Advanced Authentication as a Service (SaaS) Release Notes

January 2021

In addition to the existing on-premises and cloud-based deployments, Advanced Authentication is now available in the Software as a Service (SaaS) model. Micro Focus hosts and maintains the Advanced Authentication Servers with their databases. You can use it to secure access to your corporate resources, such as various portals, workstations, and VPN servers.

For more information about Advanced Authentication and its features, see Introduction to Advanced Authentication.

The following are the key differences between SaaS and non-SaaS models:

Feature	Advanced Authentication	Advanced Authentication as a Service
Setup	Installation is required	Installation is not required
Billing	License-based	Subscription-based
Hardware	Must meet the recommended system requirements	Does not require extensive hardware

For more information about this release and for the latest release notes, see the Advanced Authentication NetIQ Documentation page. For more information about the product and support, see the Advanced Authentication Product 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 at the Advanced Authentication NetIQ Documentation page.

What's New?

Advanced Authentication as a Service January 2021 update includes the following:

Enhancements

This release provides the following enhancements:

- Custom Branding Policy for New Enrollment Portal and Administration Portal
- Custom Branding and Custom Message per Tenant
- Cloud Bridge Enhancements
- Provision to Configure the Cached Offline Logon Duration
- Google reCAPTCHA Support for the New Enrollment Portal
- Support to Disable Self Enrollment of TOTP
- Allows to Login Without Tenant Name
- Support for Risk Service

Custom Branding Policy for New Enrollment Portal and Administration Portal

This release introduces the Custom Branding policy. This policy enables you to customize the look and feel of the new Enrollment portal and Administration portal. Using this policy, you can change the title, logos, and colors of the application bar.

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

Custom Branding and Custom Message per Tenant

With this release, the Tenant Administrators can customize the Branding and Messages in the Web Authentication policy.

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

Cloud Bridge Enhancements

This release includes the following enhancements for Cloud Bridge External Repo:

- Provides updated error messages for better understanding.
- Introduces the **Test Configuration** button to verify the configuration while adding, updating, or troubleshooting Cloud Bridge.

  For more information, see Testing Cloud Bridge in the *Advanced Authentication - Administration* guide.
- Introduces the **Force Configuration** button to impose the changes that have been made in the repository.

  For more information, see Force Configuring Cloud Bridge in the *Advanced Authentication - Administration* guide.
- Introduces the following options to specify the batch size and timeout:
  - Batch size limit
  - Cloud Bridge chunk request timeout
  - Cloud Bridge LDAP read timeout
  - Cloud Bridge users_page size limit
  - Cloud Bridge groups page size limit

  For more information, see Cloud Bridge Attributes in the *Advanced Authentication - Administration* guide.

- The Cloud Bridge scripts accept special characters in the LDAP password and space in the LDAP username. It also validates required tools, such as wget.
- In case of Cloud Bridge Agent or Cloud Bridge client reboot, the External Repository will gracefully handle and reconnects the repositories once Cloud Bridge Agent or Cloud Bridge client is up without explicit use of synchronization.
- The Cloud Bridge script generates `install.log`. The `install.log` contains docker and docker-compose output as well as stack traces of any errors and session metrics.

  For more information, see Installing Cloud Bridge Agent in the *Advanced Authentication - Administration* guide.

NOTE: This release verifies the following Cloud Bridge Agent and repository combinations:

- One Cloud Bridge Agent with two Active Directory repositories.
- One Cloud Bridge Agent with one Active Directory repository and one eDirectory repository.
- One Cloud Bridge Agent with two eDirectory repositories.
- One Cloud Bridge Agent with one Active Directory repository and another Cloud Bridge Agent with a eDirectory repository.

Provision to Configure the Cached Offline Logon Duration

This release introduces the **Cached logon offline period (minutes)** option in the **LDAP Password** method. Using this option, you can set the duration for which a user can perform offline login when the repository is unavailable. The authentication occurs with stored user authenticators during the configured period.

If a user-specified password and the password stored in the Advanced Authentication server do not match, authentication fails. However, the cached password resets only after exceeding the set cached logon offline period.

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

Google reCAPTCHA Support for the New Enrollment Portal

With this release, the new Enrollment portal supports Google reCAPTCHA. Using reCAPTCHA, the administrator can prevent the bot attacks by confirming the user trying to log in is a human, not a robot. After the confirmation, the authentication chain is displayed.

For more information, see Google reCAPTCHA Options in the *Advanced Authentication - Administration* guide.

Support to Disable Self Enrollment of TOTP

With this release, the new Enrollment portal supports the **Disable self enrollment** option in the TOTP method. With this option, the administrator can prevent manual enrollment of the TOTP method. This option is used in combination with **Enroll TOTP method when enrolling Smartphone** in the Smartphone method.

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

Allows to Login Without Tenant Name

In this release, RADIUS Agent solution allows the users to use RADIUS authentication without entering their tenant names.

Support for Risk Service

From this release, Advanced Authentication as a Service (SaaS) supports Risk Service. Risk Service evaluates the level of risk during each login attempt using the contextual information, such as IP address, HTTP header, and so on without influencing the end-user experience.

With Risk Service, Advanced Authentication controls access to a protected resource based on the risk level. An administrator can define an appropriate action for the defined risk levels.

For more information, see Configuring Risk Service in the *Advanced Authentication - Administration* guide.

Security Updates for Dependent Components

This release updates the version the following dependent components to enhance the security:

- openSUSE
- OpenJDK
- Apache Tomcat
- OpenSSL FIPS
- Python

Software Fixes

Advanced Authentication as a Service includes the following software fixes:

Component	Issue Description
Administration Portal	When an administrator uploads the LDAPS CA certificate, the Advanced Authentication server verifies whether the certificate meets the set standards and removes the new lines.
Administration Portal	Sometimes, the repository configured in the Administration portal is not synchronized. This issue occurs due to a sync exception and the use of repository name as a key.
Administration Portal	When an administrator tries to export the tenant configuration, the export fails and displays an error message.
Administration Portal	The administrator and tenant administrator are allowed to delete the login domain entries in the **Login Options** policy without a confirmation message.
Administration Portal	When an administrator initiates an API call to add a group to the SCIM managed repository, a 404 error is displayed.
Administration Portal	Disabling **Verify the SSL Certificate** does not remove the certificate that has been uploaded to **LDAPS CA certificates**. This results in the synchronization issue.
Administration Portal	If the Cloud Bridge Agent is unavailable and a tenant administrator tries to log in to the Administration portal, there is a significant delay to display the following message: `Repository Agent has failed to respond.`

Component	Issue Description
Administration Portal	When an administrator imports the configuration file that has been exported from an on-premises setup, Advanced Authentication as a Service (SaaS) displays an error message.
Web Authentication	When a user tries to authenticate, after specifying the credentials, the user is redirected back to the login page if the **signAuthnRequest** and **ForceAuthn** attributes in SAML SP are set to **True**.
Web Authentication	When a user tries to log in to the Identity Governance user account, the user is redirected to the web authentication username prompt instead of opening the Identity Governance user account page. Similarly, when a user tries to log out of Access Manager, instead of being redirected to Access Manager's login page, the user is redirected to the web authentication username prompt.
New Enrollment Portal	The secondary tenants are unable to enroll the Facial Recognition and the U2F methods on the new Enrollment portal.
Web Portals	While authenticating to the web portals with the Smartphone (offline authentication) method, the users are unable to locate the **OTP** field to specify the TOTP.
Cloud Bridge	When eDirectory is configured as the repository, and a user tries to log in to an event using the email address as the username, the authentication fails.
Cloud Bridge	The user is not able to edit the port number from 389 to 636 to turn on **SSL option**, the changes are not saved.
Cloud Bridge	This release resolves several synchronization issues.
Cloud Bridge	When a user changes the external repository configuration and initiate full synchronization, the saving was unsuccessful and changes are not applied until the user force configure the changes.
Multitenancy	When a user tries to authenticate to the SaaS tenant, the following error message is displayed: `No available authentication chain was found.`

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

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see http://www.microfocus.com/about/legal/.