



User Self Service Guide

ForgeRock Access Management 5

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

Copyright © 2016-2017 ForgeRock AS.

Abstract

Guide to configuring and using ForgeRock# Access Management User Self Service features.



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 at free . fr.

Admonition graphics by Yannick Lung. Free for commercial use. Available at FreeCnS.Cumulus.

Table of Contents

Preface	iv
1. Introducing User Self Service	1
1.1. About User Self Service	1
1.2. User Self Service Process Flows	2
2. Implementing User Self Service	7
2.1. Configuring the Signing and Encryption Key Aliases	7
2.2. Configuring the Email Service	8
2.3. Configuring the Google reCAPTCHA Plugin	9
2.4. Configuring Knowledge-Based Security Questions	10
2.5. Configuring User Self Registration	11
2.6. Configuring the Forgotten Password Reset Feature	13
2.7. Configuring the Forgotten Username Feature	14
2.8. User Management of Passwords and Security Questions	15
3. Using User Self Service	17
3.1. RESTful User Self Service	17
3.2. Registering Users	17
3.3. Retrieving Forgotten Usernames	21
3.4. Replacing Forgotten Passwords	25
4. User Self Service Reference	31
4.1. User Self-Service	31
4.2. Legacy User Self Service	38
A. Getting Support	41
A.1. Accessing Documentation Online	41
A.2. Joining the ForgeRock Community	42
A.3. Getting Support and Contacting ForgeRock	42
Glossary	43

Preface

The User Self Service Guide shows you how to configure, maintain, and troubleshoot the User Self Service feature provided by ForgeRock Access Management, which automates account registration and account name retrieval, and forgotten password reset.

This guide is written for access management designers, developers, and administrators who build, deploy, and maintain services and features for their organizations.

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

Introducing User Self Service

OpenAM provides a user self service feature that enables your customers to self-register to your web site, securely reset forgotten passwords, and retrieve their usernames.

OpenAM's user self service capabilities greatly reduces help desk costs and offers a rich online experience that strengthens customer loyalty.

Note

The Password Reset service, located in the AM console at [Configure > Global Services](#), is deprecated.

1.1. About User Self Service

OpenAM's user self service feature supports automated account registration for new users, forgotten password reset, and forgotten username retrieval for your existing customer base. The user self service features include the following capabilities:

- **User Self Registration.** Allows non-authenticated users to register to your site on their own. You can add additional security features like email verification, knowledge-based authentication (KBA) security questions, Google reCAPTCHA, and custom plugins to add to your User Self Registration process.
- **Knowledge-based authentication security questions.** Supports the capability to present security questions during the registration process. When enabled, the user is prompted to enter answers to pre-configured or custom security questions. Then, during the forgotten password or forgotten username process, the user is presented with the security questions and must answer them correctly to continue the process.
- **Forgotten password reset.** Allows registered users already in your system to reset their passwords. The default password policy is set in the underlying directory server and requires a minimum password length of eight characters by default. If security questions are enabled, users must also correctly answer their pre-configured security questions before resetting their passwords.
- **Forgotten username support.** Allows users to retrieve their forgotten usernames. If security questions are enabled, users must also correctly answer their pre-configured security questions before retrieving their usernames.
- **Google reCAPTCHA plugin.** Supports the ability to add a Google reCAPTCHA plugin to the registration page. This plug-in protects against any software bots that may be used against your site.

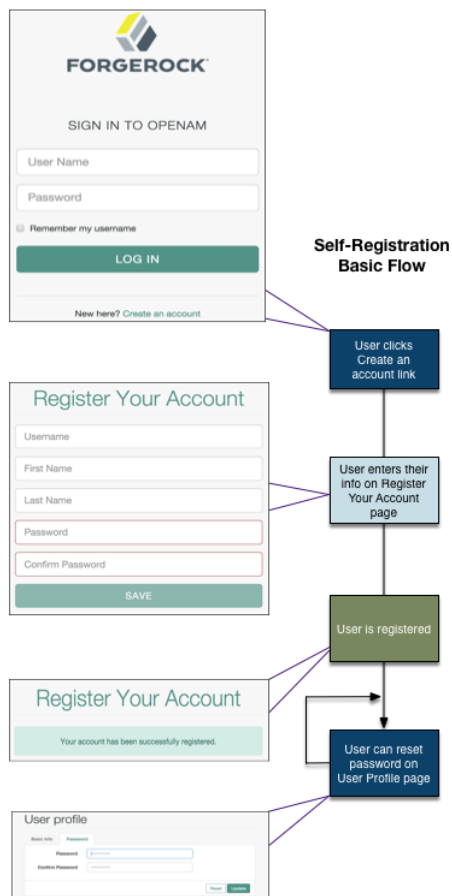
- **Configurable plugins.** Supports the ability to add plugins to customize the user services process flow. You can develop your custom code and drop the `.jar` file into your container.
- **Customizable confirmation emails.** Supports the ability to customize or localize confirmation email in plain text or HTML.
- **Password policy configuration.** Supports password policy configuration, which is enforced by the underlying OpenDJ directory server and manually aligned with frontend UI templates. The default password policy requires a password with a minimum length of eight characters.
- **Self registration user attribute whitelist.** Supports attribute whitelisting, which allows you to specify which attributes can be set by the user during account creation.

1.2. User Self Service Process Flows

The user self service feature supports a number of different user flows depending on how you configure your security options. These options include email verification, security questions, Google reCAPTCHA, and any custom plugins that you create.

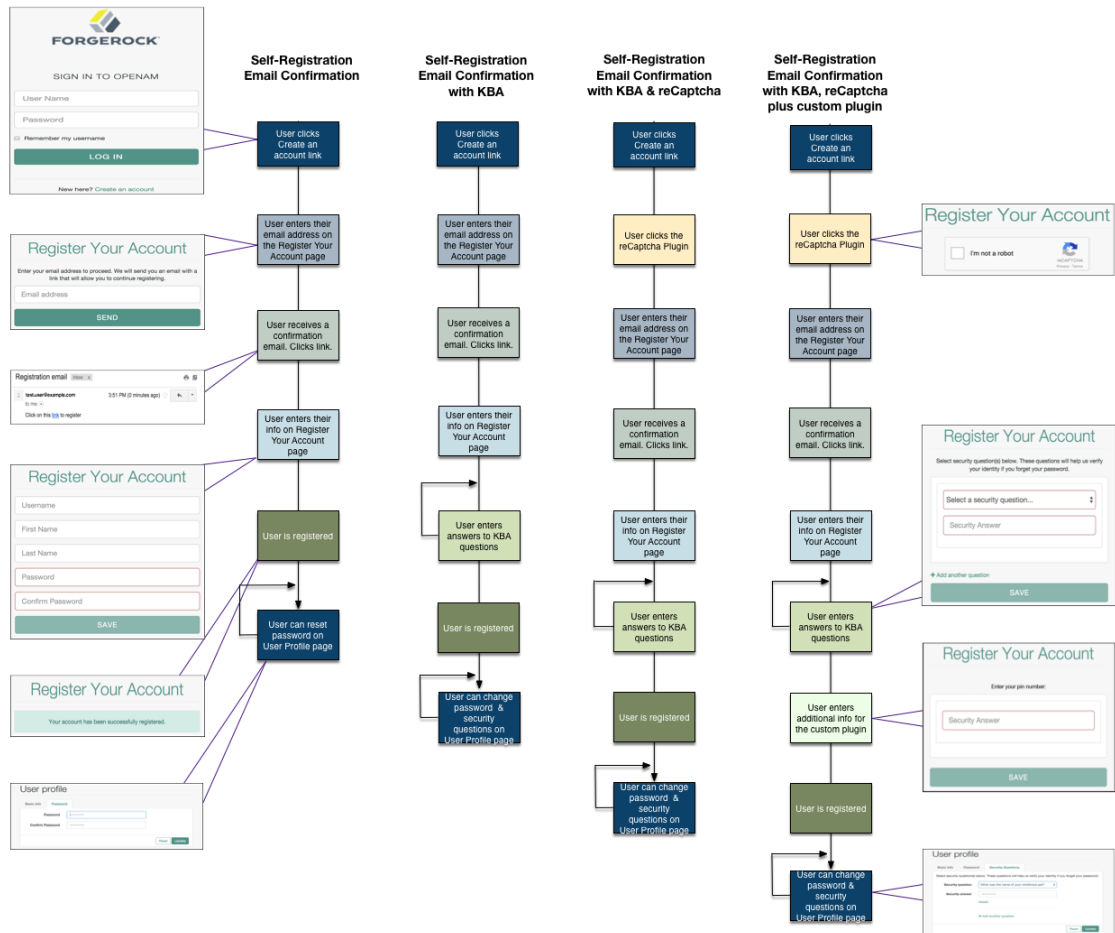
The following diagram shows the basic User Self Registration flow without the optional features:

Figure 1.1. User Self Registration Basic Flow



The following diagrams show the possible flows for User Self Registration flow with the optional features:

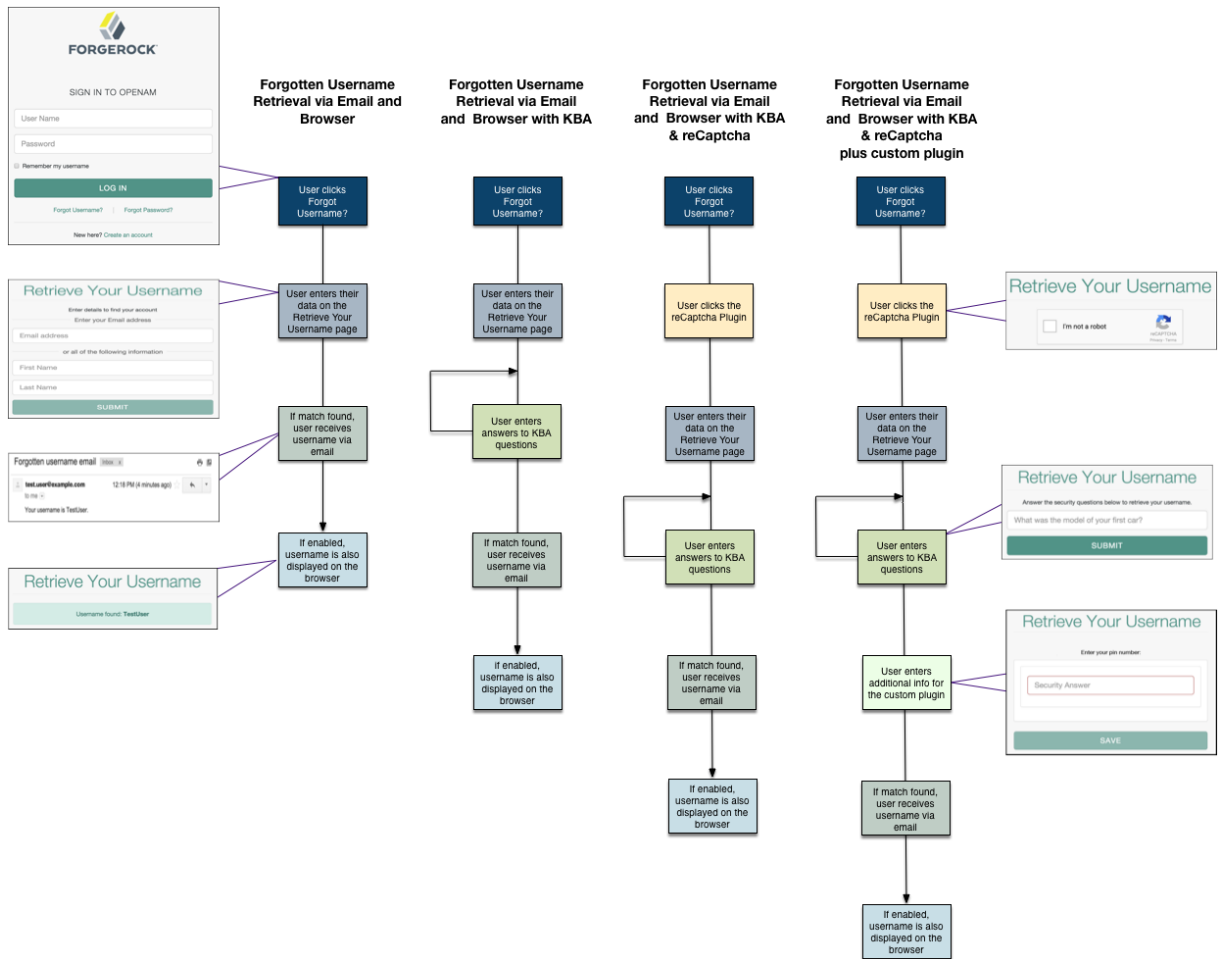
Figure 1.2. User Self Registration Flow With Options



Forgotten username retrieval and forgotten password reset support various user flows depending on how you configure your security options. If you enabled security questions and the user entered responses to each question during self-registration, the security questions are presented to the user in random order.

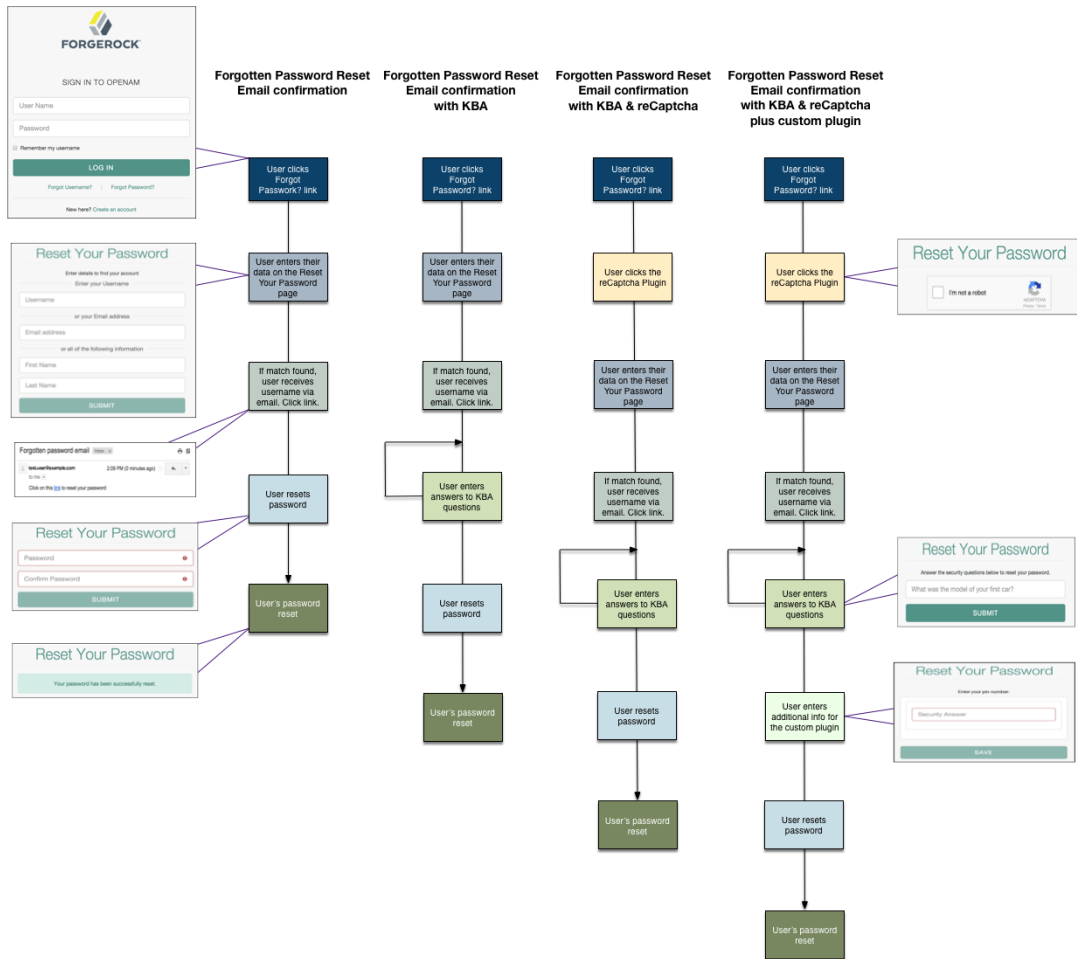
The following diagram shows the possible flows for forgotten username:

Figure 1.3. Forgotten Username Flow



The following diagram shows the possible flows for forgotten password reset:

Figure 1.4. Forgotten Password Flow



Chapter 2

Implementing User Self Service

You can configure the user self service features to use email address verification, which sends an email containing a link for user self-registration and forgotten password reset via OpenAM's email service. You can also send the forgotten username to the user by email if configured.

Follow the sections on this chapter to implement the user self service features using the AM console. For information on how to use the RESTful API functionality, see Section 3.1, "RESTful User Self Service".

Important

Each individual user must have a unique email address to use the email features of user self service.

Follow the steps in the sections below:

- Section 2.1, "Configuring the Signing and Encryption Key Aliases"
- Section 2.2, "Configuring the Email Service"
- Section 2.3, "Configuring the Google reCAPTCHA Plugin"
- Section 2.4, "Configuring Knowledge-Based Security Questions"
- Section 2.5, "Configuring User Self Registration"
- Section 2.6, "Configuring the Forgotten Password Reset Feature"
- Section 2.7, "Configuring the Forgotten Username Feature"

2.1. Configuring the Signing and Encryption Key Aliases

OpenAM's user self service feature requires two key aliases: one secret key alias for signing and one key pair alias for encryption. OpenAM is pre-configured with a JCEKS keystore with three key aliases that you can use for testing purposes. For more information about keystores and key aliases in OpenAM, see Chapter 5, "*Setting Up Keys and Keystores*" in the *Setup and Maintenance Guide*.

Unlike a JKS keystore that supports asymmetric keys, the JCEKS keystore supports both asymmetric keys for encryption and symmetric keys for signing. In an OpenAM site with multiple OpenAM servers deployed behind a load balancer, the JCEKS keystore allows one server to decrypt and validate a JSON Web Token (JWT) from the other server.

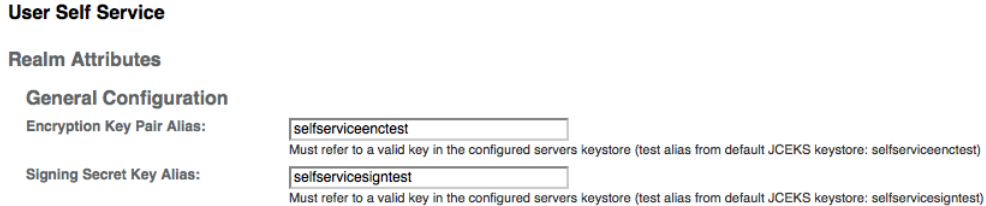
The key aliases *must* exist in the JCEKS keystore before the user self service feature can be configured, since they need to be specified at configuration time.

Procedure 2.1. To Configure Self Service Key Aliases

To provide user self service features, you must configure suitable key aliases. Perform the following steps to populate the values of the Encryption Key Pair Alias and the Signing Secret Key Alias properties:

1. Log in to the AM console as an administrator, for example, `amadmin`.
2. Navigate to Configure > Global Services > User Self Service.
3. Populate the values of the Encryption Key Pair Alias and the Signing Secret Key Alias properties with the names of the key pair aliases in your JCEKS keystore. For example, if you are using the demo keys in the default `keystore.jceks` file, set the properties as follows:
 - Encryption Key Pair Alias to `selfserviceentest`.
 - Signing Secret Key Alias to `selfservicesigntest`.

Figure 2.1. User Self Service Key Pair Aliases



User Self Service

Realm Attributes

General Configuration

Encryption Key Pair Alias:
Must refer to a valid key in the configured servers keystore (test alias from default JCEKS keystore: selfserviceentest)

Signing Secret Key Alias:
Must refer to a valid key in the configured servers keystore (test alias from default JCEKS keystore: selfservicesigntest)

4. Save your changes.

2.2. Configuring the Email Service

The user self service feature lets you send confirmation emails via OpenAM's SMTP Email Service to users who are registering at your site or resetting forgotten passwords. If you choose to send confirmation emails, you can configure the Email Service globally.

Procedure 2.2. To Configure the Email Service

By default, OpenAM expects the SMTP service to listen on `localhost:465`. You can change this setting.

1. Log in to the AM console as the administrator.

2. On the Realms page, click the realm in which you will install the Email Service, and then click Services.
3. Click Services, and then click Add a Service.
4. On the Choose a Service drop-down list, select Email Service, and then enter the following:
 - a. Enter the Mail Server Hostname. If you are using the Google SMTP server, you must also configure the Google Mail settings to enable access for less secure applications.
 - b. Enter the Mail Server Authentication Username. The default is `amadmin`. If you are testing on a Google account, you can enter a known Gmail address.
 - c. Enter the Mail Server Authentication Password property value.
 - d. Enter the Email From Address. The default is `no-reply@example.com`.
 - e. Click Create.

2.3. Configuring the Google reCAPTCHA Plugin

The user self service feature supports the Google reCAPTCHA plugin, which can be placed on the Register Your Account, Reset Your Password, and Retrieve Your Username pages. The Google reCAPTCHA plugin protects your user self service implementation from software bots.

Note

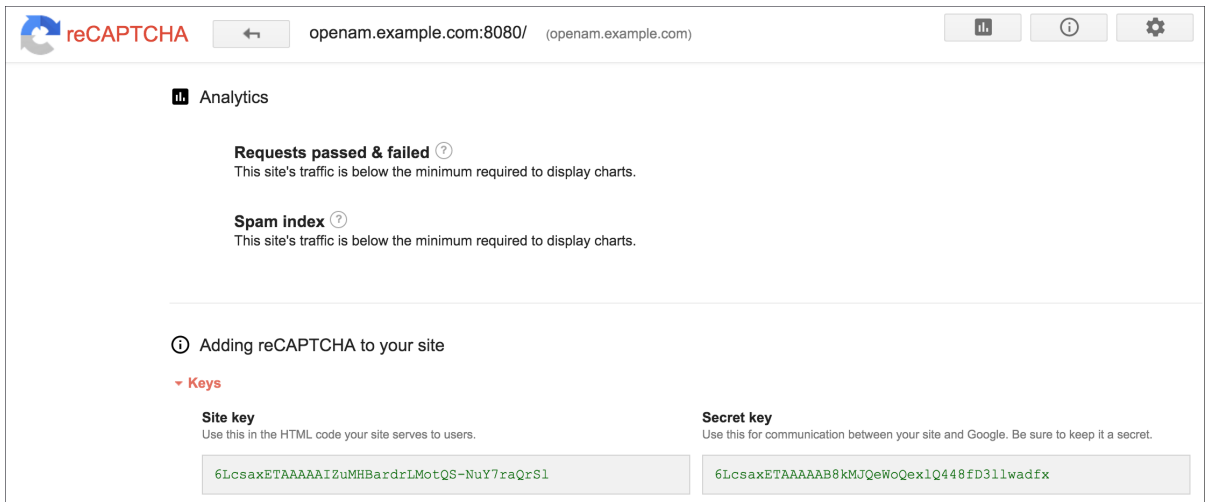
Google reCAPTCHA is the only supported plugin for user self service. Any other Captcha service will require a custom plugin.

Procedure 2.3. To Configure the Google reCAPTCHA Plugin

1. Register your web site at a Captcha provider, such as Google reCAPTCHA, to get your site and secret key.

When you register your site for Google reCAPTCHA, you only need to obtain the site and secret key, which you enter in the User Self Service configuration page in the AM console. You do not have to do anything with client-side integration and server-side integration. The Google reCAPTCHA plugin appears automatically on the Register Your Account, Reset Your Password, and Retrieve Your Username pages after you configure it in the AM console.

Figure 2.2. Google reCAPTCHA Page



2. Log in to the AM console as an administrator.
3. Click Configure > Global Services > User Self Service.
4. In the Google Recaptcha Site Key field, enter the site key that you obtained from the Google reCAPTCHA site.
5. In the Google Recaptcha Secret Key field, enter the secret key that you obtained from the Google reCAPTCHA site.
6. In the Google Recaptcha Verification URL field, keep the default.

2.4. Configuring Knowledge-Based Security Questions

Knowledge-based authentication (KBA) is an authentication mechanism in which the user must correctly answer a number of pre-configured security questions that are set during the initial registration setup. If successful, the user is granted the privilege to carry out an action, such as registering an account, resetting a password, or retrieving a username. The security questions are presented in a random order to the user during the User Self Registration, forgotten password reset, and forgotten username processes.

OpenAM provides a default set of security questions and easily allows OpenAM administrators and users to add their own custom questions.

Procedure 2.4. To Configure Security Questions

1. Log in to the AM console as the administrator.
2. Click Configure > Global Services > User Self Service.
3. On the User Self Service page, scroll to the Security Questions section. Enter your own security question in the New Value field, and then click Add. The syntax is: `OrderNum|ISO-3166-2 Country Code|Security Question`. For example, `5|en|What is your dog's name?`. Make sure that order numbers are unique.

Warning

You should never remove any security questions as a user may have reference to a given question.

4. In the Minimum Answers to Define field, enter the number of security questions that will be presented to the user during the registration process.
5. In the Minimum Answers to Verify field, enter the number of security questions that must be answered during the Forgotten Password and Forgotten Username services.
6. Click Finish to save your changes.

2.5. Configuring User Self Registration

OpenAM provides a self-registration feature that allows users to create an account to your web site. Although you can configure user self registration without any additional security mechanisms, such as email verification or KBA security questions, we recommend configuring the email verification service with user self registration at a minimum.

Procedure 2.5. To Configure User Self Registration

1. Log in to the AM console as the administrator.
2. Configure the email service presented in Section 2.2, "Configuring the Email Service".
3. Click Configure > Global Services > User Self Service.
4. On the User Self Service page, click Enabled next to User Registration.
5. For Captcha, click Enabled to turn on the Google reCAPTCHA plugin. Make sure you configured the plugin as presented in Section 2.3, "Configuring the Google reCAPTCHA Plugin".
6. For Email Verification, clear the Enabled box if you want to turn off the email verification service. We recommend that you keep it selected.

7. For Security Questions, click Enabled to display security questions to the user during the self registration, after which the user must enter their answers to the questions. During the forgotten password or forgotten username services, the user will be presented with the security questions to be able to reset their passwords or retrieve their usernames if Security Questions is enabled.
8. In the Token LifeTime field, enter an appropriate number of seconds for the token lifetime. If the token lifetime expires before the user self-registers, then the user will need to restart the registration process over again.

Default: 900 seconds.

9. To customize the Self Registration outgoing email, run the following steps:
 - a. In the Outgoing Email Subject field, enter the Subject line of your email in the New Value field, and then click Add.

The subject line format is `lang|subject-text`, where `lang` is the ISO-639 language code, such as `en` for English, `fr` for French, and others. For example, the subject line values could be: `en|Registration Email` and `fr|Inscription E-mail`.
 - b. In the Outgoing Email Body field, enter the text of your email in the New Value field, and then click Add.

The email body text format is `lang|email-text`, where `lang` is the ISO-639 language code. Note that email body text must be all on one line and can contain any HTML tags within the body of the text.

For example, the email body text could be: `en|Thank you for registration to our site! Click here to register to the site.`

10. In the Valid Creation Attributes field, enter the user attributes the user can set during the User Self Registration. The attributes are based on the OpenAM identity repository.
11. For Destination After Successful Registration, select one of the following:
 - User is automatically logged in and sent to the appropriate page within the system.
 - User is sent to a success page without being logged in. In this case, OpenAM displays a "You have successfully registered" page. The user can then click the Login link to log in to OpenAM. This is the default selection.
 - User is sent to the login page to authenticate.
12. Under Advanced Configuration, configure the User Registration Confirmation Email URL for your deployment. The default is: `http://openam.example.com:8080/openam/XUI/?realm=#register/`.
13. Click Finish to apply your changes.

2.6. Configuring the Forgotten Password Reset Feature

The forgotten password feature allows existing users to reset their passwords when they cannot remember them.

Procedure 2.6. To Configure the Forgotten Password Feature

1. Log in to the AM console as the administrator.
2. Click Configure > Global Services > User Self Service.
3. On the User Self Service page, click Enabled next to Forgotten Passwords.
4. For Captcha, click Enabled to turn on the Google reCAPTCHA plugin. Make sure you configured the plugin as presented in Section 2.3, "Configuring the Google reCAPTCHA Plugin".
5. For Email Verification, clear the Enabled box if you want to turn off the email verification service. We recommend that you keep it selected.
6. For Security Questions, click Enabled to display security questions to the user during the forgotten password reset process. The user must correctly answer the security questions to be able to reset passwords.
7. In the Forgotten Password Token LifeTime field, enter an appropriate number of seconds for the token lifetime. If the token lifetime expires before the user resets their password, then the user will need to restart the forgotten password process over again.

Default: 900 seconds.

8. To customize the Forgotten Password outgoing email, run the following steps:
 - a. In the Outgoing Email Subject field, enter the subject line of your email in the New Value field, and then click Add.

The subject line format is `lang|subject-text`, where `lang` is the ISO-639 language code, such as `en` for English, `fr` for French, and others. For example, the subject line value could be: `en|Forgotten Password Email`.
 - b. In the Outgoing Email Body field, enter the text of your email in the New Value field, and then click Add.

The email body text format is `lang|email-text`, where `lang` is the ISO-639 language code. Note that email body text must be all on one line and can contain any HTML tags within the body of the text.

For example, the email body text could be: `en|Thank you for request! Click here to reset your password.`

9. Under Advanced Configuration, change the default Forgotten Password Confirmation Email URL for your deployment. The default is: <http://openam.example.com:8080/openam/XUI/?realm=/#passwordReset/>.

2.7. Configuring the Forgotten Username Feature

The forgotten username feature allows existing users to retrieve their usernames when they cannot remember them.

Procedure 2.7. To Configure the Forgotten Username Feature

1. Log in to the AM console as the administrator.
2. Click Configure > Global Services > User Self Service.
3. On the User Self Service page, click Enabled next to Forgotten Username.
4. For Captcha, click Enabled to turn on the Google reCAPTCHA plugin. Make sure you configured the plugin as presented in Section 2.3, "Configuring the Google reCAPTCHA Plugin".
5. For Security Questions, click Enabled to display security questions to the user during the forgotten username process. The users must correctly answer the security questions to be able to retrieve their usernames.
6. For Email Username, click Enabled if you want the user to receive the retrieved username by email.
7. For Show Username, click Enabled if you want the user to see their retrieved username on the browser.
8. In the Forgotten Username Token LifeTime field, enter an appropriate number of seconds for the token lifetime. If the token lifetime expires before the user retrieves their username, then the user will need to restart the forgotten username process.

Default: 900 seconds.

9. To customize the Forgotten Username outgoing email, run the following steps:
 - a. In the Outgoing Email Subject field, enter the subject line of your email in the New Value field, and then click Add.

The subject Line format is `lang|subject-text`, where `lang` is the ISO 639 language code, such as `en` for English, `fr` for French, and others. For example, the subject line value could be: `en|Forgotten username email`.
 - b. In the Outgoing Email Body field, enter the text of your email in the New Value field, and then click Add.

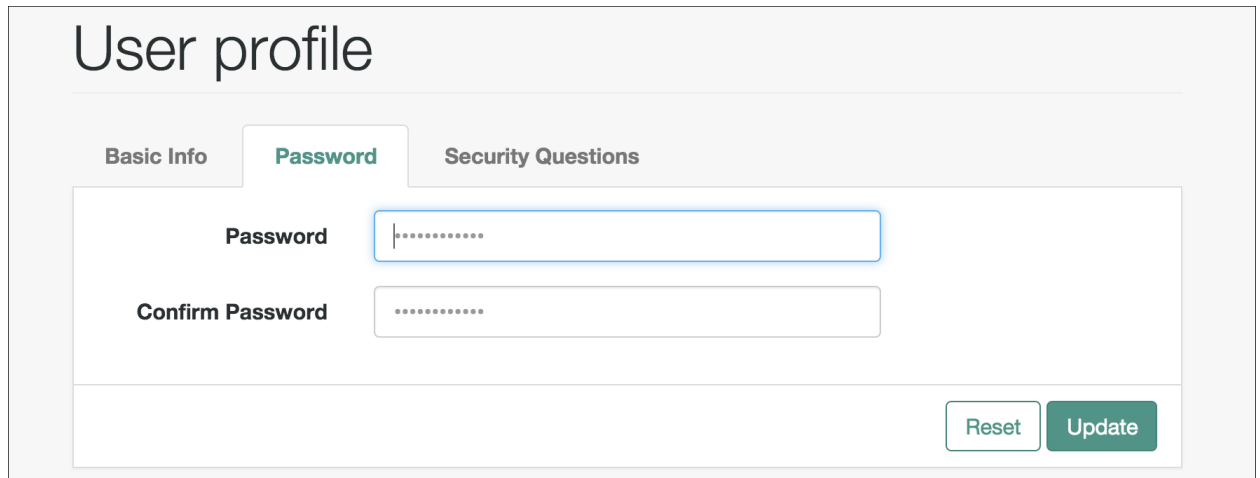
The email body text format is `lang|email-text`, where `lang` is the ISO 639 language code. Note that email body text must be all on one line and can contain any HTML tags within the body of the text.

For example, the email body text could be: `en|Thank you for your inquiry! Your username is %username%.`

2.8. User Management of Passwords and Security Questions

Once the user has self-registered to your system, the user can change their password and security questions at any time on the user profile page. The user profile page provides tabs to carry out these functions.

Figure 2.3. User Profile Page Password Tab



The screenshot shows the 'User profile' page with three tabs: 'Basic Info', 'Password', and 'Security Questions'. The 'Password' tab is active. It contains two input fields: 'Password' and 'Confirm Password', both masked with dots. Below the input fields are two buttons: 'Reset' and 'Update'.

Basic Info	Password	Security Questions
<p>Password <input type="password" value="....."/></p> <p>Confirm Password <input type="password" value="....."/></p> <p><input type="button" value="Reset"/> <input type="button" value="Update"/></p>		

Figure 2.4. User Profile Page Security Questions Tab

User profile

Basic Info

Password

Security Questions

Select security question(s) below. These questions will help us verify your identity if you forget your password.

Security question

What was the name of your childhood pet? ▾

Security answer

.....

Delete

+ Add another question

Reset

Update

Chapter 3

Using User Self Service

This chapter covers client interaction with OpenAM using OpenAM APIs over supported protocols for use with the user self service feature.

3.1. RESTful User Self Service

This section shows how to use the OpenAM RESTful interfaces for user self service functionality: User Self Registration, forgotten password reset, forgotten username retrieval, dashboard configuration, and device profile reset.

The steps to perform user self service via the REST APIs varies depending on the configured User Self Service process flow. For more information, see [Section 1.2, "User Self Service Process Flows"](#).

When performing user self service functions, you can enable one or more security methods, such as email validation, Google reCAPTCHA, knowledge-based authentication, or custom plugins. Each configured security method requires requests to be sent from OpenAM to the client, and completed responses returned to OpenAM to verify.

Important

At least one security method should be enabled for each user self service feature.

A unique token is provided in the second request to the client that must be used in any subsequent responses, so that OpenAM can maintain the state of the user self service process.

In this section, long URLs are wrapped to fit the printed page, and some of the output is formatted for easier reading.

3.2. Registering Users

This section explains how to use the REST APIs for registering a user in OpenAM.

Procedure 3.1. To Register a User with the REST APIs

1. Create a GET request to the `/selfservice/userRegistration` endpoint. Notice that the request does not require any form of authentication.

```
$ curl \
https://openam.example.com:8443/openam/json/realms/root/selfservice/userRegistration
{
  "type": "emailValidation",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Verify your email address",
    "type": "object",
    "required": [
      "mail"
    ],
    "properties": {
      "mail": {
        "description": "Email address",
        "type": "string"
      }
    }
  }
}
```

OpenAM sends the first request for security information. In this example, the first request is of type `emailValidation`, but other types include `captcha` if the Google reCAPTCHA plugin is enabled, and `kbaSecurityAnswerDefinitionStage` if knowledge-based authentication is required.

The `required` array defines the data that must be returned to OpenAM to progress past this step of the registration.

The `properties` element contains additional information about the required response, such as a description of the required field, or the site key required to generate a reCAPTCHA challenge.

2. Create a POST response back to the `/selfservice/userRegistration` endpoint with a query string containing `_action=submitRequirements`. In the POST data, include an `input` element in the JSON structure, which should contain values for each element in the `required` array of the request.

In this example, a `mail` value was requested.

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{"input": {
  "mail": "demo.user@example.com"
}}' \
https://openam.example.com:8443/openam/json/realms/root/selfservice/userRegistration\
?_action=submitRequirements
{
  "type": "emailValidation",
  "tag": "validateCode",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Verify emailed code",
    "type": "object",
    "required": [
      "code"
    ],
    "properties": {
      "code": {
        "description": "Enter code emailed",
        "type": "string"
      }
    }
  },
  "token": "eyJhcHis...PIF-lN4s"
}
```

If the response was accepted, OpenAM continues with the registration process and sends the next request for information. In this example, the email address was accepted and a code was emailed to the address, which OpenAM requires in the response in an element named `code` before continuing.

The value of the `token` element should be included in this and any subsequent responses to OpenAM for this registration.

3. Continue returning POST data to OpenAM containing the requested information, in the format specified in the request. Also return the `token` value in the POST data, so that OpenAM can track which stage of the registration process is being completed.

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{"input": {
  "code": "cf53fcb6-3bf2-44eb-a437-885296899699"
},
"token": "eyJhcHis...PIF-lN4s"
}' https://openam.example.com:8443/openam/json/realms/root/selfservice/userRegistration\
?_action=submitRequirements
{
  "type": "userDetails",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "New user details",
    "type": "object",
    "required": [
      "user"
    ],
    "properties": {
      "user": {
        "description": "User details",
        "type": "object"
      }
    }
  }
},
"token": "eyJhcHis...PIF-lN4s"
}
```

4. When requested—when the `type` value in the request is `userDetails`—supply the details of the new user as an object in the POST data.


```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{
  "input": {
    "user": {
      "username": "demo",
      "givenName": "Demo User",
      "sn": "User",
      "userPassword": "d3m0",
      "inetUserStatus": "Active"
    }
  },
  "token": "eyJhcHis...PIF-lN4s"
}' https://openam.example.com:8443/openam/json/realms/root/selfservice/userRegistration\
?_action=submitRequirements
{
  "type": "selfRegistration",
  "tag": "end",
  "status": {
    "success": true
  },
  "additions": {}
}
```

When the process is complete, the **tag** element has a value of **end**. If the **success** element in the **status** element has a value of **true**, then self-registration is complete and the user account was created.

3.3. Retrieving Forgotten Usernames

This section explains how to use the REST APIs to retrieve a forgotten username.

Procedure 3.2. To Retrieve a Forgotten Username with the REST APIs

1. Create a GET request to the `/selfservice/forgottenUsername` endpoint. Notice that the request does not require any form of authentication.

```
$ curl \
https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenUsername
{
  "type": "captcha",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Captcha stage",
    "type": "object",
    "required": [
      "response"
    ],
    "properties": {
      "response": {
        "recaptchaSiteKey": "6Lfr1...cIqbd",
        "description": "Captcha response",
        "type": "string"
      }
    }
  }
}
```

In this example, the Google reCAPTCHA plugin is enabled, so the first request is of the **captcha** type.

2. Create a POST response back to the **/selfservice/forgottenUsername** endpoint with a query string containing **_action=submitRequirements**. In the POST data, include an **input** element in the JSON structure, which should contain values for each element in the **required** array of the request.

In this example, a **response** value was requested, which should be the user input as provided after completing the Google reCAPTCHA challenge.

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{
  "input": {
    "response": "03AHJ...qiE1x4"
  }
}' https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenUsername\
?_action=submitRequirements
{
  "type": "userQuery",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Find your account",
    "type": "object",
    "required": [
      "queryFilter"
    ],
    "properties": {
      "queryFilter": {
        "description": "filter string to find account",
        "type": "string"
      }
    }
  },
  "token": "eyJhcHis...PIF-lN4s"
}
```

If the response was accepted, OpenAM continues with the username retrieval process and sends the next request for information. In this example, the Google reCAPTCHA was verified and OpenAM is requesting details about the account name to retrieve, which must be provided in a `queryFilter` element.

The value of the `token` element should be included in this and all subsequent responses to OpenAM for this retrieval process.

3. Create a POST response to OpenAM with a `queryFilter` value in the POST data containing the user's email address associated with their account.

For more information on query filters, see [Section 2.3.12, "Query"](#) in the *Development Guide*.

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{
  "input": {
    "queryFilter": "mail eq \"demo.user@example.com\""
  },
  "token": "eyJhcHis...PIF-lN4s"
}' https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenUsername\
?_action=submitRequirements
```

```
{
  "type": "kbaSecurityAnswerVerificationStage",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Answer security questions",
    "type": "object",
    "required": [
      "answer1"
    ],
    "properties": {
      "answer1": {
        "systemQuestion": {
          "en": "What was the model of your first car?"
        },
        "type": "string"
      }
    }
  },
  "token": "eyJhcHis...PIF-lN4s"
}
```

If a single subject is located that matches the provided query filter, the retrieval process continues.

If KBA is enabled, OpenAM requests answers to the configured number of KBA questions, as in this example.

If a subject is not found, an HTTP 400 Bad Request status is returned, and an error message in the JSON data:

```
{
  "code": 400,
  "reason": "Bad Request",
  "message": "Unable to find account"
}
```

4. Return a POST response with the answers as values of the elements specified in the **required** array, in this example **answer1**. Ensure the same **token** value is sent with each response.

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{
  "input": {
    "answer1": "Mustang"
  },
  "token": "eyJhcHis...PIF-lN4s"
}' \
https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenUsername\
?_action=submitRequirements
{
  "type": "retrieveUsername",
  "tag": "end",
  "status": {
    "success": true
  },
  "additions": {
    "userName": "demo"
  }
}
```

When the process is complete, the **tag** element has a value of **end**. If the **success** element in the **status** element has a value of **true**, then username retrieval is complete and the username is emailed to the registered address.

If the Show Username option is enabled for username retrieval, the username retrieved is also returned in the JSON response as the value of the **userName** element, as in the example above.

3.4. Replacing Forgotten Passwords

This section explains how to use the REST APIs to replace a forgotten password.

Procedure 3.3. To Replace a Forgotten Password with the REST APIs

1. Create a GET request to the **/selfservice/forgottenPassword** endpoint. Notice that the request does not require any form of authentication.

```
$ curl \
https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenPassword
{
  "type": "captcha",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Captcha stage",
    "type": "object",
    "required": [
      "response"
    ],
    "properties": {
      "response": {
        "recaptchaSiteKey": "6Lfr1...cIqbd",
        "description": "Captcha response",
        "type": "string"
      }
    }
  }
}
```

In this example the Google reCAPTCHA plugin is enabled, so the first request is of the `captcha` type.

2. Create a POST response back to the `/selfservice/forgottenPassword` endpoint with a query string containing `_action=submitRequirements`. In the POST data, include an `input` element in the JSON structure, which should contain values for each element in the `required` array of the request.

In this example, a `response` value was requested, which should be the user input as provided after completing the Google reCAPTCHA challenge.

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{"input": {
  "response": "03AHJ...qiE1x4"
},
  "https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenPassword\
?_action=submitRequirements
{
  "type": "userQuery",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Find your account",
    "type": "object",
    "required": [
      "queryFilter"
    ],
    "properties": {
      "queryFilter": {
        "description": "filter string to find account",
        "type": "string"
      }
    }
  },
  "token": "eyJhcHis...PIF-lN4s"
}
```

If the response was accepted, OpenAM continues with the password reset process and sends the next request for information. In this example, the Google reCAPTCHA was verified and OpenAM is requesting details about the account with the password to replace, which must be provided in a `queryFilter` element.

The value of the `token` element should be included in this and all subsequent responses to OpenAM for this reset process.

3. Create a POST response to OpenAM with a `queryFilter` value in the POST data containing the username of the subject with the password to replace.

For more information on query filters, see Section 2.3.12, "Query" in the *Development Guide*.

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{"input": {
  "queryFilter": "uid eq \"demo\""
}
```

```

    },
    "token": "eyJhcHis...PIF-lN4s"
  }' https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenPassword\
    ?_action=submitRequirements
{
  "type": "kbaSecurityAnswerVerificationStage",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Answer security questions",
    "type": "object",
    "required": [
      "answer1"
    ],
    "properties": {
      "answer1": {
        "systemQuestion": {
          "en": "What was the model of your first car?"
        },
        "type": "string"
      }
    }
  }
},
"token": "eyJhcHis...PIF-lN4s"
}

```

If a single subject is located that matches the provided query filter, the password reset process continues.

If a subject is not found, an HTTP 400 Bad Request status is returned, and an error message in the JSON data:

```

{
  "code": 400,
  "reason": "Bad Request",
  "message": "Unable to find account"
}

```

4. Continue returning POST data to OpenAM containing the requested information, in the format specified in the request. Also return the **token** value in the POST data, so that OpenAM can track which stage of the password reset process is being completed.


```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{"input": {
  "answer1": "Mustang"
},
"token": "eyJhcHis...PIF-lN4s"
}' https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenPassword\
?_action=submitRequirements
{
  "type": "resetStage",
  "tag": "initial",
  "requirements": {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Reset password",
    "type": "object",
    "required": [
      "password"
    ],
    "properties": {
      "password": {
        "description": "Password",
        "type": "string"
      }
    }
  },
  "token": "eyJhcHis...PIF-lN4s"
}
```

5. When requested—when the `type` value in the request is `resetStage`—supply the new password in the POST data.

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--data \
'{"input": {
  "password": "User1234"
},
"token": "eyJhcHis...PIF-lN4s"}' \
https://openam.example.com:8443/openam/json/realms/root/selfservice/forgottenPassword\
?_action=submitRequirements
{
  "type": "resetStage",
  "tag": "end",
  "status": {
    "success": true
  },
  "additions": {}
}
```

When the process is complete, the `tag` element has a value of `end`. If the `success` element in the `status` element has a value of `true`, then password reset is complete and the new password is now active.

If the password is not accepted, an HTTP 400 Bad Request status is returned, and an error message in the JSON data:

```
{
  "code": 400,
  "reason": "Bad Request",
  "message": "Minimum password length is 8."
}
```

Chapter 4

User Self Service Reference

This chapter covers OpenAM configuration properties for the user self service feature, which is accessible through the Configure tab of the AM console, most of which can also be set by using the **ssoadm** command. The chapter is organized to follow the AM console layout.

4.1. User Self-Service

ssoadm service name: `selfService`

4.1.1. General Configuration

The following settings appear on the **General Configuration** tab:

Encryption Key Pair Alias

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.

For example, you might set this property to: `selfserviceenctest`

ssoadm attribute: `encryptionKeyPairAlias`

Signing Secret Key Alias

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.

For example, you might set this property to: `selfservicesigntest`

ssoadm attribute: `signingSecretKeyAlias`

Google reCAPTCHA Site Key

Google reCAPTCHA plugin site key.

ssoadm attribute: `captchaSiteKey`

Google reCAPTCHA Secret Key

Google reCAPTCHA plugin secret key.

ssoadm attribute: `captchaSecretKey`

Google Re-captcha Verification URL

Google reCAPTCHA plugin verification URL.

Default value: `https://www.google.com/recaptcha/api/siteverify`

ssoadm attribute: `captchaVerificationUrl`

Security Questions

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.

Format is `unique key|locale|question`.

Default value:

```
4|en|What is your mother's maiden name?
3|en|What was the name of your childhood pet?
2|en|What was the model of your first car?
1|en|What is the name of your favourite restaurant?
```

ssoadm attribute: `kbaQuestions`

Minimum Answers to Define

Specifies the minimum number of KBA answers that users must define.

Default value: `1`

ssoadm attribute: `minimumAnswersToDefine`

Minimum Answers to Verify

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 `0` to `50`.

Default value: `1`

ssoadm attribute: `minimumAnswersToVerify`

Valid Query Attributes

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.

Default value:

```
uid
mail
givenName
```

sn

ssoadm attribute: `validQueryAttributes`

4.1.2. User Registration

The following settings appear on the **User Registration** tab:

User Registration

If enabled, new users can sign up for an account.

Default value: `false`

ssoadm attribute: `userRegistrationEnabled`

Captcha

If enabled, users must pass a Google reCAPTCHA challenge during user self-registration to mitigate against software bots.

Default value: `false`

ssoadm attribute: `userRegistrationCaptchaEnabled`

Email Verification

If enabled, users who self-register must perform email address verification.

Default value: `true`

ssoadm attribute: `userRegistrationEmailVerificationEnabled`

Security Questions

If enabled, users must set up their security questions during the self-registration process.

Default value: `false`

ssoadm attribute: `userRegistrationKbaEnabled`

Token Lifetime (seconds)

Maximum lifetime of the token allowing User Self-Registration, in seconds.

Default value: `900`

ssoadm attribute: `userRegistrationTokenTTL`

Outgoing Email Subject

Customize the User Self-Registration verification email subject text. Format is `locale|subject text`.

Default value: `en|Registration_email`

ssoadm attribute: `userRegistrationEmailSubject`

Outgoing Email Body

Customize the User Self-Registration verification email body text. Format is: `locale|body_text`.

Default value: `en|<h2>Click on this link to register.</h2>`

ssoadm attribute: `userRegistrationEmailBody`

Valid Creation Attributes

Specifies a whitelist of user attributes that can be set during user creation.

Default value:

```
userPassword
mail
kbaInfo
givenName
inetUserStatus
sn
username
```

ssoadm attribute: `userRegistrationValidUserAttributes`

Destination After Successful Self-Registration

Specifies the action to be taken after a user successfully registers a new account. Choose from:

- `default`. User is sent to a success page without being logged in.
- `login`. User is sent to the login page to authenticate.
- `autoLogin`. User is automatically logged in and sent to the appropriate page.

The possible values for this property are:

```
default
login
auto-login
```

Default value: `default`

ssoadm attribute: `userRegisteredDestination`

4.1.3. Forgotten Password

The following settings appear on the **Forgotten Password** tab:

Forgotten Password

If enabled, users can reset their forgotten password.

Default value: `false`

ssoadm attribute: `forgottenPasswordEnabled`

Captcha

If enabled, users must pass a Google reCAPTCHA challenge during password reset to mitigate against software bots.

Default value: `false`

ssoadm attribute: `forgottenPasswordCaptchaEnabled`

Email Verification

If enabled, users who reset passwords must perform email address verification.

Default value: `true`

ssoadm attribute: `forgottenPasswordEmailVerificationEnabled`

Security Questions

If enabled, users must answer their security questions during the forgotten password process.

Default value: `false`

ssoadm attribute: `forgottenPasswordKbaEnabled`

Token Lifetime (seconds)

Maximum lifetime for the token allowing forgotten password reset, in seconds.

Specify a value from `0` to `2147483647`.

Default value: `900`

ssoadm attribute: `forgottenPasswordTokenTTL`

Outgoing Email Subject

Customize the forgotten password email subject text. Format is `locale|subject text`.

Default value: `en|Forgotten password email`

ssoadm attribute: `forgottenPasswordEmailSubject`

Outgoing Email Body

Customize the forgotten password email body text. Format is `locale|body text`.

Default value: `en|<h2>Click on this link to reset your password.</h2>`

ssoadm attribute: `forgottenPasswordEmailBody`

4.1.4. Forgotten Username

The following settings appear on the **Forgotten Username** tab:

Forgotten Username

If enabled, users can retrieve their forgotten username.

Default value: `false`

ssoadm attribute: `forgottenUsernameEnabled`

Captcha

If enabled, users must pass a Google reCAPTCHA challenge during the forgotten username retrieval process to mitigate against software bots.

Default value: `false`

ssoadm attribute: `forgottenUsernameCaptchaEnabled`

Security Questions

If enabled, users must answer their security questions during the forgotten username process.

Default value: `false`

ssoadm attribute: `forgottenUsernameKbaEnabled`

Email Username

If enabled, users receive their forgotten username by email.

Default value: `true`

ssoadm attribute: `forgottenUsernameEmailUsernameEnabled`

Show Username

If enabled, users see their forgotten username on the browser page.

Default value: `false`

ssoadm attribute: `forgottenUsernameShowUsernameEnabled`

Token LifeTime (seconds)

Maximum lifetime for the token allowing forgotten username, in seconds.

Default value: 900

ssoadm attribute: forgottenUsernameTokenTTL

Outgoing Email Subject

Customizes the forgotten username email subject text. Format is `locale|subject text`.

Default value: en|Forgotten username email

ssoadm attribute: forgottenUsernameEmailSubject

Outgoing Email Body

Customizes the forgotten username email body text. Format is `locale|body text`.

Default value: en|<h2>Your username is %username%.</h2>

ssoadm attribute: forgottenUsernameEmailBody

4.1.5. Profile Management

The following settings appear on the **Profile Management** tab:

Protected Update Attributes

Specifies a profile's protected user attributes, which causes re-authentication when the user attempts to modify these attributes.

ssoadm attribute: profileProtectedUserAttributes

4.1.6. Advanced Configuration

The following settings appear on the **Advanced Configuration** tab:

User Registration Confirmation Email URL

Specifies the confirmation URL that the user receives during the self-registration process. The `${realm}` string is replaced with the current realm.

Default value: `http://openam.example.com:8080/openam/XUI/?realm=${realm}#register/`

ssoadm attribute: userRegistrationConfirmationUrl

Forgotten Password Confirmation Email URL

Specifies the confirmation URL that the user receives after confirming their identity during the forgotten password process. The `${realm}` string is replaced with the current realm.

Default value: `http://openam.example.com:8080/openam/XUI/?realm=${realm}#passwordReset/`

ssoadm attribute: forgottenPasswordConfirmationUrl

User Registration Service Config Provider Class

Specifies the provider class to configure any custom plugins.

Default value: `org.forgerock.openam.selfservice.config.flows.UserRegistrationConfigProvider`

ssoadm attribute: `userRegistrationServiceConfigClass`

Forgotten Password Service Config Provider Class

Specifies the provider class to configure any custom plugins.

Default value: `org.forgerock.openam.selfservice.config.flows.ForgottenPasswordConfigProvider`

ssoadm attribute: `forgottenPasswordServiceConfigClass`

Forgotten Username Service Config Provider Class

Specifies the provider class to configure any custom plugins.

Default value: `org.forgerock.openam.selfservice.config.flows.ForgottenUsernameConfigProvider`

ssoadm attribute: `forgottenUsernameServiceConfigClass`

4.2. Legacy User Self Service

ssoadm service name: `security`

4.2.1. Realm Defaults

The following settings appear on the *Realm Defaults* tab:

Legacy Self-Service REST Endpoint

Specify whether to enable the legacy self-service endpoint.

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.

The Legacy User Self-Service will be deprecated in a future release.

Default value: `false`

ssoadm attribute: `selfServiceEnabled`

Self-Registration for Users

If enabled, new users can sign up using a REST API client.

Default value: `false`

ssoadm attribute: `selfRegistrationEnabled`

Self-Registration Token LifeTime (seconds)

Maximum life time for the token allowing User Self-Registration using the REST API.

Default value: `900`

ssoadm attribute: `selfRegistrationTokenLifetime`

Self-Registration Confirmation Email URL

This page handles the HTTP GET request when the user clicks the link sent by email in the confirmation request.

Default value: `http://openam.example.com:8080/openam/XUI/confirm.html`

ssoadm attribute: `selfRegistrationConfirmationUrl`

Forgot Password for Users

If enabled, users can assign themselves a new password using a REST API client.

Default value: `false`

ssoadm attribute: `forgotPasswordEnabled`

Forgot Password Token Lifetime (seconds)

Maximum life time for the token that allows a user to process a forgotten password using the REST API.

Default value: `900`

ssoadm attribute: `forgotPasswordTokenLifetime`

Forgot Password Confirmation Email URL

This page handles the HTTP GET request when the user clicks the link sent by email in the confirmation request.

Default value: `http://openam.example.com:8080/openam/XUI/confirm.html`

ssoadm attribute: `forgotPasswordConfirmationUrl`

Destination After Successful Self-Registration

Specifies the behavior when self-registration has successfully completed.

The possible values for this property are:

```
default
login
autologin
```

Default value: `default`

ssoadm attribute: `userRegisteredDestination`

Protected User Attributes

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.

ssoadm attribute: `protectedUserAttributes`

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.

Glossary

Access control	Control to grant or to deny access to a resource.
Account lockout	The act of making an account temporarily or permanently inactive after successive authentication failures.
Actions	Defined as part of policies, these verbs indicate what authorized subjects can do to resources.
Advice	In the context of a policy decision denying access, a hint to the policy enforcement point about remedial action to take that could result in a decision allowing access.
Agent administrator	User having privileges only to read and write policy agent profile configuration information, typically created to delegate policy agent profile creation to the user installing a policy agent.
Agent authenticator	Entity with read-only access to multiple agent profiles defined in the same realm; allows an agent to read web service profiles.
Application	<p>In general terms, a service exposing protected resources.</p> <p>In the context of OpenAM policies, the application is a template that constrains the policies that govern access to protected resources. An application can have zero or more policies.</p>
Application type	<p>Application types act as templates for creating policy applications.</p> <p>Application types define a preset list of actions and functional logic, such as policy lookup and resource comparator logic.</p>

	Application types also define the internal normalization, indexing logic, and comparator logic for applications.
Attribute-based access control (ABAC)	Access control that is based on attributes of a user, such as how old a user is or whether the user is a paying customer.
Authentication	The act of confirming the identity of a principal.
Authentication chaining	A series of authentication modules configured together which a principal must negotiate as configured in order to authenticate successfully.
Authentication level	Positive integer associated with an authentication module, usually used to require success with more stringent authentication measures when requesting resources requiring special protection.
Authentication module	OpenAM authentication unit that handles one way of obtaining and verifying credentials.
Authorization	The act of determining whether to grant or to deny a principal access to a resource.
Authorization Server	In OAuth 2.0, issues access tokens to the client after authenticating a resource owner and confirming that the owner authorizes the client to access the protected resource. OpenAM can play this role in the OAuth 2.0 authorization framework.
Auto-federation	Arrangement to federate a principal's identity automatically based on a common attribute value shared across the principal's profiles at different providers.
Bulk federation	Batch job permanently federating user profiles between a service provider and an identity provider based on a list of matched user identifiers that exist on both providers.
Circle of trust	Group of providers, including at least one identity provider, who have agreed to trust each other to participate in a SAML v2.0 provider federation.
Client	In OAuth 2.0, requests protected web resources on behalf of the resource owner given the owner's authorization. OpenAM can play this role in the OAuth 2.0 authorization framework.
Conditions	Defined as part of policies, these determine the circumstances under which which a policy applies. Environmental conditions reflect circumstances like the client IP address, time of day, how the subject authenticated, or the authentication level achieved.

	Subject conditions reflect characteristics of the subject like whether the subject authenticated, the identity of the subject, or claims in the subject's JWT.
Configuration datastore	LDAP directory service holding OpenAM configuration data.
Cross-domain single sign-on (CDSSO)	OpenAM capability allowing single sign-on across different DNS domains.
Delegation	Granting users administrative privileges with OpenAM.
Entitlement	Decision that defines which resource names can and cannot be accessed for a given subject in the context of a particular application, which actions are allowed and which are denied, and any related advice and attributes.
Extended metadata	Federation configuration information specific to OpenAM.
Extensible Access Control Markup Language (XACML)	Standard, XML-based access control policy language, including a processing model for making authorization decisions based on policies.
Federation	Standardized means for aggregating identities, sharing authentication and authorization data information between trusted providers, and allowing principals to access services across different providers without authenticating repeatedly.
Fedlet	Service provider application capable of participating in a circle of trust and allowing federation without installing all of OpenAM on the service provider side; OpenAM lets you create Java Fedlets.
Hot swappable	Refers to configuration properties for which changes can take effect without restarting the container where OpenAM runs.
Identity	Set of data that uniquely describes a person or a thing such as a device or an application.
Identity federation	Linking of a principal's identity across multiple providers.
Identity provider (IdP)	Entity that produces assertions about a principal (such as how and when a principal authenticated, or that the principal's profile has a specified attribute value).
Identity repository	Data store holding user profiles and group information; different identity repositories can be defined for different realms.
Java EE policy agent	Java web application installed in a web container that acts as a policy agent, filtering requests to other applications in the container with policies based on application resource URLs.

Metadata	Federation configuration information for a provider.
Policy	Set of rules that define who is granted access to a protected resource when, how, and under what conditions.
Policy Agent	Agent that intercepts requests for resources, directs principals to OpenAM for authentication, and enforces policy decisions from OpenAM.
Policy Administration Point (PAP)	Entity that manages and stores policy definitions.
Policy Decision Point (PDP)	Entity that evaluates access rights and then issues authorization decisions.
Policy Enforcement Point (PEP)	Entity that intercepts a request for a resource and then enforces policy decisions from a PDP.
Policy Information Point (PIP)	Entity that provides extra information, such as user profile attributes that a PDP needs in order to make a decision.
Principal	<p>Represents an entity that has been authenticated (such as a user, a device, or an application), and thus is distinguished from other entities.</p> <p>When a Subject successfully authenticates, OpenAM associates the Subject with the Principal.</p>
Privilege	In the context of delegated administration, a set of administrative tasks that can be performed by specified subjects in a given realm.
Provider federation	Agreement among providers to participate in a circle of trust.
Realm	<p>OpenAM unit for organizing configuration and identity information.</p> <p>Realms can be used for example when different parts of an organization have different applications and user data stores, and when different organizations use the same OpenAM deployment.</p> <p>Administrators can delegate realm administration. The administrator assigns administrative privileges to users, allowing them to perform administrative tasks within the realm.</p>
Resource	<p>Something a user can access over the network such as a web page.</p> <p>Defined as part of policies, these can include wildcards in order to match multiple actual resources.</p>
Resource owner	In OAuth 2.0, entity who can authorize access to protected web resources, such as an end user.

Resource server	In OAuth 2.0, server hosting protected web resources, capable of handling access tokens to respond to requests for such resources.
Response attributes	Defined as part of policies, these allow OpenAM to return additional information in the form of "attributes" with the response to a policy decision.
Role based access control (RBAC)	Access control that is based on whether a user has been granted a set of permissions (a role).
Security Assertion Markup Language (SAML)	Standard, XML-based language for exchanging authentication and authorization data between identity providers and service providers.
Service provider (SP)	Entity that consumes assertions about a principal (and provides a service that the principal is trying to access).
Session	The interval that starts with the user authenticating through OpenAM and ends when the user logs out, or when their session is terminated. For browser-based clients, OpenAM manages user sessions across one or more applications by setting a session cookie. See also Stateful session and Stateless session .
Session high availability	Capability that lets any OpenAM server in a clustered deployment access shared, persistent information about users' sessions from the CTS token store. The user does not need to log in again unless the entire deployment goes down.
Session token	Unique identifier issued by OpenAM after successful authentication. For a Stateful session , the session token is used to track a principal's session.
Single log out (SLO)	Capability allowing a principal to end a session once, thereby ending her session across multiple applications.
Single sign-on (SSO)	Capability allowing a principal to authenticate once and gain access to multiple applications without authenticating again.
Site	<p>Group of OpenAM servers configured the same way, accessed through a load balancer layer.</p> <p>The load balancer handles failover to provide service-level availability. Use sticky load balancing based on <code>amlbcookie</code> values to improve site performance.</p> <p>The load balancer can also be used to protect OpenAM services.</p>
Standard metadata	Standard federation configuration information that you can share with other access management software.
Stateful session	An OpenAM session that resides in the Core Token Service's token store. Stateful sessions might also be cached in memory on one or

more OpenAM servers. OpenAM tracks stateful sessions in order to handle events like logout and timeout, to permit session constraints, and to notify applications involved in SSO when a session ends.

Stateless session

An OpenAM session for which state information is encoded in OpenAM and stored on the client. The information from the session is not retained in the CTS token store. For browser-based clients, OpenAM sets a cookie in the browser that contains the session information.

Subject

Entity that requests access to a resource

When a subject successfully authenticates, OpenAM associates the subject with the [Principal](#) that distinguishes it from other subjects. A subject can be associated with multiple principals.

User data store

Data storage service holding principals' profiles; underlying storage can be an LDAP directory service, a relational database, or a custom [IdRepo](#) implementation.

Web policy agent

Native library installed in a web server that acts as a policy agent with policies based on web page URLs.