ORACLE
Consulting

Identity Access Services

P20 Access Manager Configuration

Release 2.0.0

ORACLE

Identity Access Services

P20 Access Manager Configuration

Release 2.0.0

by Sophie Strecke, Melinda Nath-Richter, Tomas Sebo, Dieter Steding, Jovan Lakic, and Sylvert Bernet

Table of Contents

Preface

Audience

This document is intended for people who deal with the administration of the Oracle Identity and Access Management infrastructure.

Confidentiality

The material contained in this documentation represents proprietary, confidential information pertaining to Oracle products and methods.

The audience agrees that the information in this documentation shall not be disclosed outside of Oracle, and shall not be duplicated, used, or disclosed for any purpose other than to evaluate this procedure.

Notational Conventions

The key words **MUST**, **MUST NOT**, **REQUIRED**, **SHALL**, **SHALL NOT**, **SHOULD**, **SHOULD NOT**, **RECOMMENDED**, **MAY**, and **OPTIONAL** in this document are to be interpreted as described in *[RFC2119]* These key words are capitalized when used to unambiguously specify requirements of the protocol or application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

Typographical Conventions

The following table describes the typographic changes that are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Symbol Conventions

The following table explains symbols that might be used in this document.

Convention	Meaning
[ ]	Contains optional arguments and command options.
{ | }	Contains a set of choices for a required command option.
${ }	Indicates a variable reference.
-	Joins simultaneous multiple keystrokes.
+	Joins consecutive multiple keystrokes.

Convention	Meaning
>	Indicates menu item selection in a graphical user interface.

Related Documents

For information about installing and using Oracle Identity and Access Management, visit the following Oracle Help Center pages:

No.	Document
1	*Install Oracle Identity Management*
2	*Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*
3	*Performing Self Service Tasks with Oracle Identity Governance*

Requirements

Hardware and Software Certification

The platform-specific hardware and software requirements listed in this document are current as of the date this document was created. As new platforms and operating systems may be certified after this document is published, it is recommended that you consult the certification matrix on Oracle Technology Network. There you will find the latest statements on certified platforms and operating systems.

Die jeweilige Zertifizierungsmatrix für Produkte der Oracle Identity und Access Management Suite sind unter folgenden URLs verfügbar:

Review of Requirements

Required Versions

Component	Version
Oracle Java Development Kit	JDK 1.8.0_133 or higher
Oracle Infrastruktur	Oracle® WebLogic 12c (12.2.1.3.0)
Oracle Datenbank	Oracle® RDBMS 12c (12.2.0.1.0 or higher
Oracle Access Manager	Oracle® Access Manager 12c Release 12.2.1.4.0

Required Patches

Component	Version
Oracle Infrastruktur	FMW PLATFORM 12.2.1.4.0 SPU FOR APRCPU2021
Oracle Infrastruktur	FMW THIRDPARTY BUNDLE PATCH 12.2.1.4.230628
Oracle Infrastruktur	WLS PATCH SET UPDATE 12.2.1.4.230702
Oracle Access Manager	OAM Bundle Patch 12.2.1.4.230628 Generic for all Server Platforms (Oracle® Access Management Bundle Patch 12.2.1.4.0 (ID:35546625)

Identity Store Configuration

General

Parameter	Value
Store Name	*FederationIdentityStore*
Store Type	*OUD: Oracle Unified Directory*
Description	*Identity Store used to translate external User Principal Names to internal User Principal Names.*
Enable SSL	*<unchecked>*
Use Native ID Store Settings	*<unchecked>*
Prefetched Attributes	*uid,mail,cn,sn,givenName,krbPrincipalName*

Location and Credentials

Parameter	Value
Location	*fedvip.zds.bka.bund.de:7389*
Bind DN	*uid=oamadmin,cn=System,dc=bka,dc=bund,dc=de*
Password	*<see wallet >*

Users and Groups

Parameter	Value
Login ID Attribute	*cn*
User Password Attribute	*userPassword*
User Search Base	*ou=App,dc=bka,dc=bund,dc=de*
User Filter Object Classes	*inetOrgPerson*
Group Name Attribute	*cn*
Group Search Base	*ou=Gropus,dc=bka,dc=bund,dc=de*
Group Filter Classes	*groupOfUniqueNames*
Enable Group Membership Cache	*<unchecked>*

Connection Details

Parameter	Value
Minimum Pool Size	*50*
Maximum Pool Size	*100*
Wait Timeout (in milliseconds)	*1000*
Inactivity Timeout (in seconds)	*0*

Parameter	Value
Results time limit (in seconds)	*0*
Retry Count	*3*
Referral Policy	*<leer>*

Password Management

Password management remains disabled.

Host Identifier

FederationAgent

General

Parameter	Value
Name	*FederationAgent*
Description	*The Host Name variations that can occur accessing resources during authentication and authorization flows.*

Host Name Variation

Host Name	Port
sso.cinnamonstar.oam	*80*
sso.cinnamonstar.oam	*443*
FederationIdentityAgent	*<empty>*

FederationConfig

General

Parameter	Value
Name	*FederationConfig*
Description	*The Host Name variations that can occur accessing resources belonging to Identity Config Domain.*

Host Name Variation

Host Name	Port
icd.cinnamonstar.oam	*80*
icd.cinnamonstar.oam	*443*

FederationAccess

General

Parameter	Value
Name	*FederationAccess*
Description	*The Host Name variations that can occur accessing resources belonging to Identity Access Domain.*

Host Name Variation

Host Name	Port
iad.cinnamonstar.oam	*80*
iad.cinnamonstar.oam	*443*

FederationIdentity

General

Parameter	Value
Name	*FederationIdentity*
Description	*The Host Name variations that can occur accessing resources belonging to Identity Governance Domain.*

Host Name Variation

Host Name	Port
igd.cinnamonstar.oam	*80*
igd.cinnamonstar.oam	*443*

FederationService

General

Parameter	Value
Name	*FederationIdentity*
Description	*The Host Name variations that can occur accessing resources belonging to Identity Governance Domain.*

Host Name Variation

Host Name	Port
uid.cinnamonstar.oam	*443*
igs.cinnamonstar.oam	*443*

Authentication Module

Standard

Parameter	Value
Name	*FederationDirectoryProvider*
User Identity Store	*FederationIdentityStore*

OpenIDIdentityProviderLocal

Parameter	Value
Name	*OpenIDIdentityProviderLocal*
Description	*Mechanism to authenticate a user through an OpenIDConnect 3-leg flow using the FederationIdentityStore to identify the authenticated user.*

Steps

Challenge

Parameter	Value
Step Name	*UserChallenge*
Description	*Challenging a user to authenticate leveraging an OpenIDConnect 3-leg flow.*
Plug-in Name	*OpenIDConnectPlugin*
id_domain	*SecureDomain2*
ouath_client_secret	*<see wallet>*
token_end_point	*<empty>*
authz_end_point	*<empty>*
require_proxy	*<empty>*
provider	*<empty>*
scope	*<empty>*
userinfo_end_point	*<empty>*
additional_parameters	*<empty>*
discovery_url	*http://sso.cinnamonstar.oam*
username_attr	*sub*
oauth_client_id	*igsservice*

Identification

Parameter	Value
Step Name	*UserIdentification*

Parameter	Value
Description	*Identity the user in the FederationIdentityStore.*
Plug-in Name	*UserIdentificationPlugIn*
KEY_IDENTITY_STORE_REF	*FederationIdentityStore*
KEY_LDAP_FILTER	*<empty>*
KEY_SEARCH_BASE_URL	*<empty>*

Flow

Initial Step: *UserChallenge*

Name	On Success	On Failure	On Error
UserChallenge	*UserIdentification*	*failure*	*failure*
UserIdentification	*success*	*failure*	*failure*

OpenIDIdentityProviderExternal

Parameter	Value
Name	*OpenIDIdentityProviderExternal*
Description	*Mechanism to authenticate a user through an OpenIDConnect 3-leg flow using an external Identity Provider to authenticate users and the FederationIdentityStore to identify such users.*

Steps

Challenge

Parameter	Value
Step Name	*UserChallenge*
Description	*Challenging a user to authenticate leveraging an OpenIDConnect 3-leg flow.*
Plug-in Name	*OpenIDConnectPlugin*
id_domain	*PlayGroundDomain*
ouath_client_secret	*<see wallet>*
token_end_point	*<empty>*
authz_end_point	*<empty>*
require_proxy	*<empty>*
provider	*oam*
scope	*<empty>*
userinfo_end_point	*<empty>*
additional_parameters	*<empty>*
discovery_url	*http://sso.cinnamonstar.net:1080*
username_attr	*sub*

Parameter	Value
oauth_client_id	*PlayGroundClient*

Identification

Parameter	Value
Step Name	*UserIdentification*
Description	*Identity the user in the FederationIdentityStore.*
Plug-in Name	*UserIdentificationPlugIn*
KEY_IDENTITY_STORE_REF	*FederationIdentityStore*
KEY_LDAP_FILTER	*(&(objectClass=inetOrgPerson)(| (uid={KEY_USERNAME}) (mail={KEY_USERNAME})))*
KEY_SEARCH_BASE_URL	*<empty>*

Flow

Initial Step: *UserChallenge*

Name	On Success	On Failure	On Error
UserChallenge	*UserIdentification*	*failure*	*failure*
UserIdentification	*success*	*failure*	*failure*

Authentication Schemes

FederationIdentityScheme

Parameter	Value
Name	*FederationIdentityScheme*
Description	*Leveraging FederationIdentityModule to authenticate a user in the FederationIdentityStore.*
Authentication Level	*2*
Default	*<unchecked>*
Challenge Method	*FORM*
Challenge Redirect URL	*/oam/server*
Authentication Module	*FederationIdentityModule*
Challenge URL	*/pages/login.jsp*
Context Type	*default*
Context Value	*/oam*
Challenge Parameter	*<empty>*

OpenIDExternalScheme

Parameter	Value
Name	*OpenIDExternalScheme*
Description	*Authentication Scheme leveraging OpenID Connect functionality.*
Authentication Level	*2*
Default	*<unchecked>*
Challenge Method	*FORM*
Challenge Redirect URL	*/oam/server*
Authentication Module	*OpenIDIdentityProviderExternal*
Challenge URL	*/pages/login.jsp*
Context Type	*default*
Context Value	*/oam*
Challenge Parameter	*IS_OAUTH_OAM_SSO_LINK_ENABLED=true IS_OAUTH_USER_ASSERTION_ENABLED=true OAUTH_TOKEN_RESPONSE_TYPE=header initial_command=NONE*

OpenIDLocalScheme

Parameter	Value
Name	*OpenIDLocalScheme*

Parameter	Value
Description	*Authentication Scheme leveraging OpenID Connect functionality.*
Authentication Level	*2*
Default	*<unchecked>*
Challenge Method	*FORM*
Challenge Redirect URL	*/oam/server*
Authentication Module	*OpenIDIdentityProviderLocal*
Challenge URL	*/p20*
Context Type	*external*
Challenge Parameter	*<empty>*

PlayGroundDirectoryScheme

Parameter	Value
Name	*PlayGroundDirectoryScheme*
Description	*Authentication Scheme leveraging FederationIdentityStore for autehntication purpose.*
Authentication Level	*2*
Default	*<unchecked>*
Challenge Method	*FORM*
Challenge Redirect URL	*/oam/server*
Authentication Module	*PlayGroundDirectoryProvider*
Challenge URL	*/p20*
Context Type	*external*
Challenge Parameter	*<empty>*

Application Domains

Single Sign On Domain

Summary

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Parameter	Value
Name	*Single Sign On Domain*
Description	*The security policies enabling Access Manager Agent to protect resources involved in the authentication and authorization flows.*
Session Idle Timeout (minutes)	*0*
Enable Policy Ordering	*<uncheched*

Authentication Policies

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

Unprotected Resources

Parameter	Value
Name	*authn-public*
Description	*Authenticate access to public resources in Single Sign On Domain.*
Authentication Scheme	*AnonymousScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Protected Resources

Parameter	Value
Name	*authn-protected*
Description	*Authenticate access to protected resources in Single Sign On Domain.*
Authentication Scheme	*FederationIdentityScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Authorization Policies

Authorization policy contains a set of conditions that define whether a user should be permitted or denied access to the resources protected by the policy. Authorization rules and conditions apply to all resources within a specific Authorization policy.

Unprotected Resources

Parameter	Value
Name	*authz-public*
Description	*Authorize access to public resources in Single Sign On Domain.*
Success URL	*<empty>*
Failure URL	*<empty>*

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

There are no responses defined in this policy.

Protected Resources

Conditions

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

Name	Type	Value
oam_remote_user	*Header*	*$user.userid*

Resources

Define a Resource and the URL prefix that identifies the resource (document or entity) stored on a server. Individual resource URLs need not be unique across domains, but the combination of a resource URL, Query String, and a host identifier must be unique across domains.

/oam

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover all of the resources being accessed in the application Access Manager Challenge Response operations in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/oam/**
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/oamsso

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover all of the resources being accessed in the Access Manager Single Sign On flows in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/oamsso/**
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/oamfed

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover all of the resources being accessed in the Identity Federation Services provided by the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/oamfed/**
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/otpfp

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover all of the resources being accessed in the Access Manager Forgotten Password capabilities in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/otpfp/**
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/.well-known

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover all of the resources being accessed in the OpenID Connect endpoint discovery provided by OAuth in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/.well-known/**
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/oauth2/rest

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover the Runtime REST APIs for 2-legged and 3-legged OAuth Services flows in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/oauth2/rest/**
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/ecc

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover all the resources being accessed in the Access Manager Embedded Credential Collector forms in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/ecc/***
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/p20

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover all the resources being accessed in the Access Manager Embedded Credential Collector forms in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/p20/***
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/favicon.ico

Parameter	Value
Type	*HTTP*
Description	*Context URL to the page bookmark icon in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/favicon.ico*
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/p20/consent

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover user approval of a 3-legged OAuth authentication flow in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/p20/consent*
Operations Available	*All*
Protection Level	*Protected*
Authentication Policy	*authn-protected*
Authorization Policy	*authz-protected*

/oam/pages/consent.jsp

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover user approval of a 3-legged OAuth authentication flow in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/oam/pages/consent.jsp*
Operations Available	*All*
Protection Level	*Protected*
Authentication Policy	*authn-protected*
Authorization Policy	*authz-protected*

/oauth2/rest/approval/skip

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover user approval of a 3-legged OAuth authentication flow in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/oauth2/rest/approval*
Operations Available	*All*
Protection Level	*Protected*
Authentication Policy	*authn-protected*
Authorization Policy	*authz-protected*

/oauth2/rest/approval

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover user approval of a 3-legged OAuth authentication flow in the Single Sign On Domain.*
Host Identifier	*FederationAgent*
Resource URL	*/oauth2/rest/approval*
Operations Available	*All*
Protection Level	*Protected*
Authentication Policy	*authn-protected*
Authorization Policy	*authz-protected*

Identity Config Domain

Summary

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Parameter	Value
Name	*Identity Config Domain*
Description	*The security policies enabling Access Manager Agent to protect resources deployed in the Identity Config Domain.*
Session Idle Timeout (minutes)	*0*
Enable Policy Ordering	*<uncheched*

Authentication Policies

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

Unprotected Resources

Parameter	Value
Name	*authn-public*
Description	*Authenticate access to public resources in Identity Config Domain.*
Authentication Scheme	*AnonymousScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Protected Resources

Parameter	Value
Name	*authn-protected*
Description	*Authenticate access to public resources in Identity Config Domain.*
Authentication Scheme	*FederationIdentityScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Authorization Policies

Authorization policy contains a set of conditions that define whether a user should be permitted or denied access to the resources protected by the policy. Authorization rules and conditions apply to all resources within a specific Authorization policy.

Unprotected Resources

Parameter	Value
Name	*authz-public*
Description	*Authorize access to public resources in Identity Config Domain.*
Success URL	*<empty>*
Failure URL	*<empty>*

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

There are no responses defined in this policy.

Protected Resources

Conditions

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

Name	Type	Value
oam_remote_user	*Header*	*$user.userid*

Resources

Define a Resource and the URL prefix that identifies the resource (document or entity) stored on a server. Individual resource URLs need not be unique across domains, but the combination of a resource URL, Query String, and a host identifier must be unique across domains.

Identity Access Domain

Summary

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Parameter	Value
Name	*Identity Access Domain*
Description	*The security policies enabling Access Manager Agent to protect resources deployed in the Identity Access Domain.*
Session Idle Timeout (minutes)	*0*
Enable Policy Ordering	*<unchecked*

Authentication Policies

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

Unprotected Resources

Parameter	Value
Name	*authn-public*
Description	*Authenticate access to public resources in Identity Access Domain.*
Authentication Scheme	*AnonymousScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Protected Resources

Parameter	Value
Name	*authn-protected*
Description	*Authenticate access to public resources in Identity Access Domain.*

Parameter	Value
Authentication Scheme	*FederationIdentityScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Authorization Policies

Authorization policy contains a set of conditions that define whether a user should be permitted or denied access to the resources protected by the policy. Authorization rules and conditions apply to all resources within a specific Authorization policy.

Unprotected Resources

Parameter	Value
Name	*authz-public*
Description	*Authorize access to public resources in Identity Access Domain.*
Success URL	*<empty>*
Failure URL	*<empty>*

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

There are no responses defined in this policy.

protected Resources

Conditions

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

Name	Type	Value
oam_remote_user	*Header*	*$user.userid*

Resources

Define a Resource and the URL prefix that identifies the resource (document or entity) stored on a server. Individual resource URLs need not be unique across domains, but the combination of a resource URL, Query String, and a host identifier must be unique across domains.

/console

Parameter	Value
Type	*HTTP*
Description	*Context URL to the WebLogic Administration Console in the Identity Access Domain.*
Host Identifier	*FederationAccess*
Resource URL	*/console/**
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/em

Parameter	Value
Type	*HTTP*
Description	*Context URL to the Fusion Middleware Control in the Identity Access Domain.*
Host Identifier	*FederationAccess*
Resource URL	*/em/**
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/oamconsole

Parameter	Value
Type	*HTTP*
Description	*Context URL to the Access Manager Configuration Console in the Identity Access Domain.*
Host Identifier	*FederationAccess*
Resource URL	*/oamconsole/**
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/favicon.ico

Parameter	Value
Type	*HTTP*
Description	*Context URL to the page bookmark icon in the Identity Access Domain.*
Host Identifier	*FederationAccess*
Resource URL	*/favicon.ico*
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/access

Parameter	Value
Type	*HTTP*
Description	*Context URL to the Policy Manager Console in the Identity Access Domain.*
Host Identifier	*FederationAccess*
Resource URL	*/access/***
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/oudsm

Parameter	Value
Type	*HTTP*
Description	*Context URL to the Directory Service Manager Console in the Identity Access Domain.*
Host Identifier	*FederationAccess*
Resource URL	*/oudsm/***
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/oam

Parameter	Value
Type	*HTTP*
Description	*Context URL to the Access Manager Services in the Identity Access Domain.*

Parameter	Value
Host Identifier	*FederationAccess*
Resource URL	*/oam/**
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/opss

Parameter	Value
Type	*HTTP*
Description	*Context URL to the Platform Security Services in the Identity Access Domain.*
Host Identifier	*FederationAccess*
Resource URL	*/opss/**
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/iam

Parameter	Value
Type	*HTTP*
Description	*Context URL to the Access Manager Administrationin the Identity Access Domain.*
Host Identifier	*FederationAccess*
Resource URL	*/iam/**
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

Identity Governance Domain

Summary

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Parameter	Value
Name	*Identity Service Domain*

Parameter	Value
Description	*The security policies enabling Access Manager Agent to protect resources deployed in the Identity Service Domain.*
Session Idle Timeout (minutes)	*0*
Enable Policy Ordering	*<uncheched*

Authentication Policies

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

Unprotected Resources

Parameter	Value
Name	*authn-public*
Description	*Authenticate access to public resources in Identity Identity Domain.*
Authentication Scheme	*AnonymousScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Protected Resources

Parameter	Value
Name	*authn-protected*
Description	*Authenticate access to public resources in Identity Governance Domain.*
Authentication Scheme	*FederationIdentityScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Authorization Policies

Authorization policy contains a set of conditions that define whether a user should be permitted or denied access to the resources protected by the policy. Authorization rules and conditions apply to all resources within a specific Authorization policy.

Unprotected Resources

Parameter	Value
Name	*authz-public*
Description	*Authorize access to public resources in Identity Governance Domain.*
Success URL	*<empty>*
Failure URL	*<empty>*

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

There are no responses defined in this policy.

Protected Resources

Conditions

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

Name	Type	Value
oam_remote_user	*Header*	*$user.userid*

Resources

Define a Resource and the URL prefix that identifies the resource (document or entity) stored on a server. Individual resource URLs need not be unique across domains, but the combination of a resource URL, Query String, and a host identifier must be unique across domains.

Identity Service Domain

Summary

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Parameter	Value
Name	*Identity Service Domain*
Description	*The security policies enabling Access Manager Agent to protect resources deployed in the Identity Service Domain.*
Session Idle Timeout (minutes)	*0*
Enable Policy Ordering	*<uncheched*

Authentication Policies

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

Unprotected Resources

Parameter	Value
Name	*authn-public*
Description	*Authenticate access to public resources in Identity Service Domain.*
Authentication Scheme	*AnonymousScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Protected Resources

Parameter	Value
Name	*authn-protected*
Description	*Authenticate access to protected resources in Identity Service Domain leveraging an OpenIdConnect 3-leg flow.*
Authentication Scheme	*PlayGroundDirectoryScheme*
Success URL	*<empty>*
Failure URL	*<empty>*

Authorization Policies

Authorization policy contains a set of conditions that define whether a user should be permitted or denied access to the resources protected by the policy. Authorization rules and conditions apply to all resources within a specific Authorization policy.

Unprotected Resources

Parameter	Value
Name	*authz-public*
Description	*Authorize access to public resources in Identity Service Domain.*
Success URL	*<empty>*
Failure URL	*<empty>*

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

There are no responses defined in this policy.

Protected Resources

Conditions

Conditions

Name	Type	Description
TRUE	*True*	*This condition always evaluates to true.*

Rules

Rule Mode	Allow Rule	Deny Rule
Simple	*TRUE(True)*	*<empty>*

Responses

Name	Type	Value
oam_remote_user	*Header*	*$user.userid*

Resources

Define a Resource and the URL prefix that identifies the resource (document or entity) stored on a server. Individual resource URLs need not be unique across domains, but the combination of a resource URL, Query String, and a host identifier must be unique across domains.

/igs

Parameter	Value
Type	*HTTP*
Description	*Context URL to the REST service API the Identity Service Domain.*
Host Identifier	*FederationService*
Resource URL	*/igs/**
Operations Available	*All*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/

Parameter	Value
Type	*HTTP*
Description	*Context URL to the administration the Identity Service Domain.*

Parameter	Value
Host Identifier	*FederationService*
Resource URL	*/uid/**
Operations Available	*All*
Protection Level	*Protected*
Authentication Policy	*authn-protected*
Authorization Policy	*authn-protected*

/favicon.ico

Parameter	Value
Type	*HTTP*
Description	*Context URL to the page bookmark icon in the Identity Service Domain.*
Host Identifier	*FederationService*
Resource URL	*/favicon.ico*
Operations Available	*GET*
Protection Level	*Excluded*
Authentication Policy	*<empty>*
Authorization Policy	*<empty>*

/

Parameter	Value
Type	*HTTP*
Description	*Context URL to cover all resources.*
Host Identifier	*FederationService*
Resource URL	*/**
Operations Available	*All*
Protection Level	*Protected*
Authentication Policy	*authn-protected*
Authorization Policy	*authn-protected*