



OpenAM Release Notes

Version 12.0.0

Mark Craig
Mike Jang
Vanessa Richie

ForgeRock AS
33 New Montgomery St.,
Suite 1500
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Copyright © 2011-2014 ForgeRock AS

Abstract

Notes covering OpenAM prerequisites, fixes, known issues. OpenAM provides open source Authentication, Authorization, Entitlement and Federation software.



This work is licensed under the [Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License](http://creativecommons.org/licenses/by-nc-nd/3.0/).

To view a copy of this license, visit <http://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™ is the trademark 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.

Table of Contents

1. What's New in OpenAM 12.0.0	1
2. Before You Install OpenAM 12.0.0 Software	17
2.1. OpenAM Operating System Requirements	17
2.2. Java Requirements	18
2.3. OpenAM Web Application Container Requirements	18
2.4. Data Store Requirements	18
2.5. Browser Requirements	19
2.6. Native Application Platform Requirements	20
2.7. Special Requests	20
3. OpenAM Changes & Deprecated Functionality	21
3.1. Important Changes to Existing Functionality	21
3.2. Deprecated Functionality	23
3.3. Removed Functionality	24
3.4. REST API Changes & Deprecated Functionality	24
4. OpenAM Fixes, Limitations, & Known Issues	27
4.1. Key Fixes	27
4.2. Limitations	27
4.3. Known Issues	28
5. How to Report Problems & Provide Feedback	29
6. Support	31

Chapter 1

What's New in OpenAM 12.0.0

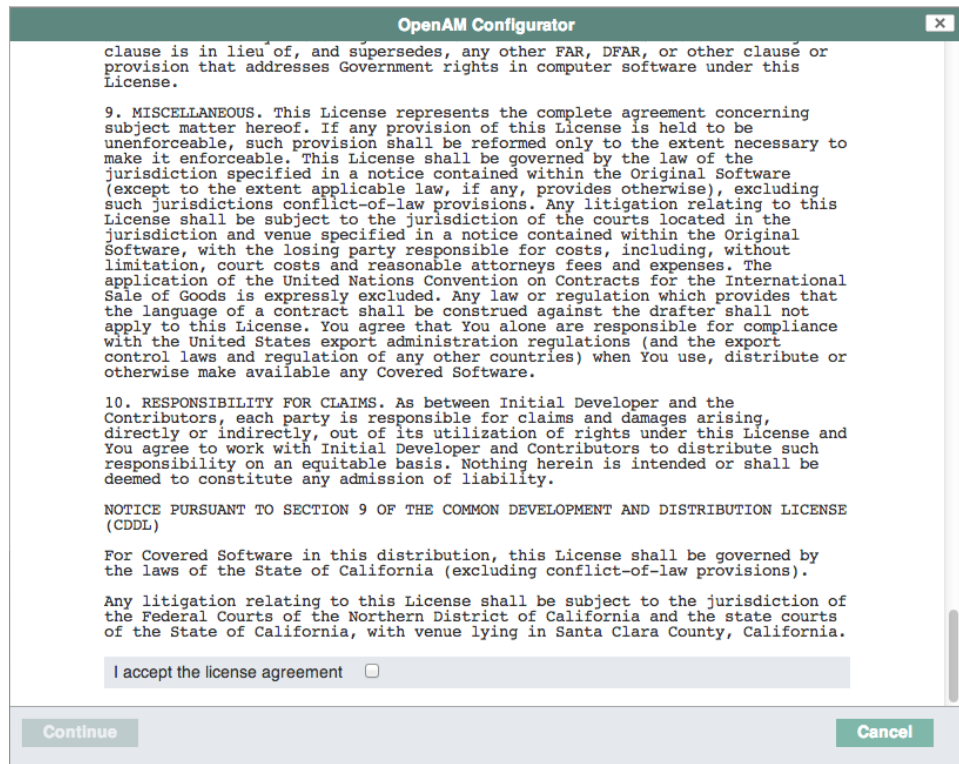
OpenAM 12.0.0 fixes a number of issues, and provides the following additional features.

Major New Features

- **Click-Through Licensing.** OpenAM now displays a software license acceptance screen when configuring the core server, OpenAM tools, and Web and J2EE agents. You must agree to the license to complete the installation of OpenAM and its components.

You can view a copy of the license at `<server-root>/legal-notices/license.txt`. The default folder location for the licenses is stored at `WEB-INF/legal-notices`.

- *GUI Installer.* When you select either the Create Default Configuration or Create New Configuration link on the OpenAM Configurator page, the software license agreement screen is displayed. Click the checkbox to accept the license and continue the configuration.



- **Web and J2EE Agent Installers.** The **agentadmin --install** command now displays the software license acceptance screen prior to installing the agent. You can scroll through the license by pressing <Enter>. At the prompt, enter yes to accept the license and continue the installation.

```
$ bin/agentadmin --install
```

```
Please read the following License Agreement carefully:
```

```
Press <Enter> to continue...] or [Enter n To Finish]
```

```
Do you completely agree with all the terms and conditions of this License Agreement (yes/no): [no]:
```

For scripted or silent installs, OpenAM provides a new command-line option, **--acceptLicense**, to suppress the license acceptance screen. Using the option indicates that you have read and accepted the terms stated in the license.

- **SSOADM.** The **ssoadm** tool has been updated to display the license acceptance screen when the **setup** or **setup.bat** command is run. Enter yes to accept the license and continue the configuration.

```
Do you accept the license? yes
```

For scripted or silent installs, you can modify the **setup** or **setup.bat** script with the addition of the `--acceptLicense` option. Simply append the option to the end of the script as follows:

```
$JAVA_HOME/bin/java -D"load.config=yes" -D"help.print=$help_print" \  
-D"path.AMConfig=$path_AMConfig" -D"path.debug=$path_debug" \  
-D"path.log=$path_log" \  
-cp "$CLASSPATH" com.sun.identity.tools.bundles.Main \  
--acceptLicense
```

- **Configurator and Upgrader Jar Files.** The executable jar files, `openam-configurator-tool-12.0.0.jar` and `openam-upgrade-tool-12.0.0.jar`, now support an optional `ACCEPT_LICENSES` property that can be added to the configuration file. If `ACCEPT_LICENSES=true`, the license acceptance screen will be skipped when the jar file is run with the configuration file. Any other value will be assumed to equal `false`, resulting in the presentation of the license acceptance screen. Default value is `false`.

The configurator and upgrader executable jar files also accept the `--acceptLicense` option on the command line. The configuration property, `ACCEPT_LICENSES`, has precedence over the command-line option, `--acceptLicense`.

- **RESTful Security Token Service.** OpenAM now include support for the RESTful Security Token Service, inspired by the WS-Trust STS. Given the variety of token types in use today, it can be helpful to have a configurable service that transform tokens.

For more information, see [The RESTful Security Token Service](#).

- **GSMA Mobile Connect Support.** OpenAM now includes support for GSMA Mobile Connect, an application of OpenID Connect 1.0. Mobile Connect lets users authenticate with their mobile phones, regardless of the service or the device on which it is consumed. This allows Mobile Network Operators to serve as identity providers for their customers.

For more information, see [Using OpenAM with Mobile Connect](#).

- **Support for JWT Profile for OAuth 2.0.** OpenAM now supports the [JSON Web Token \(JWT\) Profile for OAuth 2.0 Client Authentication and Authorization Grants](#) ([OPENAM-4394](#)). This profile allows OAuth 2.0 clients to use JWTs for authentication and to request access tokens. For details, see the *Administration Guide* section on [Authorization](#).
- **CORS support for OpenAM APIs.** OpenAM now supports cross-origin resource sharing (CORS) to allow requests to be made across domains from user agents.

Applications in browsers that support CORS can therefore now successfully make calls to an OpenAM server that runs in a different domain from the application.

Instead, you must configure CORS support in OpenAM's deployment descriptor. For instructions, see [Enabling CORS Support](#).

- **Session failover across Sites.** OpenAM now allows session failover across OpenAM Sites. In order to take advantage of this capability, you must make sure that the underlying Core Token Service replicates session data across your OpenAM Sites.

For details on setting up the underlying Core Token Service, see [Configuring the Core Token Service](#).

- **New REST APIs for policy.** OpenAM now exposes new common REST APIs for requesting decisions, and for defining policies, applications, and conditions. For details, see the *Developer Guide* section on [Authorization](#).
- **REST API Versioning.** OpenAM now assigns REST API features version numbers, to help with backwards-compatibility. For details, see the *Developer Guide* section on [REST API Versioning](#).
- **Scripted Authentication Modules.** OpenAM now supports scripted authentication modules. A scripted authentication module runs a script to perform authentication, making it easier than ever before to develop custom authentication modules.

Scripted authentication modules have access to the same data as other modules in the chain, can access user profile data during authentication, can make HTTP calls to external services, and are sandboxed for more secure operation. The scripts are stored in OpenAM configuration data, and so transparently available across OpenAM Sites. Server-side scripts can be written in either Groovy or JavaScript.

For details on writing authentication module scripts, see the *Developer Guide* chapter, [Scripting Authentication](#).

For details on configuring scripted authentication modules, see the *Administration Guide* section on [Hints For Scripted Authentication Modules](#).

Additional New Features

- **TODO:** Update for next version
- **Audit Logging to Syslog Servers.** OpenAM now supports logging audit messages to a syslog server.

For more information, see [Audit Logging to a Syslog Server](#) in the *Administration Guide*.

- **Policy Configuration Improvements.** OpenAM policy configuration now supports applications. OpenAM applications act as templates for all the policies that govern access to the protected resources in your applications. Furthermore applications, policies, and requests for policy decisions can be fully managed through REST APIs, enabling new web-based PEPs.

When you create or edit a policy in OpenAM console for a particular realm, you first choose the application that the policy belongs to, and then create the policy or choose the policy to edit. When applications share policies across realms, you must create referrals between the applications so that OpenAM can find the policies when making policy decisions. You can create and edit referrals in OpenAM console as well, though you must first enable the referral editor, which is not enabled by default.

OpenAM policies are fully backwards compatible with existing policy agents. However, existing policy agents expect to find an application of the default type starting at the top level realm. For new installations of OpenAM with realms and new applications, to route policy agent requests to the correct application and realm, this release introduces new properties in the policy agent profile Policy Client Service to identify the application and the realm. These properties are for OpenAM only. They are not used by the policy agent itself.

For details on how to configure OpenAM policies, see the *Administration Guide* chapter, [Defining Authorization Policies](#).

- **Persistent Cookie from Client IP Issued.** The Persistent Cookie module has been enhanced to enforce that the persistent cookie can only be used from the same client IP to which the cookie was issued.
- **CREST Policy Filter Rules.** OpenAM now supports CREST Policy Filter rules that simplify the configuration to protect ForgeRock common REST APIs.

For instructions on configuring a CREST Policy Filter rule, see [To Define CREST Policy Filter Rules](#) in the *Administration Guide*.

- **Fine-Grained Settings for LDAP Connections.** OpenAM now provides additional options for tuning LDAP connection pool sizes and timeouts related to the Core Token Service and to other components that use LDAP connections. For details, see the *Administration Guide* section on [Tuning LDAP CTS & Configuration Store Settings](#).
- **OAuth 2.0 Scope Conditions.** OpenAM now supports an OAuth2 Scope condition that lets the you set required OAuth 2.0 scopes as a policy condition.

-
- **OpenID Connect 1.0 Authentication Module.** OpenAM now provides an authentication module that lets OpenAM rely on an OpenID Connect provider's ID Token to authenticate an end user. For details on configuring the module, see [Hints for the OpenID Connect Token Authentication Module](#) in the *Administration Guide*.
 - **Configurable DN Cache for LDAP Data Stores.** OpenAM now has the capability to enable and disable DN caching. DN caching helps avoid DN lookups that can happen in bursts during authentication. ([OPENAM-3822](#)).
 - **Quicker UI Customization.** While customizing the UI, you can set the advanced server property, `org.forgerock.openam.core.resource.lookup.cache.enabled`, to false to allow OpenAM immediately to pick up changes to the files as you customize them ([OPENAM-3989](#)). You can set advanced server properties in OpenAM Console under Configuration > Servers and Sites > *Server Name* > Advanced. For production servers, leave this set to the default, true.
 - **Whitelist for Custom Login URIs.** OpenAM now includes a property that specifies a whitelist for custom login URIs so that the CDCServlet and the Distributed Authentication UI (DAS) can check login URI values against those in the whitelist.

The property name is `org.forgerock.openam.cdc.validLoginURIs`. For more information about this property, see the *Reference* section on advanced properties, [Servers > Advanced](#).
 - **OpenID Connect Registration Without an Access Token.** OpenAM can now be configured to let OpenID Connect clients register dynamically without having to provide an access token ([OPENAM-3604](#)). For details, see the documentation on the advanced server property, `org.forgerock.openam.openidconnect.allow.open.dynamic.registration`, in the *OpenAM Reference* section, [Servers > Advanced](#).
 - **Policy Support for Common HTTP Operations.** OpenAM policies now let you allow and deny not only HTTP GET and HTTP POST, but also HTTP DELETE, HEAD, OPTIONS, PATCH, and PUT ([OPENAM-336](#)).
 - **Device ID (Match) and Device ID (Save) Authentication Modules.** OpenAM 12.0 introduces new Device ID (Match) and Device ID (Save) authentication modules that support the ability to customize your device fingerprinting implementations.

The Device ID (Match), HMAC One-Time Password (HOTP), and Device ID (Save) modules, configured together in an authentication chain, provide the same functionality as the Device Print Authentication module that is present in OpenAM 11.x versions. The Device ID (Match) module also requires the DataStore module or any other module that can provide an authenticated username as an input.

New installations of OpenAM 12.0 or later do not display the Device Print authentication module in the OpenAM console and only provide access to the Device ID (Match) and Device ID (Save) modules.

The Device Print authentication module is only available for OpenAM 11.x versions and their upgrades. Customers who have upgraded from OpenAM 11.x to OpenAM 12.0 can still use the Device Print module, customize it, and create new instances of the module or use the Device ID (Match) and Device ID (Save) modules.

Important

The Device ID (Match) profiles (that is, device fingerprints) are incompatible with profiles created from the Device Print authentication module. If the user has existing device print profiles, created from the Device Print authentication module, these old profiles will always fail to match the client's new device profiles using the scripted Device ID (Match) module even when using the same device.

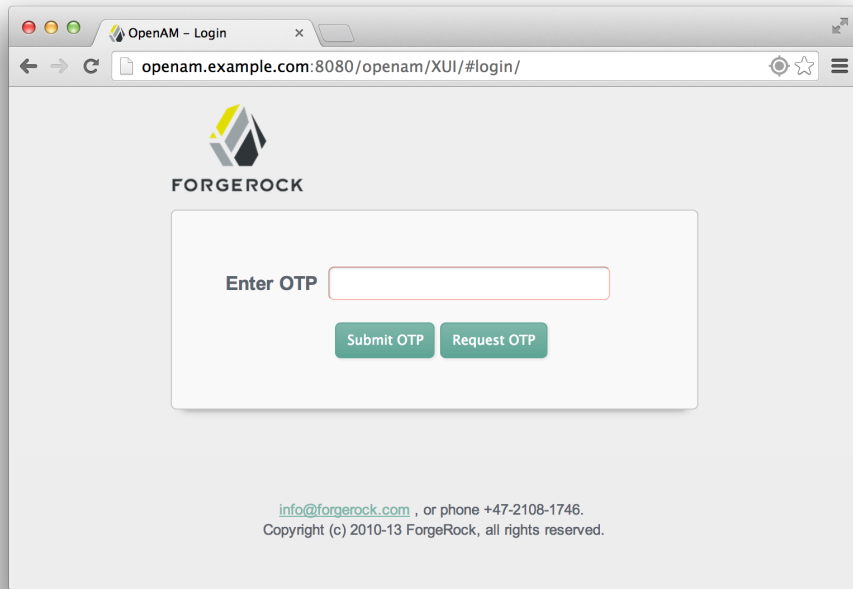
With the Device ID (Match) and Device ID (Save) modules, the user must re-save each device profile, which deletes the old 11.x profiles stored for the user.

For more information on the Device ID (Match) module, see [Hints for the Device ID \(Match\) Authentication Module](#).

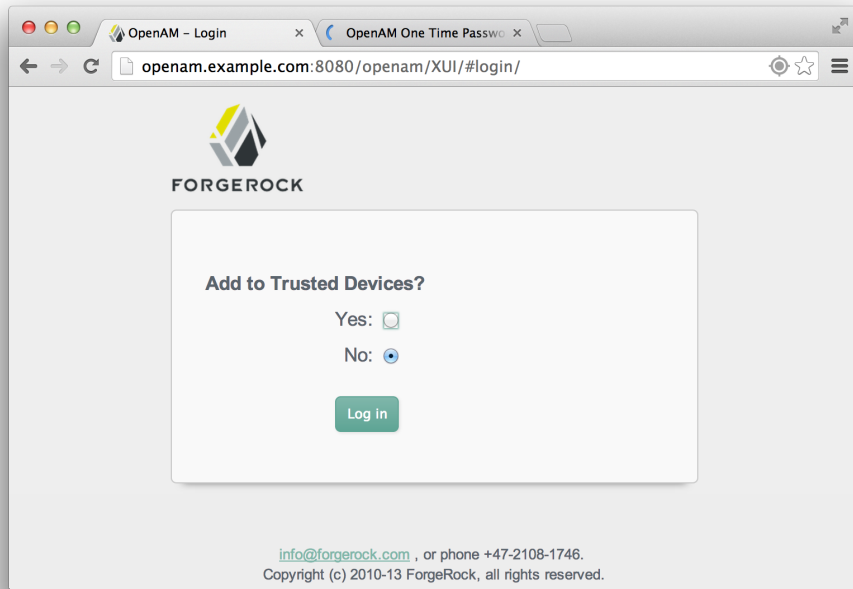
For more information on the Device ID (Save) module, see [Hints for the Device ID \(Save\) Authentication Module](#).

- **User Management of Trusted Devices.** Authentication chains that include the Device ID (Match) and Device ID (Save) modules also allow users to manage their own list of trusted devices from their Dashboard page.

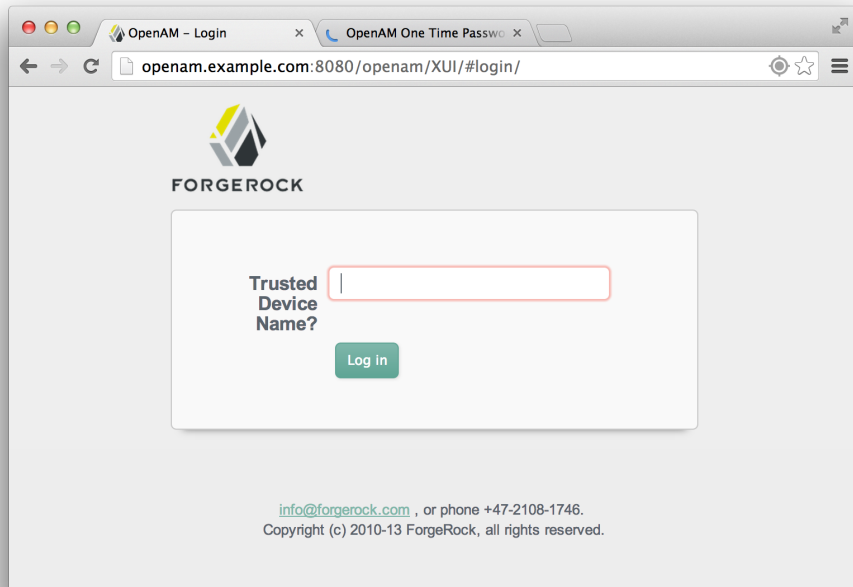
When the user logs on to the console, OpenAM determines if the user's device differs from that of the stored profile. If there are differences, OpenAM sends an "Enter OTP" page, requiring the user to enter a one-time password, which will be sent to the user via email or SMS. The user also has the option to request a one-time password.



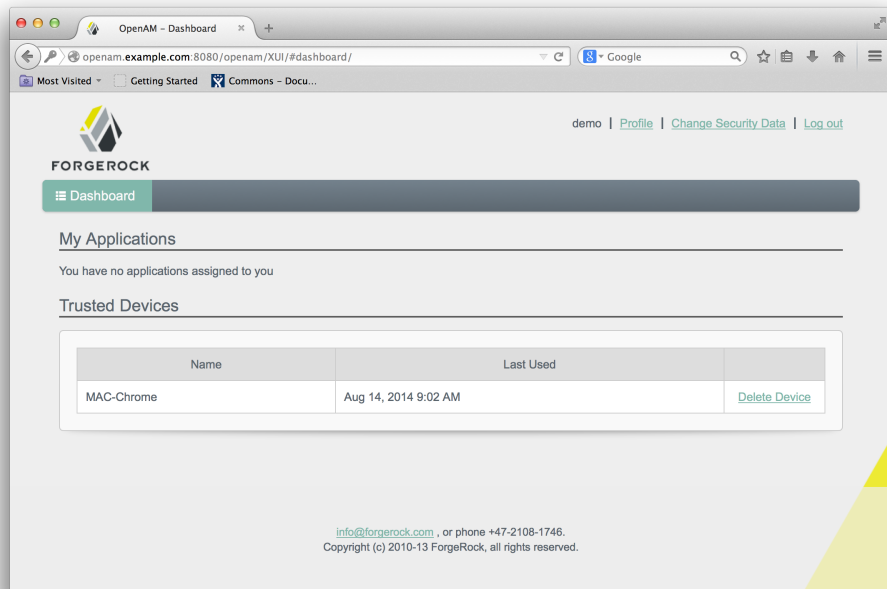
Next, OpenAM presents the user with a "Add to Trusted Devices?" page, asking if she wants to add the device to the list of trusted device profiles.



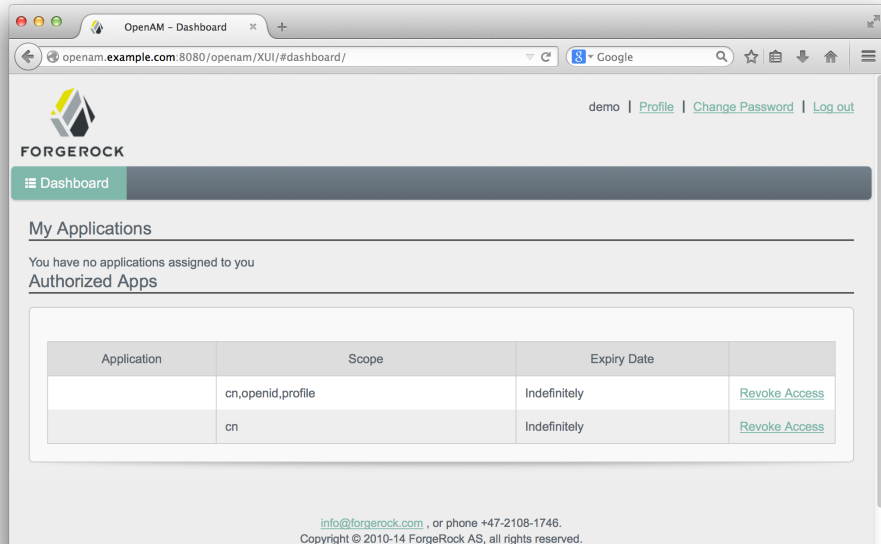
If the user clicks "Yes", OpenAM prompts the user to enter a descriptive name for the trusted device.



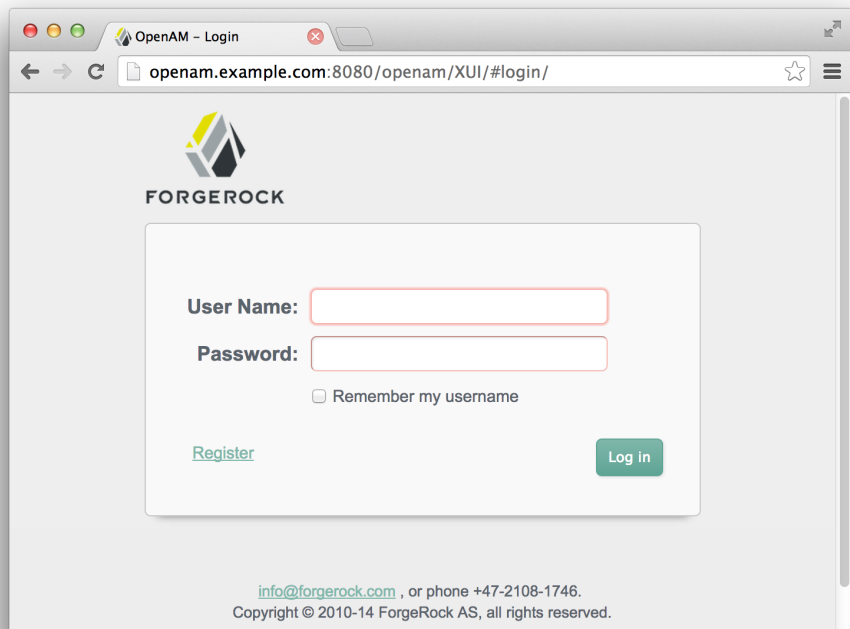
OpenAM presents the user with the User Profile page, where the user can click the Dashboard link in the upper left corner to access the My Applications and Trusted Devices page. Once on the Dashboard, the user can view the list of trusted devices or remove the device by clicking the Delete Device link.



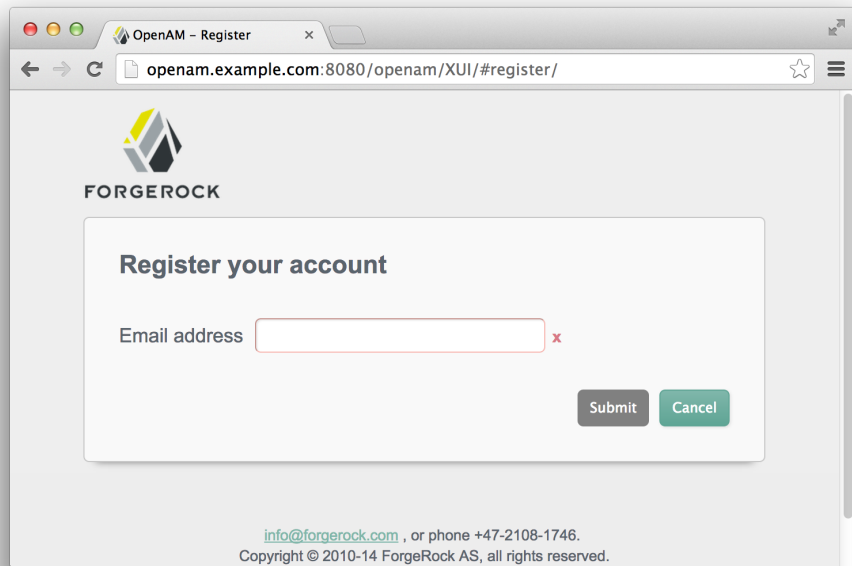
- **User Management of OAuth 2.0 Tokens.** OAuth 2.0 clients can now manage their OAuth 2.0 tokens on their user pages via the OpenAM console. For example, log in to the OpenAM console as demo, and then click the Dashboard link on the Profile page. In the Authorized Apps section, view your OAuth 2.0 tokens or remove them by clicking the Revoke Access link.



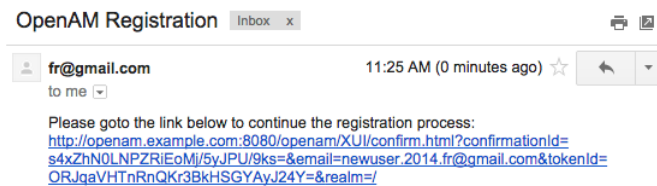
- **User Self-Registration.** The OpenAM now offers its user self-registration service through its XUI interface. Users can click a Register link on the Login page to add themselves to the system.



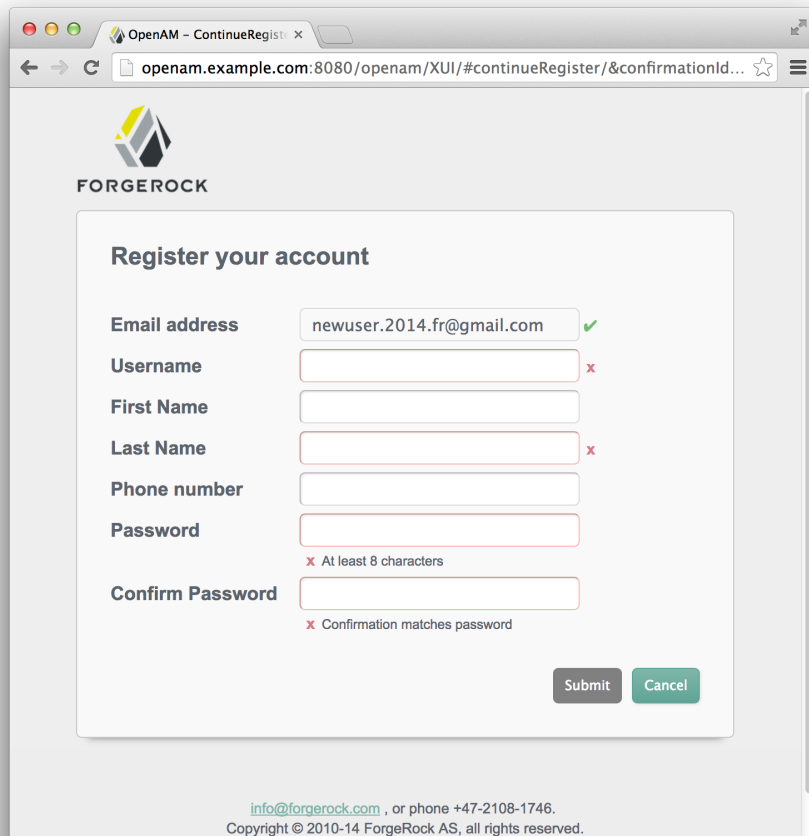
When the user clicks the Register link, OpenAM responds by sending a Register your account page where the user enters his or her email address.



OpenAM responds by sending a confirmation email to the user's email address. The user clicks the link in the email.



After the user clicks the email link, OpenAM presents the user with a Register Your Account page, where the user enters his or her account information. The user clicks Submit and can now log in to the system.



OpenAM - Continue Register

openam.example.com:8080/openam/XUI/#continueRegister/&confirmationId...

FORGEROCK

Register your account

Email address ✓

Username ✗

First Name

Last Name ✗

Phone number

Password ✗ At least 8 characters

Confirm Password ✗ Confirmation matches password

Submit Cancel

info@forgerock.com , or phone +47-2108-1746.
Copyright © 2010-14 ForgeRock AS, all rights reserved.

For more information on configuring the User Self-Registration, see [User Self-Registration](#).

For more information on the User Self-Registration using REST, see [User Self-Registration](#).

- **CREST Logging.** OpenAM now supports auditing logging and debug notifications for any request going to a CREST endpoint. OpenAM audits any request going to any CREST endpoint and writes to two files: `amRest.access` and `amRest.authx`.

The `amRest.access` records all accesses to a CREST endpoint (except `/authenticate`), regardless of whether the request successfully reached the endpoint through policy authorization.

The `amRest.authz` records all CREST authorization results regardless of success. If a request has an entry in the `amRest.access` log, but no corresponding entry in `amRest.authz`, then that endpoint was not protected by an authorization filter and therefore the request was granted access to the resource.

OpenAM now provides additional information in its debug notifications depending on the message type (error, warning or message) including realm, user, and result of the operation.

For more information on CREST logging, see [Logging](#).

- **Updates to OAuth 2.0 and OpenID Connect Authentication Modules.** Any custom implementations of `org.forgerock.openam.authentication.modules.oauth2.AccountMapper` or `org.forgerock.openam.authentication.modules.oauth2.AttributeMapper` no longer works, and needs to be reimplemented against `org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper` and/or `org.forgerock.openam.authentication.modules.common.mapping.AccountProvider` as appropriate.

Chapter 2

Before You Install OpenAM 12.0.0 Software

This chapter covers software and hardware prerequisites for installing and running OpenAM server software.

ForgeRock supports customers using the versions specified here. Other versions and alternative environments might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on a combination covered here.

TODO: Update for release

2.1 OpenAM Operating System Requirements

ForgeRock supports customers using OpenAM server software on the following operating system versions.

- CentOS 6, 7
- Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2
- Oracle Linux 6, 7
- Oracle Solaris x64 10, 11
- Oracle Solaris SPARC 10, 11

- Red Hat Enterprise Linux 6, 7
- SuSE Linux 11
- Ubuntu Linux 12.04 LTS, 14.04 LTS

2.2 Java Requirements

OpenAM server software runs in a Java EE Web container, and requires a Java Development Kit.

ForgeRock supports customers using the following Java versions. ForgeRock recommends the most recent Java update, with the latest security fixes.

- Oracle Java Development Kit 6, 7, or 8
- IBM Java Development Kit 6 or 7 (when deploying in WebSphere only)

2.3 OpenAM Web Application Container Requirements

ForgeRock supports customers using OpenAM server software in the following web application container versions.

- Apache Tomcat 6, 7, 8 (ForgeRock's preferred web container for OpenAM)
- IBM WebSphere Application Server 8, 8.5
- JBoss Enterprise Application Platform 6
- JBoss Application Server 7
- Oracle WebLogic Server 11g, 12c

The web application container must be able to write to its own home directory, where OpenAM stores configuration files.

2.4 Data Store Requirements

The following table summarizes OpenAM data store support.

Table 2.1. Supported Data Stores

Data Store	Versions	Core Token Service (CTS) Data Store	Configuration Data Store	User Data Store
Embedded OpenDJ (included in OpenAM)	2.6.2	Supported	Supported	Supported
External OpenDJ	2.6, 2.6.2	Supported	Supported	Supported
IBM Tivoli Directory Server	6.3			Supported
Microsoft Active Directory	2008, 2008 R2, 2012, 2012 R2			Supported
Oracle Directory Server Enterprise Edition	11g	NOT SUPPORTED	Supported When using DSEE as a configuration store, you must set up an external OpenDJ directory service as a Core Token Service data store as well, and you must configure OpenAM to use the external OpenDJ directory service as the CTS data store.	Supported
Oracle Unified Directory	11g		Supported	Supported

2.5 Browser Requirements

The following table summarizes browser support.

Table 2.2. Supported Platforms & Browsers

Client Platform	Chrome 16 or later	Internet Explorer 9 or later	Firefox 3.6 or later	Safari 5 or later
Apple iOS 7 or later	Supported			Supported
Apple Mac OS X 10.8 or later	Supported		Supported	Supported
Google Android 4.3 or later	Supported			
Microsoft Windows 7 or later	Supported	Supported	Supported	Supported
Ubuntu Linux 12.04 LTS or later	Supported		Supported	

2.6 Native Application Platform Requirements

ForgeRock supports customers' use of OpenAM REST and other client APIs in native applications on the following platforms.

- Apple iOS 7 or later
- Apple Mac OS X 10.8 or later
- Google Android 4.3 or later
- Microsoft Windows 7 or later
- Ubuntu Linux 12.04 LTS or later

Other combinations might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on one of these platforms.

2.7 Special Requests

If you have a special request regarding support for a combination not listed here, contact ForgeRock at info@forgerock.com.

Chapter 3

OpenAM Changes & Deprecated Functionality

This chapter covers both major changes to existing functionality, and also deprecated and removed functionality.

3.1 Important Changes to Existing Functionality

- TODO: Finish updating before release
- All OpenAM core server, tools, and agent installers now display a software license acceptance screen prior to configuration. You must agree to the license to continue the configuration.

For users implementing scripted or silent installs, the installers and upgrader tools provide a `--acceptLicense` command-line option, indicating that you have read and accepted the terms of the license. If the option is not present on the command-line invocation, the installer or upgrader will interactively present a license agreement screen to the user.

- When you visit the Policies tab for a realm in OpenAM console, OpenAM now directs you to the new policy editor. For instructions on using the new policy editor, see the *Administration Guide* chapter, [Defining Authorization Policies](#). Notice that policies now belong to applications as described in that chapter.

OpenAM has changed its internal representation for policies to better fit the underlying implementation, which is based on the newer engine designed

for higher performance and finer grained policies. When you upgrade to this version, OpenAM migrates your policies to the new representation.

Depending on your existing policies before upgrade, you can see the following differences.

- Existing policies with multiple resource rules map to multiple new policies.

When a single policy maps to multiple policies during migration, OpenAM appends a number to the existing name for each new policy. This allows you to recognize the set of policies when you must manage them together, for example to change them all in the same way.

This behavior is to optimize policy evaluation performance. The newer policy engine matches resources to policies during evaluation with indexing that proves very efficient as long as each policy specifies one resource pattern. OpenAM processes the list of resources in policies in linear fashion, so long lists of resources can slow policy evaluation.

- Conditions in existing policies map to newer representations.

New representations exist for all existing conditions provided in OpenAM out of the box. Custom conditions developed for your deployment do not map to any of the newer conditions provided. In that case you must implement your custom conditions by implementing the newer service provider interfaces, and then replace your existing policies to use them.

To see how to implement a custom policy plugin, see the *Developer's Guide* chapter, [Customizing Policy Evaluation](#).

- When OpenAM encounters issues migrating policies during upgrade, it writes messages about the problems in the upgrade log. When you open a policy in the policy editor that caused problems during the upgrade process the policy editor shows the issues, but does not let you fix them directly. Instead you must create equivalent, corrected policies in order to use them in OpenAM.

OpenAM configuration has changed in several ways to accommodate the changes to the way policies are managed.

- The policy service configuration has changed to simplify the Policy Configuration pages in OpenAM console. For details see the *Reference* section, [Policy Configuration](#).
- OpenAM now requires policy referrals only when an application is administered across multiple realms, as can be the case when one policy agent protects multiple applications. Otherwise, OpenAM can use new settings in policy agent profiles to direct policy agent requests to the appropriate realm and application.

The web and Java EE policy agent profiles includes the new settings under OpenAM Services > Policy Client Service in OpenAM console. These new settings allow you to set the realm and application for a policy agent. The settings are compatible with existing policy agents, as they are not used by the policy agents themselves, but instead by OpenAM when handling policy agent requests.

The fix for [OPENAM-3509](#) ensures that OpenAM considers a trailing slash as part of the resource name to match. This improves compatibility between self and subtree modes, and compatibility with older policy agents.

- Following a change to the SAML 2.0 pages in OpenAM, you no longer customize `saml2login.template` and `saml2loginwithrelay.template` to add a progress bar for single sign on. Instead, customize `saml2/jsp/autosubmitaccessrights.jsp` as described in the procedure, *[To Indicate Progress During SSO](#)*.
- When running OpenAM on WebLogic 11g, you must add a WebLogic-specific descriptor file, `WEB-INF/weblogic.xml` in the `.war` before deployment.
- The class hierarchy for the `ResourceName` interfaces has changed. Previous implementations should be source-compatible, but will not be binary-compatible, and will need recompiling.
- The distributed authentication service (DAS) and cross-domain single sign-on (CDSSO) do not support the `iPSPCookie/DProPCookie` query string parameter to set a `DProPCookie` in the user-agent as a mechanism for cookie persistence. Neither DAS nor CDSSO retains `iPSPCookie=yes`.

3.2 Deprecated Functionality

The following functionality is deprecated in OpenAM 12.0.0, and is likely to be removed in a future release.

- TODO: Update before release
- Classic (JATO-based) UI is deprecated for end user pages. OpenAM offers the JavaScript-based XUI as a replacement. Classic UI for end user pages is likely to be removed in a future release.
- With the implementation of OAuth 2.0 in this release, OAuth 1.0 has been deprecated. OAuth 1.0 support was originally provided in OpenAM 9.
- The Netscape LDAP API is to be removed from OpenAM, with OpenAM using the OpenDJ LDAP SDK instead. This affects all classes in `com.sun.identity.shared.ldap.*` packages.

- OpenAM currently uses Sun Java System Application Framework (JATO). JATO is deprecated and is likely to be replaced in a future release.
- With the implementation of the Persistent Cookie authentication module, the Core Authentication module persistent cookie options are deprecated and are likely to be removed in a future release.
- The OAuth 2.0 plugin interface for custom scopes, [Scope](#) is deprecated and likely to be removed in a future release.

Custom OAuth 2.0 scopes plugins now implement the [ScopeValidator](#) interface instead. For an example, see the *Developer's Guide* chapter, [Customizing OAuth 2.0 Scope Handling](#).

- The OAuth 2.0 plugin interface for custom response types, [ResponseType](#) is deprecated and likely to be removed in a future release.

Custom OAuth 2.0 response type plugins now implement the [ResponseTypeHandler](#) interface instead.

3.3 Removed Functionality

- TODO: Finish updating before release

3.4 REST API Changes & Deprecated Functionality

This section covers changes to existing REST API functionality, and also deprecated and removed REST API functionality.

OpenAM 12.0.0 contains the following changes to the REST API.

- Changing Passwords

Changing passwords by using a PUT REST API call is no longer supported.

Use a POST request to `/json/subrealm/users/username?_action=changePassword` to change a password.

- `/json/authenticate`

The response returned when submitting incorrect credentials has changed.

Table 3.1. REST End Points

OpenAM 11.0.1	OpenAM 12.0.0

OpenAM 11.0.1

```
{
  "errorMessage": "Authentication Failed!!",
  "failureUrl": "https://openam.example.com:8443"
}
```

OpenAM 12.0.0

```
{
  "code": 401,
  "reason": "Unauthorized",
  "message": "Authentication Failed!!",
  "detail": {
    "failureUrl": "https://openam.example.com:8443"
  }
}
```

- Older REST services relying on the following end points are deprecated.

/identity/attributes	/identity/read
/identity/authenticate	/identity/search
/identity/authorize	/identity/update
/identity/create	/ws/1/entitlement/decision
/identity/delete	/ws/1/entitlement/decisions
/identity/isTokenValid	/ws/1/entitlement/entitlement
/identity/logout	/ws/1/entitlement/entitlements

The following table shows how legacy and newer end points correspond.

Table 3.2. REST End Points

Deprecated URIs	Newer Evolving URIs
/identity/attributes	/json/users
N/A	/json/applications
N/A	/json/applicationtypes
/identity/authenticate	/json/authenticate
N/A	/json/conditiontypes
/identity/authorize	/json/policies?_action=evaluate, / json/policies?_evaluateTree
/identity/create, /identity/delete, / identity/read, /identity/search, / identity/update	/json/agents, /json/groups, /json/ realms, /json/users
/identity/isTokenValid	/json/sessions/tokenId? _action=validate
/identity/logout	/json/sessions/?_action=logout
/ws/1/entitlement/decision, /ws/1/ entitlement/decisions, /ws/1/ entitlement/entitlement, /ws/1/ entitlement/entitlements	/json/policies?_action=evaluate, / json/policies?_evaluateTree
N/A	/json/dashboard

REST API Changes & Deprecated Functionality

Deprecated URIs	Newer Evolving URIs
N/A	/json/policies
N/A	/json/serverinfo

Find examples in the *Developer Guide* chapter on [Using RESTful Web Services](#) in OpenAM.

Support for the older REST services is likely to be removed in a future release in favor of the newer REST services. Older REST services will be removed only after replacement REST services are introduced.

Chapter 4

OpenAM Fixes, Limitations, & Known Issues

OpenAM issues are tracked at <https://bugster.forgerock.org/jira/browse/OPENAM>. This chapter covers the status of key issues and limitations at release 12.0.0.

4.1 Key Fixes

The following bugs were fixed in release 12.0.0. For details, see the [OpenAM issue tracker](#).

- TODO
- OPENAM-3964: The class hierarchy for ResourceName interfaces has changed in this issue. Previous implementations should still be source-compatible but are not binary-compatible. You must recompile your custom code if you implemented the ResourceName interfaces ([OPENAM-3964](#)).

4.2 Limitations

- **Session Failover with External OpenDJ Servers.** When session failover is configured to use external OpenDJ directory servers, OpenAM must access those directory servers through an LDAP load balancer that can fail over connections from OpenAM whenever a directory server goes offline. Otherwise, sessions could continue to persist after users logout of OpenAM.

- **Different OpenAM Version within a Site.** Do not run different versions of OpenAM together in the same OpenAM site.
- **Deleting Referral Policy.** OpenAM allows you to delete a referral policy even if policies depending on the referral still exist in the target realm. Deleting a referral policy that other policies depend on can cause problems during policy evaluation. You must therefore make sure that no policies depend on any referrals that you delete.
- **Deploying OpenAM on Windows in an IPv6 Network.** When deploying OpenAM components on Microsoft Windows in an IPv6 environment, you must use the Java 7 Development Kit on Windows (due to [JDK-6230761](#), which is fixed only in Java 7).
- **Database Repository Type is Experimental.** The Database Repository type of data store is experimental and not supported for production use.
- **Enforcing Session Quotas with Session Failover.** By default OpenAM does not enforce session quotas when running in Site mode without session failover. To work around this behavior, set the server configuration property `openam.session.useLocalSessionsInMultiServerMode=true`. You can set this property in OpenAM console under Configuration > Servers and Sites > Servers > Server Name > Advanced.
- **OpenAM with Embedded Directory Server in IPv6 Networks.** On hosts with pure IPv6 networks, OpenAM configuration has been seen to fail while starting the embedded OpenDJ directory server ([OPENAM-3008](#)).
- **JBoss 6.3 Support for Java 8.** As of this writing, JBoss 6.3/AS 7.4.0 does not support Java 8. Until JBoss 6.3 fully supports Java 8, you can use JDK 1.7.0_56 ([OPENAM-4876](#)).
- **Note about HttpServletResponse & HttpServletRequest.** The `HttpServletRequest` instance passed to `AMPostAuthProcessInterface#onLogout` will be null. The `HttpServletResponse` instance passed to `AMPostAuthProcessInterface#onLogout` is not the actual `HttpServletResponse` corresponding to the request but a faux instance whose only purpose is to transfer headers back to the actual `HttpServletResponse` ([OPENAM-4045](#)).

4.3 Known Issues

The following important known issues remained open at the time release 12.0.0 became available. For details and information on other issues, see the [OpenAM issue tracker](#).

TODO

Chapter 5

How to Report Problems & Provide Feedback

If you have questions regarding OpenAM which are not answered by the documentation, there is a mailing list which can be found at <https://lists.forgerock.org/mailman/listinfo/openam> where you are likely to find an answer.

If you have found issues or reproducible bugs within OpenAM 12.0.0, report them in <https://bugster.forgerock.org>.

When requesting help with a problem, include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Description of the environment, including the following information:
 - Machine type
 - Operating system and version
 - Web server or container and version
 - Java version
 - OpenAM version
 - Any patches or other software that might be affecting the problem

-
- Steps to reproduce the problem
 - Any relevant access and error logs, stack traces, or core dumps

Chapter 6

Support

You can purchase OpenAM support subscriptions and training courses from ForgeRock and from consulting partners around the world and in your area. To contact ForgeRock, send mail to info@forgerock.com. To find a partner in your area, see <http://forgerock.com/partners/find-a-partner/>.

