Advanced Authentication 6.4 Service Pack 2 Release Notes

September 2023

Advanced Authentication 6.4 Service Pack 2 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: Before attempting to upgrade from Advanced Authentication 6.4.x to 6.4.2, it is recommended to verify that the server has minimum of 40% free disk space for seamless upgrade and performance.

Use the following command in the appliance console to verify the free disk space:

```
df -h /dev/sda1
```

IMPORTANT: Before upgrading to Advanced Authentication 6.4.2, the administrator must remove or replace the Bluetooth method from all existing authentication chains and events. Advanced Authentication 6.4.2 removes the Bluetooth method and might result in failure of user logins if the Bluetooth method is not removed.

What’s New?

Advanced Authentication 6.4 Service Pack 2 provides the following:

- “New Feature” on page 2
- “Enhancements” on page 2
- “Security Improvements” on page 5

New Feature

This release includes the following feature:

Support for the Bluetooth eSec Method

Advanced Authentication facilitates contactless authentication with the **Bluetooth eSec** method. Users can authenticate to any web application and Windows Client using the Bluetooth supported device within the discoverable range.

NOTE: Logon using the **Bluetooth eSec** method to the Linux PAM Client and Mac OS Client are not supported in this release.

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

Enhancements

Advanced Authentication 6.4 Service Pack 2 includes the following enhancements:

- Client Login Extension Integration
- Support for Windows 11 Operating System
- Enhanced WebAuth Logs
- TLS Upgrade
- Improved Error Messages for the HANIS Face Method
- Ability to Prevent Users from Updating LDAP Password in the Self-Service Portal
- Ability to Send Customized LDAP Attribute In the SAML Assertion
- An Option to Send the Custom User Attributes as NameID In the SAML Response
- New Parameters for PKI Service
- Step-Up Authentication Support for OAuth2 and SAML2 Events
- Ability to Improve the OSP Security
- Ability to Disable TLS 1.2
- Ability to Add Multiple Intermediate Certificates with the Same Subject Name

Client Login Extension Integration

This release introduces the `CLEIntegeration` configuration setting to enable Windows Client integration with Client Login Extension (CLE) and Self Service Password Reset (SSPR). This setting allows users to reset their LDAP password that comply with the configured SSPR password policy.

For more information, see Integrating with Client Login Extension in the Advanced Authentication - Windows Client guide.

Support for Windows 11 Operating System

In this release the following components of Advanced Authentication supports Windows 11 version 21H2 and 22H2 operating system:

- Device Service
- Authentication Agent
- Virtual Desktop Agent
- Desktop OTP Tool
- Windows Client

Enhanced WebAuth Logs

WebAuth logs are enhanced by adding a unique ID for users, to trace their authentication attempts.

TLS Upgrade

In this release, Advanced Authentication supports TLS v1.3 that the Device Service uses for establishing a secure connection with the Advanced Authentication Server.

For more information, see Configuring the TLS Version in the Advanced Authentication - Device Service guide.

Improved Error Messages for the HANIS Face Method

This release improves the error messages displayed for the HANIS Face authentication issues to enhance the troubleshooting experience.

For more information, see Testing the HANIS Face Authenticator in the Advanced Authentication- User guide.

Ability to Prevent Users from Updating LDAP Password in the Self-Service Portal

This release introduces the **Disable password change in Self-Service portal** option in the **LDAP Password** method that enables you to hide the current and new LDAP password fields on the Self-Service Portal. This prevents the user from updating their LDAP password that is stored in the repository and bypassing the Self Service Password Reset policy during enrollment.

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

Ability to Send Customized LDAP Attribute In the SAML Assertion

This release enables administrators to customize the LDAP repository attributes and display the customized attributes in the SAML assertion.

For more information, see Customizing LDAP Attributes in the SAML Assertion in the Advanced Authentication - Administration guide.

An Option to Send the Custom User Attributes as NameID In the SAML Response

In addition to predefined attributes that can be sent as NameID in the SAML assertion for the service provider, Advanced Authentication allows administrators to send custom user attributes, such as UPN (User Principal Name), Windows domain qualified name, and so on as NameID. Use the **NameID Format** list to select the preferred format.

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

New Parameters for PKI Service

This release introduces the following new parameters in the Advanced Authentication Device Service:

- `pki.manufacturerID.<pki_lib_name>`
- `pki.model.<pki_lib_name>`

These parameters enable the Device Service to identify and select the right PKI devices and collect the inputs.

For more information, see Identifying and Selecting the PKI Device in the Advanced Authentication - Device Service guide.

Step-Up Authentication Support for OAuth2 and SAML2 Events

Advanced Authentication simplifies the user experience with the step-up authentication feature. The step-up authentication facilitates users to authenticate with a method just once throughout the session and prevents re-authentication with the same method that has succeeded for another event during the session.

For more information, see Creating an OAuth 2.0 / OpenID Connect Event and Creating a SAML 2.0 Event in the Advanced Authentication - Administration guide.

Ability to Improve the OSP Security

This release introduces the **Enable Content Security Policy for Webauth Service** option in the **HTTPS Options** policy which allows you to append the Content Security Policy (CSP) to Web Authentication URLs, such as New Enrollment login, OAuth2, and SAML2 events.

This protects users from the Cross-Site Scripting (XSS) and clickjacking attacks.

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

Ability to Disable TLS 1.2

This release introduces the **Enable TLS 1.2** option in the **HTTPS Options** policy. This allows the administrator to enable or disable the communication between the Advanced Authentication Server and clients using TLS 1.2.

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

Ability to Add Multiple Intermediate Certificates with the Same Subject Name

In this release, Advanced Authentication allows an administrator to upload multiple intermediate CA certificates with the same `SubjectName` but a unique `SubjectKeyIdentifier`.

Security Improvements

This release includes updates to the following components to improve security:

- Postgres database
- Zlib library
- Jetty web server
- The web server is improved to include a **Cache-Control** header with appropriate directives
- The Device Service debug logs are improved to hide the PKI device PIN in the logs

Resolved Issues

This release includes the following software fixes:

Component	Description
Administration Portal	Even when the administrator sets **Disable Offline OTP Options** to **ON** in the **Smartphone** method, the **Offline OTP Options** option is displayed during authentication to the **Web Authentication** event.
Administration Portal	When an administrator configures the **CEF Log Forward** policy with the transport type set to **TCP with TLS**, the CEF forwards the logs to an external Syslog server without verifying the certificate.
Administration Portal	When an administrator configures the **Facial Recognition** method with the **Contactable KYC Service** as the API provider and then switches to the **Azure Cognitive Services**, the following error message is displayed on the Windows Client when a user tries to authenticate using the Facial recognition method: `Face Service not available`
Administration Portal	When an administrator creates new users and attempts to configure the **Emergency Password** method for those users by using REST API, then users are unable to use the **Emergency Password** method. Later, an administrator attempts to delete those users from the repository using REST API, then the repository displays two records of enrolled users. This is due to the same Base DN for users with two or more different LDAP repositories.
Administration Portal	If an IPv6 address is assigned while installing Advanced Authentication Server under a static IP, the appliance console appears blank and the web server displays the following error message: `Appliance is under maintenance/starting up`
Administration Portal	While integrating Access Manager with Advanced Authentication in a clustered environment, OAuth integration frequently fails with some of the Advanced Authentication servers in the cluster.
Administration Portal	If an administrator attempts to access the logs available on the Administration Portal by using the URL without being authenticated, the website turns blank, and users are unable to authenticate.

Component	Description
Administration Portal	When an administrator sets the Risk Service to **Manual** and attempts to reboot it, then the Risk Service does not start automatically after the reboot.
Administration Portal	After upgrading the Global Master Server from 6.3 Service Pack 7 Patch 2 to 6.4 Service Pack 1 Patch 1, the `aucore` container does not start. If you attempt to start the `aucore` container, an error message is displayed.
Administration Portal	When an unauthenticated user attempts to access the Advanced Authentication Syslog page by entering the URL (aaserver.com/admin/logs/syslog), it displays the faint Advanced Authentication Syslog page with no log information and the user interface with no data instead of redirecting the user to the login page for authentication.
Administration and Helpdesk Portal	Administration and Helpdesk portals display the chain icon instead of the specific method icon.
All clients	The cache service logs the SSL certificate version mismatch error in the `cacheservice.log` file. The following error message is displayed: `CERTIFICATE VERSION MISMATCH !!!`
Enrollment Portal	While enrolling the **Smartphone** method, the database deadlock can cause a temporary replication conflicts between the servers in a cluster.
Enrollment Portal	After upgrading to Advanced Authentication 6.4 Service Pack 1 with the defined event category, the Enrollment Portal displays the error message `Method exists in the category`. This prevents users from enrolling new methods and viewing the enrolled methods.
Enrollment Portal	While logging in to the Enrollment Portal, if the user's account is locked out because of exceeding failed login attempts than the configured number of **Attempts failed** values in the **Lockout options** policy, the Syslog displays `Error Code 102` instead of `Error Code 107`.
Enrollment Portal	When a user logs in to the Enrollment Portal using the **Web Authentication** method and attempts to logout, the Advanced Authentication Server logs the user out. However user remains logged into the upstream provider such as Access Manager. As a result, when the second user logs in to the Enrollment Portal with the same browser, the user is still authenticated to the upstream provider but with their own Advanced Authentication credentials.
HANIS Face	When a user attempts to authenticate using the HANIS Face method through a Device Service, the following error message is displayed while scanning the face: `CAPTURE_ERROR`
HANIS Face	When the user attempts to authenticate with the NetIQ Advanced Authentication server using the **HANIS Face** method with someone else's credentials, they can authenticate successfully by scanning their face regardless of the actual user's enrolled face in the National Identification System.

Component	Description
Helpdesk Portal	If the administrator renames the default administrator username of the **Local Repository** and the helpdesk user logs into Helpdesk Portal with the renamed username and clicks the **User Report** tab to monitor the authentication report of the specific user, the following error message is displayed: `User not found`
Helpdesk Portal	The **Result** column on the **User Report** page does not display a check mark or X mark to indicate whether authentication is successful or failed.
Linux PAM Client	The required Linux PAM client configuration is not available when using the eDirectory repository. When eDirectory is used as the LDAP repository then ensure Linux PAM Client's realm name matches the repository name for SSH logins.
New Enrollment Portal	The New Enrollment portal fails to remove the **Display Name** of the enrolled **Card** method once it is set to a non-empty value. Once the display name for the **Card** method is set to a non-empty value, it can be modified but cannot be reset to an empty value.
Out-of-Band Portal	While logging in to Out-of-Band portal, the sensitive inputs, such as the answers to the security questions and TOTP inputs, are not hidden by default. The user must click the hide button in order to manually hide input data.
RADIUS Event	After upgrading to Advanced Authentication 6.3 Service Pack 7, the `radiusd` service on the RADIUS server stops working in high utilization after about a week of uptime.
Web Portal	When a user enrolls multiple tokens for a **FIDO2** method, the Advanced Authentication Windows credential provider, Web Authentication portal, and all the Web portals display the Event Category selection option when authenticating by using **FIDO2**method. The user must select the specific category with which they will authenticate when using **FIDO2** method. Now, the Event Category selection option will not be displayed on any of the Advanced Authentication portals while authenticating by using **FIDO2**.
Windows Client	While logging into the Windows client, the replication conflict occurs intermittently.

Upgrading

You can directly upgrade to Advanced Authentication 6.4 Service Pack 2 from 6.4 and 6.3.7.

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 2 includes the following known issue:

- Risk Service Is Unable to Retrieve the User History Details During Authentication Post Upgrade

Risk Service Is Unable to Retrieve the User History Details During Authentication Post Upgrade

Pre-conditions:

- The **User History Database** enabled for Risk Service
- **Built-in Data Store** set to store history details
- Select **Check user history** in the **IP Address Rule** of Risk Service Policy

Before upgrading to Advanced Authentication 6.4 Service Pack 2, user logs in through step-up authentication and succeeds the IP Address Rule validation. The user details get saved according to the configuration.

Post upgrade, users whose history was saved fail in the IP Address Rule validation and might get a prompt for additional authentication. This happens because built-in data store is used to record the user history details. However, data is recreated once the user authenticates again and the user history is restored.

Planned End of Support

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

- Old Enrollment Portal
  - The **Enrollment Options** policy will not be available.
  - The new features and functionality will only be 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.

    By default, the **Enable New Enrollment Options** option in the **Enrollment Options** policy is set to **ON**.

- Repo Agent
  - As there are no changes to the component, the Repo Agent will not ship along with Advanced Authentication 6.4 Service Pack 2.
  - Repo Agent-related configuration in the administrator portal will not be available.

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

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see https://www.microfocus.com/en-us/legal (https://www.microfocus.com/en-us/legal).