Enabling Multi-Factor Authentication Using Advanced Authentication for the Forgotten Password Module

October 2021.

Let us assume Reltic Data, Inc. wants to implement multi-factor authentication for the Forgotten Password module. This document explains the prerequisites, flow of actions, and step-by-step configuration details to achieve this.

This example refers to the following user profiles:

- Susan: An administrator of Reltic Data, Inc.
- Sam: An employee of Reltic Data, Inc.

Susan, an administrator, wants to enforce multi-factor authentication with the Card and Email OTP methods for changing the password. After multi-factor authentication is implemented, Sam needs to authenticate both methods to change his password successfully.

- "Prerequisites" on page 1
- "Configuring Advanced Authentication Server" on page 2
- "Configuring Self Service Password Reset for Advanced Authentication" on page 4
- "End User Tasks" on page 5

Prerequisites

When using Advanced Authentication for the Forgotten Password module, Susan must ensure the following:

- Install and configure the Advanced Authentication server. For more information about installing and configuring the Advanced Authentication server, see the Advanced Authentication- Server Installation and Upgrade (https://www.netiq.com/documentation/advanced-authentication-63/install-upgrade-guide/data/bookinfo.html) and Configuring Advanced Authentication (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/part_config_applnc.html).

- An LDAP repository for Reltic Data, Inc is configured, and the repository contains the information of all users. For more information, see Adding a Repository (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/add_repo.html) in the Advance Authentication Server Administration Guide (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/bookinfo.html).

  This example uses Active Directory Domain Services as an LDAP repository.

Configuring Advanced Authentication Server

Susan must first configure the Advanced Authentication server and then add Advanced Authentication server details in Self Service Password Reset to integrate both products. Perform the following steps to configure the Advanced Authentication server:

1. Log in to the Advanced Authentication Administrative Portal as an administrator.
2. Configure the Card (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/card.html) and Email OTP (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/email_otp.html) methods in Methods (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/config_methods.html). The Card and Email OTP methods work as expected with the pre-defined value.

   The Advanced Authentication methods verify the identity of a user who tries to access resources. Instead of challenge-response, this example uses the methods in Advanced Authentication to verify the identity of a Sam.

   NOTE: For more information to use the card method, see the following links:

   For more information to identify and obtain ideal contactless card readers and cards for employees, see Supported Card Readers and Cards (https://www.netiq.com/documentation/advanced-authentication-63/device-service-installation/data/supported_card_readers_and_cards.html#supported_card_readers_and_cards).

   For more information to install Advanced Authentication Device Service, see Installing and Upgrading Device Service (https://www.netiq.com/documentation/advanced-authentication-63/device-service-installation/data/installing_and_upgrading_device_service.html#installing_and_upgrading_device_service).

   For more information about the parameters specific to the card reader are configured in the Device Service, see Configuring the Card Settings.

   ---

3. Open **Chains > New Chain**.

   A chain is a combination of methods. A user needs to execute and succeed all methods of a chain to be authenticated.
4. Specify the following details:

Field	Description
Name	A name for the chain. **NOTE:** Ensure to remember the name of the chain for further use. In this example, we named the chain as Card+ Email ID.
Is enabled	Set to **ON** to enable the chain.
Methods	Select the Card and Email OTP methods to add to the chain.

5 Click **Save**.

6 Click **Events > New Event**.

Advanced Authentication provides authentication events for Self Service Password Reset. An event leverages the Advanced Authentication functionalities for Self Service Password Reset. Self Service Password Reset triggers the respective authentication event when a user tries to access it.

7 Specify the following details:

Field	Action
Name	Specify a unique name for this event.
Is enabled	Ensure that this option is set to **ON**.
Event type	Select **OAuth2/OpenID Connect**.
Chains	Select the Card+ Email ID chain that you created in Step 4.
Client ID	Copy this client ID to use later in the Self Service Password Reset configuration.
Client secret	Copy this client secret to use later in the Self Service Password Reset configuration.
Redirect URIs. One URI per line	Specify the Self Service Password Reset site URL with /public/oauth at the end of the URL. Open **Configuration Editor > Settings > Application > Application** in the your Self Service Password Reset, then you can find the site URL in **Site URL**. In this example: `https://realticsol/sspr/public/oauth`

8 Click **Save**.

9 Open **Policies > Web Authentication**.

10 Specify the Identity Provider URL in **Identity Provider URL**.

11 Click **Download IdP SAML 2.0 Metadata** and save it.

12 Click **Save**.

13 Open **Policies > Mail Sender** to configure the Email OTP method.

14 Specify the following details:

Field	Description
Host	Specify the outgoing mail server name.
Port	Specify the port number.
Username	Specify the username of an account that is used to send the authentication email messages.
Password	Specify the password for the specified account.
Sender email	Specify the email address of the sender.

15 Click **Save**.

16 Open **Server Options**.

17 Enable **WebAuth**.

NOTE: Susan is required to enable web authentications only in Advance Authentication 6.3 Service Pack 1 and later versions.

---

18 Click **Save**.

Configuring Self Service Password Reset for Advanced Authentication

After configuring Advanced Authentication, Susan needs to perform the following steps to configure Self Service Password Reset:

1 Log in to Self Service Password Reset as an administrator.

2 In the top-right corner of the Dashboard screen, click the user name.

3 Click **Configuration Editor**.

4 Open **Modules > Public > Forgotten Password > Profiles > default > Definition > Verification Method**.

5 Set **Challenge/Response Answers** to **Optional**.

6 Set **OAuth** to **Optional**.

7 Change **Minimum Optional Required** to a value of 1.

8 In the toolbar, click **Save changes**.

9 Open **Modules > Public > Forgotten Password > Profiles > default > OAuth**.

10 In **OAuth Login URL**, click the **Edit** icon, then specify the Identity Provider URL added in Advanced Authentication.

For example, `https://oauthserver.example.com/osp/a/idm/auth/oauth2/auth`.

11 In **OAuth Code Resolve Service URL**, click **Add Value** to specify the Advanced Authentication Resolve Service URL.

For example, `https://dns-name-advanced-authentication/osp/a/TOP/auth/oauth2/authcoderesolve`.

12 In **OAuth Profile Service URL**, click **Add Value** to specify the web service URL provided by the Advanced Authentication to return attribute data about the user.

For example, `https://dns-name-advanced-authentication/osp/a/TOP/auth/oauth2/getattributes`.

13 Click **Import From Server** in **OAuth Web Service Server Certificate** to import the certificate from the Advanced Authentication server.

NOTE: To import the certificate, you must resolve the domain name within the Serf Service Password reset docker's host file.

---

14 In **OAuth Client ID**, click **Add**, and paste the Client ID from Advanced Authentication.

15 In **OAuth Shared Secret**, click **Store Value**, and paste the Client secret from Advance Authentication.

16 In **OAuth User Name/DN Login Attribute**, click **Add Value**, specify `user_name`.

17 In **OAuth Inject User Name Value**, click **Add Value**, then add your Advanced Authentication repository name with a macro appended containing the user name.

   In this example, the value is `sspredir\@LDAP:cn@`.

18 In the toolbar, click **Save changes**.

End User Tasks

Sam, an employee, must perform the following actions to change his password:

NOTE: Sam must be enrolled with his Email OTP and Card. For more information, see Card (https://www.netiq.com/documentation/advanced-authentication-63/server-user-guide/data/cardnewui.html) and Email OTP (https://www.netiq.com/documentation/advanced-authentication-63/server-user-guide/data/email_otpnewui.html) method enrollment in the Advanced Authentication- User (https://www.netiq.com/documentation/advanced-authentication-63/server-user-guide/data/bookinfo.html) guide.

---

1 Launch `https://realticsol/sspr/private/login`.

2 Click **Forgotten Password**.

3 Specify the username.

4 Click **Search**.

5 Select **External OAuth Authentication**.

   The page redirects to the Advanced Authentication server authentication screen.

   Ensure the card reader is plugged into the workstation.

6 Select the Chain.

7 Click **Next**.

8 Tap the card on the reader.

9 Check Sam's email. Sam will receive an email with an OTP.

10 Specify the OTP from email in **Password**.

11 Click **Next**.

   The page redirects to the Self Service Password Reset page.

12 Specify the new password in **New Password** and **Confirm Password**.

13 Click **Change Password**.

   Now, Sam can login with the new password.

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

© Copyright 2021 Micro Focus or one of its affiliates.