Advanced Authentication 6.4 Service Pack 2 Patch 1 Release Notes

December 2023

Advanced Authentication 6.4 Service Pack 2 Patch 1 includes enhancements, improves usability, 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 as part of OpenText Cybersecurity 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.

IMPORTANT: Advanced Authentication 6.4.2.1 removes the **Bluetooth** method. Hence, before upgrading to Advanced Authentication 6.4.2.1, the administrator must remove or replace the **Bluetooth** method from all the existing authentication chains and events to avoid failure of user logins.

What's New?

Advanced Authentication 6.4 Service Pack 2 Patch 1 provides the following:

- "Enhancements" on page 2
- "Security Improvements" on page 2

Enhancements

Ability to Auto-Enroll the PKI Method Based on Directory Attribute

Advanced Authentication facilitates auto-enrollment of smart cards using the PKI method. The auto-enrollment capability is dependent on the availability of a specific value in the `altSecurityIdentities` attribute of the LDAP repository for a specific user.

The auto-enrollment is supported on Windows machines that have the Advanced Authentication Device Service installed.

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

Security Improvements

Advanced Authentication 6.4 Service Pack 2 Patch 1 includes the following security improvements:

- Apache Tomcat has been upgraded to address the issue of false positive vulnerabilities identified by scanning tools.
- Addresses CVE-2023-38545 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38545).
- Advanced Authentication server now supports authentication through a unique **Client Secret** to create a secure connection between the OAuth 2 application and the Advanced Authentication server.

Resolved Issues

This release includes the following software fixes:

Component	Description of the Issue
Web Authentication, New Enrollment UI, OAuth, and SAML2 Events	If a user selected the desired chain on the **Select Authentication Chain** screen during the login process, the user could not authenticate by pressing the Enter key. Instead, the user had to press the Tab key and then the Enter key, or the user had to use the mouse to click the **Next** button.
Administration Portal	After upgrading to Advanced Authentication 6.4 Service Pack 2, the **Username-less login enabled** toggle button and **Username-less login RP ID** option under the **FIDO2** method were not displayed.
Windows Client	After setting the parameter `forceCachedLogon` to `True` in the `config.properties` file, when a user tried to authenticate to a Windows workstation with **Card** and **PKI** methods using the 1:N feature, the following error message was displayed after tapping the card on the reader: `Template not found error message`
Web Authentication	Users with very large `userGroup` attributes were rejected by the nginx reverse proxy and were unable to log in.
Web Portal	After upgrading to Advanced Authentication 6.4 Service Pack 2, if the user entered the card PIN using the **PKI** and **Card** method and pressed the Enter key instead of clicking the **Next** button, the user login failed.

Component	Description of the Issue
Administration Portal	After upgrading to Advanced Authentication 6.4 Service Pack 2, the **Enable client event selection** and **Enable client chain selection** options under the **Web Authentication** policy were not displayed.
Administration Portal	After upgrading to Advanced Authentication 6.4 Service Pack 2, when an administrator attempted to add a new site in the clustered environment, the newly added node joined the cluster, but a randomly selected node disappeared from the cluster. If you examined the cluster status page for the disappeared node, an error message was displayed. However, the other nodes in the cluster did not display any error message and persisted in the replication process.
Administration Portal	After upgrading to Advanced Authentication 6.4 Service Pack 2, when an administrator tried to set the **Relative Intervals** in the **Dashboard** to less than an hour or less than one hour, the following error message was displayed: `RequestError RequestError(400, 'x_content_parse_exception', '[1:331] [date_histogram] failed to parse field [calendar_interval]') (Internal Server Error)`
Windows Client	When you removed the U2F, FIDO, PKI, and Card devices from a computer, it did not force log off or lock a session.
Administration Portal	When an administrator attempted to export the Replication logs, the replication log files were not exported in the downloaded folder.
Windows Client	When a user attempted to authenticate to a Windows workstation in offline mode using the **FIDO2** method, the authentication process was unsuccessful, and the following error message was displayed: `No message received`
Administration Portal	The administrators were unable to install Open VM Tools because the libxmlsec1-1 file was missing from the Advanced Authentication 6.4 appliance.

Upgrading

You can directly upgrade to Advanced Authentication 6.4 Service Pack 2 Patch 1 from 6.4.2.

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 Issues

Advanced Authentication 6.4 Service Pack 2 Patch 1 does not have any known issues.

Planned End of Support

The following options will not be available in an upcoming Advanced Authentication release:

- Old Enrollment Portal
  - The Old Enrollment Portal will be deprecated in the Advanced Authentication 6.4 Service Pack 3 release.
  - The **Enrollment Options** policy will no longer be available.
  - The new features and functionalities are implemented for the New Enrollment Portal.
  - With the Advanced Authentication 6.4 Service Pack 2 release, the New Enrollment Portal is set as the default enrollment option (**Enable New Enrollment Options** in the **Enrollment Options** policy is set to **ON**).
- Repo Agent
  - Support for the Repo Agent will be deprecated starting with the Advanced Authentication 6.4 Service Pack 3 release.
  - As there are no changes to the component, the Repo Agent is not shipped along with Advanced Authentication 6.4 Service Pack 2 Patch 1.
  - Repo Agent-related configuration in the administrator portal is not available.
- Support for the following Operating Systems will be deprecated starting with the Advanced Authentication 6.4 Service Pack 3 release:
  - macOS Catalina
  - macOS Big Sur including M1 chip in the emulation mode
  - CentOS 8
  - SUSE Linux Enterprise Desktop 12 Service Pack4
  - SUSE Linux Enterprise Server 12 Service Pack4
  - SUSE Linux Enterprise Server 15 Service Pack1, Service Pack2, and Service Pack3
  - Red Hat Enterprise Linux Workstation 7
  - Red Hat Enterprise Linux Server 7
  - Debian 9
  - Ubuntu 16 and 18

- Microsoft Windows 8.1
- Microsoft Windows 10 v1903, v1909, v2004, and 20H2
- Microsoft Windows Server 2012 R2

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