
```

### 1.109.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query ScriptStore --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.109.1.7. read

Usage:

```
am> read ScriptStore --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.109.1.8. update

Usage:

```
am> update ScriptStore --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "context" : {
```

```

    "title" : "Script type",
    "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
AUTHENTICATION_SERVER_SIDE : Server-side Authentication AUTHENTICATION_CLIENT_SIDE : Client-side
Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "script" : {
    "title" : "Script",
    "description" : "The source code of the script. The source code is in UTF-8 format and encoded
into Base64",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "createdBy" : {
    "title" : "Created by",
    "description" : "A string containing the universal identifier DN of the subject that created the
script",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "description" : {
    "title" : "Script description",
    "description" : "An optional text string to help identify the script",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lastModifiedBy" : {
    "title" : "Last modifier",
    "description" : "A string containing the universal identifier DN of the subject that most
recently updated the script. If the script has not been modified since it was created, this property
will have the same value as createdBy",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lastModifiedDate" : {
    "title" : "Last modification date",
    "description" : "A string containing the last modified date and time, in ISO 8601 format. If
the script has not been modified since it was created, this property will have the same value as
creationDate",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "creationDate" : {
    "title" : "Creation date",
    "description" : "An integer containing the creation date and time, in ISO 8601 format",
    "propertyOrder" : 1000,

```

```
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "name" : {
    "title" : "Script name",
    "description" : "The name provided for the script",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "language" : {
    "title" : "Script language",
    "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
```

## 1.110. ScriptTypes

### 1.110.1. Global Operations

Resource path: `/global-config/services/scripting/contexts`

Resource version: `1.0`

#### 1.110.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptTypes --global --actionName getAllTypes
```

#### 1.110.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptTypes --global --actionName getCreatableTypes
```



### 1.110.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptTypes --global --actionName nextdescendents
```

### 1.110.1.4. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query ScriptTypes --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.110.1.5. read

Usage:

```
am> read ScriptTypes --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.110.1.6. update

Usage:

```
am> update ScriptTypes --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultScript" : {
      "title" : "Default Script",
      "description" : "The source code that is presented as the default when creating a new script of
this type.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "languages" : {
      "title" : "Scripting languages",
      "description" : "The language the script is written in.<br><br>This is used to determine how to
validate the script, as well as which engine to run the script within.",
      "propertyOrder" : 1100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.111. ScriptedModule

### 1.111.1. Realm Operations

Resource path: `/realm-config/authentication/modules/scripted`

Resource version: `1.0`

#### 1.111.1.1. create

Usage:

```
am> create ScriptedModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverScript" : {
      "title" : "Server-side Script",
      "description" : "The server-side script to execute.<br><br>This script will be run on the
server, subsequent to any client script having returned.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientScriptEnabled" : {
      "title" : "Client-side Script Enabled",
      "description" : "Enable this setting if the client-side script should be executed.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "clientScript" : {
      "title" : "Client-side Script",
      "description" : "The client-side script.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.111.1.2. delete

Usage:

```
am> delete ScriptedModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.111.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptedModule --realm Realm --actionName getAllTypes
```

### 1.111.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptedModule --realm Realm --actionName getCreatableTypes
```

### 1.111.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptedModule --realm Realm --actionName nextdescendents
```

### 1.111.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query ScriptedModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.111.1.7. read

Usage:

```
am> read ScriptedModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.111.1.8. update

Usage:

```
am> update ScriptedModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverScript" : {
      "title" : "Server-side Script",
      "description" : "The server-side script to execute.<br><br>This script will be run on the
server, subsequent to any client script having returned.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientScriptEnabled" : {
      "title" : "Client-side Script Enabled",
      "description" : "Enable this setting if the client-side script should be executed.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "clientScript" : {
      "title" : "Client-side Script",
      "description" : "The client-side script.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.111.2. Global Operations

Resource path: `/global-config/authentication/modules/scripted`

Resource version: `1.0`

### 1.111.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptedModule --global --actionName getAllTypes
```

### 1.111.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptedModule --global --actionName getCreatableTypes
```

### 1.111.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptedModule --global --actionName nextdescendents
```

### 1.111.2.4. read

Usage:

```
am> read ScriptedModule --global
```

### 1.111.2.5. update

Usage:

```
am> update ScriptedModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with the authentication module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientScriptEnabled" : {
          "title" : "Client-side Script Enabled",
          "description" : "Enable this setting if the client-side script should be executed.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientScript" : {
          "title" : "Client-side Script",
          "description" : "The client-side script.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "serverScript" : {
          "title" : "Server-side Script",
          "description" : "The server-side script to execute.<br><br>This script will be run on the server, subsequent to any client script having returned.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

## 1.112. Scripting

### 1.112.1. Global Operations

Resource path: `/global-config/services/scripting`

Resource version: `1.0`

### 1.112.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Scripting --global --actionName getAllTypes
```

### 1.112.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Scripting --global --actionName getCreatableTypes
```

### 1.112.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Scripting --global --actionName nextdescendents
```

### 1.112.1.4. read

Usage:

```
am> read Scripting --global
```

### 1.112.1.5. update

Usage:

```
am> update Scripting --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:



```
{
  "type" : "object",
  "properties" : {
    "defaultContext" : {
      "title" : "Default Script Type",
      "description" : "The default script context type when creating a new script.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.113. ScriptingEngineConfiguration

### 1.113.1. Global Operations

Resource path: `/global-config/services/scripting/contexts/{contexts}/engineConfiguration`

Resource version: **1.0**

#### 1.113.1.1. create

Usage:

```
am> create ScriptingEngineConfiguration --global --contexts contexts --body body
```

Parameters:

**--contexts**

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "maxThreads" : {
      "title" : "Maximum thread pool size",
      "description" : "The maximum size of the thread pool from which scripts will operate.<br><br>New threads will be created up to this size once the task queue reaches capacity. Has no effect if the queue is unbounded.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "blackList" : {
      "title" : "Java class blacklist",
```

```

    "description" : "List of patterns of Java classes that must not be accessed by a
script.<br><br>This blacklist is applied after the whitelist to apply additional restrictions. For
instance you may whitelist java.lang.* and then blacklist java.lang.System and java.lang.Runtime. It
is recommended to always prefer specific whitelists where possible.",
    "propertyOrder" : 700,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"whitelist" : {
    "title" : "Java class whitelist",
    "description" : "List of patterns of allowed Java classes that may be loaded/accessed by
scripts.<br><br>Each Java class accessed by a script must match at least one of these patterns. Use
'*' as a wildcard, e.g. <code>java.lang.*</code>",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"useSecurityManager" : {
    "title" : "Use system SecurityManager",
    "description" : "Indicates whether the system SecurityManager should also be consulted when
checking access to Java classes.<br><br>If enabled, then the checkPackageAccess method will be called
for each Java class accessed. If no SecurityManager is configured, then this has no effect.",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"queueSize" : {
    "title" : "Thread pool queue size",
    "description" : "Size of queue to use for buffering script execution request when core pool is
at capacity.<br><br>Use -1 for an unbounded queue (this disables the maximum pool size setting). For
short, CPU-bound scripts, consider a small pool size and larger queue length. For I/O-bound scripts
(e.g., REST calls) consider a larger maximum pool size and a smaller queue. Not hot-swappable:
restart server for changes to take effect.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"coreThreads" : {
    "title" : "Core thread pool size",
    "description" : "The core size of the thread pool from which scripts will operate.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"serverTimeout" : {
    "title" : "Server-side Script Timeout",
    "description" : "The maximum execution time any individual script should take on the server (in
seconds).<br><br>Server-side scripts will be forcibly stopped after this amount of execution time.",

```

```
    "propertyOrder" : 100,  
    "required" : true,  
    "type" : "integer",  
    "exampleValue" : ""  
  },  
  "idleTimeout" : {  
    "title" : "Thread idle timeout (seconds)",  
    "description" : "Length of time (in seconds) to wait before terminating threads.<br><br>Length  
of time (in seconds) to wait before terminating threads that were started when the queue reached  
capacity. Only applies to threads beyond the core pool size (up to the maximum size).",  
    "propertyOrder" : 500,  
    "required" : true,  
    "type" : "integer",  
    "exampleValue" : ""  
  }  
}  
}
```

### 1.113.1.2. delete

Usage:

```
am> delete ScriptingEngineConfiguration --global --contexts contexts
```

Parameters:

**--contexts**

### 1.113.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptingEngineConfiguration --global --contexts contexts --actionName getAllTypes
```

Parameters:

**--contexts**

### 1.113.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptingEngineConfiguration --global --contexts contexts --actionName getCreatableTypes
```

Parameters:

**--contexts**

### 1.113.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptingEngineConfiguration --global --contexts contexts --actionName nextdescendents
```

Parameters:

**--contexts**

### 1.113.1.6. read

Usage:

```
am> read ScriptingEngineConfiguration --global --contexts contexts
```

Parameters:

**--contexts**

### 1.113.1.7. update

Usage:

```
am> update ScriptingEngineConfiguration --global --contexts contexts --body body
```

Parameters:

**--contexts**

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "maxThreads" : {
      "title" : "Maximum thread pool size",
      "description" : "The maximum size of the thread pool from which scripts will operate.<br><br>New threads will be created up to this size once the task queue reaches capacity. Has no effect if the queue is unbounded.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "blackList" : {
      "title" : "Java class blacklist",
      "description" : "List of patterns of Java classes that must not be accessed by a script.<br><br>This blacklist is applied after the whitelist to apply additional restrictions. For
```

```
instance you may whitelist java.lang.* and then blacklist java.lang.System and java.lang.Runtime. It
is recommended to always prefer specific whitelists where possible.",
  "propertyOrder" : 700,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"whiteList" : {
  "title" : "Java class whitelist",
  "description" : "List of patterns of allowed Java classes that may be loaded/accessed by
scripts.<br><br>Each Java class accessed by a script must match at least one of these patterns. Use
'*' as a wildcard, e.g. <code>java.lang.*</code>",
  "propertyOrder" : 600,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"useSecurityManager" : {
  "title" : "Use system SecurityManager",
  "description" : "Indicates whether the system SecurityManager should also be consulted when
checking access to Java classes.<br><br>If enabled, then the checkPackageAccess method will be called
for each Java class accessed. If no SecurityManager is configured, then this has no effect.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"queueSize" : {
  "title" : "Thread pool queue size",
  "description" : "Size of queue to use for buffering script execution request when core pool is
at capacity.<br><br>Use -1 for an unbounded queue (this disables the maximum pool size setting). For
short, CPU-bound scripts, consider a small pool size and larger queue length. For I/O-bound scripts
(e.g., REST calls) consider a larger maximum pool size and a smaller queue. Not hot-swappable:
restart server for changes to take effect.",
  "propertyOrder" : 400,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"coreThreads" : {
  "title" : "Core thread pool size",
  "description" : "The core size of the thread pool from which scripts will operate.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"serverTimeout" : {
  "title" : "Server-side Script Timeout",
  "description" : "The maximum execution time any individual script should take on the server (in
seconds).<br><br>Server-side scripts will be forcibly stopped after this amount of execution time.",
  "propertyOrder" : 100,
  "required" : true,
```

```
    "type" : "integer",
    "exampleValue" : ""
  },
  "idleTimeout" : {
    "title" : "Thread idle timeout (seconds)",
    "description" : "Length of time (in seconds) to wait before terminating threads.<br><br>Length of time (in seconds) to wait before terminating threads that were started when the queue reached capacity. Only applies to threads beyond the core pool size (up to the maximum size).",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }
}
```

## 1.114. Scripts

### 1.114.1. Realm Operations

The script resources service is responsible for managing scripts used for client-side and server-side scripted authentication, custom policy conditions, and handling OpenID Connect claims. Scripts are represented in JSON and take the following form. Scripts are built from standard JSON objects and values (strings, numbers, objects, sets, arrays, true, false, and null). Each script has a system-generated universally unique identifier (UUID), which must be used when modifying existing scripts. Renaming a script will not affect the UUID

Resource path: `/scripts`

Resource version: `1.1`

#### 1.114.1.1. create

Create a script in a realm. The value for script must be in UTF-8 format and then encoded into Base64.

Usage:

```
am> create Scripts --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Script resource endpoint json schema",
```

```

"type" : "object",
"title" : "Script resource schema",
"properties" : {
  "_id" : {
    "title" : "Script unique ID",
    "description" : "A unique ID for a script configuration, provided by the server",
    "type" : "string"
  },
  "name" : {
    "title" : "Script name",
    "description" : "The name provided for the script",
    "type" : "string"
  },
  "description" : {
    "title" : "Script description",
    "description" : "An optional text string to help identify the script",
    "type" : "string"
  },
  "script" : {
    "title" : "Script",
    "description" : "The source code of the script. The source code is in UTF-8 format and encoded
into Base64",
    "type" : "string"
  },
  "language" : {
    "title" : "Script language",
    "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
    "type" : "string"
  },
  "context" : {
    "title" : "Script type",
    "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
AUTHENTICATION_SERVER_SIDE : Server-side Authentication AUTHENTICATION_CLIENT_SIDE : Client-side
Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims",
    "type" : "string"
  },
  "createdBy" : {
    "title" : "Created by",
    "description" : "A string containing the universal identifier DN of the subject that created the
script",
    "type" : "string"
  },
  "creationDate" : {
    "title" : "Creation date",
    "description" : "An integer containing the creation date and time, in ISO 8601 format",
    "type" : "number"
  },
  "lastModifiedBy" : {
    "title" : "Last modifier",
    "description" : "A string containing the universal identifier DN of the subject that most
recently updated the script. If the script has not been modified since it was created, this property
will have the same value as createdBy",
    "type" : "string"
  },
  "lastModifiedDate" : {
    "title" : "Last modification date",
    "description" : "A string containing the last modified date and time, in ISO 8601 format. If
the script has not been modified since it was created, this property will have the same value as
creationDate",

```

```
    "type" : "number"
  },
  "required" : [ "name", "description", "script", "language", "context" ]
}
```

### 1.114.1.2. delete

Delete an individual script in a realm specified by the UUID parameter

Usage:

```
am> delete Scripts --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.114.1.3. query

List all the scripts in a realm, as well as any global scripts

Usage:

```
am> query Scripts --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

### 1.114.1.4. read

Read an individual script in a realm by specifying the UUID parameter

Usage:

```
am> read Scripts --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.114.1.5. update

Update an individual script in a realm specified by the UUID parameter



## Usage:

```
am> update Scripts --realm Realm --id id --body body
```

## Parameters:

### --id

The unique identifier for the resource.

### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Script resource endpoint json schema",
  "type" : "object",
  "title" : "Script resource schema",
  "properties" : {
    "_id" : {
      "title" : "Script unique ID",
      "description" : "A unique ID for a script configuration, provided by the server",
      "type" : "string"
    },
    "name" : {
      "title" : "Script name",
      "description" : "The name provided for the script",
      "type" : "string"
    },
    "description" : {
      "title" : "Script description",
      "description" : "An optional text string to help identify the script",
      "type" : "string"
    },
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
into Base64",
      "type" : "string"
    },
    "language" : {
      "title" : "Script language",
      "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
      "type" : "string"
    },
    "context" : {
      "title" : "Script type",
      "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
AUTHENTICATION_SERVER_SIDE : Server-side Authentication AUTHENTICATION_CLIENT_SIDE : Client-side
Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims",
      "type" : "string"
    },
    "createdBy" : {
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject that created the
script",
      "type" : "string"
    },
    "creationDate" : {
```

```

    "title" : "Creation date",
    "description" : "An integer containing the creation date and time, in ISO 8601 format",
    "type" : "number"
  },
  "lastModifiedBy" : {
    "title" : "Last modifier",
    "description" : "A string containing the universal identifier DN of the subject that most
recently updated the script. If the script has not been modified since it was created, this property
will have the same value as createdBy",
    "type" : "string"
  },
  "lastModifiedDate" : {
    "title" : "Last modification date",
    "description" : "A string containing the last modified date and time, in ISO 8601 format. If
the script has not been modified since it was created, this property will have the same value as
creationDate",
    "type" : "number"
  }
},
"required" : [ "name", "description", "script", "language", "context" ]
}

```

### 1.114.1.6. validate

Validate a script. Include a JSON representation of the script and the script language, JAVASCRIPT or GROOVY, in the POST data. The value for script must be in UTF-8 format and then encoded into Base64

Usage:

```
am> action Scripts --realm Realm --body body --actionName validate
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```

{
  "description" : "Validate action request schema",
  "type" : "object",
  "title" : "Validate request schema",
  "properties" : {
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
into Base64",
      "type" : "string"
    },
    "language" : {
      "title" : "Script language",
      "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
      "type" : "string"
    }
  },
  "required" : [ "script", "language" ]
}

```

## 1.115. SdkProperties

### 1.115.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/sdk`

Resource version: `1.0`

#### 1.115.1.1. read

Usage:

```
am> read SdkProperties --global --serverName serverName
```

Parameters:

**--serverName**

An object of property key-value pairs

#### 1.115.1.2. update

Usage:

```
am> update SdkProperties --global --serverName serverName --body body
```

Parameters:

**--serverName**

An object of property key-value pairs

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.datastore" : {
      "title" : "Data Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "com.sun.identity.sm.enableDataStoreNotification" : {
          "title" : "Enable Datastore Notification",
          "type" : "object",
          "propertyOrder" : 0,
```

```

    "description" : "Specifies if backend datastore notification is enabled. If
this value is set to 'false', then in-memory notification is enabled. (property name:
com.sun.identity.sm.enableDataStoreNotification)",
    "properties" : {
        "value" : {
            "type" : "boolean",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
},
"com.sun.identity.sm.ldap.enableProxy" : {
    "title" : "Enable Directory Proxy",
    "type" : "object",
    "propertyOrder" : 1,
    "description" : "This indicates to Service Management that the Directory Proxy must be used
for read, write, and/or modify operations to the Directory Server. This flag also determines if ACIs
or delegation privileges are to be used. (property name: com.sun.identity.sm.ldap.enableProxy)",
    "properties" : {
        "value" : {
            "type" : "boolean",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
},
"com.sun.identity.sm.notification.threadpool.size" : {
    "title" : "Notification Pool Size",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "Specifies the size of the sm notification thread pool (total number of
threads). (property name: com.sun.identity.sm.notification.threadpool.size)",
    "properties" : {
        "value" : {
            "type" : "integer",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
}
},
"amconfig.header.eventservice" : {
    "title" : "Event Service",
    "type" : "object",
    "propertyOrder" : 1,
    "properties" : {
        "com.iplanet.am.event.connection.num.retries" : {
            "title" : "Number of retries for Event Service connections",
            "type" : "object",

```

```

        "propertyOrder" : 0,
        "description" : "Specifies the number of attempts made to successfully re-establish the
Event Service connections. (property name: com.ipplanet.am.event.connection.num.retries)",
        "properties" : {
            "value" : {
                "type" : "integer",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.ipplanet.am.event.connection.delay.between.retries" : {
        "title" : "Delay between Event Service connection retries",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "Specifies the delay in milliseconds between retries to re-establish the
Event Service connections. (property name: com.ipplanet.am.event.connection.delay.between.retries)",
        "properties" : {
            "value" : {
                "type" : "integer",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.ipplanet.am.event.connection.ldap.error.codes.retries" : {
        "title" : "Error codes for Event Service connection retries",
        "type" : "object",
        "propertyOrder" : 2,
        "description" : "This secifies the LDAP exception error codes for which
retries to re-establish Event Service connections will trigger. (property name:
com.ipplanet.am.event.connection.ldap.error.codes.retries)",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.sun.am.event.connection.disable.list" : {
        "title" : "Disabled Event Service Connection",
        "type" : "object",
        "propertyOrder" : 3,
        "description" : "Specifies which event connection (persistent search) to be disabled. There
are three valid values - aci, sm and um (case insensitive). Multiple values should be separated with
\", \". (property name: com.sun.am.event.connection.disable.list)",
        "properties" : {
            "value" : {
                "type" : "string",

```

```

        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  }
},
"amconfig.header.ldapconnection" : {
  "title" : "LDAP Connection",
  "type" : "object",
  "propertyOrder" : 2,
  "properties" : {
    "com.ipplanet.am.ldap.connection.num.retries" : {
      "title" : "Number of retries for LDAP Connection",
      "type" : "object",
      "propertyOrder" : 0,
      "description" : "Specifies the number of attempts made to successfully re-establish LDAP
Connection. (property name: com.ipplanet.am.ldap.connection.num.retries)",
      "properties" : {
        "value" : {
          "type" : "integer",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    },
    "com.ipplanet.am.ldap.connection.delay.between.retries" : {
      "title" : "Delay between LDAP connection retries",
      "type" : "object",
      "propertyOrder" : 1,
      "description" : "Specifies the delay in milliseconds between retries to re-establish the
LDAP connections. (property name: com.ipplanet.am.ldap.connection.delay.between.retries)",
      "properties" : {
        "value" : {
          "type" : "integer",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  }
},
"com.ipplanet.am.ldap.connection.ldap.error.codes.retries" : {
  "title" : "Error codes for LDAP connection retries",
  "type" : "object",
  "propertyOrder" : 2,
  "description" : "This secifies the LDAP exception error codes for
which retries to re-establish LDAP connections will trigger. (property name:
com.ipplanet.am.ldap.connection.ldap.error.codes.retries)",
  "properties" : {
    "value" : {
      "type" : "string",

```

```

        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "amconfig.header.cachingreplica" : {
    "title" : "Caching and Replica",
    "type" : "object",
    "propertyOrder" : 3,
    "properties" : {
      "com.iplanet.am.sdk.cache.maxSize" : {
        "title" : "SDK Caching Max. Size",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "Specifies the size of the cache when SDK caching is enabled. The size should be an integer greater than 0, or default size (10000) will be used. Changing this value will reset (clear) the contents of the cache. (property name: com.iplanet.am.sdk.cache.maxSize)",
        "properties" : {
          "value" : {
            "type" : "integer",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "com.iplanet.am.replica.num.retries" : {
        "title" : "SDK Replica Retries",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "Specifies the number of times to retry when an Entry Not Found error is returned to the SDK. (property name: com.iplanet.am.replica.num.retries)",
        "properties" : {
          "value" : {
            "type" : "integer",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  },
  "com.iplanet.am.replica.delay.between.retries" : {
    "title" : "Delay between SDK Replica Retries",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "Specifies the delay time in milliseconds between the retries. (property name: com.iplanet.am.replica.delay.between.retries)",
    "properties" : {
      "value" : {
        "type" : "integer",

```

```

        "required" : false
    },
    "inherited" : {
        "type" : "boolean",
        "required" : true
    }
}
},
"amconfig.header.sdktimetoliveconfig" : {
    "title" : "Time To Live Configuration",
    "type" : "object",
    "propertyOrder" : 4,
    "properties" : {
        "com.ipplanet.am.sdk.cache.entry.expire.enabled" : {
            "title" : "Cache Entry Expiration Enabled",
            "type" : "object",
            "propertyOrder" : 0,
            "description" : "If this property is set, the cache entries will expire
based on the time specified in User Entry Expiration Time property. (property name:
com.ipplanet.am.sdk.cache.entry.expire.enabled)",
            "properties" : {
                "value" : {
                    "type" : "boolean",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        },
        "com.ipplanet.am.sdk.cache.entry.user.expire.time" : {
            "title" : "User Entry Expiration Time",
            "type" : "object",
            "propertyOrder" : 1,
            "description" : "This property specifies time in minutes for which the user entries remain
valid in cache after their last modification. After this specified period of time elapses (after the
last modification/read from the directory), the data for the entry that is cached will expire. At
that instant new requests for data for these user entries will result in reading from the Directory.
(property name: com.ipplanet.am.sdk.cache.entry.user.expire.time)",
            "properties" : {
                "value" : {
                    "type" : "integer",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        }
    }
},
"com.ipplanet.am.sdk.cache.entry.default.expire.time" : {
    "title" : "Default Entry Expiration Time",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "This property specifies time in minutes for which the non-user entries
remain valid in cache after their last modification. After this specified period of time elapses

```



(after the last modification/read from the directory), the data for the entry that is cached will expire. At that instant new requests for data for these non-user entries will result in reading from the Directory. (property name: com.ipplanet.am.sdk.cache.entry.default.expire.time)",

```
"properties" : {  
  "value" : {  
    "type" : "integer",  
    "required" : false  
  },  
  "inherited" : {  
    "type" : "boolean",  
    "required" : true  
  }  
}  
}  
}  
}  
}
```

## 1.116. SecurIdModule

### 1.116.1. Realm Operations

Resource path: `/realm-config/authentication/modules/securid`

Resource version: `1.0`

#### 1.116.1.1. create

Usage:

```
am> create SecurIdModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "serverConfigPath" : {
      "title" : "ACE/Server Configuration Path",
      "description" : "The path to the ACE/Server configuration files",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

### 1.116.1.2. delete

Usage:

```
am> delete SecurIdModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.116.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SecurIdModule --realm Realm --actionName getAllTypes
```

### 1.116.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SecurIdModule --realm Realm --actionName getCreatableTypes
```

### 1.116.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SecurIdModule --realm Realm --actionName nextdescendents
```

### 1.116.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query SecurIdModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.116.1.7. read

Usage:

```
am> read SecurIdModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.116.1.8. update

Usage:

```
am> update SecurIdModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "serverConfigPath" : {
      "title" : "ACE/Server Configuration Path",
      "description" : "The path to the ACE/Server configuration files",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.116.2. Global Operations

Resource path: `/global-config/authentication/modules/securid`

Resource version: `1.0`

### 1.116.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SecurIdModule --global --actionName getAllTypes
```

### 1.116.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SecurIdModule --global --actionName getCreatableTypes
```

### 1.116.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SecurIdModule --global --actionName nextdescendents
```

## 1.116.2.4. read

Usage:

```
am> read SecurIdModule --global
```

## 1.116.2.5. update

Usage:

```
am> update SecurIdModule --global --body body
```

Parameters:

### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "serverConfigPath" : {
          "title" : "ACE/Server Configuration Path",
          "description" : "The path to the ACE/Server configuration files",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : null,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

## 1.117. SecurityProperties

### 1.117.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/security`

Resource version: `1.0`

#### 1.117.1.1. read

Usage:

```
am> read SecurityProperties --global --serverName serverName
```

Parameters:

**--serverName**

An object of property key-value pairs

#### 1.117.1.2. update

Usage:

```
am> update SecurityProperties --global --serverName serverName --body body
```

Parameters:

**--serverName**

An object of property key-value pairs

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.encryption" : {
      "title" : "Encryption",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "am.encryption.pwd" : {
          "title" : "Password Encryption Key",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "The encryption key value for decrypting passwords stored in the Service Management System configuration. (property name: am.encryption.pwd)",
```

```

    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "com.iplanet.am.service.secret" : {
    "title" : "Authentication Service Shared Secret",
    "type" : "object",
    "propertyOrder" : 1,
    "description" : "The shared secret for application authentication module. (property name: com.iplanet.am.service.secret)",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "com.iplanet.security.encryptor" : {
    "title" : "Encryption class",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "The default encryption class. (property name: com.iplanet.security.encryptor)",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "com.iplanet.security.SecureRandomFactoryImpl" : {
    "title" : "Secure Random Factory Class",
    "type" : "object",
    "propertyOrder" : 3,
    "description" : "This property is used for specifying SecureRandomFactory class. Available values for this property are com.iplanet.am.util.JSSSecureRandomFactoryImpl that is using JSS and com.iplanet.am.util.SecureRandomFactoryImpl that is using pure Java only. (property name: com.iplanet.security.SecureRandomFactoryImpl)",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {

```

```

        "type" : "boolean",
        "required" : true
    }
}
},
"amconfig.header.validation" : {
    "title" : "Validation",
    "type" : "object",
    "propertyOrder" : 1,
    "properties" : {
        "com.ipplanet.services.comm.server.pllrequest.maxContentLength" : {
            "title" : "Platform Low Level Comm. Max. Content Length",
            "type" : "object",
            "propertyOrder" : 0,
            "description" : "Maximum content-length for an HttpRequest. (property name: com.ipplanet.services.comm.server.pllrequest.maxContentLength)",
            "properties" : {
                "value" : {
                    "type" : "integer",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        },
        "com.ipplanet.am.clientIPCheckEnabled" : {
            "title" : "Client IP Address Check",
            "type" : "object",
            "propertyOrder" : 1,
            "description" : "Specifies whether or not the IP address of the client is checked in all single sign on token creations or validations. (property name: com.ipplanet.am.clientIPCheckEnabled)",
            "properties" : {
                "value" : {
                    "type" : "boolean",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        }
    }
},
"amconfig.header.cookie" : {
    "title" : "Cookie",
    "type" : "object",
    "propertyOrder" : 2,
    "properties" : {
        "com.ipplanet.am.cookie.name" : {
            "title" : "Cookie Name",
            "type" : "object",
            "propertyOrder" : 0,

```



```

    "description" : "The cookie name used by Authentication Service to set the valid
session handler ID. This name is used to retrieve the valid session information. (property name:
com.ipplanet.am.cookie.name)",
    "properties" : {
        "value" : {
            "type" : "string",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
},
"com.ipplanet.am.cookie.secure" : {
    "title" : "Secure Cookie",
    "type" : "object",
    "propertyOrder" : 1,
    "description" : "Specifies whether to set cookie in a secure mode in which the browser
will only return the cookie when a secure protocol such as HTTP(s) is used. (property name:
com.ipplanet.am.cookie.secure)",
    "properties" : {
        "value" : {
            "type" : "boolean",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
},
"com.ipplanet.am.cookie.encode" : {
    "title" : "Encode Cookie Value",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "Specifies whether to URL encode the cookie value. (property name:
com.ipplanet.am.cookie.encode)",
    "properties" : {
        "value" : {
            "type" : "boolean",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
}
},
"amconfig.header.securitykey" : {
    "title" : "Key Store",
    "type" : "object",
    "propertyOrder" : 3,
    "properties" : {
        "com.sun.identity.saml.xmlsig.keystore" : {
            "title" : "Keystore File",
            "type" : "object",

```

```

        "propertyOrder" : 0,
        "description" : "Specifies the location of the keystore file. (property name:
com.sun.identity.saml.xmlsig.keystore)",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.sun.identity.saml.xmlsig.storetype" : {
        "title" : "Keystore Type",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "Specifies the keystore type. (property name:
com.sun.identity.saml.xmlsig.storetype)",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.sun.identity.saml.xmlsig.storepass" : {
        "title" : "Keystore Password File",
        "type" : "object",
        "propertyOrder" : 2,
        "description" : "Specifies the location of the file that contains the password used to
access the keystore file. (property name: com.sun.identity.saml.xmlsig.storepass)",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "com.sun.identity.saml.xmlsig.keypass" : {
        "title" : "Private Key Password File",
        "type" : "object",
        "propertyOrder" : 3,
        "description" : "Specifies the location of the file that contains the
password used to protect the private key of a generated key pair. (property name:
com.sun.identity.saml.xmlsig.keypass)",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            }
        }
    }
}

```

```

    },
    "inherited" : {
      "type" : "boolean",
      "required" : true
    }
  }
},
"com.sun.identity.saml.xmlsig.certalias" : {
  "title" : "Certificate Alias",
  "type" : "object",
  "propertyOrder" : 4,
  "description" : "(property name: com.sun.identity.saml.xmlsig.certalias)",
  "properties" : {
    "value" : {
      "type" : "string",
      "required" : false
    },
    "inherited" : {
      "type" : "boolean",
      "required" : true
    }
  }
}
}
},
"amconfig.header.crlcache" : {
  "title" : "Certificate Revocation List Caching",
  "type" : "object",
  "propertyOrder" : 4,
  "properties" : {
    "com.sun.identity.crl.cache.directory.host" : {
      "title" : "LDAP server host name",
      "type" : "object",
      "propertyOrder" : 0,
      "description" : "",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  }
},
"com.sun.identity.crl.cache.directory.port" : {
  "title" : "LDAP server port number",
  "type" : "object",
  "propertyOrder" : 1,
  "description" : "",
  "properties" : {
    "value" : {
      "type" : "integer",
      "required" : false
    },
    "inherited" : {
      "type" : "boolean",
      "required" : true
    }
  }
}
}

```

```

    }
  },
  "com.sun.identity.crl.cache.directory.ssl" : {
    "title" : "SSL/TLS Enabled",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "boolean",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "com.sun.identity.crl.cache.directory.user" : {
    "title" : "LDAP server bind user name",
    "type" : "object",
    "propertyOrder" : 3,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "com.sun.identity.crl.cache.directory.password" : {
    "title" : "LDAP server bind password",
    "type" : "object",
    "propertyOrder" : 4,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false,
        "format" : "password"
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "com.sun.identity.crl.cache.directory.searchlocs" : {
    "title" : "LDAP search base DN",
    "type" : "object",
    "propertyOrder" : 5,
    "description" : "",
    "properties" : {
      "value" : {

```

```

        "type" : "string",
        "required" : false
    },
    "inherited" : {
        "type" : "boolean",
        "required" : true
    }
},
{
    "com.sun.identity.crl.cache.directory.searchattr" : {
        "title" : "Search Attributes",
        "type" : "object",
        "propertyOrder" : 6,
        "description" : "Any DN component of issuer's subjectDN can be used to retrieve CRL from
local LDAP server. It is single value string, like, \"cn\". All Root CA need to use the same search
attribute.",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    }
},
{
    "amconfig.header.ocsp.check" : {
        "title" : "Online Certificate Status Protocol Check",
        "type" : "object",
        "propertyOrder" : 5,
        "properties" : {
            "com.sun.identity.authentication.ocspCheck" : {
                "title" : "Check Enabled",
                "type" : "object",
                "propertyOrder" : 0,
                "description" : "",
                "properties" : {
                    "value" : {
                        "type" : "boolean",
                        "required" : false
                    },
                    "inherited" : {
                        "type" : "boolean",
                        "required" : true
                    }
                }
            }
        }
    },
    "com.sun.identity.authentication.ocsp.responder.url" : {
        "title" : "Responder URL",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            }
        }
    }
}

```



## 1.118. ServerInformation

### 1.118.1. Realm Operations

Provides information about the server.

Resource path: `/serverinfo`

Resource version: `1.1`

#### 1.118.1.1. read

Read the server information.

Usage:

```
am> read ServerInformation --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.119. ServerVersion

### 1.119.1. Realm Operations

Server Version schema

Resource path: `/serverinfo/version`

Resource version: `1.0`

#### 1.119.1.1. read

It returns information about OpenAM such as: version, revision and date

Usage:

```
am> read ServerVersion --realm Realm
```

## 1.120. Servers

### 1.120.1. Global Operations

Servers resource provider is responsible for managing Servers and their configuration for an OpenAM instance.

Resource path: `/global-config/servers`

Resource version: `1.0`

#### 1.120.1.1. clone

Clone the specified Server, keeping it's settings but using a different URL.

Usage:

```
am> action Servers --global --body body --actionName clone
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Container for required data to clone a Server.",
  "type" : "object",
  "title" : "Clone Server Request schema",
  "properties" : {
    "clonedUrl" : {
      "type" : "string",
      "title" : "Cloned Server URL",
      "description" : "The new URL of the cloned server. Must be unique."
    }
  }
}
```

#### 1.120.1.2. create

Create a Server.

Usage:

```
am> create Servers --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.



--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Describes the data that a Server Resource could contain.",
  "type" : "object",
  "title" : "Server resource schema",
  "properties" : {
    "_id" : {
      "type" : "string",
      "title" : "Server id",
      "description" : "Unique identifier of the Server."
    },
    "siteName" : {
      "type" : "string",
      "title" : "Site name",
      "description" : "The Server's name."
    },
    "url" : {
      "type" : "string",
      "title" : "Url",
      "description" : "The URL of the Server."
    }
  }
}
```

### 1.120.1.3. delete

Delete a Server.

Usage:

```
am> delete Servers --global --id id
```

Parameters:

--id

The unique identifier for the resource.

### 1.120.1.4. query

Query the collection of the Servers.

Usage:

```
am> query Servers --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

## 1.120.1.5. read

Read a Server.

Usage:

```
am> read Servers --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.121. Services

### 1.121.1. Realm Operations

The collection of services available on a realm.

Resource path: `/realm-config/services`

Resource version: `1.0`

#### 1.121.1.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Services --realm Realm --actionName getAllTypes
```

#### 1.121.1.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Services --realm Realm --actionName getCreatableTypes
```

#### 1.121.1.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Services --realm Realm --actionName nextdescendents
```

#### 1.121.1.4. query

Find services provisioned for the realm - query for a particular service by identifier, or request all services using `\_queryFilter=true`

Usage:

```
am> query Services --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\_id]

### 1.121.2. Global Operations

Global and default configuration for services

Resource path: `/global-config/services`

Resource version: `1.0`

#### 1.121.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Services --global --actionName getAllTypes
```

#### 1.121.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Services --global --actionName getCreatableTypes
```

#### 1.121.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Services --global --actionName nextdescendents
```

## 1.122. Session

### 1.122.1. Realm Operations

Resource path: `/realm-config/services/session`

Resource version: `1.0`

#### 1.122.1.1. create

Usage:

```
am> create Session --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "maxCachingTime" : {
          "title" : "Maximum Caching Time",
          "description" : "Maximum time before OpenAM refreshes a session that has been cached, in minutes.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxSessionTime" : {
          "title" : "Maximum Session Time",
          "description" : "Maximum time a session can remain valid before OpenAM requires the user to authenticate again, in minutes.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxIdleTime" : {
          "title" : "Maximum Idle Time",
          "description" : "Maximum time a stateful session can remain idle before OpenAM requires the user to authenticate again, in minutes.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "quotaLimit" : {
```

```
        "title" : "Active User Sessions",
        "description" : "Maximum number of concurrent stateful sessions OpenAM allows a user to
have.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
},
"type" : "object",
"title" : "Dynamic Attributes"
}
}
```

### 1.122.1.2. delete

Usage:

```
am> delete Session --realm Realm
```

### 1.122.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Session --realm Realm --actionName getAllTypes
```

### 1.122.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Session --realm Realm --actionName getCreatableTypes
```

### 1.122.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Session --realm Realm --actionName nextdescendents
```

### 1.122.1.6. read

Usage:

```
am> read Session --realm Realm
```

## 1.122.1.7. update

Usage:

```
am> update Session --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "maxCachingTime" : {
          "title" : "Maximum Caching Time",
          "description" : "Maximum time before OpenAM refreshes a session that has been cached, in
minutes.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxSessionTime" : {
          "title" : "Maximum Session Time",
          "description" : "Maximum time a session can remain valid before OpenAM requires the user to
authenticate again, in minutes.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxIdleTime" : {
          "title" : "Maximum Idle Time",
          "description" : "Maximum time a stateful session can remain idle before OpenAM requires the
user to authenticate again, in minutes.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "quotaLimit" : {
          "title" : "Active User Sessions",
          "description" : "Maximum number of concurrent stateful sessions OpenAM allows a user to
have.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  },
}
```

```
    "type" : "object",  
    "title" : "Dynamic Attributes"  
  }  
}  
}
```

## 1.122.2. Global Operations

Resource path: `/global-config/services/session`

Resource version: `1.0`

### 1.122.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Session --global --actionName getAllTypes
```

### 1.122.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Session --global --actionName getCreatableTypes
```

### 1.122.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Session --global --actionName nextdescendents
```

### 1.122.2.4. read

Usage:

```
am> read Session --global
```

### 1.122.2.5. update

Usage:

```
am> update Session --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "notifications" : {
      "type" : "object",
      "title" : "Session Property Change Notifications",
      "propertyOrder" : 2,
      "properties" : {
        "propertyChangeNotifications" : {
          "title" : "Enable Property Change Notifications",
          "description" : "If on, then OpenAM notifies other applications participating in SSO when a session property in the Notification Properties list changes on a stateful session.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "notificationPropertyList" : {
          "title" : "Notification Properties",
          "description" : "Lists session properties for which OpenAM can send notifications upon modification. Session notification applies to stateful sessions only.",
          "propertyOrder" : 1200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "stateless" : {
      "type" : "object",
      "title" : "Stateless Sessions",
      "propertyOrder" : 4,
      "properties" : {
        "openam-session-stateless-blacklist-purge-delay" : {
          "title" : "Blacklist Purge Delay (minutes)",
          "description" : "When added to the maximum session time, specifies the amount of time that OpenAM tracks logged out sessions.<br><br>Increase the blacklist purge delay if you expect system clock skews in a cluster of OpenAM servers to be greater than one minute. There is no need to increase the blacklist purge delay for servers running a clock synchronization protocol, such as Network Time Protocol.<p><p>Applies only to deployments using stateless sessions and session blacklisting.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "statelessEncryptionAesKey" : {
          "title" : "Symmetric AES Key",
          "description" : "AES key for use with Direct or AES KeyWrap encryption modes.<br><br>The symmetric AES key is a base64-encoded random key.<p><p>For direct encryption with <code>AES-GCM</code>"
        }
      }
    }
  }
}
```



```
code> or for <code>AES-KeyWrap</code> with any content encryption method, this should be 128, 192, or
256 bits.<p><p>For direct encryption with <code>AES-CBC-HMAC</code>, the key should be double those
sizes (one half for the AES key, the other have for the HMAC key).<p><p>AES key sizes greater than
128 bits require installation of the JCE Unlimited Strength policy files in your JRE.",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "openam-session-stateless-enable-session-blacklisting" : {
    "title" : "Enable Session Blacklisting",
    "description" : "Enables session blacklisting for logged out stateless sessions.<br><br>It
is recommended to enable this setting if the maximum session time is high. Blacklist state is stored
in the core token service (CTS) until the session token expires in order to ensure that session
tokens cannot continue to be used. Requires a server restart for changes to take effect.",
    "propertyOrder" : 2400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "statelessCompressionType" : {
    "title" : "Compression Algorithm",
    "description" : "If enabled the session state will be compressed before signing and
encryption.<br><br><strong>WARNING</strong>: Enabling compression may compromise encryption. This may
leak information about the content of the session state if encryption is enabled.",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "statelessSigningRsaCertAlias" : {
    "title" : "Signing RSA/ECDSA Certificate Alias",
    "description" : "Specify the alias of a certificate containing a public/private key pair
that OpenAM uses when performing RSA or ECDSA signing on the stateless session JWT. Specify a signing
certificate alias when using a \"Signing Algorithm Type\" of <code>RS256</code>, <code>ES256</code>,
<code>ES384</code>, or <code>ES512</code>.<br><br>Certificate will be retrieved from the keystore
specified by the <code>com.sun.identity.saml.xmlsig.keystore</code> property.",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-session-stateless-blacklist-cache-size" : {
    "title" : "Session Blacklist Cache Size",
    "description" : "Number of blacklisted stateless sessions to cache in memory to speed up
blacklist checks and reduce load on the CTS. The cache size should be around the number of logouts
expected in the maximum session time.<p><p>Applies only to deployments using stateless sessions.",
    "propertyOrder" : 2500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "statelessSigningType" : {
    "title" : "Signing Algorithm Type",
    "description" : "Specifies the algorithm that OpenAM uses to sign a JSON Web Token (JWT)
containing a stateless session. Signing the JWT enables tampering detection. Note that OpenAM stores
stateless sessions in a JWT that resides in an HTTP cookie.<br><br>Applies only to deployments using
stateless sessions. OpenAM supports the following signing algorithms: <ul><li><strong>HS256</strong>.
```

```

HMAC using SHA-256.</li><li><strong>HS384</strong>. HMAC using SHA-384.</li><li><strong>HS512</strong>. HMAC using SHA-512.</li><li><strong>RS256</strong>. RSASSA-PKCS1-v1_5 using SHA-256.</li><li><strong>ES256</strong>. ECDSA using SHA-256 and NIST standard P-256 elliptic curve.</li><li><strong>ES384</strong>. ECDSA using SHA-384 and NIST standard P-384 elliptic curve.</li><li><strong>ES512</strong>. ECDSA using SHA-512 and NIST standard P-521 elliptic curve.</li></ul>",
    "propertyOrder" : 1900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "statelessEncryptionRsaCertAlias" : {
    "title" : "Encryption RSA Certificate Alias",
    "description" : "Specifies the alias of a certificate containing a public/private key pair that OpenAM uses when encrypting a JWT. Specify an encryption certificate alias when using an Encryption Algorithm Type of RSA.<p><p>Applies only to deployments using stateless sessions.<br><br>Certificate will be retrieved from the keystore referenced by the <code>com.sun.identity.saml.xmlsig.keystore</code> property.",
    "propertyOrder" : 2300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "statelessSigningHmacSecret" : {
    "title" : "Signing HMAC Shared Secret",
    "description" : "Specifies the shared secret that OpenAM uses when performing HMAC signing on the stateless session JWT.<p><p>Specify a shared secret when using a \"Signing Algorithm Type\" of <code>HS256</code>, <code>HS384</code>, or <code>HS512</code>. Applies only to deployments using stateless sessions.",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-session-stateless-blacklist-poll-interval" : {
    "title" : "Blacklist Poll Interval (seconds)",
    "description" : "Specifies the interval at which OpenAM polls the Core Token Service for changes to logged out sessions, in seconds.<br><br>The longer the polling interval, the more time a malicious user has to connect to other OpenAM servers in a cluster and make use of a stolen session cookie. Shortening the polling interval improves the security for logged out sessions, but might incur a minimal decrease in overall OpenAM performance due to increased network activity. Set to <code>0</code> to disable this feature completely.<p><p>Applies only to deployments using stateless sessions and session blacklisting.",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "statelessEncryptionType" : {
    "title" : "Encryption Algorithm",
    "description" : "Specifies the algorithm that OpenAM uses to encrypt JWTs containing stateless sessions.<br><br>Applies only to deployments using stateless sessions. OpenAM supports the following algorithms:<ul><li><strong>NONE</strong>. No encryption is selected.</li><li><strong>RSA</strong>. Session content is encrypted with AES using a unique key. The key is then encrypted with an RSA public key and appended to the JWT.<p><p>OpenAM supports the three padding modes, which you can set using the <code>org.forgerock.openam.session.stateless.rsa.padding</code> advanced property:<ul><li><code>RSA1_5</code>. RSA with PKCS#1 v1.5 padding.</li><li><code>RSA-OAEP</code>. RSA with optimal asymmetric encryption padding (OAEP) and SHA-1.</li><li><code>RSA-OAEP-256</code>. RSA with OAEP padding and SHA-256.</li></ul></li><li><strong>AES KeyWrapping</strong>. Session content is encrypted with AES using a unique key and is then wrapped using AES

```

KeyWrap and the master key. This provides additional security, compared to RSA, at the cost of 128 or 256 bits (or 32 bytes) depending on the size of the master key. This method provides authenticated encryption, which removes the need for a separate signature and decreases the byte size of the JWT. See <https://tools.ietf.org/html/rfc3394> RFC 3394.

**Direct AES Encryption**. Session content is encrypted with direct AES encryption with a symmetric key. This method provides authenticated encryption, which removes the need for a separate signature and decreases the byte size of the JWT.

**Important**: To prevent users from accidentally disabling all authentication support, which can be accomplished by disabling signing and not using an authenticated encryption mode, you must set the `org.forgerock.openam.session.stateless.signing.allownone` system property to `true` to turn off signing completely.

```

    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
},
"general" : {
  "type" : "object",
  "title" : "General",
  "propertyOrder" : 0,
  "properties" : {
    "timeoutHandlers" : {
      "title" : "Session Timeout Handler implementations",
      "description" : "Lists plugin classes implementing session timeout handlers. Specify the fully qualified name.",
      "propertyOrder" : 1800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "latestAccessTimeUpdateFrequency" : {
      "title" : "Latest Access Time Update Frequency",
      "description" : "Defaults to 60 seconds. At most, OpenAM updates a session's latest access time this often. Subsequent touches to the session that occur less than the specified number of seconds after an update will not cause additional updates to the session's access time. Refreshing a session returns the idle time as the number of seconds since an update has occurred, which will be between 0 and the specified Latest Access Time Update Frequency.",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "dnRestrictionOnly" : {
      "title" : "DN Restriction Only Enabled",
      "description" : "If enabled, OpenAM will not perform DNS lookups when checking restrictions in cookie hijacking mode.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
},

```

```

    "iplanet-am-session-constraint-resulting-behavior" : {
      "title" : "Resulting behavior if session quota exhausted",
      "description" : "Specify the action to take if a session quota is exhausted:<ul><li><strong>Deny
Access</strong>. New session creation requests will be denied.</li><li><strong>Destroy Next
Expiring</strong>. The session that would expire next will be destroyed.</li><li><strong>Destroy
Oldest</strong>. The oldest session will be destroyed.</li><li><strong>Destroy All</strong>. All
previous sessions will be destroyed.</li></ul>",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "search" : {
      "type" : "object",
      "title" : "Session Search",
      "propertyOrder" : 1,
      "properties" : {
        "maxSessionListSize" : {
          "title" : "Maximum Number of Search Results",
          "description" : "Maximum number of results from a session search. Do not set this attribute
to a large value, for example more than 1000, unless sufficient system resources are allocated.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sessionListRetrievalTimeout" : {
          "title" : "Timeout for Search",
          "description" : "Time after which OpenAM sees an incomplete search as having failed, in
seconds.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "quotas" : {
      "type" : "object",
      "title" : "Session Quotas",
      "propertyOrder" : 3,
      "properties" : {
        "denyLoginWhenRepoDown" : {
          "title" : "Deny user login when session repository is down",
          "description" : "This property only takes effect when the session quota constraint is
enabled, and the session data store is unavailable.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "iplanet-am-session-enable-session-constraint" : {
      "title" : "Enable Quota Constraints",
      "description" : "If on, then OpenAM allows you to set quota constraints on stateful
sessions.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }

```

```

    },
    "quotaConstraintMaxWaitTime" : {
      "title" : "Read Timeout for Quota Constraint",
      "description" : "Maximum wait time after which OpenAM considers a search for live session
count as having failed if quota constraints are enabled, in milliseconds.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "behaviourWhenQuotaExhausted" : {
      "title" : "Resulting behavior if session quota exhausted",
      "description" : "Specify the action to take if a session quota is
exhausted:<ul><li><strong>Deny Access</strong>. New session creation requests will be denied.</
li><li><strong>Destroy Next Expiring</strong>. The session that would expire next will be destroyed.</
li><li><strong>Destroy Oldest</strong>. The oldest session will be destroyed.</li><li><strong>Destroy
All</strong>. All previous sessions will be destroyed.</li></ul>",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
},
"dynamic" : {
  "properties" : {
    "maxSessionTime" : {
      "title" : "Maximum Session Time",
      "description" : "Maximum time a session can remain valid before OpenAM requires the user to
authenticate again, in minutes.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxIdleTime" : {
      "title" : "Maximum Idle Time",
      "description" : "Maximum time a stateful session can remain idle before OpenAM requires the
user to authenticate again, in minutes.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxCachingTime" : {
      "title" : "Maximum Caching Time",
      "description" : "Maximum time before OpenAM refreshes a session that has been cached, in
minutes.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "quotaLimit" : {
      "title" : "Active User Sessions",
      "description" : "Maximum number of concurrent stateful sessions OpenAM allows a user to
have.",
      "propertyOrder" : 800,
      "required" : true,

```

```
        "type" : "integer",
        "exampleValue" : ""
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}
```

## 1.123. SessionProperties

### 1.123.1. Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/session`

Resource version: `1.0`

#### 1.123.1.1. read

Usage:

```
am> read SessionProperties --global --serverName serverName
```

Parameters:

**--serverName**

An object of property key-value pairs

#### 1.123.1.2. update

Usage:

```
am> update SessionProperties --global --serverName serverName --body body
```

Parameters:

**--serverName**

An object of property key-value pairs

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```

"properties" : {
  "amconfig.header.sessionthresholds" : {
    "title" : "Session Limits",
    "type" : "object",
    "propertyOrder" : 0,
    "properties" : {
      "org.forgerock.openam.session.service.access.persistence.caching.maxsize" : {
        "title" : "Maximum Session Cache Size",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "The maximum number of sessions to cache in the per-server internal session
cache. (property name: org.forgerock.openam.session.service.access.persistence.caching.maxsize)",
        "properties" : {
          "value" : {
            "type" : "integer",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "com.iplanet.am.session.invalidsessionmaxtime" : {
        "title" : "Invalidate Session Max Time",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "Duration in minutes after which the invalid session will be removed
from the session table if it is created and the user does not login. This value should always
be greater than the timeout value in the Authentication module properties file. (property name:
com.iplanet.am.session.invalidsessionmaxtime)",
        "properties" : {
          "value" : {
            "type" : "integer",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  },
  "amconfig.header.sessionlogging" : {
    "title" : "Statistics",
    "type" : "object",
    "propertyOrder" : 1,
    "properties" : {
      "com.iplanet.am.stats.interval" : {
        "title" : "Logging Interval (in seconds)",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "Number of seconds to elapse between statistics logging. The interval
should be at least 5 seconds to avoid CPU saturation. An interval value less than 5 seconds will be
interpreted as 5 seconds. (property name: com.iplanet.am.stats.interval)",
        "properties" : {
          "value" : {
            "type" : "integer",

```

```

        "required" : false
    },
    "inherited" : {
        "type" : "boolean",
        "required" : true
    }
},
"com.iplanet.services.stats.state" : {
    "title" : "State",
    "type" : "object",
    "propertyOrder" : 1,
    "description" : "Statistics state 'file' will write to a file under the
specified directory, and 'console' will write into webserver log files. (property name:
com.iplanet.services.stats.state)",
    "properties" : {
        "value" : {
            "enum" : [ "off", "file", "console" ],
            "options" : {
                "enum_titles" : [ "Off", "File", "Console" ]
            },
            "type" : "string",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
},
"com.iplanet.services.stats.directory" : {
    "title" : "Directory",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "Directory where the statistic files will be created. Use forward slashes
\"/\" to separate directories, not backslash \"\\\\\". Spaces in the file name are allowed for Windows.
(property name: com.iplanet.services.stats.directory)",
    "properties" : {
        "value" : {
            "type" : "string",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
},
"com.sun.am.session.enableHostLookup" : {
    "title" : "Enable Host Lookup",
    "type" : "object",
    "propertyOrder" : 3,
    "description" : "Enables or disables host lookup during session logging. (property name:
com.sun.am.session.enableHostLookup)",
    "properties" : {
        "value" : {
            "type" : "boolean",
            "required" : false
        }
    }
},

```



```

        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
}
},
"amconfig.header.sessionnotification" : {
    "title" : "Notification",
    "type" : "object",
    "propertyOrder" : 2,
    "properties" : {
        "com.iplanet.am.notification.threadpool.size" : {
            "title" : "Notification Pool Size",
            "type" : "object",
            "propertyOrder" : 0,
            "description" : "Specifies the size of the notification thread pool (total number of
threads). (property name: com.iplanet.am.notification.threadpool.size)",
            "properties" : {
                "value" : {
                    "type" : "integer",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        },
        "com.iplanet.am.notification.threadpool.threshold" : {
            "title" : "Notification Thread Pool Threshold",
            "type" : "object",
            "propertyOrder" : 1,
            "description" : "Specifies the maximum task queue length for serving notification threads.
(property name: com.iplanet.am.notification.threadpool.threshold)",
            "properties" : {
                "value" : {
                    "type" : "integer",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        }
    }
},
"amconfig.header.sessionvalidation" : {
    "title" : "Validation",
    "type" : "object",
    "propertyOrder" : 3,
    "properties" : {
        "com.sun.am.session.caseInsensitiveDN" : {
            "title" : "Case Insensitive client DN comparison",
            "type" : "object",
            "propertyOrder" : 0,

```

```
"description" : "Specifies if client distinguished name comparison is case insensitive/  
sensitive. (property name: com.sun.am.session.caseInsensitiveDN)",  
"properties" : {  
  "value" : {  
    "type" : "boolean",  
    "required" : false  
  },  
  "inherited" : {  
    "type" : "boolean",  
    "required" : true  
  }  
}  
}  
}  
}  
}
```

## 1.124. SessionPropertyWhiteList

### 1.124.1. Realm Operations

Resource path: `/realm-config/services/amSessionPropertyWhitelist`

Resource version: `1.0`

#### 1.124.1.1. create

Usage:

```
am> create SessionPropertyWhiteList --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sessionPropertyWhitelist" : {
      "title" : "Whitelisted Session Property Names",
      "description" : "A list of properties that users may read, edit the value of, or delete from their session.<p><p> Adding properties to sessions can impact OpenAM's performance. Because there is no size constraint limiting the set of properties that you can add to sessions, and no limit on the number of session properties you can add, keep in mind that adding session properties can increase the load on an OpenAM deployment in the following areas: <ul><li>OpenAM server memory</li><li>OpenDJ storage</li><li>OpenDJ replication</li></ul><p>Protected attributes will NOT be allowed to be set, edited or deleted, even if they are included in this whitelist.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

### 1.124.1.2. delete

Usage:

```
am> delete SessionPropertyWhiteList --realm Realm
```

### 1.124.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SessionPropertyWhiteList --realm Realm --actionName getAllTypes
```

### 1.124.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SessionPropertyWhiteList --realm Realm --actionName getCreatableTypes
```

### 1.124.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SessionPropertyWhiteList --realm Realm --actionName nextdescendents
```

### 1.124.1.6. read

Usage:

```
am> read SessionPropertyWhiteList --realm Realm
```

### 1.124.1.7. update

Usage:

```
am> update SessionPropertyWhiteList --realm Realm --body body
```

Parameters:

#### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sessionPropertyWhitelist" : {
      "title" : "Whitelisted Session Property Names",
      "description" : "A list of properties that users may read, edit the value of, or delete from their session.<p><p> Adding properties to sessions can impact OpenAM's performance. Because there is no size constraint limiting the set of properties that you can add to sessions, and no limit on the number of session properties you can add, keep in mind that adding session properties can increase the load on an OpenAM deployment in the following areas: <ul><li>OpenAM server memory</li><li>OpenDJ storage</li><li>OpenDJ replication</li></ul><p>Protected attributes will NOT be allowed to be set, edited or deleted, even if they are included in this whitelist.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.124.2. Global Operations

Resource path: [/global-config/services/amSessionPropertyWhitelist](#)

Resource version: 1.0

### 1.124.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SessionPropertyWhiteList --global --actionName getAllTypes
```

### 1.124.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SessionPropertyWhiteList --global --actionName getCreatableTypes
```

### 1.124.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SessionPropertyWhiteList --global --actionName nextdescendents
```

### 1.124.2.4. read

Usage:

```
am> read SessionPropertyWhiteList --global
```

### 1.124.2.5. update

Usage:

```
am> update SessionPropertyWhiteList --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "sessionPropertyWhitelist" : {
          "title" : "Whitelisted Session Property Names",
          "description" : "A list of properties that users may read, edit the value of, or delete from
their session.<p><p> Adding properties to sessions can impact OpenAM's performance. Because there is
no size constraint limiting the set of properties that you can add to sessions, and no limit on the
number of session properties you can add, keep in mind that adding session properties can increase
the load on an OpenAM deployment in the following areas: <ul><li>OpenAM server memory</li><li>OpenDJ
storage</li><li>OpenDJ replication</li></ul><p>Protected attributes will NOT be allowed to be set,
edited or deleted, even if they are included in this whitelist.",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

## 1.125. Sessions

### 1.125.1. Realm Operations

Represents Sessions that can queried via a REST interface.

Resource path: `/sessions`

Resource version: `2.0`

#### 1.125.1.1. getSessionInfo

It reads and returns the information about the requested session.

Usage:

```
am> action Sessions --realm Realm --tokenId tokenId --actionName getSessionInfo
```

Parameters:

**--tokenId**

Represents Sessions that can queried via a REST interface.

### 1.125.1.2. getSessionProperties

It reads and returns all of the whitelisted properties for the requested session.

Usage:

```
am> action Sessions --realm Realm --tokenId tokenId --actionName getSessionProperties
```

Parameters:

**--tokenId**

Represents Sessions that can queried via a REST interface.

### 1.125.1.3. logout

It does logout from OpenAM

Usage:

```
am> action Sessions --realm Realm --tokenId tokenId --actionName logout
```

Parameters:

**--tokenId**

Represents Sessions that can queried via a REST interface.

### 1.125.1.4. logoutByHandle

It logs out sessions based on the provided session handles.

Usage:

```
am> action Sessions --realm Realm --body body --actionName logoutByHandle
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Logout By Handle request",
  "type" : "object",
  "title" : "Logout By Handle request",
  "properties" : {
    "sessionHandles" : {
      "title" : "Session handles",
      "description" : "The array of session handles that needs to be invalidated.",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "sessionHandles" ]
}
```

### 1.125.1.5. query

It queries all sessions using the provided query filter.

Usage:

```
am> query Sessions --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [username, realm]

### 1.125.1.6. refresh

Suggests to OpenAM that it should refresh this session (update its latest access time and reset its idleTime to 0). This will only be obeyed if the time between the session's previous latest access time and now is greater than the value configured for the server's Latest Access Time Update Frequency setting, which defaults to 60 seconds.

Usage:

```
am> action Sessions --realm Realm --tokenId tokenId --actionName refresh
```

Parameters:

**--tokenId**

Represents Sessions that can queried via a REST interface.

### 1.125.1.7. updateSessionProperties

It updates and returns all of the whitelisted properties for the requested session.



Usage:

```
am> action Sessions --realm Realm --tokenId tokenId --actionName updateSessionProperties
```

Parameters:

**--tokenId**

Represents Sessions that can queried via a REST interface.

### 1.125.1.8. validate

It checks that the specified SSO Token Id is valid or not. If there is any problem getting or validating the token which causes an exception the json response will be false. In addition if the token is expired then the json response will be set to true. Otherwise it will be set to true.

Usage:

```
am> action Sessions --realm Realm --tokenId tokenId --actionName validate
```

Parameters:

**--tokenId**

Represents Sessions that can queried via a REST interface.

## 1.126. SharedAgents

### 1.126.1. Realm Operations

Agents handler that is responsible for managing agents

Resource path: [/realm-config/agents/SharedAgent](#)

Resource version: [1.0](#)

#### 1.126.1.1. create

Usage:

```
am> create SharedAgents --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "cdssoRootUrl" : {
      "title" : "Agent Root URL for CDSSO",
      "description" : "The agent root URL for CDSSO. The valid value is in the following format:  
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.  
The hostname represents the host name of the machine on which the agent resides. The port represents  
the port number on which the agent is installed. The slash following the port number is required.",
      "propertyOrder" : 22700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "agentProfilesAllowedToRead" : {
      "title" : "Agent Profiles allowed to Read.",
      "description" : "",
      "propertyOrder" : 22600,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.126.1.2. delete

Usage:

```
am> delete SharedAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.126.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SharedAgents --realm Realm --actionName getAllTypes
```

### 1.126.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SharedAgents --realm Realm --actionName getCreatableTypes
```

### 1.126.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SharedAgents --realm Realm --actionName nextdescendents
```

### 1.126.1.6. query

Querying the agents of a specific type

Usage:

```
am> query SharedAgents --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.126.1.7. read

Usage:

```
am> read SharedAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.126.1.8. update

Usage:

```
am> update SharedAgents --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "cdssoRootUrl" : {
      "title" : "Agent Root URL for CDSSO",
      "description" : "The agent root URL for CDSSO. The valid value is in the following format:  
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.  
The hostname represents the host name of the machine on which the agent resides. The port represents  
the port number on which the agent is installed. The slash following the port number is required.",
      "propertyOrder" : 22700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
}
```

```
"agentProfilesAllowedToRead" : {  
  "title" : "Agent Profiles allowed to Read.",  
  "description" : "",  
  "propertyOrder" : 22600,  
  "required" : true,  
  "items" : {  
    "type" : "string"  
  },  
  "type" : "array",  
  "exampleValue" : ""  
}  
}
```

## 1.127. Sites

### 1.127.1. Global Operations

This version 1.0 sites service represents a Sites resource with CQ operations on the users collection and CRUDPA operations available for the site item. Items can have server version 1.0 subresources.

Resource path: `/global-config/sites`

Resource version: `1.0`

#### 1.127.1.1. create

Create new site entry

Usage:

```
am> create Sites --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "$schema" : "http://json-schema.org/draft-04/schema#",  
  "description" : "Site schema.",  
  "type" : "object",  
  "title" : "Site schema",  
  "properties" : {  
    "_id" : {  
      "type" : "string",  
      "title" : "Name",  
    },  
  },  
}
```

```

    "description" : "Site name."
  },
  "id" : {
    "type" : "string",
    "title" : "Site id",
    "description" : "Site's unique identifier.",
    "javaName" : "siteId"
  },
  "url" : {
    "type" : "string",
    "title" : "Primary URL",
    "description" : "Site primary URL."
  },
  "secondaryURLs" : {
    "type" : "array",
    "title" : "Secondary URLs",
    "description" : "Secondary URLs for this site.",
    "items" : {
      "type" : "string"
    }
  },
  "servers" : {
    "type" : "array",
    "title" : "Assigned Servers",
    "description" : "Servers assigned to this site.",
    "items" : {
      "type" : "object",
      "properties" : {
        "id" : {
          "type" : "string",
          "title" : "Server id",
          "description" : "Server's unique identifier for the site."
        },
        "url" : {
          "type" : "string",
          "title" : "Server URL",
          "description" : "Server URL of the site"
        }
      }
    }
  }
}

```

## 1.127.1.2. delete

Delete site entry

Usage:

```
am> delete Sites --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.127.1.3. query

Query the collection of site entries

Usage:

```
am> query Sites --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\_id, url]

### 1.127.1.4. read

Read a site entry

Usage:

```
am> read Sites --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.127.1.5. schema

Sites schema action that returns the sites schema json

Usage:

```
am> action Sites --global --actionName schema
```

### 1.127.1.6. template

Sites template action that returns a template json object for site insert

Usage:

```
am> action Sites --global --actionName template
```

### 1.127.1.7. update

Update a site entry

Usage:

```
am> update Sites --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Site schema.",
  "type" : "object",
  "title" : "Site schema",
  "properties" : {
    "_id" : {
      "type" : "string",
      "title" : "Name",
      "description" : "Site name."
    },
    "id" : {
      "type" : "string",
      "title" : "Site id",
      "description" : "Site's unique identifier.",
      "javaName" : "siteId"
    },
    "url" : {
      "type" : "string",
      "title" : "Primary URL",
      "description" : "Site primary URL."
    },
    "secondaryURLs" : {
      "type" : "array",
      "title" : "Secondary URLs",
      "description" : "Secondary URLs for this site.",
      "items" : {
        "type" : "string"
      }
    },
    "servers" : {
      "type" : "array",
      "title" : "Assigned Servers",
      "description" : "Servers assigned to this site.",
      "items" : {
        "type" : "object",
        "properties" : {
          "id" : {
            "type" : "string",
            "title" : "Server id",
            "description" : "Server's unique identifier for the site."
          },
          "url" : {
            "type" : "string",
            "title" : "Server URL",
            "description" : "Server URL of the site"
          }
        }
      }
    }
  }
}
```



```
}  
}  
}
```

## 1.128. SoapSTSAgentGroups

### 1.128.1. Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/SoapSTSAgent`

Resource version: `1.0`

#### 1.128.1.1. create

Usage:

```
am> create SoapSTSAgentGroups --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "publishServicePollInterval" : {
      "title" : "Poll Interval",
      "description" : "Interval, in seconds, to poll the sts publish service for newly-published SOAP
STS instances.",
      "propertyOrder" : 26300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

### 1.128.1.2. delete

Usage:

```
am> delete SoapSTSAgentGroups --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.128.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SoapSTSAgentGroups --realm Realm --actionName getAllTypes
```

### 1.128.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SoapSTSAgentGroups --realm Realm --actionName getCreatableTypes
```

### 1.128.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SoapSTSAgentGroups --realm Realm --actionName nextdescendents
```

### 1.128.1.6. query

Querying the agent groups of a specific type

Usage:

```
am> query SoapSTSAgentGroups --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.128.1.7. read

Usage:

```
am> read SoapSTSAgentGroups --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.128.1.8. update

Usage:

```
am> update SoapSTSAgentGroups --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "publishServicePollInterval" : {
      "title" : "Poll Interval",
      "description" : "Interval, in seconds, to poll the sts publish service for newly-published SOAP
STS instances.",
      "propertyOrder" : 26300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

## 1.129. SoapStsAgents

### 1.129.1. Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/SoapSTSAgent`

Resource version: `1.0`

#### 1.129.1.1. create

Usage:

```
am> create SoapStsAgents --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "publishServicePollInterval" : {
      "title" : "Poll Interval",
      "description" : "Interval, in seconds, to poll the sts publish service for newly-published SOAP
STS instances.",
      "propertyOrder" : 26300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

### 1.129.1.2. delete

Usage:

```
am> delete SoapStsAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.129.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SoapStsAgents --realm Realm --actionName getAllTypes
```

### 1.129.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SoapStsAgents --realm Realm --actionName getCreatableTypes
```

### 1.129.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SoapStsAgents --realm Realm --actionName nextdescendents
```

### 1.129.1.6. query

Querying the agents of a specific type

Usage:

```
am> query SoapStsAgents --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.129.1.7. read

Usage:

```
am> read SoapStsAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.129.1.8. update

Usage:

```
am> update SoapStsAgents --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "publishServicePollInterval" : {
      "title" : "Poll Interval",
      "description" : "Interval, in seconds, to poll the sts publish service for newly-published SOAP
STS instances.",
      "propertyOrder" : 26300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

## 1.130. SocialAuthentication

### 1.130.1. Realm Operations

Resource path: `/realm-config/services/socialauthentication`

Resource version: `1.0`

#### 1.130.1.1. create

Usage:

```
am> create SocialAuthentication --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabledKeys" : {
      "title" : "Enabled Implementations",
      "description" : "Provide a key that has been used to define the settings above to enable that
set of settings.<br><br>For example: google",

```

```

    "propertyOrder" : 400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "displayNames" : {
    "title" : "Display Names",
    "description" : "The display names for the implementations - this will be used to provide a name
for the icon displayed on the login page. The key should be used across all the settings on this page
to join them together.<br><br>For example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</
td><td>Google</td></tr></table>",
    "propertyOrder" : 100,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "icons" : {
    "title" : "Icons",
    "description" : "Either a full URL or a path relative to the base of the site/server where the
image can be found. The image will be used on the login page to link to the authentication chain
defined above. The key should correspond to a key used to define a Display Name above.<br><br>For
example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</td><td>/images/google-sign-in.png</
td></tr></table>",
    "propertyOrder" : 300,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "authenticationChains" : {
    "title" : "Authentication Chains",
    "description" : "The name of the authentication chains that are the entry points to being
authenticated by each respective social authentication provider. The key should correspond to a
key used to define a Display Name above.<br><br>For example:<table><tr><th>Key</th><th>Value</th></
tr><tr><td>google</td><td>socialAuthChainGoogle</td></tr></table>",
    "propertyOrder" : 200,
    "required" : true,
    "patternProperties" : {
      ".*" : { }
    },
    "type" : "object",
    "exampleValue" : ""
  }
}
}
}

```



### 1.130.1.2. delete

Usage:

```
am> delete SocialAuthentication --realm Realm
```

### 1.130.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthentication --realm Realm --actionName getAllTypes
```

### 1.130.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthentication --realm Realm --actionName getCreatableTypes
```

### 1.130.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthentication --realm Realm --actionName nextdescendents
```

### 1.130.1.6. read

Usage:

```
am> read SocialAuthentication --realm Realm
```

### 1.130.1.7. update

Usage:

```
am> update SocialAuthentication --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabledKeys" : {
      "title" : "Enabled Implementations",
      "description" : "Provide a key that has been used to define the settings above to enable that set of settings.<br><br>For example: google",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "displayNames" : {
      "title" : "Display Names",
      "description" : "The display names for the implementations - this will be used to provide a name for the icon displayed on the login page. The key should be used across all the settings on this page to join them together.<br><br>For example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</td><td>Google</td></tr></table>",
      "propertyOrder" : 100,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "icons" : {
      "title" : "Icons",
      "description" : "Either a full URL or a path relative to the base of the site/server where the image can be found. The image will be used on the login page to link to the authentication chain defined above. The key should correspond to a key used to define a Display Name above.<br><br>For example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</td><td>/images/google-sign-in.png</td></tr></table>",
      "propertyOrder" : 300,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "authenticationChains" : {
      "title" : "Authentication Chains",
      "description" : "The name of the authentication chains that are the entry points to being authenticated by each respective social authentication provider. The key should correspond to a key used to define a Display Name above.<br><br>For example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</td><td>socialAuthChainGoogle</td></tr></table>",
      "propertyOrder" : 200,

```

```
    "required" : true,
    "patternProperties" : {
      ".*" : { }
    },
    "type" : "object",
    "exampleValue" : ""
  }
}
```

## 1.130.2. Global Operations

Resource path: `/global-config/services/socialauthentication`

Resource version: `1.0`

### 1.130.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthentication --global --actionName getAllTypes
```

### 1.130.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthentication --global --actionName getCreatableTypes
```

### 1.130.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthentication --global --actionName nextdescendents
```

### 1.130.2.4. read

Usage:

```
am> read SocialAuthentication --global
```

### 1.130.2.5. update

## Usage:

```
am> update SocialAuthentication --global --body body
```

## Parameters:

### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "enabledKeys" : {
          "title" : "Enabled Implementations",
          "description" : "Provide a key that has been used to define the settings above to enable
that set of settings.<br><br>For example: google",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "icons" : {
          "title" : "Icons",
          "description" : "Either a full URL or a path relative to the base of the site/server where
the image can be found. The image will be used on the login page to link to the authentication chain
defined above. The key should correspond to a key used to define a Display Name above.<br><br>For
example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</td><td>/images/google-sign-in.png</
td></tr></table>",
          "propertyOrder" : 300,
          "required" : true,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "displayNames" : {
          "title" : "Display Names",
          "description" : "The display names for the implementations - this will be used to provide
a name for the icon displayed on the login page. The key should be used across all the settings
on this page to join them together.<br><br>For example:<table><tr><th>Key</th><th>Value</th></
tr><tr><td>google</td><td>Google</td></tr></table>",
          "propertyOrder" : 100,
          "required" : true,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    },
    "authenticationChains" : {
      "title" : "Authentication Chains",
      "description" : "The name of the authentication chains that are the entry points to being
authenticated by each respective social authentication provider. The key should correspond to a
key used to define a Display Name above.<br><br>For example:<table><tr><th>Key</th><th>Value</th></
tr><tr><td>google</td><td>socialAuthChainGoogle</td></tr></table>",
      "propertyOrder" : 200,
      "required" : true,
      "patternProperties" : {
        ".*" : { }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "type" : "object",
  "title" : "Realm Defaults"
}
}
}

```

## 1.131. Splunk

### 1.131.1. Realm Operations

Resource path: `/realm-config/services/audit/Splunk`

Resource version: **1.0**

#### 1.131.1.1. create

Usage:

```
am> create Splunk --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```

{
  "type" : "object",
  "properties" : {
    "splunkBuffering" : {
      "type" : "object",
      "title" : "Buffering",

```

```

    "propertyOrder" : 3,
    "properties" : {
      "maxEvents" : {
        "title" : "Queue Capacity",
        "description" : "Maximum number of audit evens in the batch queue; additional events are
dropped.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "batchSize" : {
        "title" : "Batch Size",
        "description" : "Number of audit log events to batch before submitting to Splunk.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "writeInterval" : {
        "title" : "Write interval (in milliseconds)",
        "description" : "Interval at which buffered events are written to Splunk.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      }
    }
  },
  "splunkConfig" : {
    "type" : "object",
    "title" : "Splunk Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "authzToken" : {
        "title" : "Authorization Token",
        "description" : "Authorization token used to connect to Splunk HTTP Event Collector
endpoint.",
        "propertyOrder" : null,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "port" : {
        "title" : "Server Port",
        "description" : "Port number of Splunk server.",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "sslEnabled" : {
        "title" : "SSL Enabled",
        "description" : "Use HTTPS protocol for communication with Splunk.",
        "propertyOrder" : 500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  },

```

```

    "host" : {
      "title" : "Server Hostname",
      "description" : "Host name or IP address of Splunk server.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
      "handlerFactory" : {
        "title" : "Factory Class Name",
        "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
        "propertyOrder" : null,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
      "topics" : {
        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 200,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  }
}

```

## 1.131.1.2. delete

Usage:

```
am> delete Splunk --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.131.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Splunk --realm Realm --actionName getAllTypes
```

## 1.131.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Splunk --realm Realm --actionName getCreatableTypes
```

## 1.131.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Splunk --realm Realm --actionName nextdescendents
```

## 1.131.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Splunk --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.



## 1.131.1.7. read

Usage:

```
am> read Splunk --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.131.1.8. update

Usage:

```
am> update Splunk --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "splunkBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit evens in the batch queue; additional events are
dropped.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Number of audit log events to batch before submitting to Splunk.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Interval at which buffered events are written to Splunk.",
```

```

        "propertyOrder" : 800,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
},
"splunkConfig" : {
    "type" : "object",
    "title" : "Splunk Configuration",
    "propertyOrder" : 2,
    "properties" : {
        "authzToken" : {
            "title" : "Authorization Token",
            "description" : "Authorization token used to connect to Splunk HTTP Event Collector endpoint.",
            "propertyOrder" : null,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        },
        "port" : {
            "title" : "Server Port",
            "description" : "Port number of Splunk server.",
            "propertyOrder" : 400,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "sslEnabled" : {
            "title" : "SSL Enabled",
            "description" : "Use HTTPS protocol for communication with Splunk.",
            "propertyOrder" : 500,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "host" : {
            "title" : "Server Hostname",
            "description" : "Host name or IP address of Splunk server.",
            "propertyOrder" : 300,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement org.forgerock.openam.audit.AuditEventHandlerFactory.",
            "propertyOrder" : null,
            "required" : true,

```

```

        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 200,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 100,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
}
}
}
}
}

```

## 1.131.2. Global Operations

Resource path: `/global-config/services/audit/Splunk`

Resource version: `1.0`

### 1.131.2.1. create

Usage:

```
am> create Splunk --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "splunkConfig" : {
      "type" : "object",
      "title" : "Splunk Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sslEnabled" : {
          "title" : "SSL Enabled",
          "description" : "Use HTTPS protocol for communication with Splunk.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server Hostname",
          "description" : "Host name or IP address of Splunk server.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server Port",
          "description" : "Port number of Splunk server.",
          "propertyOrder" : 400,
          "required" : true,

```

```

        "type" : "integer",
        "exampleValue" : ""
    },
    "authzToken" : {
        "title" : "Authorization Token",
        "description" : "Authorization token used to connect to Splunk HTTP Event Collector endpoint.",
        "propertyOrder" : null,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"splunkBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 3,
    "properties" : {
        "batchSize" : {
            "title" : "Batch Size",
            "description" : "Number of audit log events to batch before submitting to Splunk.",
            "propertyOrder" : 600,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "writeInterval" : {
            "title" : "Write interval (in milliseconds)",
            "description" : "Interval at which buffered events are written to Splunk.",
            "propertyOrder" : 800,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        },
        "maxEvents" : {
            "title" : "Queue Capacity",
            "description" : "Maximum number of audit evens in the batch queue; additional events are dropped.",
            "propertyOrder" : 700,
            "required" : true,
            "type" : "integer",
            "exampleValue" : ""
        }
    }
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : null,
            "required" : true,
            "type" : "string",

```

```
    "exampleValue" : ""  
  }  
}  
}  
}
```

### 1.131.2.2. delete

Usage:

```
am> delete Splunk --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.131.2.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Splunk --global --actionName getAllTypes
```

### 1.131.2.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Splunk --global --actionName getCreatableTypes
```

### 1.131.2.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Splunk --global --actionName nextdescendents
```

### 1.131.2.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Splunk --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

## 1.131.2.7. read

Usage:

```
am> read Splunk --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.131.2.8. update

Usage:

```
am> update Splunk --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 200,
          "required" : true,

```

```

        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      }
    },
    "splunkConfig" : {
      "type" : "object",
      "title" : "Splunk Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sslEnabled" : {
          "title" : "SSL Enabled",
          "description" : "Use HTTPS protocol for communication with Splunk.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server Hostname",
          "description" : "Host name or IP address of Splunk server.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server Port",
          "description" : "Port number of Splunk server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authzToken" : {
          "title" : "Authorization Token",
          "description" : "Authorization token used to connect to Splunk HTTP Event Collector endpoint.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "splunkBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Number of audit log events to batch before submitting to Splunk.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",

```



```

        "exampleValue" : ""
    },
    "writeInterval" : {
        "title" : "Write interval (in milliseconds)",
        "description" : "Interval at which buffered events are written to Splunk.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "maxEvents" : {
        "title" : "Queue Capacity",
        "description" : "Maximum number of audit evens in the batch queue; additional events are
dropped.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : null,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
}
}
}
}

```

## 1.132. SubjectAttributes

### 1.132.1. Realm Operations

Service for querying subject attributes stored in OpenAM. When you define a policy subject condition, the condition can depend on values of subject attributes stored in a user's profile. The list of possible subject attributes that you can use depends on the LDAP User Attributes configured for the Identity data store where OpenAM looks up the user's profile

Resource path: [/subjectattributes](#)

Resource version: [1.0](#)

### 1.132.1.1. query

Query the list of subject attributes stored in OpenAM

Usage:

```
am> query SubjectAttributes --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

## 1.133. SubjectTypes

### 1.133.1. Realm Operations

Service for querying and reading the subject types stored in OpenAM. Subject condition types describe the JSON representation of subject conditions that you can use in policy definitions

Resource path: [/subjecttypes](#)

Resource version: [1.0](#)

#### 1.133.1.1. query

Query the list of subject condition types

Usage:

```
am> query SubjectTypes --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

#### 1.133.1.2. read

Read an individual subject condition type by providing the unique identifier title

Usage:

```
am> read SubjectTypes --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.134. SunDSWithOpenAMSchema

### 1.134.1. Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForAMDS`

Resource version: `1.0`

#### 1.134.1.1. create

Usage:

```
am> create SunDSWithOpenAMSchema --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-idrepo-ldapv3-config-roles-search-attribute" : {
      "title" : "LDAP Roles Search Attribute",
      "description" : "",
      "propertyOrder" : 3900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-auth-naming-attr" : {
      "title" : "Authentication Naming Attribute",
      "description" : "",
      "propertyOrder" : 5200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-user-attributes" : {
      "title" : "LDAP User Attributes",
      "description" : "",
      "propertyOrder" : 2400,
      "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-enabled" : {
    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository  
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during  
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying  
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP  
store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-filterrole-attributes" : {
    "title" : "LDAP Filter Roles Attributes",
    "description" : "",
    "propertyOrder" : 4600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",
    "description" : "",
    "propertyOrder" : 3400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-nsrole" : {
    "title" : "Attribute Name for Filtered Role Membership",
    "description" : "",
    "propertyOrder" : 4700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-timeunit" : {
    "title" : "LDAP Connection Heartbeat Time Unit",
    "description" : "Defines the time unit corresponding to the Heartbeat Interval  
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request  
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then  
it may take up to the interval period before the problem is detected. Use along with the Heartbeat  
Interval parameter to define the exact interval.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }

```

```

},
"sun-idrepo-ldapv3-config-ldap-server" : {
  "title" : "LDAP Server",
  "description" : "Format: LDAP server host name:port | server_ID | site_ID",
  "propertyOrder" : 600,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-filterroles-search-filter" : {
  "title" : "LDAP Filter Roles Search Filter",
  "description" : "",
  "propertyOrder" : 4400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-dncache-size" : {
  "title" : "DN Cache Size",
  "description" : "In DN items, only used when DN Cache is enabled.",
  "propertyOrder" : 6000,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-groups-search-filter" : {
  "title" : "LDAP Groups Search Filter",
  "description" : "",
  "propertyOrder" : 3000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-inactive" : {
  "title" : "User Status Inactive Value",
  "description" : "",
  "propertyOrder" : 2800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sunIdRepoAttributeMapping" : {
  "title" : "Attribute Name Mapping",
  "description" : "",
  "propertyOrder" : 1800,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
  "title" : "Create User Attribute Mapping",
  "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
  "propertyOrder" : 2500,

```

```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "com.iplanet.am.ldap.connection.delay.between.retries" : {
    "title" : "The Delay Time Between Retries",
    "description" : "In milliseconds.",
    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-time-limit" : {
    "title" : "Search Timeout",
    "description" : "In seconds.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-nsroledn" : {
    "title" : "Attribute Name of Role Membership.",
    "description" : "",
    "propertyOrder" : 4800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-role-objectclass" : {
    "title" : "LDAP Roles Object Class",
    "description" : "",
    "propertyOrder" : 4100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-filter" : {
    "title" : "Persistent Search Filter",
    "description" : "",
    "propertyOrder" : 5600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {

```

```

    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-filterroles-search-attribute" : {
    "title" : "LDAP Filter Roles Search Attribute",
    "description" : "",
    "propertyOrder" : 4300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-value" : {
    "title" : "LDAP Groups Container Value",
    "description" : "",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberurl" : {
    "title" : "Attribute Name of Group Member URL",
    "description" : "",
    "propertyOrder" : 3700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-objectclass" : {
    "title" : "LDAP User Object Class",
    "description" : "",

```

```

    "propertyOrder" : 2300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-nsrolefilter" : {
    "title" : "Attribute Name of Filtered Role Filter",
    "description" : "",
    "propertyOrder" : 4900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "LDAPv3 Repository Plug-in Class Name",
    "description" : "",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-role-attributes" : {
    "title" : "LDAP Roles Attributes",
    "description" : "",
    "propertyOrder" : 4200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-value" : {
    "title" : "LDAP People Container Value",
    "description" : "",
    "propertyOrder" : 5100,

```



```
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-attribute" : {
    "title" : "LDAP Groups Search Attribute",
    "description" : "",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-filterrole-objectclass" : {
    "title" : "LDAP Filter Roles Object Class",
    "description" : "",
    "propertyOrder" : 4500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-isactive" : {
    "title" : "Attribute Name of User Status",
    "description" : "",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authpw" : {
    "title" : "LDAP Bind Password",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-name" : {
    "title" : "LDAP Groups Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoSupportedOperations" : {
    "title" : "LDAPv3 Plug-in Supported Types and Operations",
    "description" : ""
  }
```

```

    "propertyOrder" : 1900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-active" : {
    "title" : "User Status Active Value",
    "description" : "",
    "propertyOrder" : 2700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-attr" : {
    "title" : "Knowledge Based Authentication Attribute Name",
    "description" : "",
    "propertyOrder" : 5300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-interval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
},

```

```

"sun-idrepo-ldapv3-config-memberof" : {
  "title" : "Attribute Name for Group Membership",
  "description" : "",
  "propertyOrder" : 3500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-people-container-name" : {
  "title" : "LDAP People Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 5000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-users-search-filter" : {
  "title" : "LDAP Users Search Filter",
  "description" : "",
  "propertyOrder" : 2200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-max-result" : {
  "title" : "Maximum Results Returned from Search",
  "description" : "",
  "propertyOrder" : 1500,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-psearchbase" : {
  "title" : "Persistent Search Base DN",
  "description" : "",
  "propertyOrder" : 5500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-roles-search-filter" : {
  "title" : "LDAP Roles Search Filter",
  "description" : "",
  "propertyOrder" : 4000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
}
}
}

```

## 1.134.1.2. delete

### Usage:

```
am> delete SunDSWithOpenAMSchema --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.134.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SunDSWithOpenAMSchema --realm Realm --actionName getAllTypes
```

### 1.134.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SunDSWithOpenAMSchema --realm Realm --actionName getCreatableTypes
```

### 1.134.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SunDSWithOpenAMSchema --realm Realm --actionName nextdescendents
```

### 1.134.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query SunDSWithOpenAMSchema --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.134.1.7. read

Usage:

```
am> read SunDSWithOpenAMSchema --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.134.1.8. update

Usage:

```
am> update SunDSWithOpenAMSchema --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-idrepo-ldapv3-config-roles-search-attribute" : {
      "title" : "LDAP Roles Search Attribute",
      "description" : "",
      "propertyOrder" : 3900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-auth-naming-attr" : {
      "title" : "Authentication Naming Attribute",
      "description" : "",
      "propertyOrder" : 5200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-user-attributes" : {
      "title" : "LDAP User Attributes",
      "description" : "",
      "propertyOrder" : 2400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-dncache-enabled" : {
      "title" : "DN Cache",
      "description" : "Used to enable/disable the DN Cache within the OpenAM repository  
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during  
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying  
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP  
store supports persistent search and move/rename (mod_dn) results are available.",

```

```

    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-filterrole-attributes" : {
    "title" : "LDAP Filter Roles Attributes",
    "description" : "",
    "propertyOrder" : 4600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",
    "description" : "",
    "propertyOrder" : 3400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-nsrole" : {
    "title" : "Attribute Name for Filtered Role Membership",
    "description" : "",
    "propertyOrder" : 4700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-timeunit" : {
    "title" : "LDAP Connection Heartbeat Time Unit",
    "description" : "Defines the time unit corresponding to the Heartbeat Interval  

    setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request  

    to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then  

    it may take up to the interval period before the problem is detected. Use along with the Heartbeat  

    Interval parameter to define the exact interval.",
    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-filterroles-search-filter" : {

```

```

    "title" : "LDAP Filter Roles Search Filter",
    "description" : "",
    "propertyOrder" : 4400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-size" : {
    "title" : "DN Cache Size",
    "description" : "In DN items, only used when DN Cache is enabled.",
    "propertyOrder" : 6000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-filter" : {
    "title" : "LDAP Groups Search Filter",
    "description" : "",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "com.ipplanet.am.ldap.connection.delay.between.retries" : {
    "title" : "The Delay Time Between Retries",
    "description" : "In milliseconds.",
    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",

```

```

    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-time-limit" : {
    "title" : "Search Timeout",
    "description" : "In seconds.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-nsroledn" : {
    "title" : "Attribute Name of Role Membership.",
    "description" : "",
    "propertyOrder" : 4800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-role-objectclass" : {
    "title" : "LDAP Roles Object Class",
    "description" : "",
    "propertyOrder" : 4100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-filter" : {
    "title" : "Persistent Search Filter",
    "description" : "",
    "propertyOrder" : 5600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-filterroles-search-attribute" : {
    "title" : "LDAP Filter Roles Search Attribute",
    "description" : "",
    "propertyOrder" : 4300,
    "required" : true,
    "type" : "string",

```



```

    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-value" : {
    "title" : "LDAP Groups Container Value",
    "description" : "",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberurl" : {
    "title" : "Attribute Name of Group Member URL",
    "description" : "",
    "propertyOrder" : 3700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-objectclass" : {
    "title" : "LDAP User Object Class",
    "description" : "",
    "propertyOrder" : 2300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-nsrolefilter" : {
    "title" : "Attribute Name of Filtered Role Filter",
    "description" : "",
    "propertyOrder" : 4900,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "LDAPv3 Repository Plug-in Class Name",
    "description" : "",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-role-attributes" : {
    "title" : "LDAP Roles Attributes",
    "description" : "",
    "propertyOrder" : 4200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-value" : {
    "title" : "LDAP People Container Value",
    "description" : "",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-attribute" : {
    "title" : "LDAP Groups Search Attribute",
    "description" : "",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-filterrole-objectclass" : {

```

```

    "title" : "LDAP Filter Roles Object Class",
    "description" : "",
    "propertyOrder" : 4500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-isactive" : {
    "title" : "Attribute Name of User Status",
    "description" : "",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authpw" : {
    "title" : "LDAP Bind Password",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-name" : {
    "title" : "LDAP Groups Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoSupportedOperations" : {
    "title" : "LDAPv3 Plug-in Supported Types and Operations",
    "description" : "",
    "propertyOrder" : 1900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-active" : {
    "title" : "User Status Active Value",
    "description" : "",
    "propertyOrder" : 2700,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-attr" : {
    "title" : "Knowledge Based Authentication Attribute Name",
    "description" : "",
    "propertyOrder" : 5300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-interval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the
    directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
    request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
    error) then it may take up to the interval period before the problem is detected. Use along with the
    Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
    disabling heartbeat requests.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-name" : {
    "title" : "LDAP People Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 5000,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-filter" : {
    "title" : "LDAP Users Search Filter",
    "description" : "",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-max-result" : {
    "title" : "Maximum Results Returned from Search",
    "description" : "",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-roles-search-filter" : {
    "title" : "LDAP Roles Search Filter",
    "description" : "",
    "propertyOrder" : 4000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

## 1.135. SupportedIds

### 1.135.1. Global Operations

Resource path: </global-config/services/id-repositories/SupportedIdentities>

Resource version: 1.0

#### 1.135.1.1. create

Usage:

```
am> create SupportedIds --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

### 1.135.1.2. delete

Usage:

```
am> delete SupportedIds --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.135.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SupportedIds --global --actionName getAllTypes
```

### 1.135.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SupportedIds --global --actionName getCreatableTypes
```

### 1.135.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SupportedIds --global --actionName nextdescendents
```

## 1.135.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query SupportedIds --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

## 1.135.1.7. read

Usage:

```
am> read SupportedIds --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.135.1.8. update

Usage:

```
am> update SupportedIds --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "type" : "object"  
}
```

# 1.136. Syslog

## 1.136.1. Realm Operations

Resource path: `/realm-config/services/audit/Syslog`

Resource version: `1.0`

## 1.136.1.1. create

Usage:

```
am> create Syslog --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sysLogConfig" : {
      "type" : "object",
      "title" : "Syslog Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "facility" : {
          "title" : "Facility",
          "description" : "Syslog facility value to apply to all events.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server port",
          "description" : "Port number of receiving syslog server.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "transportProtocol" : {
          "title" : "Transport Protocol",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server hostname",
          "description" : "Host name or IP address of receiving syslog server.",
          "propertyOrder" : 2400,
          "required" : true,
```



```

        "type" : "string",
        "exampleValue" : ""
    },
    "connectTimeout" : {
        "title" : "Connection timeout",
        "description" : "Timeout for connecting to syslog server, in seconds.",
        "propertyOrder" : 2700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 2300,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 2200,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
},
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 3000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
},
"sysLogBuffering" : {
    "type" : "object",
    "title" : "Buffering",

```

```
"propertyOrder" : 3,
"properties" : {
  "bufferingEnabled" : {
    "title" : "Buffering Enabled",
    "description" : "Enables or disables audit event buffering.",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }
}
}
```

### 1.136.1.2. delete

Usage:

```
am> delete Syslog --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.136.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Syslog --realm Realm --actionName getAllTypes
```

### 1.136.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Syslog --realm Realm --actionName getCreatableTypes
```

### 1.136.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Syslog --realm Realm --actionName nextdescendents
```

### 1.136.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Syslog --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.136.1.7. read

Usage:

```
am> read Syslog --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.136.1.8. update

Usage:

```
am> update Syslog --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sysLogConfig" : {
      "type" : "object",
      "title" : "Syslog Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "facility" : {
          "title" : "Facility",
          "description" : "Syslog facility value to apply to all events.",
          "propertyOrder" : 2800,
          "required" : true,
```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "port" : {
        "title" : "Server port",
        "description" : "Port number of receiving syslog server.",
        "propertyOrder" : 2500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "transportProtocol" : {
        "title" : "Transport Protocol",
        "description" : "",
        "propertyOrder" : 2600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "host" : {
        "title" : "Server hostname",
        "description" : "Host name or IP address of receiving syslog server.",
        "propertyOrder" : 2400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "connectTimeout" : {
        "title" : "Connection timeout",
        "description" : "Timeout for connecting to syslog server, in seconds.",
        "propertyOrder" : 2700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 2300,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 2200,
            "required" : true,
            "type" : "boolean",

```

```

        "exampleValue" : ""
    }
}
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
            "propertyOrder" : 3000,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
        }
    }
},
"sysLogBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 3,
    "properties" : {
        "bufferingEnabled" : {
            "title" : "Buffering Enabled",
            "description" : "Enables or disables audit event buffering.",
            "propertyOrder" : 2900,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
}
}
}
}
}
}

```

## 1.136.2. Global Operations

Resource path: `/global-config/services/audit/Syslog`

Resource version: **1.0**

### 1.136.2.1. create

Usage:

```
am> create Syslog --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sysLogConfig" : {
      "type" : "object",
      "title" : "Syslog Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "transportProtocol" : {
          "title" : "Transport Protocol",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server hostname",
          "description" : "Host name or IP address of receiving syslog server.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server port",
          "description" : "Port number of receiving syslog server.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "facility" : {
          "title" : "Facility",
          "description" : "Syslog facility value to apply to all events.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectTimeout" : {
          "title" : "Connection timeout",
          "description" : "Timeout for connecting to syslog server, in seconds.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
```

```

    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
      "topics" : {
        "title" : "Topics",
        "description" : "List of topics handled by an audit event handler.",
        "propertyOrder" : 2300,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "enabled" : {
        "title" : "Enabled",
        "description" : "Enables or disables an audit event handler.",
        "propertyOrder" : 2200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  },
  "commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
      "handlerFactory" : {
        "title" : "Factory Class Name",
        "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
        "propertyOrder" : 3000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "sysLogBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 3,
    "properties" : {
      "bufferingEnabled" : {
        "title" : "Buffering Enabled",
        "description" : "Enables or disables audit event buffering.",
        "propertyOrder" : 2900,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  }
}
}
}

```

```
}
```

### 1.136.2.2. delete

Usage:

```
am> delete Syslog --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.136.2.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Syslog --global --actionName getAllTypes
```

### 1.136.2.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Syslog --global --actionName getCreatableTypes
```

### 1.136.2.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Syslog --global --actionName nextdescendents
```

### 1.136.2.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query Syslog --global --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.



## 1.136.2.7. read

Usage:

```
am> read Syslog --global --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.136.2.8. update

Usage:

```
am> update Syslog --global --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sysLogConfig" : {
      "type" : "object",
      "title" : "Syslog Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "transportProtocol" : {
          "title" : "Transport Protocol",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server hostname",
          "description" : "Host name or IP address of receiving syslog server.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server port",
          "description" : "Port number of receiving syslog server.",
          "propertyOrder" : 2500,

```

```

        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "facility" : {
        "title" : "Facility",
        "description" : "Syslog facility value to apply to all events.",
        "propertyOrder" : 2800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "connectTimeout" : {
        "title" : "Connection timeout",
        "description" : "Timeout for connecting to syslog server, in seconds.",
        "propertyOrder" : 2700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
},
"commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "topics" : {
            "title" : "Topics",
            "description" : "List of topics handled by an audit event handler.",
            "propertyOrder" : 2300,
            "required" : true,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "enabled" : {
            "title" : "Enabled",
            "description" : "Enables or disables an audit event handler.",
            "propertyOrder" : 2200,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
},
"commonHandlerPlugin" : {
    "type" : "object",
    "title" : "Audit Event Handler Factory",
    "propertyOrder" : 1,
    "properties" : {
        "handlerFactory" : {
            "title" : "Factory Class Name",
            "description" : "The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement org.forgerock.openam.audit.AuditEventHandlerFactory.",
            "propertyOrder" : 3000,

```

```

        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
},
"sysLogBuffering" : {
    "type" : "object",
    "title" : "Buffering",
    "propertyOrder" : 3,
    "properties" : {
        "bufferingEnabled" : {
            "title" : "Buffering Enabled",
            "description" : "Enables or disables audit event buffering.",
            "propertyOrder" : 2900,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
}
}
}
}

```

## 1.137. TivoliDirectoryServer

### 1.137.1. Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForTivoli`

Resource version: `1.0`

#### 1.137.1.1. create

Usage:

```
am> create TivoliDirectoryServer --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```

{
  "type" : "object",
  "properties" : {
    "sun-idrepo-ldapv3-config-connection_pool_max_size" : {

```

```

    "title" : "LDAP Connection Pool Maximum Size",
    "description" : "",
    "propertyOrder" : 1200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-attribute" : {
    "title" : "LDAP Groups Search Attribute",
    "description" : "",
    "propertyOrder" : 2900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-attribute" : {
    "title" : "LDAP Users Search Attribute",
    "description" : "",
    "propertyOrder" : 2100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-value" : {
    "title" : "LDAP People Container Value",
    "description" : "",
    "propertyOrder" : 5100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
    "title" : "Create User Attribute Mapping",
    "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
    "propertyOrder" : 2500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "com.ipplanet.am.ldap.connection.delay.between.retries" : {
    "title" : "The Delay Time Between Retries",
    "description" : "In milliseconds.",
    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-enabled" : {
    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository  

    implementation. The DN Cache is used to cache DN lookups which tend to happen in bursts during  

    authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying  

    LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP  

    store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,

```

```

    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-objectclass" : {
    "title" : "LDAP User Object Class",
    "description" : "",
    "propertyOrder" : 2300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  }

```

```

},
"sun-idrepo-ldapv3-config-group-container-name" : {
  "title" : "LDAP Groups Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 3100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-connection-mode" : {
  "title" : "LDAP Connection Mode",
  "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
  "propertyOrder" : 1000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-auth-kba-attr" : {
  "title" : "Knowledge Based Authentication Attribute Name",
  "description" : "",
  "propertyOrder" : 5300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-people-container-name" : {
  "title" : "LDAP People Container Naming Attribute",
  "description" : "",
  "propertyOrder" : 5000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-objectclass" : {
  "title" : "LDAP Groups Object Class",
  "description" : "",
  "propertyOrder" : 3300,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"sunIdRepoSupportedOperations" : {
  "title" : "LDAPv3 Plug-in Supported Types and Operations",
  "description" : "",
  "propertyOrder" : 1900,
  "required" : true,
  "items" : {
    "type" : "string"
  }
},

```

```

        "type" : "array",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
        "title" : "Knowledge Based Authentication Active Index",
        "description" : "",
        "propertyOrder" : 5400,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-time-limit" : {
        "title" : "Search Timeout",
        "description" : "In seconds.",
        "propertyOrder" : 1600,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-dftgroupmember" : {
        "title" : "Default Group Member's User DN",
        "description" : "User automatically added when group is created.",
        "propertyOrder" : 3800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-user-attributes" : {
        "title" : "LDAP User Attributes",
        "description" : "",
        "propertyOrder" : 2400,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "openam-idrepo-ldapv3-heartbeat-timeunit" : {
        "title" : "LDAP Connection Heartbeat Time Unit",
        "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
        "propertyOrder" : 1400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-max-result" : {
        "title" : "Maximum Results Returned from Search",
        "description" : "",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "integer",

```

```

    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",
    "description" : "",
    "propertyOrder" : 3400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-unique-member" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported operations.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-filter" : {
    "title" : "LDAP Users Search Filter",
    "description" : "",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-search-scope" : {
    "title" : "LDAPv3 Plug-in Search Scope",
    "description" : "",
    "propertyOrder" : 2000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-active" : {
    "title" : "User Status Active Value",
    "description" : "",
    "propertyOrder" : 2700,
    "required" : true,

```



```

    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearchbase" : {
    "title" : "Persistent Search Base DN",
    "description" : "",
    "propertyOrder" : 5500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authpw" : {
    "title" : "LDAP Bind Password",
    "description" : "",
    "propertyOrder" : 800,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-naming-attr" : {
    "title" : "Authentication Naming Attribute",
    "description" : "",
    "propertyOrder" : 5200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-interval" : {
    "title" : "LDAP Connection Heartbeat Interval",
    "description" : "Specifies how often should OpenAM send a heartbeat request to the
    directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
    request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
    error) then it may take up to the interval period before the problem is detected. Use along with the
    Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
    disabling heartbeat requests.",
    "propertyOrder" : 1300,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-value" : {
    "title" : "LDAP Groups Container Value",
    "description" : "",
    "propertyOrder" : 3200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "LDAPv3 Repository Plug-in Class Name",
    "description" : "",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-size" : {
    "title" : "DN Cache Size",

```

```
    "description" : "In DN items, only used when DN Cache is enabled.",
    "propertyOrder" : 6000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-filter" : {
    "title" : "Persistent Search Filter",
    "description" : "",
    "propertyOrder" : 5600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-filter" : {
    "title" : "LDAP Groups Search Filter",
    "description" : "",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-isactive" : {
    "title" : "Attribute Name of User Status",
    "description" : "",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
```

### 1.137.1.2. delete

Usage:

```
am> delete TivoliDirectoryServer --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.137.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TivoliDirectoryServer --realm Realm --actionName getAllTypes
```

#### 1.137.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TivoliDirectoryServer --realm Realm --actionName getCreatableTypes
```

#### 1.137.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TivoliDirectoryServer --realm Realm --actionName nextdescendents
```

#### 1.137.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query TivoliDirectoryServer --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.137.1.7. read

Usage:

```
am> read TivoliDirectoryServer --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.137.1.8. update

Usage:

```
am> update TivoliDirectoryServer --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
      "title" : "LDAP Connection Pool Maximum Size",
      "description" : "",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-groups-search-attribute" : {
      "title" : "LDAP Groups Search Attribute",
      "description" : "",
      "propertyOrder" : 2900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-users-search-attribute" : {
      "title" : "LDAP Users Search Attribute",
      "description" : "",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-people-container-value" : {
      "title" : "LDAP People Container Value",
      "description" : "",
      "propertyOrder" : 5100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
      "title" : "Create User Attribute Mapping",
      "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
      "propertyOrder" : 2500,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "com.ipplanet.am.ldap.connection.delay.between.retries" : {
      "title" : "The Delay Time Between Retries",
      "description" : "In milliseconds.",

```

```

    "propertyOrder" : 5800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-enabled" : {
    "title" : "DN Cache",
    "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
    "propertyOrder" : 5900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-organization_name" : {
    "title" : "LDAP Organization DN",
    "description" : "",
    "propertyOrder" : 900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-inactive" : {
    "title" : "User Status Inactive Value",
    "description" : "",
    "propertyOrder" : 2800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoAttributeMapping" : {
    "title" : "Attribute Name Mapping",
    "description" : "",
    "propertyOrder" : 1800,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-memberof" : {
    "title" : "Attribute Name for Group Membership",
    "description" : "",
    "propertyOrder" : 3500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-objectclass" : {
    "title" : "LDAP User Object Class",
    "description" : "",
    "propertyOrder" : 2300,
    "required" : true,
    "items" : {
      "type" : "string"
    }
  }

```

```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-ldap-server" : {
    "title" : "LDAP Server",
    "description" : "Format: LDAP server host name:port | server_ID | site_ID",
    "propertyOrder" : 600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-container-name" : {
    "title" : "LDAP Groups Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 3100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-connection-mode" : {
    "title" : "LDAP Connection Mode",
    "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-attr" : {
    "title" : "Knowledge Based Authentication Attribute Name",
    "description" : "",
    "propertyOrder" : 5300,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-people-container-name" : {
    "title" : "LDAP People Container Naming Attribute",
    "description" : "",
    "propertyOrder" : 5000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-objectclass" : {
    "title" : "LDAP Groups Object Class",
    "description" : "",
    "propertyOrder" : 3300,
    "required" : true,

```

```

    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sunIdRepoSupportedOperations" : {
    "title" : "LDAPv3 Plug-in Supported Types and Operations",
    "description" : "",
    "propertyOrder" : 1900,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
    "title" : "Knowledge Based Authentication Active Index",
    "description" : "",
    "propertyOrder" : 5400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-time-limit" : {
    "title" : "Search Timeout",
    "description" : "In seconds.",
    "propertyOrder" : 1600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-dftgroupmember" : {
    "title" : "Default Group Member's User DN",
    "description" : "User automatically added when group is created.",
    "propertyOrder" : 3800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-user-attributes" : {
    "title" : "LDAP User Attributes",
    "description" : "",
    "propertyOrder" : 2400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "openam-idrepo-ldapv3-heartbeat-timeunit" : {
    "title" : "LDAP Connection Heartbeat Time Unit",
    "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request

```

to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then it may take up to the interval period before the problem is detected. Use along with the Heartbeat Interval parameter to define the exact interval.",

```

    "propertyOrder" : 1400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-max-result" : {
    "title" : "Maximum Results Returned from Search",
    "description" : "",
    "propertyOrder" : 1500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-group-attributes" : {
    "title" : "LDAP Groups Attributes",
    "description" : "",
    "propertyOrder" : 3400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-uniquemember" : {
    "title" : "Attribute Name of Unique Member",
    "description" : "",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-authid" : {
    "title" : "LDAP Bind DN",
    "description" : "A user or admin with sufficient access rights to perform the supported operations.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-users-search-filter" : {
    "title" : "LDAP Users Search Filter",
    "description" : "",
    "propertyOrder" : 2200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-scope" : {
    "title" : "Persistent Search Scope",
    "description" : "",
    "propertyOrder" : 5700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }

```



```

},
"sun-idrepo-ldapv3-config-search-scope" : {
  "title" : "LDAPv3 Plug-in Search Scope",
  "description" : "",
  "propertyOrder" : 2000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-active" : {
  "title" : "User Status Active Value",
  "description" : "",
  "propertyOrder" : 2700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-psearchbase" : {
  "title" : "Persistent Search Base DN",
  "description" : "",
  "propertyOrder" : 5500,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-authpw" : {
  "title" : "LDAP Bind Password",
  "description" : "",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "string",
  "format" : "password",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-auth-naming-attr" : {
  "title" : "Authentication Naming Attribute",
  "description" : "",
  "propertyOrder" : 5200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"openam-idrepo-ldapv3-heartbeat-interval" : {
  "title" : "LDAP Connection Heartbeat Interval",
  "description" : "Specifies how often should OpenAM send a heartbeat request to the
  directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
  request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
  error) then it may take up to the interval period before the problem is detected. Use along with the
  Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
  disabling heartbeat requests.",
  "propertyOrder" : 1300,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"sun-idrepo-ldapv3-config-group-container-value" : {
  "title" : "LDAP Groups Container Value",
  "description" : "",
  "propertyOrder" : 3200,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sunIdRepoClass" : {
    "title" : "LDAPv3 Repository Plug-in Class Name",
    "description" : "",
    "propertyOrder" : 1700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-dncache-size" : {
    "title" : "DN Cache Size",
    "description" : "In DN items, only used when DN Cache is enabled.",
    "propertyOrder" : 6000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-psearch-filter" : {
    "title" : "Persistent Search Filter",
    "description" : "",
    "propertyOrder" : 5600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-groups-search-filter" : {
    "title" : "LDAP Groups Search Filter",
    "description" : "",
    "propertyOrder" : 3000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sun-idrepo-ldapv3-config-isactive" : {
    "title" : "Attribute Name of User Status",
    "description" : "",
    "propertyOrder" : 2600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

## 1.138. TrustedUserDevices

### 1.138.1. Realm Operations

Trusted devices service is responsible for querying and deleting trusted devices.

Resource path: `/users/{user}/devices/trusted`

Resource version: 1.0

### 1.138.1.1. delete

Delete trusted user device

Usage:

```
am> delete TrustedUserDevices --realm Realm --id id --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--user**

Trusted devices service is responsible for querying and deleting trusted devices.

### 1.138.1.2. query

Query trusted user devices

Usage:

```
am> query TrustedUserDevices --realm Realm --filter filter --user user
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

**--user**

Trusted devices service is responsible for querying and deleting trusted devices.

## 1.139. UmaDataStoreProperties

### 1.139.1. Global Operations

An object of property key-value pairs

Resource path: /global-config/servers/{serverName}/properties/uma

Resource version: 1.0

### 1.139.1.1. read

Usage:

```
am> read UmaDataStoreProperties --global --serverName serverName
```

Parameters:

**--serverName**

An object of property key-value pairs

## 1.139.1.2. update

Usage:

```
am> update UmaDataStoreProperties --global --serverName serverName --body body
```

Parameters:

**--serverName**

An object of property key-value pairs

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.org.forgerock.services.resourcesets.store.common.section" : {
      "title" : "Resource Sets Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "org.forgerock.services.resourcesets.store.location" : {
          "title" : "Store Mode",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "enum" : [ "default", "external" ],
              "options" : {
                "enum_titles" : [ "Default Token Store", "External Token Store" ]
              },
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.resourcesets.store.root.suffix" : {
          "title" : "Root Suffix",
          "type" : "object",

```

```

        "propertyOrder" : 1,
        "description" : "",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    },
    "org.forgerock.services.resourcesets.store.max.connections" : {
        "title" : "Max Connections",
        "type" : "object",
        "propertyOrder" : 2,
        "description" : "",
        "properties" : {
            "value" : {
                "type" : "string",
                "required" : false
            },
            "inherited" : {
                "type" : "boolean",
                "required" : true
            }
        }
    }
}
},
"amconfig.org.forgerock.services.resourcesets.store.external.section" : {
    "title" : "External Resource Sets Store Configuration",
    "type" : "object",
    "propertyOrder" : 1,
    "properties" : {
        "org.forgerock.services.resourcesets.store.ssl.enabled" : {
            "title" : "SSL/TLS Enabled",
            "type" : "object",
            "propertyOrder" : 0,
            "description" : "",
            "properties" : {
                "value" : {
                    "type" : "boolean",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        }
    }
},
"org.forgerock.services.resourcesets.store.directory.name" : {
    "title" : "Connection String(s)",
    "type" : "object",
    "propertyOrder" : 1,
    "description" : "An ordered list of connection strings for LDAP directories. Each connection
string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
IDs are optional parameters that will prioritize that connection to use from the specified nodes.

```

Multiple connection strings should be comma-separated, e.g. `<code>host1:389,host2:50389|server1|site1,host3:50389</code>.`

```

    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "org.forgerock.services.resourcesets.store.loginid" : {
    "title" : "Login Id",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "org.forgerock.services.resourcesets.store.password" : {
    "title" : "Password",
    "type" : "object",
    "propertyOrder" : 3,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false,
        "format" : "password"
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "org.forgerock.services.resourcesets.store.heartbeat" : {
    "title" : "Heartbeat",
    "type" : "object",
    "propertyOrder" : 4,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "integer",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  }
}

```

```

    }
  }
}
},
"amconfig.org.forgerock.services.umaaudit.store.common.section" : {
  "title" : "UMA Audit Store",
  "type" : "object",
  "propertyOrder" : 2,
  "properties" : {
    "org.forgerock.services.umaaudit.store.location" : {
      "title" : "Store Mode",
      "type" : "object",
      "propertyOrder" : 0,
      "description" : "",
      "properties" : {
        "value" : {
          "enum" : [ "default", "external" ],
          "options" : {
            "enum_titles" : [ "Default Token Store", "External Token Store" ]
          },
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    },
    "org.forgerock.services.umaaudit.store.root.suffix" : {
      "title" : "Root Suffix",
      "type" : "object",
      "propertyOrder" : 1,
      "description" : "",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  },
  "org.forgerock.services.umaaudit.store.max.connections" : {
    "title" : "Max Connections",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  }
}

```

```

    }
  }
}
},
"amconfig.org.forgerock.services.umaaudit.store.external.section" : {
  "title" : "External UMA Audit Store Configuration",
  "type" : "object",
  "propertyOrder" : 3,
  "properties" : {
    "org.forgerock.services.umaaudit.store.ssl.enabled" : {
      "title" : "SSL/TLS Enabled",
      "type" : "object",
      "propertyOrder" : 0,
      "description" : "",
      "properties" : {
        "value" : {
          "type" : "boolean",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    },
    "org.forgerock.services.umaaudit.store.directory.name" : {
      "title" : "Connection String(s)",
      "type" : "object",
      "propertyOrder" : 1,
      "description" : "An ordered list of connection strings for LDAP directories. Each connection
string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
IDs are optional parameters that will prioritize that connection to use from the specified nodes.
Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>.",
      "properties" : {
        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  },
  "org.forgerock.services.umaaudit.store.loginid" : {
    "title" : "Login Id",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  }
}

```



```

    }
  },
  "org.forgerock.services.umaudit.store.password" : {
    "title" : "Password",
    "type" : "object",
    "propertyOrder" : 3,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "string",
        "required" : false,
        "format" : "password"
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "org.forgerock.services.umaudit.store.heartbeat" : {
    "title" : "Heartbeat",
    "type" : "object",
    "propertyOrder" : 4,
    "description" : "",
    "properties" : {
      "value" : {
        "type" : "integer",
        "required" : false
      },
      "inherited" : {
        "type" : "boolean",
        "required" : true
      }
    }
  },
  "amconfig.org.forgerock.services.uma.pendingrequests.store.common.section" : {
    "title" : "Pending Requests Store",
    "type" : "object",
    "propertyOrder" : 4,
    "properties" : {
      "org.forgerock.services.uma.pendingrequests.store.location" : {
        "title" : "Store Mode",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "",
        "properties" : {
          "value" : {
            "enum" : [ "default", "external" ],
            "options" : {
              "enum_titles" : [ "Default Token Store", "External Token Store" ]
            },
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",

```

```

        "required" : true
    }
}
},
"org.forgerock.services.uma.pendingrequests.store.root.suffix" : {
    "title" : "Root Suffix",
    "type" : "object",
    "propertyOrder" : 1,
    "description" : "",
    "properties" : {
        "value" : {
            "type" : "string",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
},
"org.forgerock.services.uma.pendingrequests.store.max.connections" : {
    "title" : "Max Connections",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "",
    "properties" : {
        "value" : {
            "type" : "string",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
},
},
"amconfig.org.forgerock.services.uma.pendingrequests.store.external.section" : {
    "title" : "External Pending Requests Store Configuration",
    "type" : "object",
    "propertyOrder" : 5,
    "properties" : {
        "org.forgerock.services.uma.pendingrequests.store.ssl.enabled" : {
            "title" : "SSL/TLS Enabled",
            "type" : "object",
            "propertyOrder" : 0,
            "description" : "",
            "properties" : {
                "value" : {
                    "type" : "boolean",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        }
    }
},
},

```

```

"org.forgerock.services.uma.pendingrequests.store.directory.name" : {
  "title" : "Connection String(s)",
  "type" : "object",
  "propertyOrder" : 1,
  "description" : "An ordered list of connection strings for LDAP directories. Each connection
string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
IDs are optional parameters that will prioritize that connection to use from the specified nodes.
Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>.",
  "properties" : {
    "value" : {
      "type" : "string",
      "required" : false
    },
    "inherited" : {
      "type" : "boolean",
      "required" : true
    }
  }
},
"org.forgerock.services.uma.pendingrequests.store.loginid" : {
  "title" : "Login Id",
  "type" : "object",
  "propertyOrder" : 2,
  "description" : "",
  "properties" : {
    "value" : {
      "type" : "string",
      "required" : false
    },
    "inherited" : {
      "type" : "boolean",
      "required" : true
    }
  }
},
"org.forgerock.services.uma.pendingrequests.store.password" : {
  "title" : "Password",
  "type" : "object",
  "propertyOrder" : 3,
  "description" : "",
  "properties" : {
    "value" : {
      "type" : "string",
      "required" : false,
      "format" : "password"
    },
    "inherited" : {
      "type" : "boolean",
      "required" : true
    }
  }
},
"org.forgerock.services.uma.pendingrequests.store.heartbeat" : {
  "title" : "Heartbeat",
  "type" : "object",
  "propertyOrder" : 4,
  "description" : "",
  "properties" : {

```

```

        "value" : {
            "type" : "integer",
            "required" : false
        },
        "inherited" : {
            "type" : "boolean",
            "required" : true
        }
    }
}
},
"amconfig.org.forgerock.services.uma.labels.store.common.section" : {
    "title" : "UMA Resource Set Labels Store",
    "type" : "object",
    "propertyOrder" : 6,
    "properties" : {
        "org.forgerock.services.uma.labels.store.location" : {
            "title" : "Store Mode",
            "type" : "object",
            "propertyOrder" : 0,
            "description" : "",
            "properties" : {
                "value" : {
                    "enum" : [ "default", "external" ],
                    "options" : {
                        "enum_titles" : [ "Default Token Store", "External Token Store" ]
                    },
                    "type" : "string",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        },
        "org.forgerock.services.uma.labels.store.root.suffix" : {
            "title" : "Root Suffix",
            "type" : "object",
            "propertyOrder" : 1,
            "description" : "",
            "properties" : {
                "value" : {
                    "type" : "string",
                    "required" : false
                },
                "inherited" : {
                    "type" : "boolean",
                    "required" : true
                }
            }
        }
    },
    "org.forgerock.services.uma.labels.store.max.connections" : {
        "title" : "Max Connections",
        "type" : "object",
        "propertyOrder" : 2,
        "description" : "",
        "properties" : {

```

```

        "value" : {
          "type" : "string",
          "required" : false
        },
        "inherited" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  },
  "amconfig.org.forgerock.services.uma.labels.store.external.section" : {
    "title" : "External Resource Set Labels Store Configuration",
    "type" : "object",
    "propertyOrder" : 7,
    "properties" : {
      "org.forgerock.services.uma.labels.store.ssl.enabled" : {
        "title" : "SSL/TLS Enabled",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "",
        "properties" : {
          "value" : {
            "type" : "boolean",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "org.forgerock.services.uma.labels.store.directory.name" : {
        "title" : "Connection String(s)",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "An ordered list of connection strings for LDAP directories. Each connection string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site IDs are optional parameters that will prioritize that connection to use from the specified nodes. Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|site1,host3:50389</code>.",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  },
  "org.forgerock.services.uma.labels.store.loginid" : {
    "title" : "Login Id",
    "type" : "object",
    "propertyOrder" : 2,
    "description" : "",
    "properties" : {

```



Resource path: `/users/{user}/uma/policies`

Resource version: `1.0`

## 1.140.1.1. create

Creates an UMA Policy

Usage:

```
am> create UmaPolicies --realm Realm --id id --body body --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "A policy defining who can access a particular resource set",
  "type" : "object",
  "title" : "UMA Policy",
  "properties" : {
    "policyId" : {
      "type" : "string",
      "title" : "Policy ID",
      "description" : "The ID must correspond with an existing resource set ID"
    },
    "permissions" : {
      "type" : "array",
      "title" : "Permissions",
      "description" : "A list of subjects and the scopes they are allowed access to",
      "items" : {
        "type" : "object",
        "properties" : {
          "subject" : {
            "type" : "string",
            "title" : "Subject",
            "description" : "The username of the subject"
          },
          "scopes" : {
            "type" : "array",
            "title" : "Scopes",
            "description" : "The scopes that the user is allowed access to",
            "items" : {
              "type" : "string"
            }
          }
        }
      }
    }
  }
}
```

```
}
```

**--user**

Provides create, delete and query operations for UMA Policies

### 1.140.1.2. delete

Deletes an UMA Policy

Usage:

```
am> delete UmaPolicies --realm Realm --id id --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--user**

Provides create, delete and query operations for UMA Policies

### 1.140.1.3. query

Queries an UMA Policy

Usage:

```
am> query UmaPolicies --realm Realm --filter filter --user user
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

**--user**

Provides create, delete and query operations for UMA Policies

### 1.140.1.4. read

Reads an UMA Policy

Usage:

```
am> read UmaPolicies --realm Realm --id id --user user
```

Parameters:

**--id**

The unique identifier for the resource.



**--user**

Provides create, delete and query operations for UMA Policies

### 1.140.1.5. update

Updates an UMA Policy

Usage:

```
am> update UmaPolicies --realm Realm --id id --body body --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "A policy defining who can access a particular resource set",
  "type" : "object",
  "title" : "UMA Policy",
  "properties" : {
    "policyId" : {
      "type" : "string",
      "title" : "Policy ID",
      "description" : "The ID must correspond with an existing resource set ID"
    },
    "permissions" : {
      "type" : "array",
      "title" : "Permissions",
      "description" : "A list of subjects and the scopes they are allowed access to",
      "items" : {
        "type" : "object",
        "properties" : {
          "subject" : {
            "type" : "string",
            "title" : "Subject",
            "description" : "The username of the subject"
          },
          "scopes" : {
            "type" : "array",
            "title" : "Scopes",
            "description" : "The scopes that the user is allowed access to",
            "items" : {
              "type" : "string"
            }
          }
        }
      }
    }
  }
}
```

**--user**

Provides create, delete and query operations for UMA Policies

## 1.141. UmaProvider

### 1.141.1. Realm Operations

Resource path: `/realm-config/services/uma`

Resource version: `1.0`

#### 1.141.1.1. create

Usage:

```
am> create UmaProvider --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "emailRequestingPartyOnPendingRequestApproval" : {
      "title" : "Email Requesting Party on Pending Request approval",
      "description" : "Whether to send an email to the Requesting Party when a Pending Request is approved by the Resource Owner.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "resharingMode" : {
      "title" : "Re-Sharing Mode",
      "description" : "Whether re-sharing is off or on implicitly for all users, allowing all users to re-share resource sets that have been shared with them.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "permissionTicketLifetime" : {
      "title" : "Permission Ticket Lifetime (seconds)",
      "description" : "The maximum life of a permission ticket before it expires, in seconds.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

```

    },
    "requireTrustElevation" : {
      "title" : "Require Trust Elevation",
      "description" : "Determine if trust elevation is required and claims (such as an OpenID
Connection ID token) need to be present in the authorization request. If not, the AAT is sufficient
to determine the requesting party of the authorization request.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "rptLifetime" : {
      "title" : "Requesting Party Token Lifetime (seconds)",
      "description" : "The maximum life of a Requesting Party Token (RPT) before it expires, in
seconds.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "deleteResourceSetsOnDeleteRS" : {
      "title" : "Delete resource sets when Resource Server is removed",
      "description" : "Delete all resource sets that relate to a Resource Server when removing the
OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "emailResourceOwnerOnPendingRequestCreation" : {
      "title" : "Email Resource Owner on Pending Request creation",
      "description" : "Whether to send an email to the Resource Owner when a Pending Request is
created when a Requesting Party requests authorization to a resource.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userProfileLocaleAttribute" : {
      "title" : "User profile preferred Locale attribute",
      "description" : "User profile attribute storing the user's preferred locale.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deletePoliciesOnDeleteRS" : {
      "title" : "Delete user policies when Resource Server is removed",
      "description" : "Delete all user policies that relate to a Resource Server when removing the
OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}

```

## 1.141.1.2. delete

Usage:

```
am> delete UmaProvider --realm Realm
```

## 1.141.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UmaProvider --realm Realm --actionName getAllTypes
```

## 1.141.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UmaProvider --realm Realm --actionName getCreatableTypes
```

## 1.141.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UmaProvider --realm Realm --actionName nextdescendents
```

## 1.141.1.6. read

Usage:

```
am> read UmaProvider --realm Realm
```

## 1.141.1.7. update

Usage:

```
am> update UmaProvider --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "emailRequestingPartyOnPendingRequestApproval" : {
      "title" : "Email Requesting Party on Pending Request approval",
      "description" : "Whether to send an email to the Requesting Party when a Pending Request is approved by the Resource Owner.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "resharingMode" : {
      "title" : "Re-Sharing Mode",
      "description" : "Whether re-sharing is off or on implicitly for all users, allowing all users to re-share resource sets that have been shared with them.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "permissionTicketLifetime" : {
      "title" : "Permission Ticket Lifetime (seconds)",
      "description" : "The maximum life of a permission ticket before it expires, in seconds.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "requireTrustElevation" : {
      "title" : "Require Trust Elevation",
      "description" : "Determine if trust elevation is required and claims (such as an OpenID Connection ID token) need to be present in the authorization request. If not, the AAT is sufficient to determine the requesting party of the authorization request.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "rptLifetime" : {
      "title" : "Requesting Party Token Lifetime (seconds)",
      "description" : "The maximum life of a Requesting Party Token (RPT) before it expires, in seconds.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "deleteResourceSetsOnDeleteRS" : {
      "title" : "Delete resource sets when Resource Server is removed",
      "description" : "Delete all resource sets that relate to a Resource Server when removing the OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

```

    "exampleValue" : ""
  },
  "emailResourceOwnerOnPendingRequestCreation" : {
    "title" : "Email Resource Owner on Pending Request creation",
    "description" : "Whether to send an email to the Resource Owner when a Pending Request is
created when a Requesting Party requests authorization to a resource.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userProfileLocaleAttribute" : {
    "title" : "User profile preferred Locale attribute",
    "description" : "User profile attribute storing the user's preferred locale.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "deletePoliciesOnDeleteRS" : {
    "title" : "Delete user policies when Resource Server is removed",
    "description" : "Delete all user policies that relate to a Resource Server when removing the
OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  }
}
}

```

## 1.141.2. Global Operations

Resource path: `/global-config/services/uma`

Resource version: `1.0`

### 1.141.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UmaProvider --global --actionName getAllTypes
```

### 1.141.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UmaProvider --global --actionName getCreatableTypes
```

### 1.141.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UmaProvider --global --actionName nextdescendents
```

### 1.141.2.4. read

Usage:

```
am> read UmaProvider --global
```

### 1.141.2.5. update

Usage:

```
am> update UmaProvider --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "resharingMode" : {
          "title" : "Re-Sharing Mode",
          "description" : "Whether re-sharing is off or on implicitly for all users, allowing all
users to re-share resource sets that have been shared with them.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "emailRequestingPartyOnPendingRequestApproval" : {
          "title" : "Email Requesting Party on Pending Request approval",
          "description" : "Whether to send an email to the Requesting Party when a Pending Request is
approved by the Resource Owner.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "requireTrustElevation" : {
          "title" : "Require Trust Elevation",
          "description" : "Determine if trust elevation is required and claims (such as an OpenID
Connection ID token) need to be present in the authorization request. If not, the AAT is sufficient
to determine the requesting party of the authorization request.",
          "propertyOrder" : 900,

```

```

    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userProfileLocaleAttribute" : {
    "title" : "User profile preferred Locale attribute",
    "description" : "User profile attribute storing the user's preferred locale.",
    "propertyOrder" : 700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "emailResourceOwnerOnPendingRequestCreation" : {
    "title" : "Email Resource Owner on Pending Request creation",
    "description" : "Whether to send an email to the Resource Owner when a Pending Request is
created when a Requesting Party requests authorization to a resource.",
    "propertyOrder" : 500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "deleteResourceSetsOnDeleteRS" : {
    "title" : "Delete resource sets when Resource Server is removed",
    "description" : "Delete all resource sets that relate to a Resource Server when removing the
OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
    "propertyOrder" : 400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "permissionTicketLifetime" : {
    "title" : "Permission Ticket Lifetime (seconds)",
    "description" : "The maximum life of a permission ticket before it expires, in seconds.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "deletePoliciesOnDeleteRS" : {
    "title" : "Delete user policies when Resource Server is removed",
    "description" : "Delete all user policies that relate to a Resource Server when removing the
OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "rptLifetime" : {
    "title" : "Requesting Party Token Lifetime (seconds)",
    "description" : "The maximum life of a Requesting Party Token (RPT) before it expires, in
seconds.",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  }
},
"type" : "object",
"title" : "Realm Defaults"

```



```
}  
}  
}
```

## 1.142. UmaResourceSetLabels

### 1.142.1. Realm Operations

Provides create, delete and query operations for UMA resource set labels

Resource path: `/users/{user}/oauth2/resources/labels`

Resource version: `1.0`

#### 1.142.1.1. create

Creates a UMA Resource Set Label

Usage:

```
am> create UmaResourceSetLabels --realm Realm --id id --body body --user user
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Represents a UMA Resource Set Label",
  "id" : "urn:jsonschema:org:forgerock:openam:oauth2:resources:labels:ResourceSetLabel",
  "type" : "object",
  "title" : "UMA Resource Set Label",
  "properties" : {
    "id" : {
      "type" : "string",
      "description" : "The unique identifier of the resource set label",
      "title" : "Id"
    },
    "name" : {
      "type" : "string",
      "description" : "The displayed text of the label",
      "title" : "Name"
    },
    "type" : {
      "type" : "string",
      "description" : "The type of the label e.g. 'System'",
      "title" : "Type",
      "enum" : [ "STAR", "USER", "SYSTEM" ]
    },
    "resourceSetIds" : {
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    }
  }
}
```

#### --user

Provides create, delete and query operations for UMA resource set labels

### 1.142.1.2. delete

Deletes a UMA Resource Set Label

Usage:

```
am> delete UmaResourceSetLabels --realm Realm --id id --user user
```

Parameters:

#### --id

The unique identifier for the resource.

#### --user

Provides create, delete and query operations for UMA resource set labels

### 1.142.1.3. query

Queries the collection of UMA labels

Usage:

```
am> query UmaResourceSetLabels --realm Realm --filter filter --user user
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

**--user**

Provides create, delete and query operations for UMA resource set labels

## 1.143. UmaUserAuditHistory

### 1.143.1. Realm Operations

Provides access to UMA auditing history for a user

Resource path: `/users/{user}/uma/auditHistory`

Resource version: `1.0`

#### 1.143.1.1. getHistory

Returns the audit history of a user

Usage:

```
am> action UmaUserAuditHistory --realm Realm --user user --actionName getHistory
```

Parameters:

**--user**

Provides access to UMA auditing history for a user

#### 1.143.1.2. query

Queries the collection of auditing history

Usage:

```
am> query UmaUserAuditHistory --realm Realm --filter filter --user user
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [\*]

**--user**

Provides access to UMA auditing history for a user

## 1.144. User

### 1.144.1. Realm Operations

Resource path: `/realm-config/services/user`

Resource version: `1.0`

#### 1.144.1.1. create

Usage:

```
am> create User --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "defaultUserStatus" : {
          "title" : "Default User Status",
          "description" : "Inactive users cannot authenticate, though OpenAM stores their profiles.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "preferredTimezone" : {
          "title" : "User Preferred Timezone",
          "description" : "Time zone for accessing OpenAM console.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

```

    },
    "adminDNStartingView" : {
      "title" : "Administrator DN Starting View",
      "description" : "Specifies the DN for the initial screen when the OpenAM administrator
successfully logs in to the OpenAM console.",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "type" : "object",
  "title" : "Dynamic Attributes"
}
}
}

```

### 1.144.1.2. delete

Usage:

```
am> delete User --realm Realm
```

### 1.144.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action User --realm Realm --actionName getAllTypes
```

### 1.144.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action User --realm Realm --actionName getCreatableTypes
```

### 1.144.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action User --realm Realm --actionName nextdescendents
```

### 1.144.1.6. read

Usage:

```
am> read User --realm Realm
```

## 1.144.1.7. update

Usage:

```
am> update User --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "defaultUserStatus" : {
          "title" : "Default User Status",
          "description" : "Inactive users cannot authenticate, though OpenAM stores their profiles.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "preferredTimezone" : {
          "title" : "User Preferred Timezone",
          "description" : "Time zone for accessing OpenAM console.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "adminDNStartingView" : {
          "title" : "Administrator DN Starting View",
          "description" : "Specifies the DN for the initial screen when the OpenAM administrator successfully logs in to the OpenAM console.",
          "propertyOrder" : 200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "type" : "object",
    "title" : "Dynamic Attributes"
  }
}
```

## 1.144.2. Global Operations

Resource path: `/global-config/services/user`

Resource version: `1.0`

### 1.144.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action User --global --actionName getAllTypes
```

### 1.144.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action User --global --actionName getCreatableTypes
```

### 1.144.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action User --global --actionName nextdescendents
```

### 1.144.2.4. read

Usage:

```
am> read User --global
```

### 1.144.2.5. update

Usage:

```
am> update User --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
```

```

    "dynamic" : {
      "properties" : {
        "adminDNStartingView" : {
          "title" : "Administrator DN Starting View",
          "description" : "Specifies the DN for the initial screen when the OpenAM administrator
successfully logs in to the OpenAM console.",
          "propertyOrder" : 200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "preferredTimezone" : {
          "title" : "User Preferred Timezone",
          "description" : "Time zone for accessing OpenAM console.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultUserStatus" : {
          "title" : "Default User Status",
          "description" : "Inactive users cannot authenticate, though OpenAM stores their profiles.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}

```

## 1.145. UserRegistration

### 1.145.1. Realm Operations

Self Service endpoint for registering a new user

Resource path: `/selfservice/userRegistration`

Resource version: `1.0`

#### 1.145.1.1. read

Initialise the user registration process. A set of requirements will be returned that will need to be fulfilled and sent to the submitRequirements action.

Usage:

```
am> read UserRegistration --realm Realm
```



### 1.145.1.2. submitRequirements

Submit some fulfilled requirements. Returns either a completion status, or a token along with some more requirements. If requirements are returned, they should be submitted with the token as a fresh request to this action.

Usage:

```
am> action UserRegistration --realm Realm --body body --actionName submitRequirements
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The structure of a request to the submitRequirements action.",
  "type" : "object",
  "title" : "Submit requirements structure",
  "properties" : {
    "token" : {
      "type" : "string",
      "title" : "Token",
      "description" : "The token returned from the previous submitRequirements request."
    },
    "input" : {
      "type" : "object",
      "title" : "Input",
      "description" : "The input as collected from the new user. This object must conform to the JSON Schema of the requirements property from the last response.",
      "patternProperties" : {
        ".*" : {
          "type" : "any",
          "title" : "Input Property",
          "description" : "Valid content according to the received JSON Schema."
        }
      }
    }
  },
  "required" : [ "input" ]
}
```

## 1.146. UserSelfService

### 1.146.1. Realm Operations

Resource path: `/realm-config/services/selfService`

Resource version: `1.0`

## 1.146.1.1. create

Usage:

```
am> create UserSelfService --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "forgottenPassword" : {
      "type" : "object",
      "title" : "Forgotten Password",
      "propertyOrder" : 2,
      "properties" : {
        "forgottenPasswordEmailSubject" : {
          "title" : "Outgoing Email Subject",
          "description" : "Customize the forgotten password email subject text. Format is
<code>locale|subject text</code>.",
          "propertyOrder" : 220,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgottenPasswordEmailBody" : {
          "title" : "Outgoing Email Body",
          "description" : "Customize the forgotten password email body text. Format is
body text<code>locale|
body text</code>.",
          "propertyOrder" : 230,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgottenPasswordEnabled" : {
          "title" : "Forgotten Password",
          "description" : "If enabled, users can reset their forgotten password.",
          "propertyOrder" : 170,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenPasswordEmailVerificationEnabled" : {
          "title" : "Email Verification",
          "description" : "If enabled, users who reset passwords must perform email address
verification.",
          "propertyOrder" : 190,
          "required" : false,
```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenPasswordKbaEnabled" : {
        "title" : "Security Questions",
        "description" : "If enabled, users must answer their security questions during the forgotten
password process.",
        "propertyOrder" : 200,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenPasswordTokenTTL" : {
        "title" : "Token Lifetime (seconds)",
        "description" : "Maximum lifetime for the token allowing forgotten password reset, in
seconds.<p><p>Specify a value from <code>0</code> to <code>2147483647</code>.",
        "propertyOrder" : 210,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
    },
    "forgottenPasswordCaptchaEnabled" : {
        "title" : "Captcha",
        "description" : "If enabled, users must pass a Google reCAPTCHA challenge during password
reset to mitigate against software bots.",
        "propertyOrder" : 180,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"generalConfig" : {
    "type" : "object",
    "title" : "General Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "validQueryAttributes" : {
            "title" : "Valid Query Attributes",
            "description" : "Specifies the valid query attributes used to search for the user. This is a
list of attributes used to identify your account for forgotten password and forgotten username.",
            "propertyOrder" : 80,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "minimumAnswersToVerify" : {
            "title" : "Minimum Answers to Verify",
            "description" : "Specifies the minimum number of KBA questions that users need to answer
to be granted the privilege to carry out an action, such as registering for an account, resetting a
password, or retrieving a username. Specify a value from <code>0</code> to <code>50</code>.",
            "propertyOrder" : 70,
            "required" : false,
            "type" : "integer",
            "exampleValue" : ""
        }
    }
},

```

```

"captchaSecretKey" : {
  "title" : "Google reCAPTCHA Secret Key",
  "description" : "Google reCAPTCHA plugin secret key.",
  "propertyOrder" : 30,
  "required" : false,
  "type" : "string",
  "exampleValue" : ""
},
"signingSecretKeyAlias" : {
  "title" : "Signing Secret Key Alias",
  "description" : "A signing secret key alias in the OpenAM server's JCEKS keystore. Used to
sign the JWT token that OpenAM uses to track end users during User Self-Service operations.",
  "propertyOrder" : 10,
  "required" : true,
  "type" : "string",
  "exampleValue" : "selfservicesigntest"
},
"encryptionKeyPairAlias" : {
  "title" : "Encryption Key Pair Alias",
  "description" : "An encryption key alias in the OpenAM server's JCEKS keystore. Used to
encrypt the JWT token that OpenAM uses to track end users during User Self-Service operations.",
  "propertyOrder" : 0,
  "required" : true,
  "type" : "string",
  "exampleValue" : "selfserviceenctest"
},
"kbaQuestions" : {
  "title" : "Security Questions",
  "description" : "Specifies the default set of knowledge-based authentication (KBA) security
questions. The security questions can be set for the User Self-Registration, forgotten password
reset, and forgotten username services, respectively.<p><p>Format is <code>unique key|locale|
question</code>.",
  "propertyOrder" : 50,
  "required" : false,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"minimumAnswersToDefine" : {
  "title" : "Minimum Answers to Define",
  "description" : "Specifies the minimum number of KBA answers that users must define.",
  "propertyOrder" : 60,
  "required" : false,
  "type" : "integer",
  "exampleValue" : ""
},
"captchaSiteKey" : {
  "title" : "Google reCAPTCHA Site Key",
  "description" : "Google reCAPTCHA plugin site key.",
  "propertyOrder" : 20,
  "required" : false,
  "type" : "string",
  "exampleValue" : ""
},
"captchaVerificationUrl" : {
  "title" : "Google Re-captcha Verification URL",
  "description" : "Google reCAPTCHA plugin verification URL.",

```

```

        "propertyOrder" : 40,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    }
},
"userRegistration" : {
    "type" : "object",
    "title" : "User Registration",
    "propertyOrder" : 1,
    "properties" : {
        "userRegistrationValidUserAttributes" : {
            "title" : "Valid Creation Attributes",
            "description" : "Specifies a whitelist of user attributes that can be set during user
creation.",
            "propertyOrder" : 160,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "userRegistrationKbaEnabled" : {
            "title" : "Security Questions",
            "description" : "If enabled, users must set up their security questions during the self-
registration process.",
            "propertyOrder" : 120,
            "required" : false,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "userRegistrationTokenTTL" : {
            "title" : "Token Lifetime (seconds)",
            "description" : "Maximum lifetime of the token allowing User Self-Registration, in
seconds.",
            "propertyOrder" : 130,
            "required" : false,
            "type" : "integer",
            "exampleValue" : ""
        },
        "userRegistrationCaptchaEnabled" : {
            "title" : "Captcha",
            "description" : "If enabled, users must pass a Google reCAPTCHA challenge during user self-
registration to mitigate against software bots.",
            "propertyOrder" : 100,
            "required" : false,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "userRegistrationEmailSubject" : {
            "title" : "Outgoing Email Subject",
            "description" : "Customize the User Self-Registration verification email subject text.
Format is <code>locale|subject text</code>.",
            "propertyOrder" : 140,
            "required" : false,
            "items" : {
                "type" : "string"
            }
        }
    }
}

```

```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userRegistrationEnabled" : {
    "title" : "User Registration",
    "description" : "If enabled, new users can sign up for an account.",
    "propertyOrder" : 90,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userRegistrationEmailVerificationEnabled" : {
    "title" : "Email Verification",
    "description" : "If enabled, users who self-register must perform email address
verification.",
    "propertyOrder" : 110,
    "required" : false,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userRegistrationEmailBody" : {
    "title" : "Outgoing Email Body",
    "description" : "Customize the User Self-Registration verification email body text. Format
is: <code>locale|body text</code>.",
    "propertyOrder" : 150,
    "required" : false,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userRegisteredDestination" : {
    "title" : "Destination After Successful Self-Registration",
    "description" : "Specifies the action to be taken after a user successfully registers
a new account. Choose from:<ul><li><code>default</code>. User is sent to a success page without
being logged in.</li><li><code>login</code>. User is sent to the login page to authenticate.</
li><li><code>autologin</code>. User is automatically logged in and sent to the appropriate page.</
li></ul>",
    "propertyOrder" : 161,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
},
"advancedConfig" : {
  "type" : "object",
  "title" : "Advanced Configuration",
  "propertyOrder" : 5,
  "properties" : {
    "userRegistrationServiceConfigClass" : {
      "title" : "User Registration Service Config Provider Class",
      "description" : "Specifies the provider class to configure any custom plugins.",
      "propertyOrder" : 350,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}

```

```

    },
    "forgottenUsernameServiceConfigClass" : {
      "title" : "Forgotten Username Service Config Provider Class",
      "description" : "Specifies the provider class to configure any custom plugins.",
      "propertyOrder" : 370,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "userRegistrationConfirmationUrl" : {
      "title" : "User Registration Confirmation Email URL",
      "description" : "Specifies the confirmation URL that the user receives during the self-
registration process. The <code>${realm}</code> string is replaced with the current realm.",
      "propertyOrder" : 330,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "forgottenPasswordServiceConfigClass" : {
      "title" : "Forgotten Password Service Config Provider Class",
      "description" : "Specifies the provider class to configure any custom plugins.",
      "propertyOrder" : 360,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "forgottenPasswordConfirmationUrl" : {
      "title" : "Forgotten Password Confirmation Email URL",
      "description" : "Specifies the confirmation URL that the user receives after confirming
their identity during the forgotten password process. The <code>${realm}</code> string is replaced
with the current realm.",
      "propertyOrder" : 340,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
},
"forgottenUsername" : {
  "type" : "object",
  "title" : "Forgotten Username",
  "propertyOrder" : 3,
  "properties" : {
    "forgottenUsernameCaptchaEnabled" : {
      "title" : "Captcha",
      "description" : "If enabled, users must pass a Google reCAPTCHA challenge during the
forgotten username retrieval process to mitigate against software bots.",
      "propertyOrder" : 250,
      "required" : false,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "forgottenUsernameKbaEnabled" : {
      "title" : "Security Questions",
      "description" : "If enabled, users must answer their security questions during the forgotten
username process.",
      "propertyOrder" : 260,
      "required" : false,
      "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "forgottenUsernameEmailSubject" : {
    "title" : "Outgoing Email Subject",
    "description" : "Customizes the forgotten username email subject text. Format is
<code>locale|subject text</code>.",
    "propertyOrder" : 300,
    "required" : false,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "forgottenUsernameShowUsernameEnabled" : {
    "title" : "Show Username",
    "description" : "If enabled, users see their forgotten username on the browser page.",
    "propertyOrder" : 280,
    "required" : false,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "forgottenUsernameEnabled" : {
    "title" : "Forgotten Username",
    "description" : "If enabled, users can retrieve their forgotten username.",
    "propertyOrder" : 240,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "forgottenUsernameEmailUsernameEnabled" : {
    "title" : "Email Username",
    "description" : "If enabled, users receive their forgotten username by email.",
    "propertyOrder" : 270,
    "required" : false,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "forgottenUsernameEmailBody" : {
    "title" : "Outgoing Email Body",
    "description" : "Customizes the forgotten username email body text. Format is <code>locale|
body text</code>.",
    "propertyOrder" : 310,
    "required" : false,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "forgottenUsernameTokenTTL" : {
    "title" : "Token LifeTime (seconds)",
    "description" : "Maximum lifetime for the token allowing forgotten username, in seconds.",
    "propertyOrder" : 290,
    "required" : false,
    "type" : "integer",
    "exampleValue" : ""
  }
}

```



```

    },
    "profileManagement" : {
      "type" : "object",
      "title" : "Profile Management",
      "propertyOrder" : 4,
      "properties" : {
        "profileProtectedUserAttributes" : {
          "title" : "Protected Update Attributes",
          "description" : "Specifies a profile's protected user attributes, which causes re-
authentication when the user attempts to modify these attributes.",
          "propertyOrder" : 320,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
}
}

```

### 1.146.1.2. delete

Usage:

```
am> delete UserSelfService --realm Realm
```

### 1.146.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UserSelfService --realm Realm --actionName getAllTypes
```

### 1.146.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UserSelfService --realm Realm --actionName getCreatableTypes
```

### 1.146.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UserSelfService --realm Realm --actionName nextdescendents
```

## 1.146.1.6. read

Usage:

```
am> read UserSelfService --realm Realm
```

## 1.146.1.7. update

Usage:

```
am> update UserSelfService --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "forgottenPassword" : {
      "type" : "object",
      "title" : "Forgotten Password",
      "propertyOrder" : 2,
      "properties" : {
        "forgottenPasswordEmailSubject" : {
          "title" : "Outgoing Email Subject",
          "description" : "Customize the forgotten password email subject text. Format is
<code>locale|subject text</code>.",
          "propertyOrder" : 220,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgottenPasswordEmailBody" : {
          "title" : "Outgoing Email Body",
          "description" : "Customize the forgotten password email body text. Format is
body text<code>locale|
body text</code>.",
          "propertyOrder" : 230,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgottenPasswordEnabled" : {
          "title" : "Forgotten Password",
          "description" : "If enabled, users can reset their forgotten password.",
          "propertyOrder" : 170,
          "required" : true,
          "type" : "boolean",
```

```

        "exampleValue" : ""
    },
    "forgottenPasswordEmailVerificationEnabled" : {
        "title" : "Email Verification",
        "description" : "If enabled, users who reset passwords must perform email address
verification.",
        "propertyOrder" : 190,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenPasswordKbaEnabled" : {
        "title" : "Security Questions",
        "description" : "If enabled, users must answer their security questions during the forgotten
password process.",
        "propertyOrder" : 200,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenPasswordTokenTTL" : {
        "title" : "Token Lifetime (seconds)",
        "description" : "Maximum lifetime for the token allowing forgotten password reset, in
seconds.<p><p>Specify a value from <code>0</code> to <code>2147483647</code>.",
        "propertyOrder" : 210,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
    },
    "forgottenPasswordCaptchaEnabled" : {
        "title" : "Captcha",
        "description" : "If enabled, users must pass a Google reCAPTCHA challenge during password
reset to mitigate against software bots.",
        "propertyOrder" : 180,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"generalConfig" : {
    "type" : "object",
    "title" : "General Configuration",
    "propertyOrder" : 0,
    "properties" : {
        "validQueryAttributes" : {
            "title" : "Valid Query Attributes",
            "description" : "Specifies the valid query attributes used to search for the user. This is a
list of attributes used to identify your account for forgotten password and forgotten username.",
            "propertyOrder" : 80,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "minimumAnswersToVerify" : {
            "title" : "Minimum Answers to Verify",

```

```

    "description" : "Specifies the minimum number of KBA questions that users need to answer
to be granted the privilege to carry out an action, such as registering for an account, resetting a
password, or retrieving a username. Specify a value from <code>0</code> to <code>50</code>.",
    "propertyOrder" : 70,
    "required" : false,
    "type" : "integer",
    "exampleValue" : ""
  },
  "captchaSecretKey" : {
    "title" : "Google reCAPTCHA Secret Key",
    "description" : "Google reCAPTCHA plugin secret key.",
    "propertyOrder" : 30,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "signingSecretKeyAlias" : {
    "title" : "Signing Secret Key Alias",
    "description" : "A signing secret key alias in the OpenAM server's JCEKS keystore. Used to
sign the JWT token that OpenAM uses to track end users during User Self-Service operations.",
    "propertyOrder" : 10,
    "required" : true,
    "type" : "string",
    "exampleValue" : "selfservicesigntest"
  },
  "encryptionKeyPairAlias" : {
    "title" : "Encryption Key Pair Alias",
    "description" : "An encryption key alias in the OpenAM server's JCEKS keystore. Used to
encrypt the JWT token that OpenAM uses to track end users during User Self-Service operations.",
    "propertyOrder" : 0,
    "required" : true,
    "type" : "string",
    "exampleValue" : "selfserviceenctest"
  },
  "kbaQuestions" : {
    "title" : "Security Questions",
    "description" : "Specifies the default set of knowledge-based authentication (KBA) security
questions. The security questions can be set for the User Self-Registration, forgotten password
reset, and forgotten username services, respectively.<p><p>Format is <code>unique key|locale|
question</code>.",
    "propertyOrder" : 50,
    "required" : false,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "minimumAnswersToDefine" : {
    "title" : "Minimum Answers to Define",
    "description" : "Specifies the minimum number of KBA answers that users must define.",
    "propertyOrder" : 60,
    "required" : false,
    "type" : "integer",
    "exampleValue" : ""
  },
  "captchaSiteKey" : {
    "title" : "Google reCAPTCHA Site Key",
    "description" : "Google reCAPTCHA plugin site key.",

```

```

        "propertyOrder" : 20,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "captchaVerificationUrl" : {
        "title" : "Google Re-captcha Verification URL",
        "description" : "Google reCAPTCHA plugin verification URL.",
        "propertyOrder" : 40,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    }
},
"userRegistration" : {
    "type" : "object",
    "title" : "User Registration",
    "propertyOrder" : 1,
    "properties" : {
        "userRegistrationValidUserAttributes" : {
            "title" : "Valid Creation Attributes",
            "description" : "Specifies a whitelist of user attributes that can be set during user
creation.",
            "propertyOrder" : 160,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "userRegistrationKbaEnabled" : {
            "title" : "Security Questions",
            "description" : "If enabled, users must set up their security questions during the self-
registration process.",
            "propertyOrder" : 120,
            "required" : false,
            "type" : "boolean",
            "exampleValue" : ""
        },
        "userRegistrationTokenTTL" : {
            "title" : "Token Lifetime (seconds)",
            "description" : "Maximum lifetime of the token allowing User Self-Registration, in
seconds.",
            "propertyOrder" : 130,
            "required" : false,
            "type" : "integer",
            "exampleValue" : ""
        },
        "userRegistrationCaptchaEnabled" : {
            "title" : "Captcha",
            "description" : "If enabled, users must pass a Google reCAPTCHA challenge during user self-
registration to mitigate against software bots.",
            "propertyOrder" : 100,
            "required" : false,
            "type" : "boolean",
            "exampleValue" : ""
        }
    }
},

```

```

    "userRegistrationEmailSubject" : {
      "title" : "Outgoing Email Subject",
      "description" : "Customize the User Self-Registration verification email subject text.
Format is <code>locale|subject text</code>.",
      "propertyOrder" : 140,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userRegistrationEnabled" : {
      "title" : "User Registration",
      "description" : "If enabled, new users can sign up for an account.",
      "propertyOrder" : 90,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userRegistrationEmailVerificationEnabled" : {
      "title" : "Email Verification",
      "description" : "If enabled, users who self-register must perform email address
verification.",
      "propertyOrder" : 110,
      "required" : false,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userRegistrationEmailBody" : {
      "title" : "Outgoing Email Body",
      "description" : "Customize the User Self-Registration verification email body text. Format
is: <code>locale|body text</code>.",
      "propertyOrder" : 150,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userRegisteredDestination" : {
      "title" : "Destination After Successful Self-Registration",
      "description" : "Specifies the action to be taken after a user successfully registers
a new account. Choose from:<ul><li><code>default</code>. User is sent to a success page without
being logged in.</li><li><code>login</code>. User is sent to the login page to authenticate.</
li><li><code>autologin</code>. User is automatically logged in and sent to the appropriate page.</
li></ul>",
      "propertyOrder" : 161,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "advancedConfig" : {
    "type" : "object",
    "title" : "Advanced Configuration",
    "propertyOrder" : 5,

```

```

"properties" : {
  "userRegistrationServiceConfigClass" : {
    "title" : "User Registration Service Config Provider Class",
    "description" : "Specifies the provider class to configure any custom plugins.",
    "propertyOrder" : 350,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "forgottenUsernameServiceConfigClass" : {
    "title" : "Forgotten Username Service Config Provider Class",
    "description" : "Specifies the provider class to configure any custom plugins.",
    "propertyOrder" : 370,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "userRegistrationConfirmationUrl" : {
    "title" : "User Registration Confirmation Email URL",
    "description" : "Specifies the confirmation URL that the user receives during the self-
registration process. The <code>${realm}</code> string is replaced with the current realm.",
    "propertyOrder" : 330,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "forgottenPasswordServiceConfigClass" : {
    "title" : "Forgotten Password Service Config Provider Class",
    "description" : "Specifies the provider class to configure any custom plugins.",
    "propertyOrder" : 360,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  },
  "forgottenPasswordConfirmationUrl" : {
    "title" : "Forgotten Password Confirmation Email URL",
    "description" : "Specifies the confirmation URL that the user receives after confirming
their identity during the forgotten password process. The <code>${realm}</code> string is replaced
with the current realm.",
    "propertyOrder" : 340,
    "required" : false,
    "type" : "string",
    "exampleValue" : ""
  }
}
},
"forgottenUsername" : {
  "type" : "object",
  "title" : "Forgotten Username",
  "propertyOrder" : 3,
  "properties" : {
    "forgottenUsernameCaptchaEnabled" : {
      "title" : "Captcha",
      "description" : "If enabled, users must pass a Google reCAPTCHA challenge during the
forgotten username retrieval process to mitigate against software bots.",
      "propertyOrder" : 250,
      "required" : false,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}

```

```

    },
    "forgottenUsernameKbaEnabled" : {
      "title" : "Security Questions",
      "description" : "If enabled, users must answer their security questions during the forgotten
username process.",
      "propertyOrder" : 260,
      "required" : false,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "forgottenUsernameEmailSubject" : {
      "title" : "Outgoing Email Subject",
      "description" : "Customizes the forgotten username email subject text. Format is
<code>locale|subject text</code>.",
      "propertyOrder" : 300,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "forgottenUsernameShowUsernameEnabled" : {
      "title" : "Show Username",
      "description" : "If enabled, users see their forgotten username on the browser page.",
      "propertyOrder" : 280,
      "required" : false,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "forgottenUsernameEnabled" : {
      "title" : "Forgotten Username",
      "description" : "If enabled, users can retrieve their forgotten username.",
      "propertyOrder" : 240,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "forgottenUsernameEmailUsernameEnabled" : {
      "title" : "Email Username",
      "description" : "If enabled, users receive their forgotten username by email.",
      "propertyOrder" : 270,
      "required" : false,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "forgottenUsernameEmailBody" : {
      "title" : "Outgoing Email Body",
      "description" : "Customizes the forgotten username email body text. Format is <code>locale|
body text</code>.",
      "propertyOrder" : 310,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "forgottenUsernameTokenTTL" : {

```



```

        "title" : "Token LifeTime (seconds)",
        "description" : "Maximum lifetime for the token allowing forgotten username, in seconds.",
        "propertyOrder" : 290,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
    }
},
"profileManagement" : {
    "type" : "object",
    "title" : "Profile Management",
    "propertyOrder" : 4,
    "properties" : {
        "profileProtectedUserAttributes" : {
            "title" : "Protected Update Attributes",
            "description" : "Specifies a profile's protected user attributes, which causes re-
authentication when the user attempts to modify these attributes.",
            "propertyOrder" : 320,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        }
    }
}
}
}
}
}

```

## 1.146.2. Global Operations

Resource path: [/global-config/services/selfService](#)

Resource version: 1.0

### 1.146.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UserSelfService --global --actionName getAllTypes
```

### 1.146.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UserSelfService --global --actionName getCreatableTypes
```

### 1.146.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UserSelfService --global --actionName nextdescendents
```

### 1.146.2.4. read

Usage:

```
am> read UserSelfService --global
```

### 1.146.2.5. update

Usage:

```
am> update UserSelfService --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "generalConfig" : {
          "type" : "object",
          "title" : "General Configuration",
          "propertyOrder" : 0,
          "properties" : {
            "kbaQuestions" : {
              "title" : "Security Questions",
              "description" : "Specifies the default set of knowledge-based authentication (KBA) security questions. The security questions can be set for the User Self-Registration, forgotten password reset, and forgotten username services, respectively.<p><p>Format is <code>unique key|locale|question</code>.",
              "propertyOrder" : 50,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "captchaVerificationUrl" : {
              "title" : "Google Re-captcha Verification URL",
              "description" : "Google reCAPTCHA plugin verification URL.",
              "propertyOrder" : 40,
              "required" : false,
```

```

        "type" : "string",
        "exampleValue" : ""
    },
    "captchaSecretKey" : {
        "title" : "Google reCAPTCHA Secret Key",
        "description" : "Google reCAPTCHA plugin secret key.",
        "propertyOrder" : 30,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "minimumAnswersToVerify" : {
        "title" : "Minimum Answers to Verify",
        "description" : "Specifies the minimum number of KBA questions that users need to answer
to be granted the privilege to carry out an action, such as registering for an account, resetting a
password, or retrieving a username. Specify a value from <code>0</code> to <code>50</code>.",
        "propertyOrder" : 70,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
    },
    "validQueryAttributes" : {
        "title" : "Valid Query Attributes",
        "description" : "Specifies the valid query attributes used to search for the user.
This is a list of attributes used to identify your account for forgotten password and forgotten
username.",
        "propertyOrder" : 80,
        "required" : false,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "encryptionKeyPairAlias" : {
        "title" : "Encryption Key Pair Alias",
        "description" : "An encryption key alias in the OpenAM server's JCEKS keystore. Used to
encrypt the JWT token that OpenAM uses to track end users during User Self-Service operations.",
        "propertyOrder" : 0,
        "required" : true,
        "type" : "string",
        "exampleValue" : "selfserviceenctest"
    },
    "captchaSiteKey" : {
        "title" : "Google reCAPTCHA Site Key",
        "description" : "Google reCAPTCHA plugin site key.",
        "propertyOrder" : 20,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "minimumAnswersToDefine" : {
        "title" : "Minimum Answers to Define",
        "description" : "Specifies the minimum number of KBA answers that users must define.",
        "propertyOrder" : 60,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
    },
    },

```

```

        "signingSecretKeyAlias" : {
            "title" : "Signing Secret Key Alias",
            "description" : "A signing secret key alias in the OpenAM server's JCEKS keystore. Used
to sign the JWT token that OpenAM uses to track end users during User Self-Service operations.",
            "propertyOrder" : 10,
            "required" : true,
            "type" : "string",
            "exampleValue" : "selfservicesigntest"
        }
    },
    "userRegistration" : {
        "type" : "object",
        "title" : "User Registration",
        "propertyOrder" : 1,
        "properties" : {
            "userRegistrationEmailSubject" : {
                "title" : "Outgoing Email Subject",
                "description" : "Customize the User Self-Registration verification email subject text.
Format is <code>locale|subject text</code>.",
                "propertyOrder" : 140,
                "required" : false,
                "items" : {
                    "type" : "string"
                },
                "type" : "array",
                "exampleValue" : ""
            },
            "userRegisteredDestination" : {
                "title" : "Destination After Successful Self-Registration",
                "description" : "Specifies the action to be taken after a user successfully registers
a new account. Choose from:<ul><li><code>default</code>. User is sent to a success page without
being logged in.</li><li><code>login</code>. User is sent to the login page to authenticate.</
li><li><code>autologin</code>. User is automatically logged in and sent to the appropriate page.</
li></ul>",
                "propertyOrder" : 161,
                "required" : true,
                "type" : "string",
                "exampleValue" : ""
            },
            "userRegistrationEmailVerificationEnabled" : {
                "title" : "Email Verification",
                "description" : "If enabled, users who self-register must perform email address
verification.",
                "propertyOrder" : 110,
                "required" : false,
                "type" : "boolean",
                "exampleValue" : ""
            },
            "userRegistrationValidUserAttributes" : {
                "title" : "Valid Creation Attributes",
                "description" : "Specifies a whitelist of user attributes that can be set during user
creation.",
                "propertyOrder" : 160,
                "required" : false,
                "items" : {
                    "type" : "string"
                },
                "type" : "array",
            }
        }
    }
}

```

```

        "exampleValue" : ""
    },
    "userRegistrationKbaEnabled" : {
        "title" : "Security Questions",
        "description" : "If enabled, users must set up their security questions during the self-
registration process.",
        "propertyOrder" : 120,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "userRegistrationEmailBody" : {
        "title" : "Outgoing Email Body",
        "description" : "Customize the User Self-Registration verification email body text.
Format is: <code>locale|body text</code>.",
        "propertyOrder" : 150,
        "required" : false,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "userRegistrationTokenTTL" : {
        "title" : "Token Lifetime (seconds)",
        "description" : "Maximum lifetime of the token allowing User Self-Registration, in
seconds.",
        "propertyOrder" : 130,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
    },
    "userRegistrationEnabled" : {
        "title" : "User Registration",
        "description" : "If enabled, new users can sign up for an account.",
        "propertyOrder" : 90,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "userRegistrationCaptchaEnabled" : {
        "title" : "Captcha",
        "description" : "If enabled, users must pass a Google reCAPTCHA challenge during user
self-registration to mitigate against software bots.",
        "propertyOrder" : 100,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"forgottenPassword" : {
    "type" : "object",
    "title" : "Forgotten Password",
    "propertyOrder" : 2,
    "properties" : {
        "forgottenPasswordKbaEnabled" : {
            "title" : "Security Questions",

```

```

        "description" : "If enabled, users must answer their security questions during the
forgotten password process.",
        "propertyOrder" : 200,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenPasswordEnabled" : {
        "title" : "Forgotten Password",
        "description" : "If enabled, users can reset their forgotten password.",
        "propertyOrder" : 170,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenPasswordEmailBody" : {
        "title" : "Outgoing Email Body",
        "description" : "Customize the forgotten password email body text. Format is
<code>locale|body text</code>.",
        "propertyOrder" : 230,
        "required" : false,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "forgottenPasswordTokenTTL" : {
        "title" : "Token Lifetime (seconds)",
        "description" : "Maximum lifetime for the token allowing forgotten password reset, in
seconds.<p><p>Specify a value from <code>0</code> to <code>2147483647</code>.",
        "propertyOrder" : 210,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
    },
    "forgottenPasswordEmailVerificationEnabled" : {
        "title" : "Email Verification",
        "description" : "If enabled, users who reset passwords must perform email address
verification.",
        "propertyOrder" : 190,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenPasswordEmailSubject" : {
        "title" : "Outgoing Email Subject",
        "description" : "Customize the forgotten password email subject text. Format is
<code>locale|subject text</code>.",
        "propertyOrder" : 220,
        "required" : false,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "forgottenPasswordCaptchaEnabled" : {
        "title" : "Captcha",

```

```

        "description" : "If enabled, users must pass a Google reCAPTCHA challenge during
password reset to mitigate against software bots.",
        "propertyOrder" : 180,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    }
},
},
"forgottenUsername" : {
    "type" : "object",
    "title" : "Forgotten Username",
    "propertyOrder" : 3,
    "properties" : {
        "forgottenUsernameEmailBody" : {
            "title" : "Outgoing Email Body",
            "description" : "Customizes the forgotten username email body text. Format is
<code>locale|body text</code>.",
            "propertyOrder" : 310,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
        "forgottenUsernameEmailSubject" : {
            "title" : "Outgoing Email Subject",
            "description" : "Customizes the forgotten username email subject text. Format is
<code>locale|subject text</code>.",
            "propertyOrder" : 300,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        },
    },
    "forgottenUsernameKbaEnabled" : {
        "title" : "Security Questions",
        "description" : "If enabled, users must answer their security questions during the
forgotten username process.",
        "propertyOrder" : 260,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenUsernameShowUsernameEnabled" : {
        "title" : "Show Username",
        "description" : "If enabled, users see their forgotten username on the browser page.",
        "propertyOrder" : 280,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenUsernameTokenTTL" : {
        "title" : "Token LifeTime (seconds)",
        "description" : "Maximum lifetime for the token allowing forgotten username, in
seconds.",

```

```

        "propertyOrder" : 290,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
    },
    "forgottenUsernameCaptchaEnabled" : {
        "title" : "Captcha",
        "description" : "If enabled, users must pass a Google reCAPTCHA challenge during the
forgotten username retrieval process to mitigate against software bots.",
        "propertyOrder" : 250,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenUsernameEnabled" : {
        "title" : "Forgotten Username",
        "description" : "If enabled, users can retrieve their forgotten username.",
        "propertyOrder" : 240,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "forgottenUsernameEmailUsernameEnabled" : {
        "title" : "Email Username",
        "description" : "If enabled, users receive their forgotten username by email.",
        "propertyOrder" : 270,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
    }
}
},
"profileManagement" : {
    "type" : "object",
    "title" : "Profile Management",
    "propertyOrder" : 4,
    "properties" : {
        "profileProtectedUserAttributes" : {
            "title" : "Protected Update Attributes",
            "description" : "Specifies a profile's protected user attributes, which causes re-
authentication when the user attempts to modify these attributes.",
            "propertyOrder" : 320,
            "required" : false,
            "items" : {
                "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
        }
    }
}
},
"advancedConfig" : {
    "type" : "object",
    "title" : "Advanced Configuration",
    "propertyOrder" : 5,
    "properties" : {
        "forgottenPasswordServiceConfigClass" : {
            "title" : "Forgotten Password Service Config Provider Class",
            "description" : "Specifies the provider class to configure any custom plugins.",

```



```

        "propertyOrder" : 360,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "forgottenUsernameServiceConfigClass" : {
        "title" : "Forgotten Username Service Config Provider Class",
        "description" : "Specifies the provider class to configure any custom plugins.",
        "propertyOrder" : 370,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "userRegistrationConfirmationUrl" : {
        "title" : "User Registration Confirmation Email URL",
        "description" : "Specifies the confirmation URL that the user receives during the self-
registration process. The <code>${realm}</code> string is replaced with the current realm.",
        "propertyOrder" : 330,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "userRegistrationServiceConfigClass" : {
        "title" : "User Registration Service Config Provider Class",
        "description" : "Specifies the provider class to configure any custom plugins.",
        "propertyOrder" : 350,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    },
    "forgottenPasswordConfirmationUrl" : {
        "title" : "Forgotten Password Confirmation Email URL",
        "description" : "Specifies the confirmation URL that the user receives after confirming
their identity during the forgotten password process. The <code>${realm}</code> string is replaced
with the current realm.",
        "propertyOrder" : 340,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
    }
    }
},
"type" : "object",
"title" : "Realm Defaults"
}
}
}

```

## 1.147. ValidationService

### 1.147.1. Realm Operations

Resource path: `/realm-config/services/validation`

Resource version: `1.0`

### 1.147.1.1. create

Usage:

```
am> create ValidationService --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "validGotoDestinations" : {
      "title" : "Valid goto URL Resources",
      "description" : "List of valid goto URL resources.<br><br>OpenAM's default behavior after login or logout is to redirect the user to the URL specified in the <code>goto</code> or <code>gotoOnFail</code> query string parameters supplied to the authentication interface during login or logout. <p><p>To enhance security, a list of valid URL resources can be specified here so OpenAM can validate the <code>goto</code> and <code>gotoOnFail</code> URL against them. <p><p>OpenAM will only redirect a user after login or logout if the URL matches any of the resources specified in this property. If the URL does not match, the user is redirected to either the user profile page or administration console after login, or the logged out page after logout. If this property is not set, it is assumed that all redirect URLs are valid.<p><p>The resources defined here can have the <code>*</code> wildcard defined, which matches all characters except <code>?</code>. Example values for this setting:<ul><li><code>http://app.example.com:80/*</code></li><li><code>http://app.example.com:80/*?*</code></li></ul>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

### 1.147.1.2. delete

Usage:

```
am> delete ValidationService --realm Realm
```

### 1.147.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ValidationService --realm Realm --actionName getAllTypes
```

#### 1.147.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ValidationService --realm Realm --actionName getCreatableTypes
```

#### 1.147.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ValidationService --realm Realm --actionName nextdescendents
```

#### 1.147.1.6. read

Usage:

```
am> read ValidationService --realm Realm
```

#### 1.147.1.7. update

Usage:

```
am> update ValidationService --realm Realm --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "validGotoDestinations" : {
      "title" : "Valid goto URL Resources",
      "description" : "List of valid goto URL resources.<br><br>OpenAM's default behavior after login or logout is to redirect the user to the URL specified in the <code>goto</code> or <code>gotoOnFail</code> query string parameters supplied to the authentication interface during login or logout. <p><p>To enhance security, a list of valid URL resources can be specified here so OpenAM can validate the <code>goto</code> and <code>gotoOnFail</code> URL against them. <p><p>OpenAM will only redirect a user after login or logout if the URL matches any of the resources specified in this property. If the URL does not match, the user is redirected to either the user profile page or administration console after login, or the logged out page after logout. If this property is not set, it is assumed that all redirect URLs are valid.<p><p>The resources defined here can have the <code>*</code> wildcard defined, which matches all characters except <code>?</code>. Example values for this setting:<ul><li><code>http://app.example.com:80/*</code></li><li><code>http://app.example.com:80/*?*</code></li></ul>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

## 1.147.2. Global Operations

Resource path: `/global-config/services/validation`

Resource version: `1.0`

### 1.147.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ValidationService --global --actionName getAllTypes
```

### 1.147.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ValidationService --global --actionName getCreatableTypes
```

### 1.147.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ValidationService --global --actionName nextdescendents
```

### 1.147.2.4. read

Usage:

```
am> read ValidationService --global
```

### 1.147.2.5. update

Usage:

```
am> update ValidationService --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "validGotoDestinations" : {
          "title" : "Valid goto URL Resources",
          "description" : "List of valid goto URL resources.<br><br>OpenAM's default behavior after login or logout is to redirect the user to the URL specified in the <code>goto</code> or <code>gotoOnFail</code> query string parameters supplied to the authentication interface during login or logout. <p><p>To enhance security, a list of valid URL resources can be specified here so OpenAM can validate the <code>goto</code> and <code>gotoOnFail</code> URL against them. <p><p>OpenAM will only redirect a user after login or logout if the URL matches any of the resources specified in this property. If the URL does not match, the user is redirected to either the user profile page or administration console after login, or the logged out page after logout. If this property is not set, it is assumed that all redirect URLs are valid.<p><p>The resources defined here can have the <code>*</code> wildcard defined, which matches all characters except <code>?</code>. Example values for this setting:<ul><li><code>http://app.example.com:80/*</code></li><li><code>http://app.example.com:80/*?*</code></li></ul>",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "type" : "object",
        "title" : "Realm Defaults"
      }
    }
  }
}
```

## 1.148. WebAgentGroups

### 1.148.1. Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/WebAgent`

Resource version: `1.0`

#### 1.148.1.1. create

Usage:

```
am> create WebAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cookieResetEnabled" : {
      "title" : "Cookie Reset",
      "description" : "Agent reset cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable) <br>Hot-swap: Yes",
      "propertyOrder" : 16500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "encodeSpecialCharsInCookies" : {
      "title" : "Encode special chars in Cookies",
      "description" : "Encode special chars in cookie by URL encoding. Useful when profile, session
and response attributes contain special chars and attributes fetch mode is set to HTTP_COOKIE.
(property name: com.sun.identity.agents.config.encode.cookie.special.chars.enable) <br>Hot-swap:
Yes",
      "propertyOrder" : 14000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "overrideProxyHostAndPort" : {
      "title" : "Override Proxy Server's Host and Port",
      "description" : "(property name: com.sun.identity.agents.config.proxy.override.host.port)
<br>Hot-swap: No",
      "propertyOrder" : 19400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "auditLogLocation" : {
      "title" : "Audit Log Location",
      "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition) <br>Hot-swap: Yes",
      "propertyOrder" : 21400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ignoreServerCheck" : {
      "title" : "Ignore Server Check",
      "description" : "Agent uses this value to check OpenAM is up before doing a 302 redirect.
(property name: com.sun.identity.agents.config.ignore.server.check) <br>Hot-swap: Yes",
      "propertyOrder" : 15500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "responseAttributeMap" : {
```

```

    "title" : "Response Attribute Map",
    "description" : "Maps the policy response attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.response.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field,
and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
    "propertyOrder" : 15300,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"primaryServerPollingPeriod" : {
    "title" : "Polling Period for Primary Server",
    "description" : "Interval in minutes, agent polls to check the primary server is up and running.
(property name: com.sun.identity.agents.config.poll.primary.server) <br>Hot-swap: No",
    "propertyOrder" : 19200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"useLtpaToken" : {
    "title" : "Use LTPA token",
    "description" : "Set to true if agent needs to use LTPA Token. (property name:
com.sun.identity.agents.config.domino.ltpa.enable)",
    "propertyOrder" : 20600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"cookieName" : {
    "title" : "Cookie Name",
    "description" : "Name of the SSO Token cookie used between the OpenAM server and the Agent.
(property name: com.sun.identity.agents.config.cookie.name)<br>Hot-swap: No",
    "propertyOrder" : 13700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"logoutResetCookies" : {
    "title" : "Logout Cookies List for Reset",
    "description" : "Any cookies to be reset upon logout in the same format as cookie reset list.
(property name: com.sun.identity.agents.config.logout.cookie.reset) <br>Hot-swap: Yes <br> Cookie1
<br> Cookie2=value;Domain=subdomain.domain.com",
    "propertyOrder" : 18100,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"changeProtocolToHttps" : {
    "title" : "Change URL Protocol to https",

```



```

        "description" : "If true, avoids IE6 security pop-ups. (property name:
com.sun.identity.agents.config.iis.owa.enable.change.protocol)",
        "propertyOrder" : 20300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "policyCachePollingInterval" : {
        "title" : "Policy Cache Polling Period",
        "description" : "Polling interval in minutes to refresh agent's policy cache. (property name:
com.sun.identity.agents.config.policy.cache.polling.interval) <br>Hot-swap: No",
        "propertyOrder" : 14400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "profileAttributesCookiePrefix" : {
        "title" : "Profile Attributes Cookie Prefix",
        "description" : "Sets cookie prefix in the attributes headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.prefix) <br>Hot-swap: Yes",
        "propertyOrder" : 17800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "authenticationType" : {
        "title" : "Authentication Type",
        "description" : "(property name: com.sun.identity.agents.config.iis.auth.type)",
        "propertyOrder" : 19900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "applicationLogoutUrls" : {
        "title" : "Logout URL List",
        "description" : "List of application logout URLs. User gets logged out from OpenAM session
when these urls accessed. (property name: com.sun.identity.agents.config.agent.logout.url). If this
property is used, user should specify a value for the below Logout Redirect URL property.<br>Hot-
swap: Yes <br> Example: <br> http://myagent.mydomain.com/logout.html",
        "propertyOrder" : 18000,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "fqdnDefault" : {
        "title" : "FQDN Default",
        "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default) <br>Hot-swap: Yes",
        "propertyOrder" : 16300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "cdssoUrls" : {
        "title" : "CDSSO Servlet URL",

```

```

    "description" : "List of URLs of the available CDSSO controllers that may be used by the Agent
for CDSSO processing. (property name: com.sun.identity.agents.config.cdsso.cdcervlet.url) <br>Hot-
swap: Yes <br> Example: <br> http://host:port/opensso/cdcervlet",
    "propertyOrder" : 17500,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"amLogoutUrl" : {
    "title" : "OpenAM Logout URL",
    "description" : "OpenAM logout page URL. (property name:
com.sun.identity.agents.config.logout.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Logout",
    "propertyOrder" : 12400,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"ltpaTokenConfigurationname" : {
    "title" : "LTPA Token Configuration Name",
    "description" : "The configuration name that the agent uses in order to employ the LTPA token
mechanism. (property name: com.sun.identity.agents.config.domino.ltpa.config.name)",
    "propertyOrder" : 20800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"goToParameterName" : {
    "title" : "Goto Parameter Name",
    "description" : "Property used only when CDSSO is enabled. Default value should
be changed only when the login URL has a landing page specified <br> Example :
com.sun.identity.agents.config.cdsso.cdcervlet.url = http://host:port/opensso/cdcervlet?
goto=http://agent:port/landing.jsp <br> The parameter is used by the Agent to append the original
request URL to this cdcservlet URL. This parameter is consumed by the landing page to redirect to
the original URL. (property name: com.sun.identity.agents.config.redirect.param) <br>Hot-swap: Yes
<br> Example: com.sun.identity.agents.config.redirect.param = goto2<br> The complete URL sent for
authentication will be <br> http://host:port/opensso/cdcervlet?goto=http://agent:port/landing.jsp?
goto2=http://agent.port/original.jsp",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"idleSessionTimeoutUrl" : {
    "title" : "Idle Session Timeout Page URL",
    "description" : "URL of the local idle session timeout page. (property name:
com.sun.identity.agents.config.iis.owa.enable.session.timeout.url)",
    "propertyOrder" : 20400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"showPasswordInHeader" : {

```

```

    "title" : "Show Password in HTTP Header",
    "description" : "Set to true if encrypted password should be set in HTTP header AUTH_PASSWORD.
(property name: com.sun.identity.agents.config.iis.password.header)",
    "propertyOrder" : 22800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "remoteLogFilename" : {
    "title" : "Remote Log Filename",
    "description" : "Name of file stored on OpenAM server that contains agent audit messages.
(property name: com.sun.identity.agents.config.remote.logfile) <br>Hot-swap: No",
    "propertyOrder" : 21500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoRedirectUri" : {
    "title" : "CDSSO Redirect URI",
    "description" : "An intermediate URI that is used by the Agent for processing CDSSO requests.
(property name: com.sun.identity.agents.config.cdsso.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 17550,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "agentConnectionTimeout" : {
    "title" : "Agent Connection Timeout",
    "description" : "Timeout period in seconds for an agent connection with OpenAM auth server.
(property name: com.sun.identity.agents.config.auth.connection.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 19100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notificationsEnabled" : {
    "title" : "Enable Notifications",
    "description" : "The notifications help in maintaining agent's sso, policy and configuration
caches. (property name: com.sun.identity.agents.config.notification.enable) <br>Hot-swap: No",
    "propertyOrder" : 14100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "replayPasswordKey" : {
    "title" : "Replay Password Key",
    "description" : "DES key for decrypting the basic authentication password in the session.
(property name: com.sun.identity.agents.config.replaypasswd.key)",
    "propertyOrder" : 20000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sessionAttributeFetchMode" : {
    "title" : "Session Attribute Fetch Mode",
    "description" : "(property name: com.sun.identity.agents.config.session.attribute.fetch.mode)
<br>Hot-swap: Yes",
    "propertyOrder" : 15000,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "userIdParameterType" : {
    "title" : "User ID Parameter Type",
    "description" : "User ID can be fetched from either SESSION and LDAP attributes. (property name: com.sun.identity.agents.config.userid.param.type) <br>Hot-swap: Yes",
    "propertyOrder" : 14700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "agentDebugLevel" : {
    "title" : "Agent Debug Level",
    "description" : "Agent debug level. (property name: com.sun.identity.agents.config.debug.level) <br>Hot-swap: Yes",
    "propertyOrder" : 21900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "secureCookies" : {
    "title" : "Cookie Security",
    "description" : "Agent sends secure cookies if communication is secure. (property name: com.sun.identity.agents.config.cookie.secure) <br>Hot-swap: No",
    "propertyOrder" : 13800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "filterConfiguredWithOwa" : {
    "title" : "Filter configured with OWA",
    "description" : "Set to true if the IIS agent filter is configured for OWA. (property name: com.sun.identity.agents.config.iis.owa.enable)",
    "propertyOrder" : 20200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ssoOnlyMode" : {
    "title" : "SSO Only Mode",
    "description" : "Agent will just enforce authentication (SSO), but no authorization for policies. (property name: com.sun.identity.agents.config.sso.only) <br>Hot-swap: Yes",
    "propertyOrder" : 16000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "overrideNotificationUrl" : {
    "title" : "Override Notification URL",
    "description" : "Set to true if the agent is sitting behind a ssl/tls off-loader, load balancer, or proxy to override the URL with the value from the property com.sun.identity.agents.config.agenturi.prefix. (property name: com.sun.identity.agents.config.override.notification.url) <br>Hot-swap: Yes",
    "propertyOrder" : 19000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
},

```

```

"status" : {
  "title" : "Status",
  "description" : "Status of the agent configuration.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"accessDeniedUrl" : {
  "title" : "Resources Access Denied URL",
  "description" : "The URL of the customized access denied page. (property name:
com.sun.identity.agents.config.access.denied.url) <br>Hot-swap: Yes",
  "propertyOrder" : 16100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"filterPriority" : {
  "title" : "Filter Priority",
  "description" : "The loading priority of filter. (property name:
com.sun.identity.agents.config.iis.filter.priority)",
  "propertyOrder" : 20100,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"profileAttributeMap" : {
  "title" : "Profile Attribute Map",
  "description" : "Maps the profile attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.profile.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field,
and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate the value of profile
attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in
Corresponding Map Value field.",
  "propertyOrder" : 14900,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"ltpaTokenCookieName" : {
  "title" : "LTPA Token Cookie Name",
  "description" : "The name of the cookie that contains the LTPA token. (property name:
com.sun.identity.agents.config.domino.ltpa.cookie.name)",
  "propertyOrder" : 20700,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"agentUriPrefix" : {
  "title" : "Agent Deployment URI Prefix",
  "description" : "(property name: com.sun.identity.agents.config.agenturi.prefix)<br>Hot-swap:
Yes",
  "propertyOrder" : 15800,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "fqdnMapping" : {
    "title" : "FQDN Virtual Host Map",
    "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN to
access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>Hot-
swap: Yes <br> Examples: <br> To map the partial hostname myserver to myserver.mydomain.com: enter
myserver in the Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map
a virtual server rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in
the Map Key field and rst.hostname.com in the Corresponding Map Value field.",
    "propertyOrder" : 16400,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    }
  },
  "type" : "object",
  "exampleValue" : ""
},
"overrideRequestProtocol" : {
  "title" : "Override Request URL Protocol",
  "description" : "Set to true if the agent is sitting behind a ssl/tls off-
loader, load balancer, or proxy to override the protocol with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.protocol) <br>Hot-swap: Yes",
  "propertyOrder" : 18700,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"notEnforcedIps" : {
  "title" : "Not Enforced Client IP List",
  "description" : "No authentication and authorization are required for the requests coming from
these client IP addresses. (property name: com.sun.identity.agents.config.notenforced.ip) <br>Hot-
swap: Yes <br> Examples: <br> 192.18.145.* <br> 192.18.146.123",
  "propertyOrder" : 17200,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"cdssoRootUrl" : {
  "title" : "Agent Root URL for CDSSO",
  "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
  "propertyOrder" : 22700,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
}

```

```

    },
    "encodeUrlSpecialCharacters" : {
      "title" : "Encode URL's Special Characters",
      "description" : "Encodes the url which has special characters before doing policy evaluation.
(property name: com.sun.identity.agents.config.encode.url.special.chars.enable) <br>Hot-swap: Yes",
      "propertyOrder" : 18500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "notEnforcedUrls" : {
      "title" : "Not Enforced URLs",
      "description" : "List of urls for which no authentication required. (property name:
com.sun.identity.agents.config.notenforced.url) <br>Hot-swap: Yes <br> Example: <br> http://
myagent.mydomain.com/*.gif",
      "propertyOrder" : 17000,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "clientHostnameHeader" : {
      "title" : "Client Hostname Header",
      "description" : "HTTP header name that holds the Hostname of the client. (property name:
com.sun.identity.agents.config.client.hostname.header) <br>Hot-swap: Yes",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "repositoryLocation" : {
      "title" : "Location of Agent Configuration Repository",
      "description" : "Indicates agent's configuration located either on agent's host or centrally on
OpenAM server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "overrideRequestPort" : {
      "title" : "Override Request URL Port",
      "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the port with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.port) <br>Hot-swap: Yes",
      "propertyOrder" : 18900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "customProperties" : {
      "title" : "Custom Properties",
      "description" : "Additional properties that allow users to augment the set of properties
supported by agent. (property name: com.sun.identity.agents.config.freeformproperties) <br>Hot-
swap: Yes <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-
value-0 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",

```

```

    "propertyOrder" : 19700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "ignorePathInfoForNotEnforcedUrls" : {
    "title" : "Ignore Path Info for Not Enforced URLs",
    "description" : "Indicate whether the path info and query should be stripped from the request
URL before being compared with the URLs of the not enforced list when those URLs have a wildcard '*'
character. (property name: com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list)
<br>Hot-swap: Yes",
    "propertyOrder" : 13900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "amLoginUrl" : {
    "title" : "OpenAM Login URL",
    "description" : "OpenAM login page URL. (property name:
com.sun.identity.agents.config.login.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Login",
    "propertyOrder" : 15700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "agentLocale" : {
    "title" : "Agent Locale",
    "description" : "The default locale for the product. (property name:
com.sun.identity.agents.config.locale) <br>Hot-swap: No",
    "propertyOrder" : 19300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "attributeMultiValueSeparator" : {
    "title" : "Attribute Multi Value Separator",
    "description" : "Specifies separator for multiple values. Applies to all
types of attributes i.e. profile, session and response attributes. (property name:
com.sun.identity.agents.config.attribute.multi.value.separator) <br>Hot-swap: Yes",
    "propertyOrder" : 22200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "encodeProfileAttributes" : {
    "title" : "Native Encoding of Profile Attributes",
    "description" : "Agent encodes the ldap header values in the default encoding of OS locale. If
false, UTF-8 gets used. (property name: com.sun.identity.agents.config.convert.mbyte.enable) <br>Hot-
swap: Yes",
    "propertyOrder" : 18400,
    "required" : true,
    "type" : "boolean",

```



```

    "exampleValue" : ""
  },
  "fqdnCheck" : {
    "title" : "FQDN Check",
    "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 16200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdsso" : {
    "title" : "Cross Domain SSO",
    "description" : "Enables Cross-Domain Single Sign On. (property name:
com.sun.identity.agents.config.cdsso.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 16700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "debugLogRotation" : {
    "title" : "Agent Debug File Rotation",
    "description" : "Debug file gets rotated based on the size specified. (property name:
com.sun.identity.agents.config.debug.file.rotate) <br>Hot-swap: Yes",
    "propertyOrder" : 22000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "localAuditLogRotation" : {
    "title" : "Rotate Local Audit Log",
    "description" : "Flag to indicate that audit log files should be rotated when reaching a certain
size. (property name: com.sun.identity.agents.config.local.log.rotate) <br>Hot-swap: Yes",
    "propertyOrder" : 21700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "anonymousUserId" : {
    "title" : "Anonymous User Default Value",
    "description" : "User id of unauthenticated users. (property name:
com.sun.identity.agents.config.anonymous.user.id) <br>Hot-swap: Yes",
    "propertyOrder" : 16800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "invertNotEnforcedUrls" : {
    "title" : "Invert Not Enforced URLs",
    "description" : "Only not enforced list of urls will be enforced. (property name:
com.sun.identity.agents.config.notenforced.url.invert) <br>Hot-swap: Yes",
    "propertyOrder" : 17100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ignorePathInfo" : {
    "title" : "Ignore Path Info in Request URL",

```

```

    "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info) <br>Hot-swap: Yes",
    "propertyOrder" : 18600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "anonymousUserEnabled" : {
    "title" : "Anonymous User",
    "description" : "Enable/Disable REMOTE_USER processing for anonymous users. (property name:
com.sun.identity.agents.config.anonymous.user.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 16900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "debugRotationSize" : {
    "title" : "Agent Debug File Size",
    "description" : "Agent debug file size in bytes. (property name:
com.sun.identity.agents.config.debug.file.size) <br>Hot-swap: Yes",
    "propertyOrder" : 22100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "ssoCachePollingInterval" : {
    "title" : "SSO Cache Polling Period",
    "description" : "Polling interval in minutes to refresh agent's sso cache. (property name:
com.sun.identity.agents.config.sso.cache.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 14500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "overrideRequestHost" : {
    "title" : "Override Request URL Host",
    "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the host with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.host) <br>Hot-swap: Yes",
    "propertyOrder" : 18800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logonAndImpersonation" : {
    "title" : "Logon and Impersonation",
    "description" : "Set to true if agent should do Windows Logon and User Impersonation. (property
name: com.sun.identity.agents.config.iis.logonuser)",
    "propertyOrder" : 22900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "agentNotificationUrl" : {
    "title" : "Agent Notification URL",
    "description" : "URL used by agent to register notification listeners. (property name:
com.sun.identity.client.notification.url) <br>Hot-swap: No",

```

```

    "propertyOrder" : 14200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "fetchAttributesForNotEnforcedUrls" : {
    "title" : "Fetch Attributes for Not Enforced URLs",
    "description" : "Agent fetches profile attributes for not enforced urls by doing policy
evaluation. (property name: com.sun.identity.agents.config.notenforced.url.attributes.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 19800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "checkUserInDomino" : {
    "title" : "Check User in Domino Database",
    "description" : "If true, agent checks user existence in Domino name database. (property name:
com.sun.identity.agents.config.domino.check.name.database)",
    "propertyOrder" : 20500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "postDataPreservation" : {
    "title" : "POST Data Preservation",
    "description" : "Enables POST data preservation. (property name:
com.sun.identity.agents.config.postdata.preserve.enable) <br> Note that this feature is not supported
in all the web agents. Please refer individual agents documentation for more details. <br>Hot-swap:
Yes",
    "propertyOrder" : 17300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "loadBalanced" : {
    "title" : "Load Balancer Setup",
    "description" : "Set to true if a load balancer is used for OpenAM services. (property name:
com.sun.identity.agents.config.load.balancer.enable) <br>Hot-swap: No",
    "propertyOrder" : 15400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "profileAttributeFetchMode" : {
    "title" : "Profile Attribute Fetch Mode",
    "description" : "(property name: com.sun.identity.agents.config.profile.attribute.fetch.mode)
<br>Hot-swap: Yes",
    "propertyOrder" : 14800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "remoteLogSendInterval" : {
    "title" : "Remote Audit Log Interval",
    "description" : "Periodic interval in minutes in which audit log messages are sent to remote log
file. (property name: com.sun.identity.agents.config.remote.log.interval) <br>Hot-swap: No",
    "propertyOrder" : 21600,
    "required" : true,

```

```

    "type" : "integer",
    "exampleValue" : ""
  },
  "logoutRedirectUrl" : {
    "title" : "Logout Redirect URL",
    "description" : "User gets redirected to this url after logout. (property name:
com.sun.identity.agents.config.logout.redirect.url). This property should be specified along with the
above Logout URL List.<br>Hot-swap: Yes",
    "propertyOrder" : 22300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userIdParameter" : {
    "title" : "User ID Parameter",
    "description" : "Agent sets value of User Id to REMOTE_USER server variable. (property name:
com.sun.identity.agents.config.userid.param) <br>Hot-swap: Yes",
    "propertyOrder" : 14600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "postDataCachePeriod" : {
    "title" : "POST Data Entries Cache Period",
    "description" : "POST cache entry lifetime in minutes. (property name:
com.sun.identity.agents.config.postcache.entry.lifetime) <br>Hot-swap: Yes",
    "propertyOrder" : 17400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "ignorePreferredNamingUrl" : {
    "title" : "Ignore Preferred Naming URL in Naming Request",
    "description" : "Agent uses this value to send preferred naming url in the naming request.
(property name: com.sun.identity.agents.config.ignore.preferred.naming.url) <br>Hot-swap: Yes",
    "propertyOrder" : 15600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyEvaluationApplication" : {
    "title" : "Application",
    "description" : "Which application contains the policies to evaluate with (property name:
org.forgerock.openam.agents.config.policy.evaluation.application) <br>Hot-swap: Yes",
    "propertyOrder" : 21200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "policyEvaluationRealm" : {
    "title" : "Realm",
    "description" : "Which realm to start evaluating from (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm) <br>Hot-swap: Yes",
    "propertyOrder" : 21100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "fetchPoliciesFromRootResource" : {

```

```

    "title" : "Fetch Policies from Root Resource",
    "description" : "Agent caches policy decision of the resource and all resources from the root of
the resource down. (property name: com.sun.identity.agents.config.fetch.from.root.resource) <br>Hot-
swap: No",
    "propertyOrder" : 18200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "retrieveClientHostname" : {
    "title" : "Retrieve Client Hostname",
    "description" : "Gets the client's hostname through DNS reverse lookup for use in policy
evaluation. (property name: com.sun.identity.agents.config.get.client.host.name) <br>Hot-swap: Yes",
    "propertyOrder" : 18300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "configurationCleanupInterval" : {
    "title" : "Configuration Cleanup Interval",
    "description" : "Interval in minutes to cleanup old agent configuration entries. (property name:
com.sun.identity.agents.config.cleanup.interval) <br>Hot-swap: No",
    "propertyOrder" : 19600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "clientIpHeader" : {
    "title" : "Client IP Address Header",
    "description" : "HTTP header name that holds the IP address of the client. (property name:
com.sun.identity.agents.config.client.ip.header) <br>Hot-swap: Yes",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributesCookieMaxAge" : {
    "title" : "Profile Attributes Cookie Maxage",
    "description" : "Maxage of attributes cookie headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.maxage) <br>Hot-swap: Yes",
    "propertyOrder" : 17900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "agentConfigChangeNotificationsEnabled" : {
    "title" : "Agent Configuration Change Notification",
    "description" : "Enable agent to receive notification messages from OpenAM server for
configuration changes. (property name: com.sun.identity.agents.config.change.notification.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 12100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdssoCookieDomain" : {
    "title" : "Cookies Domain List",
    "description" : "List of domains in which cookies have to be set in CDSSO. (property name:
com.sun.identity.agents.config.cdsso.cookie.domain) <br>Hot-swap: Yes <br> Example: <br> .sun.com",

```

```

    "propertyOrder" : 17600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "auditAccessType" : {
    "title" : "Audit Access Types",
    "description" : "Types of messages to log based on user URL access attempts. (property name: com.sun.identity.agents.config.audit.accesstype) <br>Hot-swap: Yes",
    "propertyOrder" : 21300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "caseInsensitiveUrlComparison" : {
    "title" : "URL Comparison Case Sensitivity Check",
    "description" : "Enforces case insensitivity in both policy and not enforced url evaluation. (property name: com.sun.identity.agents.config.url.comparison.case.ignore) <br>Hot-swap: Yes",
    "propertyOrder" : 14300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cookieResetList" : {
    "title" : "Cookies Reset Name List",
    "description" : "List of cookies in the format: name[=value] [];Domain=value]. (property name: com.sun.identity.agents.config.cookie.reset) <br>Hot-swap: Yes <br> Examples: <br> Cookie1 <br> Cookie2=value;Domain=subdomain.domain.com",
    "propertyOrder" : 16600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sessionAttributeMap" : {
    "title" : "Session Attribute Map",
    "description" : "Maps the session attributes to be populated under specific names for the currently authenticated user. (property name: com.sun.identity.agents.config.session.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To populate the value of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
    "propertyOrder" : 15100,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "responseAttributeFetchMode" : {
    "title" : "Response Attribute Fetch Mode",

```

```

    "description" : "(property name: com.sun.identity.agents.config.response.attribute.fetch.mode)
<br>Hot-swap: Yes",
    "propertyOrder" : 15200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientIpValidation" : {
    "title" : "Client IP Validation",
    "description" : "This validates if the subsequent browser requests come from
the same ip address that the SSO token is initially issued against. (property name:
com.sun.identity.agents.config.client.ip.validation.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 17700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Password",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "policyClockSkew" : {
    "title" : "Policy Clock Skew",
    "description" : "Time in seconds used adjust time difference between Agent machine
and OpenAM. Clock skew in seconds = AgentTime - OpenAMServerTime. (property name:
com.sun.identity.agents.config.policy.clock.skew) <br>Hot-swap: No",
    "propertyOrder" : 21000,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "configurationPollingInterval" : {
    "title" : "Configuration Reload Interval",
    "description" : "Interval in minutes to fetch agent configuration from OpenAM. (property name:
com.sun.identity.agents.config.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 19500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "ltpaTokenOrganizationName" : {
    "title" : "LTPA Token Organization Name",
    "description" : "The organization name to which the LTPA token belongs. (property name:
com.sun.identity.agents.config.domino.ltpa.org.name)",
    "propertyOrder" : 20900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "localAuditRotationSize" : {
    "title" : "Local Audit Log Rotation Size",
    "description" : "Size limit in bytes when a local audit log file is rotated to a new file.
(property name: com.sun.identity.agents.config.local.log.size) <br>Hot-swap: Yes",
    "propertyOrder" : 21800,

```

```
    "required" : true,  
    "type" : "integer",  
    "exampleValue" : ""  
  }  
}  
}
```

### 1.148.1.2. delete

Usage:

```
am> delete WebAgentGroups --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.148.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebAgentGroups --realm Realm --actionName getAllTypes
```

### 1.148.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebAgentGroups --realm Realm --actionName getCreatableTypes
```

### 1.148.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebAgentGroups --realm Realm --actionName nextdescendents
```

### 1.148.1.6. query

Querying the agent groups of a specific type

Usage:

```
am> query WebAgentGroups --realm Realm --filter filter
```



Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

## 1.148.1.7. read

Usage:

```
am> read WebAgentGroups --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

## 1.148.1.8. update

Usage:

```
am> update WebAgentGroups --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cookieResetEnabled" : {
      "title" : "Cookie Reset",
      "description" : "Agent reset cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable) <br>Hot-swap: Yes",
      "propertyOrder" : 16500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "encodeSpecialCharsInCookies" : {
      "title" : "Encode special chars in Cookies",
      "description" : "Encode special chars in cookie by URL encoding. Useful when profile, session
and response attributes contain special chars and attributes fetch mode is set to HTTP_COOKIE.
(property name: com.sun.identity.agents.config.encode.cookie.special.chars.enable) <br>Hot-swap:
Yes",
      "propertyOrder" : 14000,
      "required" : true,
      "type" : "boolean",
```

```

    "exampleValue" : ""
  },
  "overrideProxyHostAndPort" : {
    "title" : "Override Proxy Server's Host and Port",
    "description" : "(property name: com.sun.identity.agents.config.proxy.override.host.port)
<br>Hot-swap: No",
    "propertyOrder" : 19400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "auditLogLocation" : {
    "title" : "Audit Log Location",
    "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition) <br>Hot-swap: Yes",
    "propertyOrder" : 21400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ignoreServerCheck" : {
    "title" : "Ignore Server Check",
    "description" : "Agent uses this value to check OpenAM is up before doing a 302 redirect.
(property name: com.sun.identity.agents.config.ignore.server.check) <br>Hot-swap: Yes",
    "propertyOrder" : 15500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "responseAttributeMap" : {
    "title" : "Response Attribute Map",
    "description" : "Maps the policy response attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.response.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field,
and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
    "propertyOrder" : 15300,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "primaryServerPollingPeriod" : {
    "title" : "Polling Period for Primary Server",
    "description" : "Interval in minutes, agent polls to check the primary server is up and running.
(property name: com.sun.identity.agents.config.poll.primary.server) <br>Hot-swap: No",
    "propertyOrder" : 19200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "useLtpaToken" : {
    "title" : "Use LTPA token",
    "description" : "Set to true if agent needs to use LTPA Token. (property name:
com.sun.identity.agents.config.domino.ltpa.enable)",

```

```

    "propertyOrder" : 20600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cookieName" : {
    "title" : "Cookie Name",
    "description" : "Name of the SSO Token cookie used between the OpenAM server and the Agent.
(property name: com.sun.identity.agents.config.cookie.name)<br>Hot-swap: No",
    "propertyOrder" : 13700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "logoutResetCookies" : {
    "title" : "Logout Cookies List for Reset",
    "description" : "Any cookies to be reset upon logout in the same format as cookie reset list.
(property name: com.sun.identity.agents.config.logout.cookie.reset) <br>Hot-swap: Yes <br> Cookie1
<br> Cookie2=value;Domain=subdomain.domain.com",
    "propertyOrder" : 18100,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "changeProtocolToHttps" : {
    "title" : "Change URL Protocol to https",
    "description" : "If true, avoids IE6 security pop-ups. (property name:
com.sun.identity.agents.config.iis.owa.enable.change.protocol)",
    "propertyOrder" : 20300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyCachePollingInterval" : {
    "title" : "Policy Cache Polling Period",
    "description" : "Polling interval in minutes to refresh agent's policy cache. (property name:
com.sun.identity.agents.config.policy.cache.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 14400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "profileAttributesCookiePrefix" : {
    "title" : "Profile Attributes Cookie Prefix",
    "description" : "Sets cookie prefix in the attributes headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.prefix) <br>Hot-swap: Yes",
    "propertyOrder" : 17800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationType" : {
    "title" : "Authentication Type",
    "description" : "(property name: com.sun.identity.agents.config.iis.auth.type)",
    "propertyOrder" : 19900,
    "required" : true,

```

```

    "type" : "string",
    "exampleValue" : ""
  },
  "applicationLogoutUrls" : {
    "title" : "Logout URL List",
    "description" : "List of application logout URLs. User gets logged out from OpenAM session
when these urls accessed. (property name: com.sun.identity.agents.config.agent.logout.url). If this
property is used, user should specify a value for the below Logout Redirect URL property.<br>Hot-
swap: Yes <br> Example: <br> http://myagent.mydomain.com/logout.html",
    "propertyOrder" : 18000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "fqdnDefault" : {
    "title" : "FQDN Default",
    "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default) <br>Hot-swap: Yes",
    "propertyOrder" : 16300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoUrls" : {
    "title" : "CDSSO Servlet URL",
    "description" : "List of URLs of the available CDSSO controllers that may be used by the Agent
for CDSSO processing. (property name: com.sun.identity.agents.config.cdsso.cdcservlet.url) <br>Hot-
swap: Yes <br> Example: <br> http://host:port/opensso/cdcservlet",
    "propertyOrder" : 17500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "amLogoutUrl" : {
    "title" : "OpenAM Logout URL",
    "description" : "OpenAM logout page URL. (property name:
com.sun.identity.agents.config.logout.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Logout",
    "propertyOrder" : 12400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "ltpaTokenConfigurationname" : {
    "title" : "LTPA Token Configuration Name",
    "description" : "The configuration name that the agent uses in order to employ the LTPA token
mechanism. (property name: com.sun.identity.agents.config.domino.ltpa.config.name)",
    "propertyOrder" : 20800,
    "required" : true,
    "type" : "string",

```

```

    "exampleValue" : ""
  },
  "gotoParameterName" : {
    "title" : "Goto Parameter Name",
    "description" : "Property used only when CDSSO is enabled. Default value should
be changed only when the login URL has a landing page specified <br> Example :
com.sun.identity.agents.config.cdsso.cdcservlet.url = http://host:port/opensso/cdcservlet?
goto=http://agent:port/landing.jsp <br> The parameter is used by the Agent to append the original
request URL to this cdcservlet URL. This parameter is consumed by the landing page to redirect to
the original URL. (property name: com.sun.identity.agents.config.redirect.param) <br>Hot-swap: Yes
<br> Example: com.sun.identity.agents.config.redirect.param = goto2<br> The complete URL sent for
authentication will be <br> http://host:port/opensso/cdcservlet?goto=http://agent:port/landing.jsp?
goto2=http://agent.port/original.jsp",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "idleSessionTimeoutUrl" : {
    "title" : "Idle Session Timeout Page URL",
    "description" : "URL of the local idle session timeout page. (property name:
com.sun.identity.agents.config.iis.owa.enable.session.timeout.url)",
    "propertyOrder" : 20400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "showPasswordInHeader" : {
    "title" : "Show Password in HTTP Header",
    "description" : "Set to true if encrypted password should be set in HTTP header AUTH_PASSWORD.
(property name: com.sun.identity.agents.config.iis.password.header)",
    "propertyOrder" : 22800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "remoteLogFilename" : {
    "title" : "Remote Log Filename",
    "description" : "Name of file stored on OpenAM server that contains agent audit messages.
(property name: com.sun.identity.agents.config.remote.logfile) <br>Hot-swap: No",
    "propertyOrder" : 21500,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoRedirectUri" : {
    "title" : "CDSSO Redirect URI",
    "description" : "An intermediate URI that is used by the Agent for processing CDSSO requests.
(property name: com.sun.identity.agents.config.cdsso.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 17550,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "agentConnectionTimeout" : {
    "title" : "Agent Connection Timeout",
    "description" : "Timeout period in seconds for an agent connection with OpenAM auth server.
(property name: com.sun.identity.agents.config.auth.connection.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 19100,

```

```

    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notificationsEnabled" : {
    "title" : "Enable Notifications",
    "description" : "The notifications help in maintaining agent's sso, policy and configuration
caches. (property name: com.sun.identity.agents.config.notification.enable) <br>Hot-swap: No",
    "propertyOrder" : 14100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "replayPasswordKey" : {
    "title" : "Replay Password Key",
    "description" : "DES key for decrypting the basic authentication password in the session.
(property name: com.sun.identity.agents.config.replaypasswd.key)",
    "propertyOrder" : 20000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sessionAttributeFetchMode" : {
    "title" : "Session Attribute Fetch Mode",
    "description" : "(property name: com.sun.identity.agents.config.session.attribute.fetch.mode)
<br>Hot-swap: Yes",
    "propertyOrder" : 15000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "userIdParameterType" : {
    "title" : "User ID Parameter Type",
    "description" : "User ID can be fetched from either SESSION and LDAP attributes. (property name:
com.sun.identity.agents.config.userid.param.type) <br>Hot-swap: Yes",
    "propertyOrder" : 14700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "agentDebugLevel" : {
    "title" : "Agent Debug Level",
    "description" : "Agent debug level. (property name: com.sun.identity.agents.config.debug.level)
<br>Hot-swap: Yes",
    "propertyOrder" : 21900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "secureCookies" : {
    "title" : "Cookie Security",
    "description" : "Agent sends secure cookies if communication is secure. (property name:
com.sun.identity.agents.config.cookie.secure) <br>Hot-swap: No",
    "propertyOrder" : 13800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "filterConfiguredWithOwa" : {

```

```

    "title" : "Filter configured with OWA",
    "description" : "Set to true if the IIS agent filter is configured for OWA. (property name:
com.sun.identity.agents.config.iis.owa.enable)",
    "propertyOrder" : 20200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ssoOnlyMode" : {
    "title" : "SSO Only Mode",
    "description" : "Agent will just enforce authentication (SSO), but no authorization for
policies. (property name: com.sun.identity.agents.config.sso.only) <br>Hot-swap: Yes",
    "propertyOrder" : 16000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "overrideNotificationUrl" : {
    "title" : "Override Notification URL",
    "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the URL with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.notification.url) <br>Hot-swap: Yes",
    "propertyOrder" : 19000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "status" : {
    "title" : "Status",
    "description" : "Status of the agent configuration.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "accessDeniedUrl" : {
    "title" : "Resources Access Denied URL",
    "description" : "The URL of the customized access denied page. (property name:
com.sun.identity.agents.config.access.denied.url) <br>Hot-swap: Yes",
    "propertyOrder" : 16100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "filterPriority" : {
    "title" : "Filter Priority",
    "description" : "The loading priority of filter. (property name:
com.sun.identity.agents.config.iis.filter.priority)",
    "propertyOrder" : 20100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributeMap" : {
    "title" : "Profile Attribute Map",
    "description" : "Maps the profile attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.profile.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To

```

populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field, and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate the value of profile attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in Corresponding Map Value field.",

```

    "propertyOrder" : 14900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "ltpaTokenCookieName" : {
    "title" : "LTPA Token Cookie Name",
    "description" : "The name of the cookie that contains the LTPA token. (property name: com.sun.identity.agents.config.domino.ltpa.cookie.name)",
    "propertyOrder" : 20700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "agentUriPrefix" : {
    "title" : "Agent Deployment URI Prefix",
    "description" : "(property name: com.sun.identity.agents.config.agenturi.prefix)<br>Hot-swap: Yes",
    "propertyOrder" : 15800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "fqdnMapping" : {
    "title" : "FQDN Virtual Host Map",
    "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN to access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>Hot-swap: Yes <br> Examples: <br> To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field and rst.hostname.com in the Corresponding Map Value field.",
    "propertyOrder" : 16400,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "overrideRequestProtocol" : {
    "title" : "Override Request URL Protocol",
    "description" : "Set to true if the agent is sitting behind a ssl/tls off-loader, load balancer, or proxy to override the protocol with the value from the property com.sun.identity.agents.config.agenturi.prefix. (property name: com.sun.identity.agents.config.override.protocol) <br>Hot-swap: Yes",
    "propertyOrder" : 18700,
    "required" : true,
    "type" : "boolean",

```



```

    "exampleValue" : ""
  },
  "notEnforcedIps" : {
    "title" : "Not Enforced Client IP List",
    "description" : "No authentication and authorization are required for the requests coming from
these client IP addresses. (property name: com.sun.identity.agents.config.notenforced.ip) <br>Hot-
swap: Yes <br> Examples: <br> 192.18.145.* <br> 192.18.146.123",
    "propertyOrder" : 17200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "cdssoRootUrl" : {
    "title" : "Agent Root URL for CDSSO",
    "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
    "propertyOrder" : 22700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "encodeUrlSpecialCharacters" : {
    "title" : "Encode URL's Special Characters",
    "description" : "Encodes the url which has special characters before doing policy evaluation.
(property name: com.sun.identity.agents.config.encode.url.special.chars.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 18500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "notEnforcedUrls" : {
    "title" : "Not Enforced URLs",
    "description" : "List of urls for which no authentication required. (property name:
com.sun.identity.agents.config.notenforced.url) <br>Hot-swap: Yes <br> Example: <br> http://
myagent.mydomain.com/*.gif",
    "propertyOrder" : 17000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "clientHostnameHeader" : {
    "title" : "Client Hostname Header",
    "description" : "HTTP header name that holds the Hostname of the client. (property name:
com.sun.identity.agents.config.client.hostname.header) <br>Hot-swap: Yes",
    "propertyOrder" : 1100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }

```

```

    },
    "repositoryLocation" : {
      "title" : "Location of Agent Configuration Repository",
      "description" : "Indicates agent's configuration located either on agent's host or centrally on
OpenAM server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    },
    "overrideRequestPort" : {
      "title" : "Override Request URL Port",
      "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the port with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.port) <br>Hot-swap: Yes",
      "propertyOrder" : 18900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "customProperties" : {
      "title" : "Custom Properties",
      "description" : "Additional properties that allow users to augment the set of properties
supported by agent. (property name: com.sun.identity.agents.config.freeformproperties) <br>Hot-
swap: Yes <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-
value-0 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
      "propertyOrder" : 19700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    },
    "ignorePathInfoForNotEnforcedUrls" : {
      "title" : "Ignore Path Info for Not Enforced URLs",
      "description" : "Indicate whether the path info and query should be stripped from the request
URL before being compared with the URLs of the not enforced list when those URLs have a wildcard '*'
character. (property name: com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list)
<br>Hot-swap: Yes",
      "propertyOrder" : 13900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    },
    "amLoginUrl" : {
      "title" : "OpenAM Login URL",
      "description" : "OpenAM login page URL. (property name:
com.sun.identity.agents.config.login.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opnsso/UI/Login",
      "propertyOrder" : 15700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }

```

```

    },
    "agentLocale" : {
        "title" : "Agent Locale",
        "description" : "The default locale for the product. (property name:
com.sun.identity.agents.config.locale) <br>Hot-swap: No",
        "propertyOrder" : 19300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "attributeMultiValueSeparator" : {
        "title" : "Attribute Multi Value Separator",
        "description" : "Specifies separator for multiple values. Applies to all
types of attributes i.e. profile, session and response attributes. (property name:
com.sun.identity.agents.config.attribute.multi.value.separator) <br>Hot-swap: Yes",
        "propertyOrder" : 22200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "encodeProfileAttributes" : {
        "title" : "Native Encoding of Profile Attributes",
        "description" : "Agent encodes the ldap header values in the default encoding of OS locale. If
false, UTF-8 gets used. (property name: com.sun.identity.agents.config.convert.mbyte.enable) <br>Hot-
swap: Yes",
        "propertyOrder" : 18400,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "fqdnCheck" : {
        "title" : "FQDN Check",
        "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable) <br>Hot-swap: Yes",
        "propertyOrder" : 16200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "cdsso" : {
        "title" : "Cross Domain SSO",
        "description" : "Enables Cross-Domain Single Sign On. (property name:
com.sun.identity.agents.config.cdsso.enable) <br>Hot-swap: Yes",
        "propertyOrder" : 16700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "debugLogRotation" : {
        "title" : "Agent Debug File Rotation",
        "description" : "Debug file gets rotated based on the size specified. (property name:
com.sun.identity.agents.config.debug.file.rotate) <br>Hot-swap: Yes",
        "propertyOrder" : 22000,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "localAuditLogRotation" : {
        "title" : "Rotate Local Audit Log",

```

```

    "description" : "Flag to indicate that audit log files should be rotated when reaching a certain
size. (property name: com.sun.identity.agents.config.local.log.rotate) <br>Hot-swap: Yes",
    "propertyOrder" : 21700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "anonymousUserId" : {
    "title" : "Anonymous User Default Value",
    "description" : "User id of unauthenticated users. (property name:
com.sun.identity.agents.config.anonymous.user.id) <br>Hot-swap: Yes",
    "propertyOrder" : 16800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "invertNotEnforcedUrls" : {
    "title" : "Invert Not Enforced URLs",
    "description" : "Only not enforced list of urls will be enforced. (property name:
com.sun.identity.agents.config.notenforced.url.invert) <br>Hot-swap: Yes",
    "propertyOrder" : 17100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "ignorePathInfo" : {
    "title" : "Ignore Path Info in Request URL",
    "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info) <br>Hot-swap: Yes",
    "propertyOrder" : 18600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "anonymousUserEnabled" : {
    "title" : "Anonymous User",
    "description" : "Enable/Disable REMOTE_USER processing for anonymous users. (property name:
com.sun.identity.agents.config.anonymous.user.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 16900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "debugRotationSize" : {
    "title" : "Agent Debug File Size",
    "description" : "Agent debug file size in bytes. (property name:
com.sun.identity.agents.config.debug.file.size) <br>Hot-swap: Yes",
    "propertyOrder" : 22100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "ssoCachePollingInterval" : {
    "title" : "SSO Cache Polling Period",
    "description" : "Polling interval in minutes to refresh agent's sso cache. (property name:
com.sun.identity.agents.config.sso.cache.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 14500,
    "required" : true,

```

```

    "type" : "integer",
    "exampleValue" : ""
  },
  "overrideRequestHost" : {
    "title" : "Override Request URL Host",
    "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the host with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.host) <br>Hot-swap: Yes",
    "propertyOrder" : 18800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logonAndImpersonation" : {
    "title" : "Logon and Impersonation",
    "description" : "Set to true if agent should do Windows Logon and User Impersonation. (property
name: com.sun.identity.agents.config.iis.logonuser)",
    "propertyOrder" : 22900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "agentNotificationUrl" : {
    "title" : "Agent Notification URL",
    "description" : "URL used by agent to register notification listeners. (property name:
com.sun.identity.client.notification.url) <br>Hot-swap: No",
    "propertyOrder" : 14200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "fetchAttributesForNotEnforcedUrls" : {
    "title" : "Fetch Attributes for Not Enforced URLs",
    "description" : "Agent fetches profile attributes for not enforced urls by doing policy
evaluation. (property name: com.sun.identity.agents.config.notenforced.url.attributes.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 19800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "checkUserInDomino" : {
    "title" : "Check User in Domino Database",
    "description" : "If true, agent checks user existence in Domino name database. (property name:
com.sun.identity.agents.config.domino.check.name.database)",
    "propertyOrder" : 20500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "postDataPreservation" : {
    "title" : "POST Data Preservation",
    "description" : "Enables POST data preservation. (property name:
com.sun.identity.agents.config.postdata.preserve.enable) <br> Note that this feature is not supported
in all the web agents. Please refer individual agents documentation for more details. <br>Hot-swap:
Yes",
    "propertyOrder" : 17300,
    "required" : true,

```

```

        "type" : "boolean",
        "exampleValue" : ""
    },
    "loadBalanced" : {
        "title" : "Load Balancer Setup",
        "description" : "Set to true if a load balancer is used for OpenAM services. (property name:
com.sun.identity.agents.config.load.balancer.enable) <br>Hot-swap: No",
        "propertyOrder" : 15400,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "profileAttributeFetchMode" : {
        "title" : "Profile Attribute Fetch Mode",
        "description" : "(property name: com.sun.identity.agents.config.profile.attribute.fetch.mode)
<br>Hot-swap: Yes",
        "propertyOrder" : 14800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "remoteLogSendInterval" : {
        "title" : "Remote Audit Log Interval",
        "description" : "Periodic interval in minutes in which audit log messages are sent to remote log
file. (property name: com.sun.identity.agents.config.remote.log.interval) <br>Hot-swap: No",
        "propertyOrder" : 21600,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "logoutRedirectUrl" : {
        "title" : "Logout Redirect URL",
        "description" : "User gets redirected to this url after logout. (property name:
com.sun.identity.agents.config.logout.redirect.url). This property should be specified along with the
above Logout URL List.<br>Hot-swap: Yes",
        "propertyOrder" : 22300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "userIdParameter" : {
        "title" : "User ID Parameter",
        "description" : "Agent sets value of User Id to REMOTE_USER server variable. (property name:
com.sun.identity.agents.config.userid.param) <br>Hot-swap: Yes",
        "propertyOrder" : 14600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "postDataCachePeriod" : {
        "title" : "POST Data Entries Cache Period",
        "description" : "POST cache entry lifetime in minutes. (property name:
com.sun.identity.agents.config.postcache.entry.lifetime) <br>Hot-swap: Yes",
        "propertyOrder" : 17400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "ignorePreferredNamingUrl" : {

```

```

    "title" : "Ignore Preferred Naming URL in Naming Request",
    "description" : "Agent uses this value to send preferred naming url in the naming request.
(property name: com.sun.identity.agents.config.ignore.preferred.naming.url) <br>Hot-swap: Yes",
    "propertyOrder" : 15600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyEvaluationApplication" : {
    "title" : "Application",
    "description" : "Which application contains the policies to evaluate with (property name:
org.forgerock.openam.agents.config.policy.evaluation.application) <br>Hot-swap: Yes",
    "propertyOrder" : 21200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "policyEvaluationRealm" : {
    "title" : "Realm",
    "description" : "Which realm to start evaluating from (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm) <br>Hot-swap: Yes",
    "propertyOrder" : 21100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "fetchPoliciesFromRootResource" : {
    "title" : "Fetch Policies from Root Resource",
    "description" : "Agent caches policy decision of the resource and all resources from the root of
the resource down. (property name: com.sun.identity.agents.config.fetch.from.root.resource) <br>Hot-
swap: No",
    "propertyOrder" : 18200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "retrieveClientHostname" : {
    "title" : "Retrieve Client Hostname",
    "description" : "Gets the client's hostname through DNS reverse lookup for use in policy
evaluation. (property name: com.sun.identity.agents.config.get.client.host.name) <br>Hot-swap: Yes",
    "propertyOrder" : 18300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "configurationCleanupInterval" : {
    "title" : "Configuration Cleanup Interval",
    "description" : "Interval in minutes to cleanup old agent configuration entries. (property name:
com.sun.identity.agents.config.cleanup.interval) <br>Hot-swap: No",
    "propertyOrder" : 19600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "clientIpHeader" : {
    "title" : "Client IP Address Header",
    "description" : "HTTP header name that holds the IP address of the client. (property name:
com.sun.identity.agents.config.client.ip.header) <br>Hot-swap: Yes",
    "propertyOrder" : 1000,

```

```

    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributesCookieMaxAge" : {
    "title" : "Profile Attributes Cookie Maxage",
    "description" : "Maxage of attributes cookie headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.maxage) <br>Hot-swap: Yes",
    "propertyOrder" : 17900,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "agentConfigChangeNotificationsEnabled" : {
    "title" : "Agent Configuration Change Notification",
    "description" : "Enable agent to receive notification messages from OpenAM server for
configuration changes. (property name: com.sun.identity.agents.config.change.notification.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 12100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdssoCookieDomain" : {
    "title" : "Cookies Domain List",
    "description" : "List of domains in which cookies have to be set in CDSSO. (property name:
com.sun.identity.agents.config.cdsso.cookie.domain) <br>Hot-swap: Yes <br> Example: <br> .sun.com",
    "propertyOrder" : 17600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "auditAccessType" : {
    "title" : "Audit Access Types",
    "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype) <br>Hot-swap: Yes",
    "propertyOrder" : 21300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "caseInsensitiveUrlComparison" : {
    "title" : "URL Comparison Case Sensitivity Check",
    "description" : "Enforces case insensitivity in both policy and not enforced url evaluation.
(property name: com.sun.identity.agents.config.url.comparison.case.ignore) <br>Hot-swap: Yes",
    "propertyOrder" : 14300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cookieResetList" : {
    "title" : "Cookies Reset Name List",
    "description" : "List of cookies in the format: name[=value];Domain=value]. (property name:
com.sun.identity.agents.config.cookie.reset) <br>Hot-swap: Yes <br> Examples: <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
    "propertyOrder" : 16600,

```



```

    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "sessionAttributeMap" : {
    "title" : "Session Attribute Map",
    "description" : "Maps the session attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map
Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
    "propertyOrder" : 15100,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "responseAttributeFetchMode" : {
    "title" : "Response Attribute Fetch Mode",
    "description" : "(property name: com.sun.identity.agents.config.response.attribute.fetch.mode)
<br>Hot-swap: Yes",
    "propertyOrder" : 15200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientIpValidation" : {
    "title" : "Client IP Validation",
    "description" : "This validates if the subsequent browser requests come from
the same ip address that the SSO token is initially issued against. (property name:
com.sun.identity.agents.config.client.ip.validation.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 17700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Password",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "policyClockSkew" : {
    "title" : "Policy Clock Skew",
    "description" : "Time in seconds used adjust time difference between Agent machine
and OpenAM. Clock skew in seconds = AgentTime - OpenAMServerTime. (property name:
com.sun.identity.agents.config.policy.clock.skew) <br>Hot-swap: No",
    "propertyOrder" : 21000,
    "required" : true,

```

```

        "type" : "integer",
        "exampleValue" : ""
    },
    "configurationPollingInterval" : {
        "title" : "Configuration Reload Interval",
        "description" : "Interval in minutes to fetch agent configuration from OpenAM. (property name: com.sun.identity.agents.config.polling.interval) <br>Hot-swap: No",
        "propertyOrder" : 19500,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "ltpaTokenOrganizationName" : {
        "title" : "LTPA Token Organization Name",
        "description" : "The organization name to which the LTPA token belongs. (property name: com.sun.identity.agents.config.domino.ltpa.org.name)",
        "propertyOrder" : 20900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "localAuditRotationSize" : {
        "title" : "Local Audit Log Rotation Size",
        "description" : "Size limit in bytes when a local audit log file is rotated to a new file. (property name: com.sun.identity.agents.config.local.log.size) <br>Hot-swap: Yes",
        "propertyOrder" : 21800,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    }
}
}
}

```

## 1.149. WebAgents

### 1.149.1. Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/WebAgent`

Resource version: **1.0**

#### 1.149.1.1. create

Usage:

```
am> create WebAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "logoutResetCookies" : {
      "title" : "Logout Cookies List for Reset",
      "description" : "Any cookies to be reset upon logout in the same format as cookie reset list. (property name: com.sun.identity.agents.config.logout.cookie.reset) <br>Hot-swap: Yes <br> Cookie1 <br> Cookie2=value;Domain=subdomain.domain.com",
      "propertyOrder" : 18100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "loadBalanced" : {
      "title" : "Load Balancer Setup",
      "description" : "Set to true if a load balancer is used for OpenAM services. (property name: com.sun.identity.agents.config.load.balancer.enable) <br>Hot-swap: No",
      "propertyOrder" : 15400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ltpaTokenOrganizationName" : {
      "title" : "LTPA Token Organization Name",
      "description" : "The organization name to which the LTPA token belongs. (property name: com.sun.identity.agents.config.domino.ltpa.org.name)",
      "propertyOrder" : 20900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "replayPasswordKey" : {
      "title" : "Replay Password Key",
      "description" : "DES key for decrypting the basic authentication password in the session. (property name: com.sun.identity.agents.config.replaypasswd.key)",
      "propertyOrder" : 20000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "debugRotationSize" : {
      "title" : "Agent Debug File Size",
      "description" : "Agent debug file size in bytes. (property name: com.sun.identity.agents.config.debug.file.size) <br>Hot-swap: Yes",
      "propertyOrder" : 22100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

```

    },
    "notEnforcedUrls" : {
      "title" : "Not Enforced URLs",
      "description" : "List of urls for which no authentication required. (property name:
com.sun.identity.agents.config.notenforced.url) <br>Hot-swap: Yes <br> Example: <br> http://
myagent.mydomain.com/*.gif",
      "propertyOrder" : 17000,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ssoOnlyMode" : {
      "title" : "SSO Only Mode",
      "description" : "Agent will just enforce authentication (SSO), but no authorization for
policies. (property name: com.sun.identity.agents.config.sso.only) <br>Hot-swap: Yes",
      "propertyOrder" : 16000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cookieName" : {
      "title" : "Cookie Name",
      "description" : "Name of the SSO Token cookie used between the OpenAM server and the Agent.
(property name: com.sun.identity.agents.config.cookie.name)<br>Hot-swap: No",
      "propertyOrder" : 13700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ignorePreferredNamingUrl" : {
      "title" : "Ignore Preferred Naming URL in Naming Request",
      "description" : "Agent uses this value to send preferred naming url in the naming request.
(property name: com.sun.identity.agents.config.ignore.preferred.naming.url) <br>Hot-swap: Yes",
      "propertyOrder" : 15600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientHostnameHeader" : {
      "title" : "Client Hostname Header",
      "description" : "HTTP header name that holds the Hostname of the client. (property name:
com.sun.identity.agents.config.client.hostname.header) <br>Hot-swap: Yes",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteLogFilename" : {
      "title" : "Remote Log Filename",
      "description" : "Name of file stored on OpenAM server that contains agent audit messages.
(property name: com.sun.identity.agents.config.remote.logfile) <br>Hot-swap: No",
      "propertyOrder" : 21500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
  },

```

```

"anonymousUserId" : {
  "title" : "Anonymous User Default Value",
  "description" : "User id of unauthenticated users. (property name:
com.sun.identity.agents.config.anonymous.user.id) <br>Hot-swap: Yes",
  "propertyOrder" : 16800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"repositoryLocation" : {
  "title" : "Location of Agent Configuration Repository",
  "description" : "Indicates agent's configuration located either on agent's host or centrally on
OpenAM server.",
  "propertyOrder" : 400,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"cookieResetEnabled" : {
  "title" : "Cookie Reset",
  "description" : "Agent reset cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable) <br>Hot-swap: Yes",
  "propertyOrder" : 16500,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"anonymousUserEnabled" : {
  "title" : "Anonymous User",
  "description" : "Enable/Disable REMOTE_USER processing for anonymous users. (property name:
com.sun.identity.agents.config.anonymous.user.enable) <br>Hot-swap: Yes",
  "propertyOrder" : 16900,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"status" : {
  "title" : "Status",
  "description" : "Status of the agent configuration.",
  "propertyOrder" : 200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"responseAttributeMap" : {
  "title" : "Response Attribute Map",
  "description" : "Maps the policy response attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.response.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field,
and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
  "propertyOrder" : 15300,
  "required" : true,
  "patternProperties" : {
    ".*" : {
      "type" : "string"
    }
  }
},
"type" : "object",

```

```

    "exampleValue" : ""
  },
  "attributeMultiValueSeparator" : {
    "title" : "Attribute Multi Value Separator",
    "description" : "Specifies separator for multiple values. Applies to all
types of attributes i.e. profile, session and response attributes. (property name:
com.sun.identity.agents.config.attribute.multi.value.separator) <br>Hot-swap: Yes",
    "propertyOrder" : 22200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "showPasswordInHeader" : {
    "title" : "Show Password in HTTP Header",
    "description" : "Set to true if encrypted password should be set in HTTP header AUTH_PASSWORD.
(property name: com.sun.identity.agents.config.iis.password.header)",
    "propertyOrder" : 22800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "fqdnCheck" : {
    "title" : "FQDN Check",
    "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 16200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "notificationsEnabled" : {
    "title" : "Enable Notifications",
    "description" : "The notifications help in maintaining agent's sso, policy and configuration
caches. (property name: com.sun.identity.agents.config.notification.enable) <br>Hot-swap: No",
    "propertyOrder" : 14100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "logonAndImpersonation" : {
    "title" : "Logon and Impersonation",
    "description" : "Set to true if agent should do Windows Logon and User Impersonation. (property
name: com.sun.identity.agents.config.iis.logonuser)",
    "propertyOrder" : 22900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdssoRootUrl" : {
    "title" : "Agent Root URL for CDSO",
    "description" : "The agent root URL for CDSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
    "propertyOrder" : 22700,
    "required" : true,
    "items" : {
      "type" : "string"
    }
  },

```

```

    "type" : "array",
    "exampleValue" : ""
  },
  "primaryServerPollingPeriod" : {
    "title" : "Polling Period for Primary Server",
    "description" : "Interval in minutes, agent polls to check the primary server is up and running.
(property name: com.sun.identity.agents.config.poll.primary.server) <br>Hot-swap: No",
    "propertyOrder" : 19200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "profileAttributeFetchMode" : {
    "title" : "Profile Attribute Fetch Mode",
    "description" : "(property name: com.sun.identity.agents.config.profile.attribute.fetch.mode)
<br>Hot-swap: Yes",
    "propertyOrder" : 14800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributesCookiePrefix" : {
    "title" : "Profile Attributes Cookie Prefix",
    "description" : "Sets cookie prefix in the attributes headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.prefix) <br>Hot-swap: Yes",
    "propertyOrder" : 17800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "accessDeniedUrl" : {
    "title" : "Resources Access Denied URL",
    "description" : "The URL of the customized access denied page. (property name:
com.sun.identity.agents.config.access.denied.url) <br>Hot-swap: Yes",
    "propertyOrder" : 16100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "overrideProxyHostAndPort" : {
    "title" : "Override Proxy Server's Host and Port",
    "description" : "(property name: com.sun.identity.agents.config.proxy.override.host.port)
<br>Hot-swap: No",
    "propertyOrder" : 19400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "responseAttributeFetchMode" : {
    "title" : "Response Attribute Fetch Mode",
    "description" : "(property name: com.sun.identity.agents.config.response.attribute.fetch.mode)
<br>Hot-swap: Yes",
    "propertyOrder" : 15200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "encodeProfileAttributes" : {
    "title" : "Native Encoding of Profile Attributes",

```

```

    "description" : "Agent encodes the ldap header values in the default encoding of OS locale. If
false, UTF-8 gets used. (property name: com.sun.identity.agents.config.convert.mbyte.enable) <br>Hot-
swap: Yes",
    "propertyOrder" : 18400,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "idleSessionTimeoutUrl" : {
    "title" : "Idle Session Timeout Page URL",
    "description" : "URL of the local idle session timeout page. (property name:
com.sun.identity.agents.config.iis.owa.enable.session.timeout.url)",
    "propertyOrder" : 20400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ltpaTokenConfigurationname" : {
    "title" : "LTPA Token Configuration Name",
    "description" : "The configuration name that the agent uses in order to employ the LTPA token
mechanism. (property name: com.sun.identity.agents.config.domino.ltpa.config.name)",
    "propertyOrder" : 20800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sessionAttributeFetchMode" : {
    "title" : "Session Attribute Fetch Mode",
    "description" : "(property name: com.sun.identity.agents.config.session.attribute.fetch.mode)
<br>Hot-swap: Yes",
    "propertyOrder" : 15000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "configurationCleanupInterval" : {
    "title" : "Configuration Cleanup Interval",
    "description" : "Interval in minutes to cleanup old agent configuration entries. (property name:
com.sun.identity.agents.config.cleanup.interval) <br>Hot-swap: No",
    "propertyOrder" : 19600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "userpassword" : {
    "title" : "Password",
    "description" : "",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "format" : "password",
    "exampleValue" : ""
  },
  "filterPriority" : {
    "title" : "Filter Priority",
    "description" : "The loading priority of filter. (property name:
com.sun.identity.agents.config.iis.filter.priority)",
    "propertyOrder" : 20100,
    "required" : true,

```



```

        "type" : "string",
        "exampleValue" : ""
    },
    "cdsso" : {
        "title" : "Cross Domain SSO",
        "description" : "Enables Cross-Domain Single Sign On. (property name:
com.sun.identity.agents.config.cdsso.enable) <br>Hot-swap: Yes",
        "propertyOrder" : 16700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "auditAccessType" : {
        "title" : "Audit Access Types",
        "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype) <br>Hot-swap: Yes",
        "propertyOrder" : 21300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "checkUserInDomino" : {
        "title" : "Check User in Domino Database",
        "description" : "If true, agent checks user existence in Domino name database. (property name:
com.sun.identity.agents.config.domino.check.name.database)",
        "propertyOrder" : 20500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "overrideRequestPort" : {
        "title" : "Override Request URL Port",
        "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the port with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.port) <br>Hot-swap: Yes",
        "propertyOrder" : 18900,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "debugLogRotation" : {
        "title" : "Agent Debug File Rotation",
        "description" : "Debug file gets rotated based on the size specified. (property name:
com.sun.identity.agents.config.debug.file.rotate) <br>Hot-swap: Yes",
        "propertyOrder" : 22000,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "policyCachePollingInterval" : {
        "title" : "Policy Cache Polling Period",
        "description" : "Polling interval in minutes to refresh agent's policy cache. (property name:
com.sun.identity.agents.config.policy.cache.polling.interval) <br>Hot-swap: No",
        "propertyOrder" : 14400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    },

```

```

"secureCookies" : {
  "title" : "Cookie Security",
  "description" : "Agent sends secure cookies if communication is secure. (property name:
com.sun.identity.agents.config.cookie.secure) <br>Hot-swap: No",
  "propertyOrder" : 13800,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"policyClockSkew" : {
  "title" : "Policy Clock Skew",
  "description" : "Time in seconds used adjust time difference between Agent machine
and OpenAM. Clock skew in seconds = AgentTime - OpenAMServerTime. (property name:
com.sun.identity.agents.config.policy.clock.skew) <br>Hot-swap: No",
  "propertyOrder" : 21000,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"agentNotificationUrl" : {
  "title" : "Agent Notification URL",
  "description" : "URL used by agent to register notification listeners. (property name:
com.sun.identity.client.notification.url) <br>Hot-swap: No",
  "propertyOrder" : 14200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"ignorePathInfoForNotEnforcedUrls" : {
  "title" : "Ignore Path Info for Not Enforced URLs",
  "description" : "Indicate whether the path info and query should be stripped from the request
URL before being compared with the URLs of the not enforced list when those URLs have a wildcard '*'
character. (property name: com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list)
<br>Hot-swap: Yes",
  "propertyOrder" : 13900,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"cookieResetList" : {
  "title" : "Cookies Reset Name List",
  "description" : "List of cookies in the format: name[=value][;Domain=value]. (property name:
com.sun.identity.agents.config.cookie.reset) <br>Hot-swap: Yes <br> Examples: <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
  "propertyOrder" : 16600,
  "required" : true,
  "items" : {
    "type" : "string"
  },
  "type" : "array",
  "exampleValue" : ""
},
"agentDebugLevel" : {
  "title" : "Agent Debug Level",
  "description" : "Agent debug level. (property name: com.sun.identity.agents.config.debug.level)
<br>Hot-swap: Yes",
  "propertyOrder" : 21900,
  "required" : true,
  "type" : "string",

```

```

    "exampleValue" : ""
  },
  "ssoCachePollingInterval" : {
    "title" : "SSO Cache Polling Period",
    "description" : "Polling interval in minutes to refresh agent's sso cache. (property name: com.sun.identity.agents.config.sso.cache.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 14500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "retrieveClientHostname" : {
    "title" : "Retrieve Client Hostname",
    "description" : "Gets the client's hostname through DNS reverse lookup for use in policy evaluation. (property name: com.sun.identity.agents.config.get.client.host.name) <br>Hot-swap: Yes",
    "propertyOrder" : 18300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdssoRedirectUri" : {
    "title" : "CDSSO Redirect URI",
    "description" : "An intermediate URI that is used by the Agent for processing CDSSO requests. (property name: com.sun.identity.agents.config.cdsso.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 17550,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "localAuditRotationSize" : {
    "title" : "Local Audit Log Rotation Size",
    "description" : "Size limit in bytes when a local audit log file is rotated to a new file. (property name: com.sun.identity.agents.config.local.log.size) <br>Hot-swap: Yes",
    "propertyOrder" : 21800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "authenticationType" : {
    "title" : "Authentication Type",
    "description" : "(property name: com.sun.identity.agents.config.iis.auth.type)",
    "propertyOrder" : 19900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoCookieDomain" : {
    "title" : "Cookies Domain List",
    "description" : "List of domains in which cookies have to be set in CDSSO. (property name: com.sun.identity.agents.config.cdsso.cookie.domain) <br>Hot-swap: Yes <br> Example: <br> .sun.com",
    "propertyOrder" : 17600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "profileAttributeMap" : {

```

```

    "title" : "Profile Attribute Map",
    "description" : "Maps the profile attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.profile.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field,
and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate the value of profile
attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in
Corresponding Map Value field.",
    "propertyOrder" : 14900,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"fetchPoliciesFromRootResource" : {
    "title" : "Fetch Policies from Root Resource",
    "description" : "Agent caches policy decision of the resource and all resources from the root of
the resource down. (property name: com.sun.identity.agents.config.fetch.from.root.resource) <br>Hot-
swap: No",
    "propertyOrder" : 18200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"applicationLogoutUrls" : {
    "title" : "Logout URL List",
    "description" : "List of application logout URLs. User gets logged out from OpenAM session
when these urls accessed. (property name: com.sun.identity.agents.config.agent.logout.url). If this
property is used, user should specify a value for the below Logout Redirect URL property.<br>Hot-
swap: Yes <br> Example: <br> http://myagent.mydomain.com/logout.html",
    "propertyOrder" : 18000,
    "required" : true,
    "items" : {
        "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
},
"auditLogLocation" : {
    "title" : "Audit Log Location",
    "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition) <br>Hot-swap: Yes",
    "propertyOrder" : 21400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"clientIpValidation" : {
    "title" : "Client IP Validation",
    "description" : "This validates if the subsequent browser requests come from
the same ip address that the SSO token is initially issued against. (property name:
com.sun.identity.agents.config.client.ip.validation.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 17700,
    "required" : true,
    "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "customProperties" : {
    "title" : "Custom Properties",
    "description" : "Additional properties that allow users to augment the set of properties
supported by agent. (property name: com.sun.identity.agents.config.freeformproperties) <br>Hot-
swap: Yes <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-
value-0 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
    "propertyOrder" : 19700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "filterConfiguredWithOwa" : {
    "title" : "Filter configured with OWA",
    "description" : "Set to true if the IIS agent filter is configured for OWA. (property name:
com.sun.identity.agents.config.iis.owa.enable)",
    "propertyOrder" : 20200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invertNotEnforcedUrls" : {
    "title" : "Invert Not Enforced URLs",
    "description" : "Only not enforced list of urls will be enforced. (property name:
com.sun.identity.agents.config.notenforced.url.invert) <br>Hot-swap: Yes",
    "propertyOrder" : 17100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "amLogoutUrl" : {
    "title" : "OpenAM Logout URL",
    "description" : "OpenAM logout page URL. (property name:
com.sun.identity.agents.config.logout.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Logout",
    "propertyOrder" : 12400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "overrideRequestHost" : {
    "title" : "Override Request URL Host",
    "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the host with the value from
the property com.sun.identity.agents.config.agenturl.prefix. (property name:
com.sun.identity.agents.config.override.host) <br>Hot-swap: Yes",
    "propertyOrder" : 18800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  },

```

```

"postDataCachePeriod" : {
  "title" : "POST Data Entries Cache Period",
  "description" : "POST cache entry lifetime in minutes. (property name:
com.sun.identity.agents.config.postcache.entry.lifetime) <br>Hot-swap: Yes",
  "propertyOrder" : 17400,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"fetchAttributesForNotEnforcedUrls" : {
  "title" : "Fetch Attributes for Not Enforced URLs",
  "description" : "Agent fetches profile attributes for not enforced urls by doing policy
evaluation. (property name: com.sun.identity.agents.config.notenforced.url.attributes.enable)
<br>Hot-swap: Yes",
  "propertyOrder" : 19800,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"agentLocale" : {
  "title" : "Agent Locale",
  "description" : "The default locale for the product. (property name:
com.sun.identity.agents.config.locale) <br>Hot-swap: No",
  "propertyOrder" : 19300,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"encodeSpecialCharsInCookies" : {
  "title" : "Encode special chars in Cookies",
  "description" : "Encode special chars in cookie by URL encoding. Useful when profile, session
and response attributes contain special chars and attributes fetch mode is set to HTTP_COOKIE.
(property name: com.sun.identity.agents.config.encode.cookie.special.chars.enable) <br>Hot-swap:
Yes",
  "propertyOrder" : 14000,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"clientIpHeader" : {
  "title" : "Client IP Address Header",
  "description" : "HTTP header name that holds the IP address of the client. (property name:
com.sun.identity.agents.config.client.ip.header) <br>Hot-swap: Yes",
  "propertyOrder" : 1000,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"postDataPreservation" : {
  "title" : "POST Data Preservation",
  "description" : "Enables POST data preservation. (property name:
com.sun.identity.agents.config.postdata.preserve.enable) <br> Note that this feature is not supported
in all the web agents. Please refer individual agents documentation for more details. <br>Hot-swap:
Yes",
  "propertyOrder" : 17300,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},

```

```

    "logoutRedirectUrl" : {
      "title" : "Logout Redirect URL",
      "description" : "User gets redirected to this url after logout. (property name:
com.sun.identity.agents.config.logout.redirect.url). This property should be specified along with the
above Logout URL List.<br>Hot-swap: Yes",
      "propertyOrder" : 22300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "caseInsensitiveUrlComparison" : {
      "title" : "URL Comparison Case Sensitivity Check",
      "description" : "Enforces case insensitivity in both policy and not enforced url evaluation.
(property name: com.sun.identity.agents.config.url.comparison.case.ignore) <br>Hot-swap: Yes",
      "propertyOrder" : 14300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "sessionAttributeMap" : {
      "title" : "Session Attribute Map",
      "description" : "Maps the session attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map
Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
      "propertyOrder" : 15100,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "cdssoUrls" : {
      "title" : "CDSSO Servlet URL",
      "description" : "List of URLs of the available CDSSO controllers that may be used by the Agent
for CDSSO processing. (property name: com.sun.identity.agents.config.cdsso.cdcservlet.url) <br>Hot-
swap: Yes <br> Example: <br> http://host:port/opensso/cdcservlet",
      "propertyOrder" : 17500,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "notEnforcedIps" : {
      "title" : "Not Enforced Client IP List",
      "description" : "No authentication and authorization are required for the requests coming from
these client IP addresses. (property name: com.sun.identity.agents.config.notenforced.ip) <br>Hot-
swap: Yes <br> Examples: <br> 192.18.145.* <br> 192.18.146.123",
      "propertyOrder" : 17200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "type" : "object",
  "exampleValue" : ""
}

```

```

    "type" : "array",
    "exampleValue" : ""
  },
  "userIdParameter" : {
    "title" : "User ID Parameter",
    "description" : "Agent sets value of User Id to REMOTE_USER server variable. (property name: com.sun.identity.agents.config.userid.param) <br>Hot-swap: Yes",
    "propertyOrder" : 14600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ltpaTokenCookieName" : {
    "title" : "LTPA Token Cookie Name",
    "description" : "The name of the cookie that contains the LTPA token. (property name: com.sun.identity.agents.config.domino.ltpa.cookie.name)",
    "propertyOrder" : 20700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "amLoginUrl" : {
    "title" : "OpenAM Login URL",
    "description" : "OpenAM login page URL. (property name: com.sun.identity.agents.config.login.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/opensso/UI/Login",
    "propertyOrder" : 15700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "overrideNotificationUrl" : {
    "title" : "Override Notification URL",
    "description" : "Set to true if the agent is sitting behind a ssl/tls off-loader, load balancer, or proxy to override the URL with the value from the property com.sun.identity.agents.config.agenturi.prefix. (property name: com.sun.identity.agents.config.override.notification.url) <br>Hot-swap: Yes",
    "propertyOrder" : 19000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "overrideRequestProtocol" : {
    "title" : "Override Request URL Protocol",
    "description" : "Set to true if the agent is sitting behind a ssl/tls off-loader, load balancer, or proxy to override the protocol with the value from the property com.sun.identity.agents.config.agenturi.prefix. (property name: com.sun.identity.agents.config.override.protocol) <br>Hot-swap: Yes",
    "propertyOrder" : 18700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "fqdnMapping" : {
    "title" : "FQDN Virtual Host Map",

```



```

    "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN to
access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>Hot-
swap: Yes <br> Examples: <br> To map the partial hostname myserver to myserver.mydomain.com: enter
myserver in the Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map
a virtual server rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in
the Map Key field and rst.hostname.com in the Corresponding Map Value field.",
    "propertyOrder" : 16400,
    "required" : true,
    "patternProperties" : {
        ".*" : {
            "type" : "string"
        }
    },
    "type" : "object",
    "exampleValue" : ""
},
"fqdnDefault" : {
    "title" : "FQDN Default",
    "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default) <br>Hot-swap: Yes",
    "propertyOrder" : 16300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"agentConnectionTimeout" : {
    "title" : "Agent Connection Timeout",
    "description" : "Timeout period in seconds for an agent connection with OpenAM auth server.
(property name: com.sun.identity.agents.config.auth.connection.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 19100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
},
"ignorePathInfo" : {
    "title" : "Ignore Path Info in Request URL",
    "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info) <br>Hot-swap: Yes",
    "propertyOrder" : 18600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"ignoreServerCheck" : {
    "title" : "Ignore Server Check",
    "description" : "Agent uses this value to check OpenAM is up before doing a 302 redirect.
(property name: com.sun.identity.agents.config.ignore.server.check) <br>Hot-swap: Yes",
    "propertyOrder" : 15500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"configurationPollingInterval" : {
    "title" : "Configuration Reload Interval",
    "description" : "Interval in minutes to fetch agent configuration from OpenAM. (property name:
com.sun.identity.agents.config.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 19500,
    "required" : true,

```

```

        "type" : "integer",
        "exampleValue" : ""
    },
    "userIdParameterType" : {
        "title" : "User ID Parameter Type",
        "description" : "User ID can be fetched from either SESSION and LDAP attributes. (property name: com.sun.identity.agents.config.userid.param.type) <br>Hot-swap: Yes",
        "propertyOrder" : 14700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "localAuditLogRotation" : {
        "title" : "Rotate Local Audit Log",
        "description" : "Flag to indicate that audit log files should be rotated when reaching a certain size. (property name: com.sun.identity.agents.config.local.log.rotate) <br>Hot-swap: Yes",
        "propertyOrder" : 21700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "agentConfigChangeNotificationsEnabled" : {
        "title" : "Agent Configuration Change Notification",
        "description" : "Enable agent to receive notification messages from OpenAM server for configuration changes. (property name: com.sun.identity.agents.config.change.notification.enable) <br>Hot-swap: Yes",
        "propertyOrder" : 12100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "policyEvaluationApplication" : {
        "title" : "Application",
        "description" : "Which application contains the policies to evaluate with (property name: org.forgerock.openam.agents.config.policy.evaluation.application) <br>Hot-swap: Yes",
        "propertyOrder" : 21200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "remoteLogSendInterval" : {
        "title" : "Remote Audit Log Interval",
        "description" : "Periodic interval in minutes in which audit log messages are sent to remote log file. (property name: com.sun.identity.agents.config.remote.log.interval) <br>Hot-swap: No",
        "propertyOrder" : 21600,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "profileAttributesCookieMaxAge" : {
        "title" : "Profile Attributes Cookie Maxage",
        "description" : "Maxage of attributes cookie headers. (property name: com.sun.identity.agents.config.profile.attribute.cookie.maxage) <br>Hot-swap: Yes",
        "propertyOrder" : 17900,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "agentUriPrefix" : {

```

```

    "title" : "Agent Deployment URI Prefix",
    "description" : "(property name: com.sun.identity.agents.config.agenturi.prefix)<br>Hot-swap:
Yes",
    "propertyOrder" : 15800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "gotoParameterName" : {
    "title" : "Goto Parameter Name",
    "description" : "Property used only when CDSO is enabled. Default value should
be changed only when the login URL has a landing page specified <br> Example :
com.sun.identity.agents.config.cdsso.cdcservlet.url = http://host:port/opensso/cdcservlet?
goto=http://agent:port/landing.jsp <br> The parameter is used by the Agent to append the original
request URL to this cdcservlet URL. This parameter is consumed by the landing page to redirect to
the original URL. (property name: com.sun.identity.agents.config.redirect.param) <br>Hot-swap: Yes
<br> Example: com.sun.identity.agents.config.redirect.param = goto2<br> The complete URL sent for
authentication will be <br> http://host:port/opensso/cdcservlet?goto=http://agent:port/landing.jsp?
goto2=http://agent.port/original.jsp",
    "propertyOrder" : 3600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "changeProtocolToHttps" : {
    "title" : "Change URL Protocol to https",
    "description" : "If true, avoids IE6 security pop-ups. (property name:
com.sun.identity.agents.config.iis.owa.enable.change.protocol)",
    "propertyOrder" : 20300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "encodeUrlSpecialCharacters" : {
    "title" : "Encode URL's Special Characters",
    "description" : "Encodes the url which has special characters before doing policy evaluation.
(property name: com.sun.identity.agents.config.encode.url.special.chars.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 18500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "useLtpaToken" : {
    "title" : "Use LTPA token",
    "description" : "Set to true if agent needs to use LTPA Token. (property name:
com.sun.identity.agents.config.domino.ltpa.enable)",
    "propertyOrder" : 20600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyEvaluationRealm" : {
    "title" : "Realm",
    "description" : "Which realm to start evaluating from (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm) <br>Hot-swap: Yes",
    "propertyOrder" : 21100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}

```

```
}  
}  
}
```

### 1.149.1.2. delete

Usage:

```
am> delete WebAgents --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.149.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebAgents --realm Realm --actionName getAllTypes
```

### 1.149.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebAgents --realm Realm --actionName getCreatableTypes
```

### 1.149.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebAgents --realm Realm --actionName nextdescendents
```

### 1.149.1.6. query

Querying the agents of a specific type

Usage:

```
am> query WebAgents --realm Realm --filter filter
```

Parameters:

## --filter

A CREST formatted query filter, where "true" will query all.

## 1.149.1.7. read

Usage:

```
am> read WebAgents --realm Realm --id id
```

Parameters:

### --id

The unique identifier for the resource.

## 1.149.1.8. update

Usage:

```
am> update WebAgents --realm Realm --id id --body body
```

Parameters:

### --id

The unique identifier for the resource.

### --body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "logoutResetCookies" : {
      "title" : "Logout Cookies List for Reset",
      "description" : "Any cookies to be reset upon logout in the same format as cookie reset list. (property name: com.sun.identity.agents.config.logout.cookie.reset) <br>Hot-swap: Yes <br> Cookie1 <br> Cookie2=value;Domain=subdomain.domain.com",
      "propertyOrder" : 18100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "loadBalanced" : {
      "title" : "Load Balancer Setup",
      "description" : "Set to true if a load balancer is used for OpenAM services. (property name: com.sun.identity.agents.config.load.balancer.enable) <br>Hot-swap: No",
      "propertyOrder" : 15400,
      "required" : true,
      "type" : "boolean",
```

```

    "exampleValue" : ""
  },
  "ltpaTokenOrganizationName" : {
    "title" : "LTPA Token Organization Name",
    "description" : "The organization name to which the LTPA token belongs. (property name:
com.sun.identity.agents.config.domino.ltpa.org.name)",
    "propertyOrder" : 20900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "replayPasswordKey" : {
    "title" : "Replay Password Key",
    "description" : "DES key for decrypting the basic authentication password in the session.
(property name: com.sun.identity.agents.config.replaypasswd.key)",
    "propertyOrder" : 20000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "debugRotationSize" : {
    "title" : "Agent Debug File Size",
    "description" : "Agent debug file size in bytes. (property name:
com.sun.identity.agents.config.debug.file.size) <br>Hot-swap: Yes",
    "propertyOrder" : 22100,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "notEnforcedUrls" : {
    "title" : "Not Enforced URLs",
    "description" : "List of urls for which no authentication required. (property name:
com.sun.identity.agents.config.notenforced.url) <br>Hot-swap: Yes <br> Example: <br> http://
myagent.mydomain.com/*.gif",
    "propertyOrder" : 17000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "ssoOnlyMode" : {
    "title" : "SSO Only Mode",
    "description" : "Agent will just enforce authentication (SSO), but no authorization for
policies. (property name: com.sun.identity.agents.config.sso.only) <br>Hot-swap: Yes",
    "propertyOrder" : 16000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cookieName" : {
    "title" : "Cookie Name",
    "description" : "Name of the SSO Token cookie used between the OpenAM server and the Agent.
(property name: com.sun.identity.agents.config.cookie.name)<br>Hot-swap: No",
    "propertyOrder" : 13700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }

```

```

    },
    "ignorePreferredNamingUrl" : {
      "title" : "Ignore Preferred Naming URL in Naming Request",
      "description" : "Agent uses this value to send preferred naming url in the naming request.
(property name: com.sun.identity.agents.config.ignore.preferred.naming.url) <br>Hot-swap: Yes",
      "propertyOrder" : 15600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientHostnameHeader" : {
      "title" : "Client Hostname Header",
      "description" : "HTTP header name that holds the Hostname of the client. (property name:
com.sun.identity.agents.config.client.hostname.header) <br>Hot-swap: Yes",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteLogFilename" : {
      "title" : "Remote Log Filename",
      "description" : "Name of file stored on OpenAM server that contains agent audit messages.
(property name: com.sun.identity.agents.config.remote.logfile) <br>Hot-swap: No",
      "propertyOrder" : 21500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "anonymousUserId" : {
      "title" : "Anonymous User Default Value",
      "description" : "User id of unauthenticated users. (property name:
com.sun.identity.agents.config.anonymous.user.id) <br>Hot-swap: Yes",
      "propertyOrder" : 16800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "repositoryLocation" : {
      "title" : "Location of Agent Configuration Repository",
      "description" : "Indicates agent's configuration located either on agent's host or centrally on
OpenAM server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "cookieResetEnabled" : {
      "title" : "Cookie Reset",
      "description" : "Agent reset cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable) <br>Hot-swap: Yes",
      "propertyOrder" : 16500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "anonymousUserEnabled" : {
      "title" : "Anonymous User",
      "description" : "Enable/Disable REMOTE_USER processing for anonymous users. (property name:
com.sun.identity.agents.config.anonymous.user.enable) <br>Hot-swap: Yes",

```

```

    "propertyOrder" : 16900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "status" : {
    "title" : "Status",
    "description" : "Status of the agent configuration.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "responseAttributeMap" : {
    "title" : "Response Attribute Map",
    "description" : "Maps the policy response attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.response.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field,
and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
    "propertyOrder" : 15300,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "attributeMultiValueSeparator" : {
    "title" : "Attribute Multi Value Separator",
    "description" : "Specifies separator for multiple values. Applies to all
types of attributes i.e. profile, session and response attributes. (property name:
com.sun.identity.agents.config.attribute.multi.value.separator) <br>Hot-swap: Yes",
    "propertyOrder" : 22200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "showPasswordInHeader" : {
    "title" : "Show Password in HTTP Header",
    "description" : "Set to true if encrypted password should be set in HTTP header AUTH_PASSWORD.
(property name: com.sun.identity.agents.config.iis.password.header)",
    "propertyOrder" : 22800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "fqdnCheck" : {
    "title" : "FQDN Check",
    "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 16200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "notificationsEnabled" : {

```



```

    "title" : "Enable Notifications",
    "description" : "The notifications help in maintaining agent's sso, policy and configuration
    caches. (property name: com.sun.identity.agents.config.notification.enable) <br>Hot-swap: No",
    "propertyOrder" : 14100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "loginAndImpersonation" : {
    "title" : "Logon and Impersonation",
    "description" : "Set to true if agent should do Windows Logon and User Impersonation. (property
    name: com.sun.identity.agents.config.iis.logonuser)",
    "propertyOrder" : 22900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdssoRootUrl" : {
    "title" : "Agent Root URL for CDSSO",
    "description" : "The agent root URL for CDSSO. The valid value is in the following format:
    <br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
    The hostname represents the host name of the machine on which the agent resides. The port represents
    the port number on which the agent is installed. The slash following the port number is required.",
    "propertyOrder" : 22700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "primaryServerPollingPeriod" : {
    "title" : "Polling Period for Primary Server",
    "description" : "Interval in minutes, agent polls to check the primary server is up and running.
    (property name: com.sun.identity.agents.config.poll.primary.server) <br>Hot-swap: No",
    "propertyOrder" : 19200,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "profileAttributeFetchMode" : {
    "title" : "Profile Attribute Fetch Mode",
    "description" : "(property name: com.sun.identity.agents.config.profile.attribute.fetch.mode)
    <br>Hot-swap: Yes",
    "propertyOrder" : 14800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "profileAttributesCookiePrefix" : {
    "title" : "Profile Attributes Cookie Prefix",
    "description" : "Sets cookie prefix in the attributes headers. (property name:
    com.sun.identity.agents.config.profile.attribute.cookie.prefix) <br>Hot-swap: Yes",
    "propertyOrder" : 17800,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "accessDeniedUrl" : {

```

```

        "title" : "Resources Access Denied URL",
        "description" : "The URL of the customized access denied page. (property name:
com.sun.identity.agents.config.access.denied.url) <br>Hot-swap: Yes",
        "propertyOrder" : 16100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "overrideProxyHostAndPort" : {
        "title" : "Override Proxy Server's Host and Port",
        "description" : "(property name: com.sun.identity.agents.config.proxy.override.host.port)
<br>Hot-swap: No",
        "propertyOrder" : 19400,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "responseAttributeFetchMode" : {
        "title" : "Response Attribute Fetch Mode",
        "description" : "(property name: com.sun.identity.agents.config.response.attribute.fetch.mode)
<br>Hot-swap: Yes",
        "propertyOrder" : 15200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "encodeProfileAttributes" : {
        "title" : "Native Encoding of Profile Attributes",
        "description" : "Agent encodes the ldap header values in the default encoding of OS locale. If
false, UTF-8 gets used. (property name: com.sun.identity.agents.config.convert.mbyte.enable) <br>Hot-
swap: Yes",
        "propertyOrder" : 18400,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "idleSessionTimeoutUrl" : {
        "title" : "Idle Session Timeout Page URL",
        "description" : "URL of the local idle session timeout page. (property name:
com.sun.identity.agents.config.iis.owa.enable.session.timeout.url)",
        "propertyOrder" : 20400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "ltpaTokenConfigurationName" : {
        "title" : "LTPA Token Configuration Name",
        "description" : "The configuration name that the agent uses in order to employ the LTPA token
mechanism. (property name: com.sun.identity.agents.config.domino.ltpa.config.name)",
        "propertyOrder" : 20800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "sessionAttributeFetchMode" : {
        "title" : "Session Attribute Fetch Mode",
        "description" : "(property name: com.sun.identity.agents.config.session.attribute.fetch.mode)
<br>Hot-swap: Yes",
        "propertyOrder" : 15000,

```

```

        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "configurationCleanupInterval" : {
        "title" : "Configuration Cleanup Interval",
        "description" : "Interval in minutes to cleanup old agent configuration entries. (property name:
com.sun.identity.agents.config.cleanup.interval) <br>Hot-swap: No",
        "propertyOrder" : 19600,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "userpassword" : {
        "title" : "Password",
        "description" : "",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
    },
    "filterPriority" : {
        "title" : "Filter Priority",
        "description" : "The loading priority of filter. (property name:
com.sun.identity.agents.config.iis.filter.priority)",
        "propertyOrder" : 20100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "cdsso" : {
        "title" : "Cross Domain SSO",
        "description" : "Enables Cross-Domain Single Sign On. (property name:
com.sun.identity.agents.config.cdsso.enable) <br>Hot-swap: Yes",
        "propertyOrder" : 16700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "auditAccessType" : {
        "title" : "Audit Access Types",
        "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype) <br>Hot-swap: Yes",
        "propertyOrder" : 21300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "checkUserInDomino" : {
        "title" : "Check User in Domino Database",
        "description" : "If true, agent checks user existence in Domino name database. (property name:
com.sun.identity.agents.config.domino.check.name.database)",
        "propertyOrder" : 20500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "overrideRequestPort" : {

```

```

        "title" : "Override Request URL Port",
        "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the port with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.port) <br>Hot-swap: Yes",
        "propertyOrder" : 18900,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "debugLogRotation" : {
        "title" : "Agent Debug File Rotation",
        "description" : "Debug file gets rotated based on the size specified. (property name:
com.sun.identity.agents.config.debug.file.rotate) <br>Hot-swap: Yes",
        "propertyOrder" : 22000,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "policyCachePollingInterval" : {
        "title" : "Policy Cache Polling Period",
        "description" : "Polling interval in minutes to refresh agent's policy cache. (property name:
com.sun.identity.agents.config.policy.cache.polling.interval) <br>Hot-swap: No",
        "propertyOrder" : 14400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "secureCookies" : {
        "title" : "Cookie Security",
        "description" : "Agent sends secure cookies if communication is secure. (property name:
com.sun.identity.agents.config.cookie.secure) <br>Hot-swap: No",
        "propertyOrder" : 13800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "policyClockSkew" : {
        "title" : "Policy Clock Skew",
        "description" : "Time in seconds used adjust time difference between Agent machine
and OpenAM. Clock skew in seconds = AgentTime - OpenAMServerTime. (property name:
com.sun.identity.agents.config.policy.clock.skew) <br>Hot-swap: No",
        "propertyOrder" : 21000,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "agentNotificationUrl" : {
        "title" : "Agent Notification URL",
        "description" : "URL used by agent to register notification listeners. (property name:
com.sun.identity.client.notification.url) <br>Hot-swap: No",
        "propertyOrder" : 14200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "ignorePathInfoForNotEnforcedUrls" : {
        "title" : "Ignore Path Info for Not Enforced URLs",

```

```

    "description" : "Indicate whether the path info and query should be stripped from the request
URL before being compared with the URLs of the not enforced list when those URLs have a wildcard '*'
character. (property name: com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list)
<br>Hot-swap: Yes",
    "propertyOrder" : 13900,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cookieResetList" : {
    "title" : "Cookies Reset Name List",
    "description" : "List of cookies in the format: name[=value][;Domain=value]. (property name:
com.sun.identity.agents.config.cookie.reset) <br>Hot-swap: Yes <br> Examples: <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
    "propertyOrder" : 16600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "agentDebugLevel" : {
    "title" : "Agent Debug Level",
    "description" : "Agent debug level. (property name: com.sun.identity.agents.config.debug.level)
<br>Hot-swap: Yes",
    "propertyOrder" : 21900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ssoCachePollingInterval" : {
    "title" : "SSO Cache Polling Period",
    "description" : "Polling interval in minutes to refresh agent's sso cache. (property name:
com.sun.identity.agents.config.sso.cache.polling.interval) <br>Hot-swap: No",
    "propertyOrder" : 14500,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "retrieveClientHostname" : {
    "title" : "Retrieve Client Hostname",
    "description" : "Gets the client's hostname through DNS reverse lookup for use in policy
evaluation. (property name: com.sun.identity.agents.config.get.client.host.name) <br>Hot-swap: Yes",
    "propertyOrder" : 18300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "cdssoRedirectUri" : {
    "title" : "CDSSO Redirect URI",
    "description" : "An intermediate URI that is used by the Agent for processing CDSSO requests.
(property name: com.sun.identity.agents.config.cdsso.redirect.uri) <br>Hot-swap: Yes",
    "propertyOrder" : 17550,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "localAuditRotationSize" : {

```

```

    "title" : "Local Audit Log Rotation Size",
    "description" : "Size limit in bytes when a local audit log file is rotated to a new file.
(property name: com.sun.identity.agents.config.local.log.size) <br>Hot-swap: Yes",
    "propertyOrder" : 21800,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "authenticationType" : {
    "title" : "Authentication Type",
    "description" : "(property name: com.sun.identity.agents.config.iis.auth.type)",
    "propertyOrder" : 19900,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "cdssoCookieDomain" : {
    "title" : "Cookies Domain List",
    "description" : "List of domains in which cookies have to be set in CDSSO. (property name:
com.sun.identity.agents.config.cdsso.cookie.domain) <br>Hot-swap: Yes <br> Example: <br> .sun.com",
    "propertyOrder" : 17600,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "profileAttributeMap" : {
    "title" : "Profile Attribute Map",
    "description" : "Maps the profile attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.profile.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field,
and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate the value of profile
attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in
Corresponding Map Value field.",
    "propertyOrder" : 14900,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "fetchPoliciesFromRootResource" : {
    "title" : "Fetch Policies from Root Resource",
    "description" : "Agent caches policy decision of the resource and all resources from the root of
the resource down. (property name: com.sun.identity.agents.config.fetch.from.root.resource) <br>Hot-
swap: No",
    "propertyOrder" : 18200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "applicationLogoutUrls" : {
    "title" : "Logout URL List",

```

```

    "description" : "List of application logout URLs. User gets logged out from OpenAM session
when these urls accessed. (property name: com.sun.identity.agents.config.agent.logout.url). If this
property is used, user should specify a value for the below Logout Redirect URL property.<br>Hot-
swap: Yes <br> Example: <br> http://myagent.mydomain.com/logout.html",
    "propertyOrder" : 18000,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "auditLogLocation" : {
    "title" : "Audit Log Location",
    "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition) <br>Hot-swap: Yes",
    "propertyOrder" : 21400,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "clientIpValidation" : {
    "title" : "Client IP Validation",
    "description" : "This validates if the subsequent browser requests come from
the same ip address that the SSO token is initially issued against. (property name:
com.sun.identity.agents.config.client.ip.validation.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 17700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "customProperties" : {
    "title" : "Custom Properties",
    "description" : "Additional properties that allow users to augment the set of properties
supported by agent. (property name: com.sun.identity.agents.config.freeformproperties) <br>Hot-
swap: Yes <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-
value-0 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
    "propertyOrder" : 19700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "filterConfiguredWithOwa" : {
    "title" : "Filter configured with OWA",
    "description" : "Set to true if the IIS agent filter is configured for OWA. (property name:
com.sun.identity.agents.config.iis.owa.enable)",
    "propertyOrder" : 20200,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "invertNotEnforcedUrls" : {
    "title" : "Invert Not Enforced URLs",
    "description" : "Only not enforced list of urls will be enforced. (property name:
com.sun.identity.agents.config.notenforced.url.invert) <br>Hot-swap: Yes",

```

```

    "propertyOrder" : 17100,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "amLogoutUrl" : {
    "title" : "OpenAM Logout URL",
    "description" : "OpenAM logout page URL. (property name:
com.sun.identity.agents.config.logout.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Logout",
    "propertyOrder" : 12400,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "overrideRequestHost" : {
    "title" : "Override Request URL Host",
    "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the host with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.host) <br>Hot-swap: Yes",
    "propertyOrder" : 18800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "postDataCachePeriod" : {
    "title" : "POST Data Entries Cache Period",
    "description" : "POST cache entry lifetime in minutes. (property name:
com.sun.identity.agents.config.postcache.entry.lifetime) <br>Hot-swap: Yes",
    "propertyOrder" : 17400,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "fetchAttributesForNotEnforcedUrls" : {
    "title" : "Fetch Attributes for Not Enforced URLs",
    "description" : "Agent fetches profile attributes for not enforced urls by doing policy
evaluation. (property name: com.sun.identity.agents.config.notenforced.url.attributes.enable)
<br>Hot-swap: Yes",
    "propertyOrder" : 19800,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "agentLocale" : {
    "title" : "Agent Locale",
    "description" : "The default locale for the product. (property name:
com.sun.identity.agents.config.locale) <br>Hot-swap: No",
    "propertyOrder" : 19300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "encodeSpecialCharsInCookies" : {
    "title" : "Encode special chars in Cookies",

```



```

    "description" : "Encode special chars in cookie by URL encoding. Useful when profile, session
and response attributes contain special chars and attributes fetch mode is set to HTTP_COOKIE.
(property name: com.sun.identity.agents.config.encode.cookie.special.chars.enable) <br>Hot-swap:
Yes",
    "propertyOrder" : 14000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"clientIpHeader" : {
    "title" : "Client IP Address Header",
    "description" : "HTTP header name that holds the IP address of the client. (property name:
com.sun.identity.agents.config.client.ip.header) <br>Hot-swap: Yes",
    "propertyOrder" : 1000,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"postDataPreservation" : {
    "title" : "POST Data Preservation",
    "description" : "Enables POST data preservation. (property name:
com.sun.identity.agents.config.postdata.preserve.enable) <br> Note that this feature is not supported
in all the web agents. Please refer individual agents documentation for more details. <br>Hot-swap:
Yes",
    "propertyOrder" : 17300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"logoutRedirectUrl" : {
    "title" : "Logout Redirect URL",
    "description" : "User gets redirected to this url after logout. (property name:
com.sun.identity.agents.config.logout.redirect.url). This property should be specified along with the
above Logout URL List.<br>Hot-swap: Yes",
    "propertyOrder" : 22300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
},
"caseInsensitiveUrlComparison" : {
    "title" : "URL Comparison Case Sensitivity Check",
    "description" : "Enforces case insensitivity in both policy and not enforced url evaluation.
(property name: com.sun.identity.agents.config.url.comparison.case.ignore) <br>Hot-swap: Yes",
    "propertyOrder" : 14300,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
},
"sessionAttributeMap" : {
    "title" : "Session Attribute Map",
    "description" : "Maps the session attributes to be populated under
specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping) <br>Hot-swap: Yes <br> Example: <br> To
populate the value of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map
Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
    "propertyOrder" : 15100,
    "required" : true,
    "patternProperties" : {
        ".*" : {

```

```

        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "cdssoUrls" : {
    "title" : "CDSSO Servlet URL",
    "description" : "List of URLs of the available CDSSO controllers that may be used by the Agent
for CDSSO processing. (property name: com.sun.identity.agents.config.cdsso.cdcervlet.url) <br>Hot-
swap: Yes <br> Example: <br> http://host:port/opensso/cdcervlet",
    "propertyOrder" : 17500,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "notEnforcedIps" : {
    "title" : "Not Enforced Client IP List",
    "description" : "No authentication and authorization are required for the requests coming from
these client IP addresses. (property name: com.sun.identity.agents.config.notenforced.ip) <br>Hot-
swap: Yes <br> Examples: <br> 192.18.145.* <br> 192.18.146.123",
    "propertyOrder" : 17200,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "userIdParameter" : {
    "title" : "User ID Parameter",
    "description" : "Agent sets value of User Id to REMOTE_USER server variable. (property name:
com.sun.identity.agents.config.userid.param) <br>Hot-swap: Yes",
    "propertyOrder" : 14600,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "ltpaTokenCookieName" : {
    "title" : "LTPA Token Cookie Name",
    "description" : "The name of the cookie that contains the LTPA token. (property name:
com.sun.identity.agents.config.domino.ltpa.cookie.name)",
    "propertyOrder" : 20700,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "amLoginUrl" : {
    "title" : "OpenAM Login URL",
    "description" : "OpenAM login page URL. (property name:
com.sun.identity.agents.config.login.url) <br>Hot-swap: Yes <br> Example: <br> http://host:port/
opensso/UI/Login",
    "propertyOrder" : 15700,
    "required" : true,
    "items" : {
      "type" : "string"
    }
  }
}

```

```

    },
    "type" : "array",
    "exampleValue" : ""
  },
  "overrideNotificationUrl" : {
    "title" : "Override Notification URL",
    "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the URL with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.notification.url) <br>Hot-swap: Yes",
    "propertyOrder" : 19000,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "overrideRequestProtocol" : {
    "title" : "Override Request URL Protocol",
    "description" : "Set to true if the agent is sitting behind a ssl/tls off-
loader, load balancer, or proxy to override the protocol with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.protocol) <br>Hot-swap: Yes",
    "propertyOrder" : 18700,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "fqdnMapping" : {
    "title" : "FQDN Virtual Host Map",
    "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN to
access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>Hot-
swap: Yes <br> Examples: <br> To map the partial hostname myserver to myserver.mydomain.com: enter
myserver in the Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map
a virtual server rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in
the Map Key field and rst.hostname.com in the Corresponding Map Value field.",
    "propertyOrder" : 16400,
    "required" : true,
    "patternProperties" : {
      ".*" : {
        "type" : "string"
      }
    },
    "type" : "object",
    "exampleValue" : ""
  },
  "fqdnDefault" : {
    "title" : "FQDN Default",
    "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default) <br>Hot-swap: Yes",
    "propertyOrder" : 16300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "agentConnectionTimeout" : {
    "title" : "Agent Connection Timeout",
    "description" : "Timeout period in seconds for an agent connection with OpenAM auth server.
(property name: com.sun.identity.agents.config.auth.connection.timeout) <br>Hot-swap: Yes",
    "propertyOrder" : 19100,
    "required" : true,

```

```

        "type" : "integer",
        "exampleValue" : ""
    },
    "ignorePathInfo" : {
        "title" : "Ignore Path Info in Request URL",
        "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info) <br>Hot-swap: Yes",
        "propertyOrder" : 18600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "ignoreServerCheck" : {
        "title" : "Ignore Server Check",
        "description" : "Agent uses this value to check OpenAM is up before doing a 302 redirect.
(property name: com.sun.identity.agents.config.ignore.server.check) <br>Hot-swap: Yes",
        "propertyOrder" : 15500,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "configurationPollingInterval" : {
        "title" : "Configuration Reload Interval",
        "description" : "Interval in minutes to fetch agent configuration from OpenAM. (property name:
com.sun.identity.agents.config.polling.interval) <br>Hot-swap: No",
        "propertyOrder" : 19500,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
    },
    "userIdParameterType" : {
        "title" : "User ID Parameter Type",
        "description" : "User ID can be fetched from either SESSION and LDAP attributes. (property name:
com.sun.identity.agents.config.userid.param.type) <br>Hot-swap: Yes",
        "propertyOrder" : 14700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "localAuditLogRotation" : {
        "title" : "Rotate Local Audit Log",
        "description" : "Flag to indicate that audit log files should be rotated when reaching a certain
size. (property name: com.sun.identity.agents.config.local.log.rotate) <br>Hot-swap: Yes",
        "propertyOrder" : 21700,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "agentConfigChangeNotificationsEnabled" : {
        "title" : "Agent Configuration Change Notification",
        "description" : "Enable agent to receive notification messages from OpenAM server for
configuration changes. (property name: com.sun.identity.agents.config.change.notification.enable)
<br>Hot-swap: Yes",
        "propertyOrder" : 12100,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    },

```

```

"policyEvaluationApplication" : {
  "title" : "Application",
  "description" : "Which application contains the policies to evaluate with (property name:
org.forgerock.openam.agents.config.policy.evaluation.application) <br>Hot-swap: Yes",
  "propertyOrder" : 21200,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"remoteLogSendInterval" : {
  "title" : "Remote Audit Log Interval",
  "description" : "Periodic interval in minutes in which audit log messages are sent to remote log
file. (property name: com.sun.identity.agents.config.remote.log.interval) <br>Hot-swap: No",
  "propertyOrder" : 21600,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"profileAttributesCookieMaxAge" : {
  "title" : "Profile Attributes Cookie Maxage",
  "description" : "Maxage of attributes cookie headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.maxage) <br>Hot-swap: Yes",
  "propertyOrder" : 17900,
  "required" : true,
  "type" : "integer",
  "exampleValue" : ""
},
"agentUriPrefix" : {
  "title" : "Agent Deployment URI Prefix",
  "description" : "(property name: com.sun.identity.agents.config.agenturi.prefix)<br>Hot-swap:
Yes",
  "propertyOrder" : 15800,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"gotoParameterName" : {
  "title" : "Goto Parameter Name",
  "description" : "Property used only when CDSSO is enabled. Default value should
be changed only when the login URL has a landing page specified <br> Example :
com.sun.identity.agents.config.cdsso.cdcservlet.url = http://host:port/opensso/cdcservlet?
goto=http://agent:port/landing.jsp <br> The parameter is used by the Agent to append the original
request URL to this cdcservlet URL. This parameter is consumed by the landing page to redirect to
the original URL. (property name: com.sun.identity.agents.config.redirect.param) <br>Hot-swap: Yes
<br> Example: com.sun.identity.agents.config.redirect.param = goto2<br> The complete URL sent for
authentication will be <br> http://host:port/opensso/cdcservlet?goto=http://agent:port/landing.jsp?
goto2=http://agent.port/original.jsp",
  "propertyOrder" : 3600,
  "required" : true,
  "type" : "string",
  "exampleValue" : ""
},
"changeProtocolToHttps" : {
  "title" : "Change URL Protocol to https",
  "description" : "If true, avoids IE6 security pop-ups. (property name:
com.sun.identity.agents.config.iis.owa.enable.change.protocol)",
  "propertyOrder" : 20300,
  "required" : true,
  "type" : "boolean",

```

```

    "exampleValue" : ""
  },
  "encodeUrlSpecialCharacters" : {
    "title" : "Encode URL's Special Characters",
    "description" : "Encodes the url which has special characters before doing policy evaluation.
(property name: com.sun.identity.agents.config.encode.url.special.chars.enable) <br>Hot-swap: Yes",
    "propertyOrder" : 18500,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "useLtpaToken" : {
    "title" : "Use LTPA token",
    "description" : "Set to true if agent needs to use LTPA Token. (property name:
com.sun.identity.agents.config.domino.ltpa.enable)",
    "propertyOrder" : 20600,
    "required" : true,
    "type" : "boolean",
    "exampleValue" : ""
  },
  "policyEvaluationRealm" : {
    "title" : "Realm",
    "description" : "Which realm to start evaluating from (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm) <br>Hot-swap: Yes",
    "propertyOrder" : 21100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

## 1.150. WindowsDesktopSsoModule

### 1.150.1. Realm Operations

Resource path: `/realm-config/authentication/modules/windowsdesktopsso`

Resource version: `1.0`

#### 1.150.1.1. create

Usage:

```
am> create WindowsDesktopSsoModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "returnPrincipalWithDomainName" : {
      "title" : "Return Principal with Domain Name",
      "description" : "Returns the fully qualified name of the authenticated user rather than just the username.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "principalName" : {
      "title" : "Service Principal",
      "description" : "The name of the Kerberos principal used during authentication<br><br>This principal must match the name used in the keytab file created from the Active Directory server.<br>>The format of the field is as follows:<br><br><code>HTTP/openam.forgerock.com@AD_DOMAIN.COM</code>",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "kerberosRealm" : {
      "title" : "Kerberos Realm",
      "description" : "The name of the Kerberos (Active Directory) realm used for authentication",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedKerberosRealms" : {
      "title" : "Trusted Kerberos realms",
      "description" : "List of trusted Kerberos realms for User Kerberos tickets.<br><br>If realms are configured, then Kerberos tickets are only accepted if the realm part of the UserPrincipalName of the Users Kerberos ticket matches a realm from the list.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "lookupUserInRealm" : {
```

```

        "title" : "Search for the user in the realm",
        "description" : "Validate that the user has a matched user profile configured in the data
store.<br><br>If this option is enabled, the module validates whether the account corresponds to a
user profile in the Data Store for the realm. The attributes to perform the search are configured
under <i>Access Control > Realm Name > Authentication > All Core settings > Alias Search Attribute
Name</i>.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "keytabFileName" : {
        "title" : "Keytab File Name",
        "description" : "The path of the AD keytab file<br><br>This is the absolute pathname of the AD
keytab file. The keytab file is generated by the Active Directory server.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "kerberosServerName" : {
        "title" : "Kerberos Server Name",
        "description" : "The hostname/IP address of the Kerberos (Active Directory) server.",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

### 1.150.1.2. delete

Usage:

```
am> delete WindowsDesktopSsoModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.150.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --realm Realm --actionName getAllTypes
```



#### 1.150.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --realm Realm --actionName getCreatableTypes
```

#### 1.150.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --realm Realm --actionName nextdescendents
```

#### 1.150.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query WindowsDesktopSsoModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

#### 1.150.1.7. read

Usage:

```
am> read WindowsDesktopSsoModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

#### 1.150.1.8. update

Usage:

```
am> update WindowsDesktopSsoModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "returnPrincipalWithDomainName" : {
      "title" : "Return Principal with Domain Name",
      "description" : "Returns the fully qualified name of the authenticated user rather than just the username.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "principalName" : {
      "title" : "Service Principal",
      "description" : "The name of the Kerberos principal used during authentication<br><br>This principal must match the name used in the keytab file created from the Active Directory server.<br>>The format of the field is as follows:<br><br><code>HTTP/openam.forgerock.com@AD_DOMAIN.COM</code>",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "kerberosRealm" : {
      "title" : "Kerberos Realm",
      "description" : "The name of the Kerberos (Active Directory) realm used for authentication",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedKerberosRealms" : {
      "title" : "Trusted Kerberos realms",
      "description" : "List of trusted Kerberos realms for User Kerberos tickets.<br><br>If realms are configured, then Kerberos tickets are only accepted if the realm part of the UserPrincipalName of the Users Kerberos ticket matches a realm from the list.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "array",
      "exampleValue" : []
    }
  }
}
```

```

        "propertyOrder" : 700,
        "required" : true,
        "items" : {
            "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
    },
    "lookupUserInRealm" : {
        "title" : "Search for the user in the realm",
        "description" : "Validate that the user has a matched user profile configured in the data store.<br><br>If this option is enabled, the module validates whether the account corresponds to a user profile in the Data Store for the realm. The attributes to perform the search are configured under <i>Access Control > Realm Name > Authentication > All Core settings > Alias Search Attribute Name</i>.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
    },
    "keytabFileName" : {
        "title" : "Keytab File Name",
        "description" : "The path of the AD keytab file<br><br>This is the absolute pathname of the AD keytab file. The keytab file is generated by the Active Directory server.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    },
    "kerberosServerName" : {
        "title" : "Kerberos Server Name",
        "description" : "The hostname/IP address of the Kerberos (Active Directory) server.",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
    }
}
}
}

```

## 1.150.2. Global Operations

Resource path: `/global-config/authentication/modules/windowsdesktopsso`

Resource version: `1.0`

### 1.150.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --global --actionName getAllTypes
```

### 1.150.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --global --actionName getCreatableTypes
```

### 1.150.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --global --actionName nextdescendents
```

### 1.150.2.4. read

Usage:

```
am> read WindowsDesktopSsoModule --global
```

### 1.150.2.5. update

Usage:

```
am> update WindowsDesktopSsoModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "kerberosServerName" : {
          "title" : "Kerberos Server Name",
          "description" : "The hostname/IP address of the Kerberos (Active Directory) server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "returnPrincipalWithDomainName" : {
          "title" : "Return Principal with Domain Name",
          "description" : "Returns the fully qualified name of the authenticated user rather than just the username.",
          "propertyOrder" : 500,
          "required" : true,

```

```

    "type" : "boolean",
    "exampleValue" : ""
  },
  "trustedKerberosRealms" : {
    "title" : "Trusted Kerberos realms",
    "description" : "List of trusted Kerberos realms for User Kerberos tickets.<br><br>If realms
are configured, then Kerberos tickets are only accepted if the realm part of the UserPrincipalName of
the Users Kerberos ticket matches a realm from the list.",
    "propertyOrder" : 700,
    "required" : true,
    "items" : {
      "type" : "string"
    },
    "type" : "array",
    "exampleValue" : ""
  },
  "principalName" : {
    "title" : "Service Principal",
    "description" : "The name of the Kerberos principal used during authentication<br><br>This
principal must match the name used in the keytab file created from the Active Directory server.<br>
>The format of the field is as follows:<br><br><code>HTTP/openam.forgerock.com@AD_DOMAIN.COM</
code>",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationLevel" : {
    "title" : "Authentication Level",
    "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
    "propertyOrder" : 600,
    "required" : true,
    "type" : "integer",
    "exampleValue" : ""
  },
  "kerberosRealm" : {
    "title" : "Kerberos Realm",
    "description" : "The name of the Kerberos (Active Directory) realm used for authentication",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "keytabFileName" : {
    "title" : "Keytab File Name",
    "description" : "The path of the AD keytab file<br><br>This is the absolute pathname of the
AD keytab file. The keytab file is generated by the Active Directory server.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "lookupUserInRealm" : {
    "title" : "Search for the user in the realm",
    "description" : "Validate that the user has a matched user profile configured in the data
store.<br><br>If this option is enabled, the module validates whether the account corresponds to a
user profile in the Data Store for the realm. The attributes to perform the search are configured

```

```
under <i>Access Control > Realm Name > Authentication > All Core settings > Alias Search Attribute
Name</i>.",
  "propertyOrder" : 800,
  "required" : true,
  "type" : "boolean",
  "exampleValue" : ""
},
"type" : "object",
"title" : "Realm Defaults"
}
}
```

## 1.151. WindowsNtModule

### 1.151.1. Realm Operations

Resource path: `/realm-config/authentication/modules/windowsnt`

Resource version: `1.0`

#### 1.151.1.1. create

Usage:

```
am> create WindowsNtModule --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "authenticationHost" : {
```

```

    "title" : "Authentication Host",
    "description" : "The name of the Windows NT Domain Controller.",
    "propertyOrder" : 200,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "sambaConfigurationFileName" : {
    "title" : "Samba Configuration File Name",
    "description" : "The path to the Samba configuration file.<br><br>The Windows NT authentication module uses the <code>smbclient</code> command to validate the user credentials against the Windows domain controller. <br><br>For example: <code>/opt/openam/smb.conf</code><br><br><i>NB </i>The <code>smbclient</code> command must be available in the <code>PATH</code> environmental variable associated with OpenAM.",
    "propertyOrder" : 300,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  },
  "authenticationDomain" : {
    "title" : "Authentication Domain",
    "description" : "The name of the Windows Domain used for authentication",
    "propertyOrder" : 100,
    "required" : true,
    "type" : "string",
    "exampleValue" : ""
  }
}
}

```

### 1.151.1.2. delete

Usage:

```
am> delete WindowsNtModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.151.1.3. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WindowsNtModule --realm Realm --actionName getAllTypes
```

### 1.151.1.4. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WindowsNtModule --realm Realm --actionName getCreatableTypes
```

### 1.151.1.5. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WindowsNtModule --realm Realm --actionName nextdescendents
```

### 1.151.1.6. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query WindowsNtModule --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.151.1.7. read

Usage:

```
am> read WindowsNtModule --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.151.1.8. update

Usage:

```
am> update WindowsNtModule --realm Realm --id id --body body
```

Parameters:



--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each authentication module has an authentication level that can be used to indicate the level of security associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "authenticationHost" : {
      "title" : "Authentication Host",
      "description" : "The name of the Windows NT Domain Controller.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sambaConfigurationFileName" : {
      "title" : "Samba Configuration File Name",
      "description" : "The path to the Samba configuration file.<br><br>The Windows NT authentication module uses the <code>smbclient</code> command to validate the user credentials against the Windows domain controller. <br><br>For example: <code>/opt/openam/smb.conf</code><br><br><i>NB </i>The <code>smbclient</code> command must be available in the <code>PATH</code> environmental variable associated with OpenAM.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationDomain" : {
      "title" : "Authentication Domain",
      "description" : "The name of the Windows Domain used for authentication",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.151.2. Global Operations

Resource path: </global-config/authentication/modules/windowsnt>

Resource version: 1.0

### 1.151.2.1. getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WindowsNtModule --global --actionName getAllTypes
```

### 1.151.2.2. getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WindowsNtModule --global --actionName getCreatableTypes
```

### 1.151.2.3. nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WindowsNtModule --global --actionName nextdescendents
```

### 1.151.2.4. read

Usage:

```
am> read WindowsNtModule --global
```

### 1.151.2.5. update

Usage:

```
am> update WindowsNtModule --global --body body
```

Parameters:

**--body**

The resource in JSON format, described by the following JSON schema:

```
{  
  "type" : "object",
```

```

"properties" : {
  "defaults" : {
    "properties" : {
      "authenticationHost" : {
        "title" : "Authentication Host",
        "description" : "The name of the Windows NT Domain Controller.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "sambaConfigurationFileName" : {
        "title" : "Samba Configuration File Name",
        "description" : "The path to the Samba configuration file.<br><br>The Windows NT
authentication module uses the <code>smbclient</code> command to validate the user credentials
against the Windows domain controller. <br><br>For example: <code>/opt/openam/smb.conf</code><br>
><br><i>NB </i>The <code>smbclient</code> command must be available in the <code>PATH</code>
environmental variable associated with OpenAM.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "authenticationLevel" : {
        "title" : "Authentication Level",
        "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default). ",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "authenticationDomain" : {
        "title" : "Authentication Domain",
        "description" : "The name of the Windows Domain used for authentication",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    },
    "type" : "object",
    "title" : "Realm Defaults"
  }
}
}

```

## 1.152. WsEntity

### 1.152.1. Realm Operations

Resource path: </realm-config/federation/entityproviders/ws>

Resource version: 1.0

## 1.152.1.1. create

Usage:

```
am> create WsEntity --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

## 1.152.1.2. delete

Usage:

```
am> delete WsEntity --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.152.1.3. query

Get the full list of instances of this collection. This query only supports `\_queryFilter=true` filter.

Usage:

```
am> query WsEntity --realm Realm --filter filter
```

Parameters:

**--filter**

A CREST formatted query filter, where "true" will query all.

### 1.152.1.4. read

Usage:

```
am> read WsEntity --realm Realm --id id
```

Parameters:

**--id**

The unique identifier for the resource.

### 1.152.1.5. update

Usage:

```
am> update WsEntity --realm Realm --id id --body body
```

Parameters:

**--id**

The unique identifier for the resource.

**--body**

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

# Appendix A. Getting Support

For more information or resources about OpenAM and ForgeRock Support, see the following sections:

## A.1. Accessing Documentation Online

ForgeRock publishes comprehensive documentation online:

- The ForgeRock [Knowledge Base](#) offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.
- ForgeRock core documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

Core documentation therefore follows a three-phase review process designed to eliminate errors:

- Product managers and software architects review project documentation design with respect to the readers' software lifecycle needs.
- Subject matter experts review proposed documentation changes for technical accuracy and completeness with respect to the corresponding software.
- Quality experts validate implemented documentation changes for technical accuracy, completeness in scope, and usability for the readership.

The review process helps to ensure that documentation published for a ForgeRock release is technically accurate and complete.

Fully reviewed, published core documentation is available at <http://backstage.forgerock.com/>. Use this documentation when working with a ForgeRock Identity Platform release.

## A.2. Joining the ForgeRock Community

Visit the [Community resource center](#) where you can find information about each project, download trial builds, browse the resource catalog, ask and answer questions on the forums, find community events near you, and find the source code for open source software.

## A.3. Getting Support and Contacting ForgeRock

ForgeRock provides support services, professional services, classes through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see <https://www.forgerock.com>.

ForgeRock has staff members around the globe who support our international customers and partners. For details, visit <https://www.forgerock.com>, or send an email to ForgeRock at [info@forgerock.com](mailto:info@forgerock.com).