Advanced Authentication 6.4 Service Pack 1 Release Notes

November 2022

Advanced Authentication 6.4 Service Pack 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 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 provides the following:

Enhancements

Advanced Authentication 6.4 Service Pack 1 includes the following enhancements:

API Support for Auto-Enrollment of the Web Authentication Method

An API has been introduced for the enrolling the Web Authentication method. This API supports userID parameter received from third-party services to complete the enrollment.

A Drop-Down list for NameID Formatting in the SAML Event

This release combines multiple NameID format options into a single list, **NameID formatting options** in the SAML event. This list includes the following options:

- Use Default
- Send Email as NameID (suitable for G-Suite)
- Send SAMAccount as NameID
- Send CN as NameID
- Send Immutable ID (User objectId) as NameID (required for Microsoft Office 365)

For more information, see Creating a SAML 2.0 Event in the *Advanced Authentication - Administration* guide.

Syslog Improvements

This release includes the following improvements to the Syslog records:

- Code **107** is introduced in the Syslog records to indicate the user has been locked after several failed attempts.
- CEF extensions are mapped to equivalent fields on the remote Syslog server to comply with the RFC standards.

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

Ability to Detect the Presence of the Device Service

With this release, Advanced Authentication can detect whether the Device Service is available when the U2F method is used for authentication. If Device Service is available then use it to perform U2F authentication. If not, then initiate the Web Authentication API for validating U2F details.

An Option to Allow Third-Party Service Providers to Select an Event

This release introduces the **Enable event selection** option in **Web Authentication** policy to allow the third-party service providers to select a preferred event and route users to the selected event post-authentication.

For more information, see Enabling the Event Selection in the *Advanced Authentication - Administration* guide.

Support for Installing Advanced Authentication Linux PAM Client on the AIX Server Joined to the AD Domain

This release supports Advance Authentication Linux PAM Client installation on the AIX server joined to the AD domain.

For more information, see Installing and Uninstalling Linux PAM Client on AIX Server in the *Advanced Authentication- Linux PAM Client* guide.

A New Custom Attribute in the SAML Assertion

This release introduces an Active Directory attribute, **objectGUID**, to the SAML assertion for uniquely identifying an object. SAML assertion passes attributes to the Service Provider to describe the user. Users can customize the name of **objectGUID** attribute and send the SAML assertion as required.

For example, if a user's service provider does not recognize the **objectGUID** attribute but recognizes the **object_guid** attribute, then the user can change the name of attribute to meet the service provider's requirements.

Security Improvements

This release includes the following improvements:

- Apache Commons Text library has been updated to enhance the security.
- Resolves the potential access control bypass. (CVE-2022-38753 (https://cve.report/CVE-2022-38753))

  Micro Focus would like to offer a special thanks to Daniel Egelseer (Austria) for responsible disclosure of this security vulnerability.

Resolved Issues

This release includes the following software fixes:

Component	Description
Administration Portal	The data and graphs displayed on the Dashboard are not up to date. The data and graph are displayed until the date when the settings are last saved. However, the data gets updated when the administrator manually updates the **Dashboard Settings**.
Administration Portal	Specifying color in the RGB format or keeping the following fields empty in the **Custom Branding** policy results in an error message: ◆ **Title Text Color** ◆ **Background Color** ◆ **Background Color Right** Therefore, you must set the colors in the Hexadecimal format.
Administration Portal	The **Is Expired** column is removed from the **Licenses** widget of Dashboard, as it does not provide clear details about the expiry status of a specific license and causes confusion.

Component	Description
Administration Portal	The full synchronization process marks several active users for deletion. Due to this issue, active users cannot log in. This issue occurs after upgrading to Advanced Authentication 6.3 Service Pack 4 Patch 1 release.
Administration Portal	Use of special characters in the ClientID and Secret of OAuth events causes the Web Authentication parsing error.
Administration Portal	The customized brand settings break after upgrading to Advanced Authentication 6.4. This issue occurs due to the missing custom branding JAR file.
Administration Portal	Implementing the Per Tenant Hostname (PTH) feature breaks the Web Authentication method.
Administration Portal	The administrator is unable to remove the LDAP repository when the LDAP server is unavailable. The following error message is displayed: `Cannot connect to the LDAP server`
Administration Portal	The existing OAuth integrations fail after the upgrade to Advanced Authentication 6.4.
Administration Portal	When the name and number of a particular Server Metric tile are too long, then the content that is extending outside the tile is wrapped that misaligns the tile position.
Administration Portal	On the Linux PAM Client, the **End User License Agreement Message** is not formatted properly.
Appliance	Deleting the reports from the Administration Portal does not delete the exported reports (CSV and JSON) in the `/var/lib/docker/volumes/aaf_aucore-data/_data/reports` path even after rebooting the appliance.
Appliance	The upgrade of Web Servers to Advanced Authentication 6.4 fail in the cluster environment.
CAF Portal	The upgrade to Advanced Authentication 6.4 fails if the connection is via proxy.
CAF Portal	In Advanced Authentication 6.4, exporting of the Digital Certificate results in an error.
Enrollment Portal	After integrating Advanced Authentication with Access Manager using the SAML event, the redirection from Access Manager to the Enrollment Portal fails and results in a 404 error. This happens due to the missing text `webauth/` in the Callback URL.
Enrollment Portal	The enrollment of the Web Authentication Method fails even when the administrator has configured the method with valid details.

Component	Description
Linux PAM Client	When a user selects an authentication chain with the Fingerprint method on the Linux PAM client, an error message `Invalid access: cannot convert empty value` is displayed. Now, if the Fingerprint reader is not connected to the Linux machine and user attempts to log in, the authentication chain with the Fingerprint method is not displayed.
OAuth and SAML Events	The SAML Service Provider method with improper configuration bypasses authentication and grants access without any validation to the associated OAuth and SAML events.
Old Enrollment Portal	On the old Enrollment Portal, enrollment of the U2F method fails when using the Chrome browser.
SAML Event	When Advanced Authentication and Cisco AnyConnect are integrated using the SAML event, the login page is not displayed appropriately.
Web Authentication	With one Web Authentication event active for a user and the user tries to log in to another Web Authentication event, an error message stating to log out from the previous event is displayed.
Web Authentication	An authentication attempt to the Web Authentication event fails if the **Background Color** is set with RGB values in the **Custom Branding** policy. This occurs due to the use of transparent colors. Therefore, administrators must set the colors in the Hexadecimal format.
Windows Client	When users try to authenticate to Windows Client using the FIDO2 method with NFC capability, an invalid error message `Please connect a FIDO2 token` is displayed though the reader is connected to the system.
Windows Client	An invalid error message is displayed when a user removes the NFC-supported card from the card reader while authenticating to Windows Client using the Card method. Now, the following message is displayed when the user removes NFC supported card from the reader during authentication: `Tap your security key again on the reader`

Upgrading

You can directly upgrade to Advanced Authentication 6.4 Service Pack 1 from 6.4 and 6.3.7.

NOTE: The upgrade from Advanced Authentication 6.3 to 6.4 Service Pack 1 is not supported. It is required to upgrade to Advanced Authentication 6.3.7 before upgrading to Advanced Authentication 6.4 Service Pack 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 includes the following known issue:

An Issue with Web Authentication Events

Users can authenticate the OAuth2 and SAML2 events without enrolling the authentication method in the associated chain. This issue is noticed when Advanced Authentication is integrated with NetIQ Access Manager and the Security Questions method is available in the associated chain.

Deprecated Options

Advanced Authentication 6.4 Service Pack 1 deprecates the following:

- Bluetooth method

  NOTE: We recommend administrators to remove or replace the Bluetooth method from existing authentication chains and events. Advanced Authentication 6.4 Service Pack 1 blocks logins from chains that include the Bluetooth Method. Also, users cannot enroll or log in with the Bluetooth method.

- Push salt TTL and Authentication salt TTL options from the Smartphone method

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