

SafeNet Authentication Manager Integration Guide

Using RADIUS Protocol for ForgeRock OpenAM

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013302-001, Rev. A

Release Date: October 2015

Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	4
Environment	4
Audience	5
RADIUS-based Authentication using SAM	5
RADIUS Authentication Flow using SAM	5
RADIUS Prerequisites	6
Configuring SafeNet Authentication Manager	6
Synchronizing Users Stores to SAM	6
Configuring SAM's Connector for OTP Authentication	7
Assigning a Token in SAM	7
Adding ForgeRock OpenAM as a RADIUS Client in IAS/NPS	8
Configuring SAM's OTP Plug-In for Microsoft RADIUS Client	9
Configuring ForgeRock OpenAM	10
Running the Solution	16
Support Contacts	17

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as ForgeRock OpenAM.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

ForgeRock OpenAM provides open-source authentication, authorization, entitlement, and federation software.

Built for today's digital challenges, ForgeRock OpenAM is designed to give customers not only context-aware single sign-on access, but also a personalized experience on any digital channel, whether a mobile device, connected car, home appliance, or whatever the next connected innovation might be. OpenAM has a highly scalable, modular, easy-to-deploy architecture. Through ForgeRock OpenAM, the community actively continues development of OpenSSO.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in ForgeRock OpenAM using SafeNet one-time password (OTP) tokens managed by SafeNet Authentication Manager.
- Configure ForgeRock OpenAM to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the ForgeRock OpenAM environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

ForgeRock OpenAM can be configured to support multi-factor authentication in several modes. RADIUS protocol will be used for the purpose of working with SafeNet Authentication Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM that is used to deploy the solution on-premises in the organization.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Manager**—Version 8.2 (Hotfix 710)
- **ForgeRock OpenAM**—Version 12.0.0

Audience

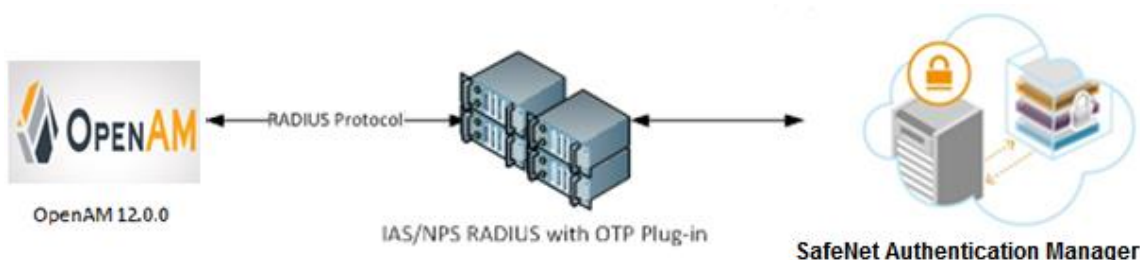
This document is targeted to system administrators who are familiar with ForgeRock OpenAM, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager.

RADIUS-based Authentication using SAM

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SAM.

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft's IAS or NPS, providing strong, authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

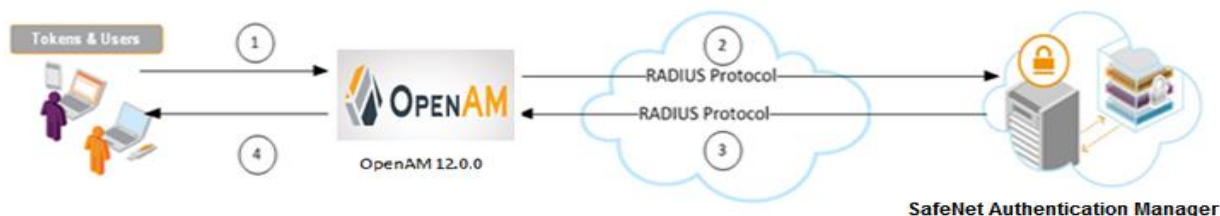


For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

RADIUS Authentication Flow using SAM

SafeNet Authentication Manager communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for ForgeRock OpenAM.



1. A user attempts to log on to ForgeRock OpenAM using an OTP token.
2. ForgeRock OpenAM sends a RADIUS request with the user's credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to ForgeRock OpenAM.
4. The user is granted or denied access to ForgeRock OpenAM based on the OTP value calculation results from SAM.

RADIUS Prerequisites

To enable SafeNet Authentication Manager to receive RADIUS requests from ForgeRock OpenAM, ensure the following:

- End users can authenticate from the ForgeRock OpenAM environment with a static password before configuring ForgeRock OpenAM to use RADIUS authentication.
- Ports 1812/1813 are open to and from ForgeRock OpenAM.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
- Java Development Kit (JDK) must be installed on the client machine.
- ForgeRock OpenAM must be deployed on the Apache Tomcat server.

Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM with ForgeRock OpenAM using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SAM, page 6
- Configuring SAM's Connector for OTP Authentication, page 7
- Assigning a Token in SAM, page 7
- Adding ForgeRock OpenAM as a RADIUS Client in IAS/NPS, page 8
- Configuring SAM's OTP Plug-In for Microsoft RADIUS Client, page 9

Synchronizing Users Stores to SAM

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Microsoft Active Directory 2003, 2008, and 2008 R2
- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SAM's Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the **Simplified OTP-only** configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The **Simplified OTP-only** configuration is as follows:

- **Connectors**—SAM Connector for OTP Authentication is installed
- **SAM Back-end Service**—Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.
- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Assigning a Token in SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through ForgeRock OpenAM.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization's premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet's tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Adding ForgeRock OpenAM as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in ForgeRock OpenAM.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in ForgeRock OpenAM.

ForgeRock OpenAM must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize ForgeRock OpenAM for authentication.



NOTE: It is assumed that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS, and are very similar to IAS.

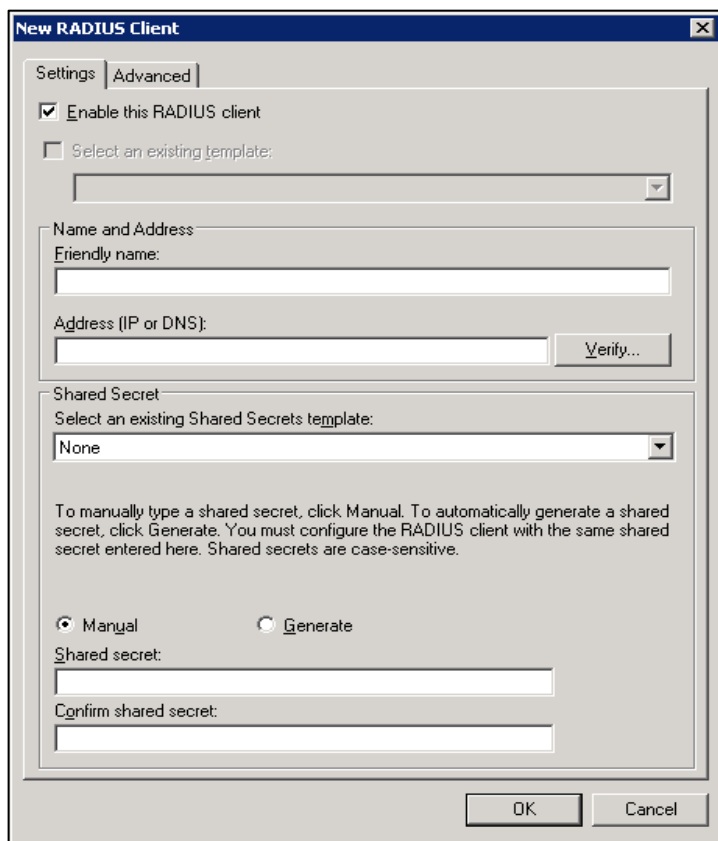
1. Click **Start > Administrative Tools > Network Policy Server**.
2. From the NPS web console, in the left pane, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients** and then click **New**.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. On the **New RADIUS Client** window, on the **Settings** tab, complete the following fields:

Enable this RADIUS client	Select this option.
Friendly name	Enter a RADIUS client name (for example, OpenAM).
Address (IP or FQDN)	Enter the ForgeRock OpenAM IP address or DNS.
Manual/Generate	Select Manual .
Shared secret	Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in ForgeRock OpenAM.
Confirm shared secret	Re-enter the shared secret.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. Click **OK**. ForgeRock OpenAM is added as a RADIUS client in NPS.

Configuring SAM's OTP Plug-In for Microsoft RADIUS Client

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug ins for the authentication process.

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft's IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator's Guide.

Configuring ForgeRock OpenAM

Configure ForgeRock OpenAM to use a RADIUS server for user authentication.

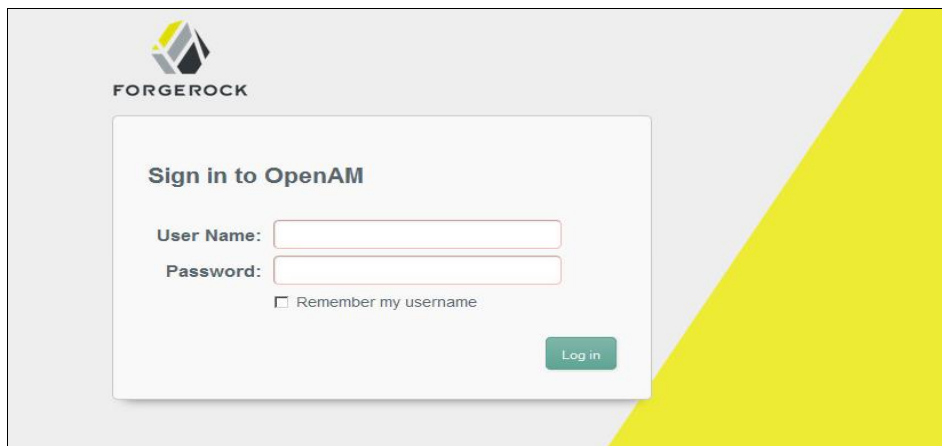
1. In a web browser, open this URL:

https://<FQDN_of_client_machine>:8080/<Name_of_OpenAM_application>

where, **FQDN_of_client_machine** is the full domain name of the client machine, **8080** is the default Apache server port number, and **Name_of_OpenAM_application** is the name of the OpenAM application specified when deploying on the Apache server.

Example: **https://openam.sso.com:8080/OpenAM-12.0.0**

2. On the **Sign in to OpenAM** window, enter the administrator user name and password, and then click **Log in**.



(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

3. On the **OpenAM Administrative Console** window, click the **Access Control** tab.



(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

4. In the **Realm Name** column, click the **/(Top Level Realm)** hyperlink.

5. Click the **Authentication** tab.

The screenshot shows the ForgeRock OpenAM Administration Console. At the top, the user is logged in as 'amAdmin' on the 'ash-server'. The navigation bar includes tabs for General, Authentication (selected), Services, Data Stores, Privileges, Policies, Subjects, Agents, and STS. The main content area is titled '(Top Level Realm) - Authentication' and includes 'Save', 'Reset', and 'Back to Access Control' buttons. On the left, there are links for 'Core' and 'Module Instances'. The 'Core' section is expanded, showing 'All Core Settings...'. Under 'Organization Authentication Configuration', the 'IdapService' is selected for the 'Default Authentication Chain for users'. Similarly, 'IdapService' is selected for the 'Administrator Authentication Configuration' and 'Default Authentication Chain for administrators'. The 'Default Success Login URL' section shows 'Current Values' as '/OpenAM-12.0.0/console' with a 'Remove' button. Below this is a 'New Value' input field and an 'Add' button. A note at the bottom states: 'Successful logins will be forwarded to this URL'.

(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

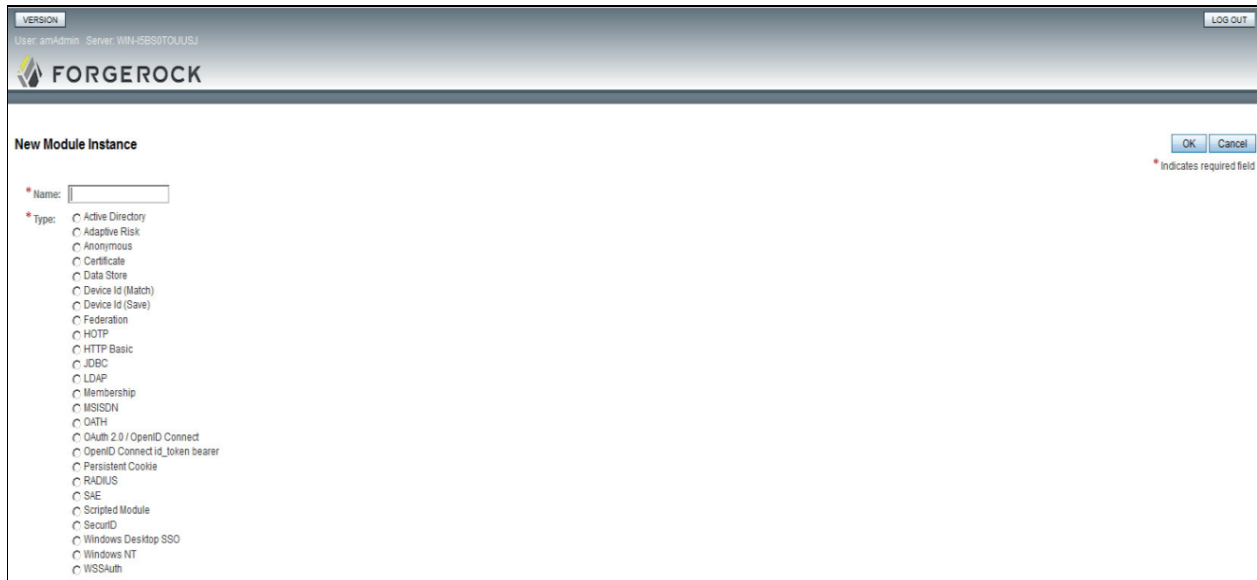
6. Scroll down to the **Module Instances** section, and then click **New**.

The screenshot shows the 'Module Instances' section of the ForgeRock OpenAM Administration Console. It features a table titled 'Module Instances (7 Items)' with columns for 'Name' and 'Type'. The table lists seven modules: DataStore, Federation, HOTP, LDAP, OATH, SAE, and WSSAuthModule. Each row has a checkbox in the 'Name' column. Below the table, a note states: 'The list of authentication modules available to this realm'.

Name	Type
<input type="checkbox"/> DataStore	Data Store
<input type="checkbox"/> Federation	Federation
<input type="checkbox"/> HOTP	HOTP
<input type="checkbox"/> LDAP	LDAP
<input type="checkbox"/> OATH	OATH
<input type="checkbox"/> SAE	SAE
<input type="checkbox"/> WSSAuthModule	WSSAuth

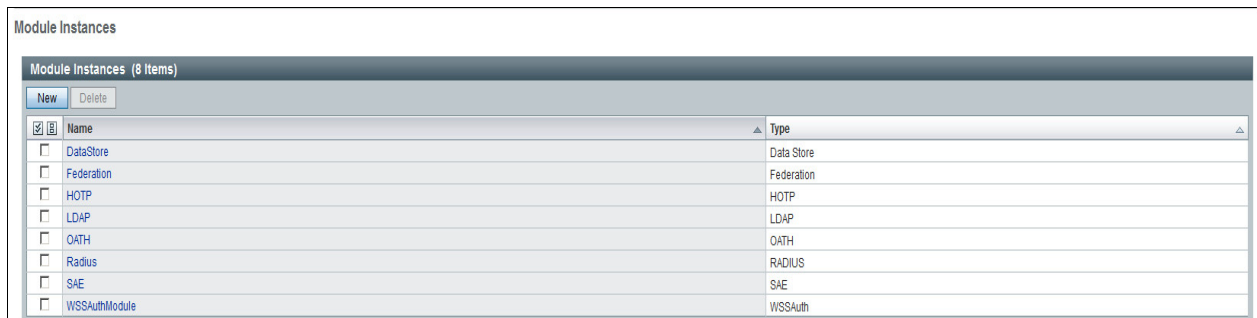
(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

7. In the **Name** field, enter a name for the RADIUS module instance (for example, **Radius**).



(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

8. In the **Type** field, select the **RADIUS** option, and then click **OK**.
9. In the **Module Instances** list, the newly created entry (for example, **Radius**) will appear. In the **Name** column, click this newly created instance hyperlink (for example, **Radius**).



Name	Type
DataStore	Data Store
Federation	Federation
HOTP	HOTP
LDAP	LDAP
OATH	OATH
Radius	RADIUS
SAE	SAE
WSSAuthModule	WSSAuth

(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)



NOTE: If the newly created instance is not visible, refresh the page. The error message “**Authentication instance <instance name> already exists.**” is shown. Ignore this error and click **Cancel**.

10. Complete the following details, and then click **Save**.

Primary Radius Servers	In the New Value text box, enter the IP Address of the primary RADIUS server, and then click Add .
Secondary Radius Servers	(Optional) In the New Value text box, enter the IP Address of the secondary RADIUS server, and then click Add .
Shared Secret	Enter the shared secret for the RADIUS client.
Shared Secret (confirm)	Re-enter the shared secret.
Port Number	Enter 1812 as the RADIUS server port.
Timeout	(Optional) Enter time in seconds, or keep the default value.
Authentication Level	Keep the default value.

The screenshot shows the ForgeRock RADIUS configuration page. The 'Primary Radius Servers' section has a 'Current Values' list and a 'New Value' text box with an 'Add' button. The 'Secondary Radius Servers' section has a similar 'Current Values' list and 'New Value' text box with an 'Add' button. Below these are fields for 'Shared Secret', 'Shared Secret (confirm)', 'Port Number' (set to 1812), 'Timeout' (set to 3), 'Health check interval' (set to 5), and 'Authentication Level' (set to 0). The 'Save' button is visible at the bottom right.

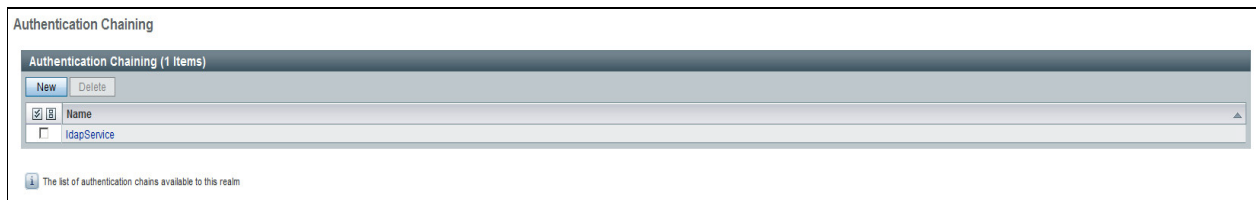
(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

11. The message, "Profile was updated." is displayed. On the right side of the window, click **Back to Authentication**.

The screenshot shows the same ForgeRock RADIUS configuration page, but now a yellow information box is displayed in the center, stating 'Profile was updated.' The 'Back to Authentication' button is visible on the right side of the page.

(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

12. Scroll down to the **Authentication Chaining** section, and then click **New**.



(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

13. On the **New Authentication Chain** window, in the **Name** field, enter a descriptive name, and then click **OK**.



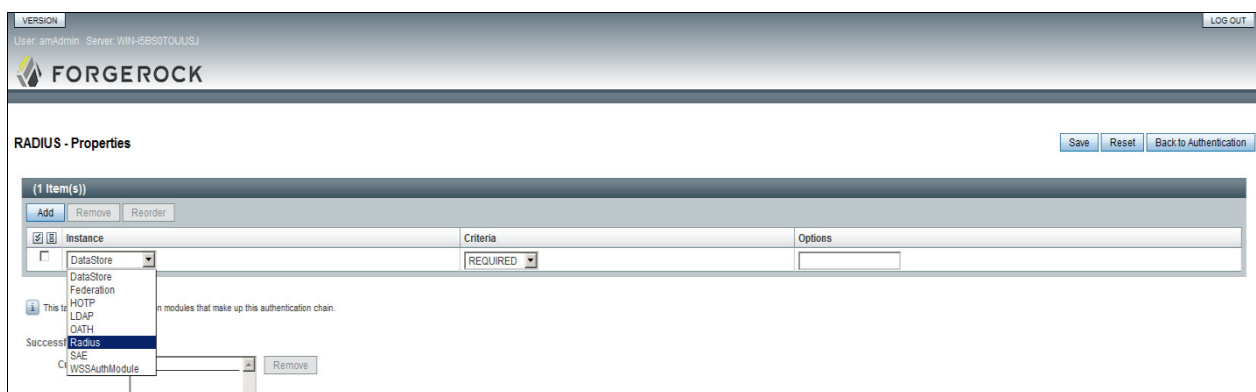
(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

14. On the **RADIUS-Properties** window, click **Add**.



(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

15. In the **Instance** column, select the newly created RADIUS module instance (for example, **Radius**), and then click **Save**.



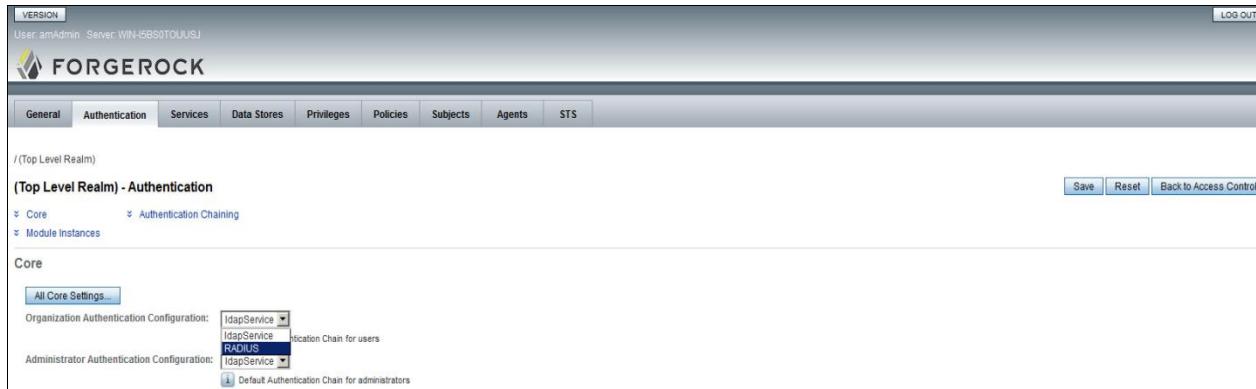
(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

16. The message, “The authentication chain properties were updated.” is displayed. On the right side of the window, click **Back to Authentication**.



(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

17. On the **Authentication** tab, under the **Core** section, in the **Organization Authentication Configuration** field, select the newly created authentication chain (for example, **RADIUS**), and then click **Save**.



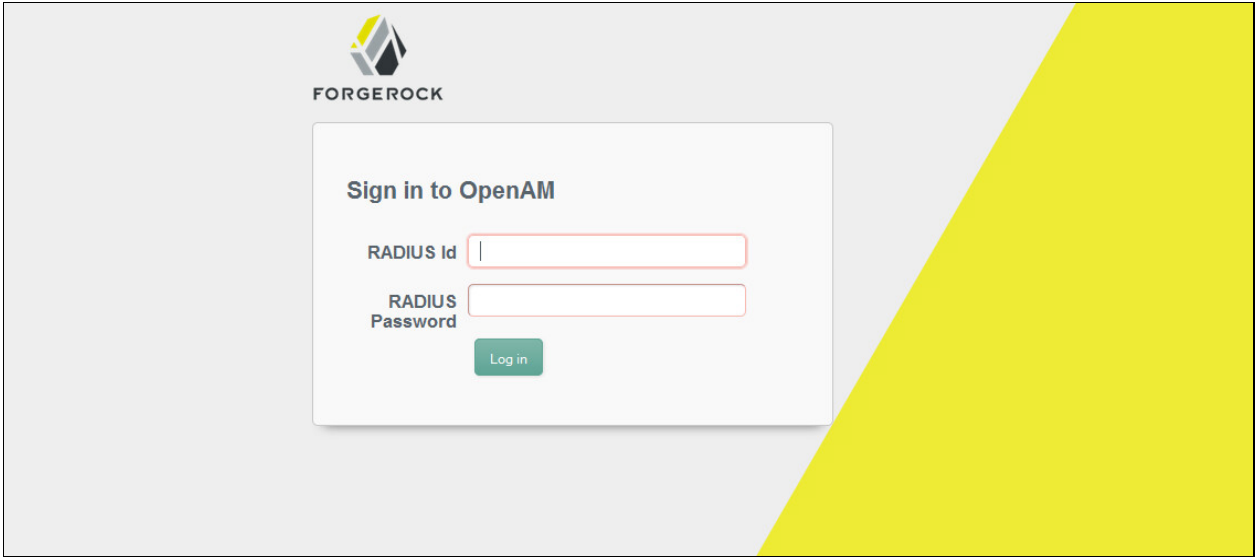
(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

Running the Solution

For this integration, the SafeNet eToken PASS is configured for authentication with the SAM solution. Before running the solution, ensure that the Tomcat server is running.

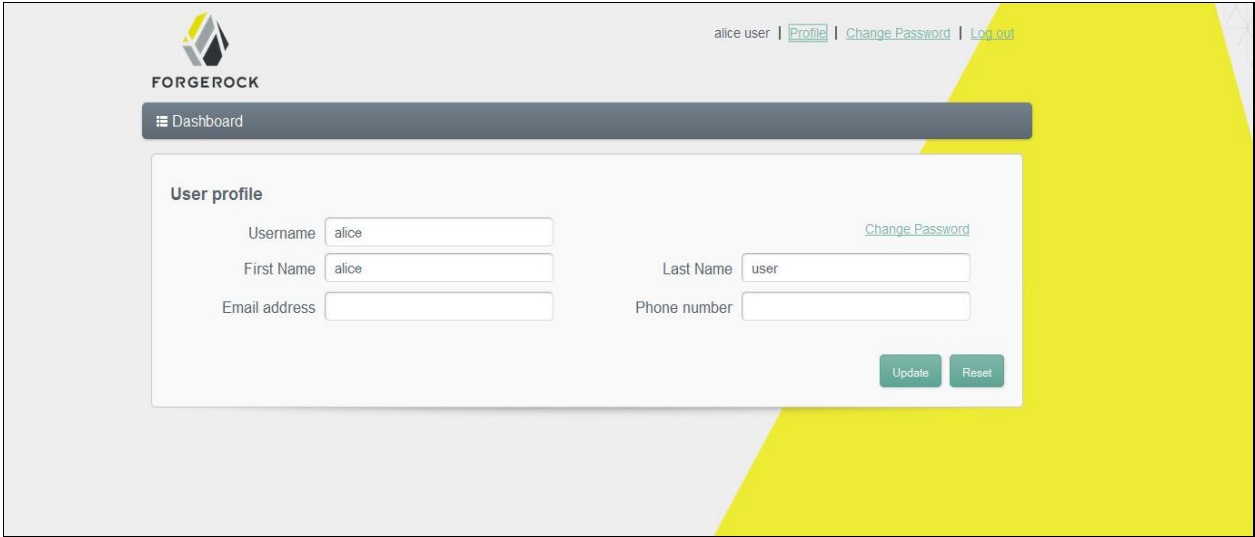
1. In a web browser, open your OpenAM application.
2. On the login window, complete the following fields, and then click **Log in**.

RADIUS Id	Enter your user name.
RADIUS Password	Generate an OTP using the SafeNet eToken PASS token, and then enter that OTP in this field.



(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

If the credentials are validated, you are successfully logged in.



(The screen image above is from ForgeRock® software. Trademarks are the property of their respective owners.)

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	