Advanced Authentication Cloud Edition Release Notes

Advanced Authentication is now available in the Software as a Service (SaaS) model also known as Cloud Edition (CE). Open Text hosts and maintains Advanced Authentication.

For the list of other documents related to Advanced Authentication, see the Advanced Authentication NetIQ Documentation (https://www.netiq.com/documentation/advanced-authentication-64/) page. For more information about the product and support, see the Advanced Authentication Product (https://www.microfocus.com/en-us/cyberres/identity-access-management/advanced-authentication) website.

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 on the Advanced Authentication NetIQ Documentation (https://www.netiq.com/documentation/advanced-authentication-64/) page.

The release number is in the **YY.QUARTER.RELEASE** format.

CE 23.4 Update

Advanced Authentication CE 23.4 includes the following updates:

- "Enhancements" on page 1
- "Security Improvements" on page 2
- "Resolved Issues" on page 2

Enhancements

This release includes the following enhancements:

- Ability to Auto-Enroll the PKI Method with PKI Smart Card
- Enhanced Lockout Options Policy
- Enhanced Security of Methods: Emergency Password and Password
- Improved Dashboard Reports

Ability to Auto-Enroll the PKI Method with PKI Smart Card

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 machine that has Advanced Authentication Device Service installed on it.

Enhanced Lockout Options Policy

With this release, the **Lockout Options** policy is enabled by default.

Enhanced Security of Methods: Emergency Password and Password

From this release, Advanced Authentication includes the following enhancements in **Emergency Password** and **Password** methods:

- **Minimum password length** is set to 10 characters by default.
- **Complexity requirements** is enabled by default.

Improved Dashboard Reports

This release revised the following reports to include accurate information about users who have auto-enrolled a method however not authenticated at least once, along with details of users who have authenticated using the auto-enrolled method:

- Enroll Activity Stream
- Users
- Authenticators

Security Improvements

This release includes security updates.

Resolved Issues

Component	Issue Description
Administration	When a user attempted to login with the expired LDAP password, the authentication failed even when the **Logon with Expired Password** was set to **Allow** for an event. `Invalid credentials` message was displayed to users.
Administration	The `Event_name` parameter was missing for the IDs 102, 103, 104, 106, and 107 in CEF logs.
Administration	With the **SSL** disabled, Advanced Authentication was unable to establish a connection with the configured repository.
Administration	In some circumstances, the scheduled fast sync for a Cloud Bridge External Repo failed to trigger and execute.
Administration	On the **Select Authentication Chain** screen during the login process, the focus is not on **Next** button by default.
Administration	The Smartphone Enrollment by link was not working as expected.
Administration	An option, **Import Tenant** has been deleted for Tenant Administrators.

Component	Issue Description
Events	For any event, if the **Logon with expired password** was set to **Ask to change**, then a user attempted to authenticate with the expired password, a prompt to change the password was not displayed. However, an error message `Login failed, try again` was displayed.
Self-Service Portal	Users were allowed to enroll the **SMS OTP** method without any phone number tagged to their profile.

23.2.1 Update

Advanced Authentication as a Service 23.2.1 includes the following updates:

- "Enhancement" on page 3
- "Updated Open Source Components" on page 3
- "Security Improvements" on page 3
- "Resolved Issues" on page 4

Enhancement

This release includes the following enhancement:

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 OAuth2 Event (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/create_custom_evnt.html#create_oauth_20_evnt) and SAML 2.0 Event (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/create_custom_evnt.html#create_saml_20_evnt) in the Tenant Administration Guide.

Updated Open Source Components

This release includes updates to some of the open source components.

Security Improvements

This release includes security improvements.

Resolved Issues

Component	Issue Description
External Repository	The fast synchronization process (runs every five minutes by default) fails to retrieve the changes.
Events	Earlier, the Oauth2 and SAML events with similar Client IDs were allowed. Now, Advanced Authentication does not allow the creation of events with duplicate Client IDs. However, if there are duplicate events available then you must correct the duplicate ID's before creating any new events.
Repository	When two repositories are configured and the browser was set to a non-english language, the login fails if the repository name is not prefixed to the username. This happens when the user record is not found in the first repository that the server validates.

23.2.0.1 Update

Advanced Authentication as a Service 23.2.0.1 includes the following update:

Resolved Issue

Component	Issue Description
Smartphone Method	When a user attempts to authenticate to any event using an authentication chain that includes the **Smartphone** method, the logon process might appear as successful; however logon fails and user is prompted to log in again.

23.2.0 Update

Advanced Authentication as a Service 23.2.0 includes the following update:

- "What's New?" on page 4
- "Deprecated Options" on page 5

What's New?

This release includes the following:

- Support for Single Sign-On
- Security Improvement

Support for Single Sign-On

In this release, Advanced Authentication is integrated with Single Sign-on. Advanced Authentication facilitates administrators to add federated services and applications in the **Applications** module. This enables end-users to access several services with a single set of credentials and prevents the need to manage multiple credentials.

Single Sign-on applies different standards, such as OAuth, SAML and so on for granting the federated access to various services and applications.

For more information, see Single Sign-on (https://www.microfocus.com/documentation/single-sign-on/help/single-sign-on-admin/welcome.html).

Security Improvement

This release includes security improvements.

Deprecated Options

Advanced Authentication 23.2.0 deprecates the following from the **Edit Cloud Bridge External repo** page:

- **Expiration time (hours)**
- **Generate Script**

Advanced Authentication does not provide the script required to install the Cloud Bridge Agent.

For more information on prerequisites and procedure to install the Cloud Bridge Agent, see Installing the Cloud Bridge Agent (https://www.microfocus.com/documentation/identity-governance-and-administration/igaas/quick-start/quick-start.html#t4dswrbn8vla). Contact the SaaS Operations team to obtain the Cloud Bridge Agent install script.

23.1.1 Update

Advanced Authentication as a Service 23.1.1 includes the following update:

Resolved Issue

Component	Issue Description
Administration	In **Cloud Bridge External Repository**, with the **Fast Sync Enabled** is set to **OFF** if the administrator performs full synchronization, the `HTTP 400 - Bad Request` error is displayed instead of `HTTP 405 - The Cloud Bridge Agent has been configured to NOT support Change collection` error.

23.1.0 Update

Advanced Authentication as a Service 23.1.0 includes the following update:

Security Improvement

Advanced Authentication as a Service 23.1.0 release addresses CVE-2023-24468.

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).