Advanced Authentication 6.4 Service Pack 1 Patch 1 Release Notes

March 2023

Advanced Authentication 6.4 Service Pack 1 Patch 1 includes enhancements, and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Advanced Authentication forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources. You can also post or vote for the ideas of enhancement requests in the Ideas forum (https://ideas.microfocus.com/MFI/advance-authentication).

For more information about this release and the latest release notes, see the NetIQ Advanced Authentication Documentation (https://www.netiq.com/documentation/advanced-authentication-64/) page.

If you have suggestions for documentation improvements, click comment on this topic at the bottom of the specific page in the HTML version of the documentation posted at the NetIQ Advanced Authentication Documentation (https://www.netiq.com/documentation/advanced-authentication-64/) page.

What's New?

Advanced Authentication 6.4 Service Pack 1 Patch 1 provides the following:

- "Enhancements" on page 1
- "Security Improvement" on page 2

Enhancements

Advanced Authentication 6.4 Service Pack 1 Patch 1 includes the following enhancements:

- "FIDO2 Improvements" on page 2
- "Ability to Add Twilio Subaccounts in the SMS Sender Policy" on page 2
- "An Option to Allow Third-Party Service Providers to Select the Chain for Any Client" on page 2

FIDO2 Improvements

The following enhancements have been added to the FIDO2 method:

◆ **Ability to Enroll Resident Credentials**

The administrator can allow users to enroll the FIDO2 method and store the Resident Credentials (security key) on the FIDO2-compliant device (YubiKey). With Resident Credentials, users can experience seamless login without specifying their username and password.

◆ **Username-less Login Support**

Advanced Authentication extends the FIDO2 method to support the username-less authentication to the Web Authentication events. The enrolled FIDO2 card contains the username. When the user taps the card, the username is filled in the respective field automatically. To configure the username-less authentication, three options have been introduced in the FIDO2 method.

◆ **Ability to Disable the PIN Prompt**

Advanced Authentication facilitates the administrator to mandate or hide the PIN prompt when users enroll, test and authenticate with the FIDO2 method.

For more information, see FIDO2 in the *Advanced Authentication - Administration* guide.

Ability to Add Twilio Subaccounts in the SMS Sender Policy

This release provides ability to add the subaccounts of Twilio Parent account. With subaccounts, you can add Country Codes based on the customer's (SMS receivers) geographic location. The subaccounts distinguish the usage based on team, customer or product, and provides clear billing data. Also, allows resource (phone number) mapping.

For more information, see SMS Sender in the *Advanced Authentication - Administration* guide.

An Option to Allow Third-Party Service Providers to Select the Chain for Any Client

This release introduces the **Enable client chain selection** option in the **Web Authentication** policy to allow the third-party service providers to select a preferred chain for any client, such as Windows Client, Mac OS X Client, and Linux PAM Client workstation. Then, route users to the selected chain during authentication.

For more information, see Enabling the Client Chain Selection (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/web_auth.html#allow_client_chain_selection) in the *Advanced Authentication - Administration* guide.

Security Improvement

Advanced Authentication 6.4 Service Pack 1 Patch 1 release addresses CVE-2023-24468.

Resolved Issues

This release includes the following software fixes:

Component	Description
Administration	When a user sets **Enable linked chains** to **ON** in the **Linked Chain** policy, then the **Required Chain** list in the **New Chain** does not display all the available chains.

Component	Description

Administration	On the **New Enrollment Portal**, enrollment of the U2F method fails on the following browser:
	
	    ◆ Google Chrome
	    ◆ Microsoft Edge
	    ◆ Mozilla Firefox

Administration	The **Enable event selection** option is modified to **Enable client event selection** in the **Web Authentication** policy.
Administration	The **Disable Offline Authentication** option is modified to **Disable Offline OTP Options** in the **Smartphone** method.
Smartphone	When a user tries to authenticate with the **FIDO2** method, a prompt to specify the PIN (User Verification) is not displayed on the Android devices.
Smartphone	When a user attempts to authenticate with the NetIQ Advanced Authentication iOS smartphone application by using the facial recognition, the application does not identify the face and prompts the user to re-authenticate. Users are experiencing infinite authentication loop.
Smartphone	When a user sets the **Face ID** option to **ON** in the NetIQ Advanced Authentication iOS smartphone application settings for face recognition authentication. Later, the user is unable to set the **Face ID** option to **OFF**.
Smartphone	When a user sets the smartphone language to Arabic, the NetIQ Advanced Authentication iOS smartphone application stops working.
Windows Client	While connecting to the remote desktop on the Windows Client, the Advanced Authentication Credential Provider does not display the chains that require Device Service for the elevated access.

Upgrading

You can directly upgrade to Advanced Authentication 6.4 Service Pack 1 Patch 1 from 6.4.1.

NOTE: The following is the recommended upgrade sequence:

1 Advanced Authentication servers
2 Plug-ins
3 Client components

   Any change in the upgrade sequence is not supported.

NOTE: The RAM requirements of Advanced Authentication have been changed in 6.4 as follows:

◆ Minimum: 8 GB per server.
◆ Recommended: 12 GB per server

Before upgrading your Advanced Authentication cluster to 6.4, ensure that the environment complies with the new requirements.

For more information, see Advanced Authentication System Requirements.

Known Issue

Advanced Authentication 6.4 Service Pack 1 Patch 1 does not have any known issue.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice