Advanced Authentication as a Service (SaaS) Release Notes 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 the list of other documents related to Advanced Authentication, see the Advanced Authentication NetIQ Documentation 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 at the Advanced Authentication NetIQ Documentation page.

The release number is in YYYY.M.RELEASE NUMBER format.

2021.9.1 Update

Advanced Authentication as a Service 2021.9.1 includes the following updates:

Enhancements

Enhancement	Description
Provision to Change the Password	Now, Helpdesk Administrator can enable users to reset the password using the option **Password must be changed**. With this option set to ON, the user must change the password during subsequent logon to the portals. For more information, see Password (https://www.netiq.com/documentation/advanced-authentication-63/helpdesk-administrator-guide/data/password.html#t46f5bzx1kx2) in the *Advanced Authentication - Helpdesk Administrator (https://www.netiq.com/documentation/advanced-authentication-63/helpdesk-administrator-guide/data/bookinfo.html)* guide.

Security Improvements

This release resolved several security vulnerabilities.

Micro Focus would like to offer special thanks and appreciation to Frank Spierings of Warpnet B.V. for following responsible disclosure practices and responsibly disclosing this vulnerability to us. (CVE-2021-22509)

Software Fixes

Component	Issue Description
Administration Portal	There are two vertical scroll bars on few portals, such as Administration, Self-Service, Helpdesk, and Tokens Management.
Administration Portal	After the full synchronization of the Active Directory that is configured as the Cloud Bridge External repository, few user entries are removed.
Administration Portal	When an administrator adds SAML identity provider details in the **Web Authentication** method and uploads the valid metadata, an error message, `Wrong IdP metadata format` is displayed. Due to this error, the administrator is unable to save the changes to the method.
Helpdesk	Administrators are unable to log in to the Helpdesk portal due to the access denied error message.
Web Authentication	When a user logs in to `aa_domain/accounts` with an expired password, the user gets authorized to the integrated product seamlessly instead of getting the login page.

2021.8.1 Update

Advanced Authentication as a Service 2021.8.1 update includes the following:

- Enhancements
- Software Fixes

Enhancements

This release provides the following enhancements:

Enhancements	Description
Cloud Bridge Repository Setup Wizard	The **Quick Start** is introduced on the left pane of Advanced Authentication Administration portal. This feature is available only during the first time login to the portal. This feature helps administrators to understand the prerequisites and configure the Cloud Bridge repository. For more information, see Quick Start (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/t4donma2ncp4.html#t4ger0k4pvuh) in the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.
Enhanced Custom Branding to Customize the Helpdesk Portal	The **Custom Branding** policy is enhanced to extend the support for the Helpdesk portal. Now, the customization of the title, logos, and application bar colors is applicable for the Helpdesk portal in addition to Administration and Enrollment portals.
Custom Branding Settings of Web Authentication Events in the Custom Branding Policy	The Custom Branding settings of Web Authentication events have been relocated from Web Authentication policy to the **Custom Branding** policy. For more information, see Customizing the Login Page of Web Authentication Events (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/custombranding.html#custom_login_page_of_web_auth_evnts) in the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.

Enhancements	Description
Provision to Select the Agent	The **Agent** list has been introduced in **New External Repository** page, under External Server section. This list allows the administrators to select the preferred `datacenter.json` file to generate the Cloud Bridge Agent script. The main objective of this list is to support multiple domains. Also, **Agents and Clients** section has been introduced in **New External Repository** page to view the following: ◆ The `datacenter.json` file content of a specific Agent ID ◆ Client URL For more information, see Adding a Cloud Bridge External Repository (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/t4donma2ncp4.html) in the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.
Support for Out-of-Band Method	Advanced Authentication introduces the Out-of-band method to facilitate users to authenticate through the OOB portal or a new Authentication Agent for Web application. During authentication, the authentication request is sent to the OOB portal, Authentication Agent for Web or Authentication Agent for Windows. Users are required to log into the portal, Authentication Agent for Web or Authentication Agent for Windows and accept the request to authenticate successfully. For more information, see Out-of-Band (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/t4ftvg1r7ymp.html) in the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide. Users can access the OOB portal using the URL: `https://<AdvancedAuthenticationServerdomainname>/oob/ui` and succeed the authentication chain to log into the portal. You can install the Authentication Agent for Web application from the OOB portal using Google Chrome on any computer, laptop, tablet or smartphone. You can also any other browser that support Progressive Web application (https://en.wikipedia.org/wiki/Progressive_web_application#Browser_support). For more information, see Logging In to Out-of-Band Portal in the *Advanced Authentication- User* guide.

Software Fixes

This release includes the following software fixes:

Component	Issue Description
Administration Portal	If the Master server initiates the fast synchronization and administrator tries to initiate the full synchronization on the Web server simultaneously, then the full synchronization fails.
Administration Portal	The administrators are unable to download the SAML metadata. Now, you can download the metadata from the Web Authentication policy. For more information, see Downloading the Identity Provider SAML Metadata (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/web_auth.html#config_sett_saml_20_evnts).
Administration Portal	Sometimes, users are accidentally removed from the Advanced Authentication database after the full sync or fast sync due to some conditions.
Cloud Bridge Agent	When there are multiple Cloud Bridge agents with more than one repository, the configuration results in errors, and the synchronization fails.
RADIUS	Sometimes, during the full synchronization, the LDAP servers do not return the users. This results in users marked for removal. The user marked for removal cannot succeed the RADIUS authentication.

2021.7.1 Update

Advanced Authentication as a Service 2021.7.1 update includes the following:

- Enhancement
- Security Improvements
- Software Fixes

Enhancement

This release provides the following enhancement:

Enhancement	Description
Customize the Hostname for Each Tenant	Earlier, a single URL is shared among all tenants. For example, `https://aa.cyberresprod.com/account/login` Now, tenant administrators can request a unique URL based on their tenant name. For example, `https://<tenantname>.cyberresprod.com/account/login` Following are some changes related to this feature: ◆ The **Email as login name** is set to **OFF** by default in the **Login options** policy for new tenants to allow the users to log in without using the email address as username. However, the tenant administrator can set the option to **ON** when required. ◆ The **Identity provider URL** is now a drop-down list in the **Web Authentication** policy for new tenants. By default, it is set to `https://tenantName.domain-name/` to allow users to specify the username without prefixing the `tenant-name\repositoy-name\` while logging in to the Advanced Authentication portals. For more information, see Web Authentication (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/web_auth.html#t4gadzfldq6t)policy.

Security Improvements

This release resolves the following security issues:

- Potential information leakage (CVE-2021-22529)
- Potential Brute Force attack (CVE-2021-22530)

Software Fixes

This release includes the following software fixes:

Component	Issue
Administration Portal	The **Out-of-band** method is not working appropriately.
Enrollment Portal	The **Emergency Password** method is displayed on the Enrollment portal and causing confusion to users.

2021.6.1 Update

Advanced Authentication as a Service 2021.6.1 update includes the following:

- Enhancements
- Software Fixes

Enhancements

This release provides the following enhancement:

Enhancement	Description
Support for Installing the Cloud Bridge Agent on RedHat	You can install the Cloud Bridge agent on RHEL 8.3 server using the Podman instead of a docker-compose. The administrator is required to run the generated script on the RHEL server. For more information, see Installing Cloud Brigde Agent (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/t4donma2ncp4.html#t4e0xvryj14s) in the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.
Support for Denmark National ID	Advanced Authentication introduces the Denmark National ID method to facilitate citizens of Denmark to authenticate using their CPR (Danish social security number), a password, and the PIN which is provided during the enrollment of Denmark National ID. For more information, see Denmark National ID (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/nemidmethod.html) in the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.
Option to Lock Users Who Fail While Testing the Enrolled Methods	The **Lock if authenticator test was failed** option is introduced in the **Lockout Options** policy. This option enables you to lock the users who have failed an authenticator's test in the Self-Enrollment portal for the number of times specified in **Attempts failed**. For more information, see Lockout Options (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/lockout_opts.html) in the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.

Software Fixes

Advanced Authentication as a Service includes the following software fixes:

Component	Issue
Cloud Bridge Agent	A space in the username of the administrator and space while configuring the DN details cause the failure of Cloud Bridge agent installation.
Cloud Bridge Agent	The Cloud Bridge agent does not initiate automatically after restarting the host machine where the agent is installed.
Enrollment Portal	After integrating a product with Advanced Authentication, a user of the integrated product is granted access to the new Enrollment portal with an expired password.
Enrollment Portal	Pre-condition: Enroll HOTP or TOTP method and delete the method. With the above precondition, when a user tries to enroll the HOTP or TOTP method again, the Secret or OTPs of the previously enrolled method gets auto-filled. This happens because the OTP or Secret is saved in the browser.
Enrollment Portal	If a user tries to test any enrolled method on the Enrollment portal, an error message that states the event could not be found is displayed.
Enrollment Portal	The users are unable to enroll the PKI method when the digital certificate is based on the OCSP (Online Certificate Status Protocol) protocol and HTTP proxy is in use.
Enrollment Portal	When a user tries to enroll the TOTP authenticator and chooses manual TOTP, instead of populating the auto-generated secret, the TOTP secret field is blank.
RADIUS	The **Result Specification** rule configured for a RADIUS event does not apply if the **Result Specification** rule in the **RADIUS Options** policy is empty.
Web Authentication	When some users try to authenticate using SAML, the authentication fails. This issue occurs because the Advanced Authentication replaces the space character with question mark(?) in the SAML assertion.

2021.5.1 Update

Advanced Authentication as a Service 2021.5.1 update includes the following:

- Enhancements
- Software Fixes

Enhancements

This release provides the following enhancement:

Enhancement	Description
Settings to Retrieve User Groups after Authentication	The options, **Return Group on Logon** and **Groups** are introduced in all events (existing and new events). These options allow an administrator to retrieve the list of groups a user is associated with after successfully authenticating to an event. **NOTE:** The **Return Group on Logon** is enabled by default for all the events except the Authenticators Management, Smartphone Enrollment, OAuth 2.0, and SAML 2.0 events. For more information, see Configuring an Existing Event (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/config_exst_event.html) in the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.
Settings to Allow SAML Service Providers to Select the Authentication Chain and Event	The options, **SAML client chain selection** and **SAML client event selection** are introduced in the **Web Authentication** policy. These options allow SAML service provider to select the following: ◆ Preferred authentication chain: Using, which users can authenticate ◆ Preferred event: Application or device, which users can access For more information, see Web Authentication policy (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/config_policies.html) the *Advanced Authentication - Tenant (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.
Improved Certificate Selection for PKI Method	The **Key** field in the **PKI** authenticator in the new Enrollment Portal populates only the certificates with the authentication key and its expiry date. It is possible to click the button **Show All** to show all the certificates. For more information, see PKI in the Advanced Authentication- User.
Enhanced New Enrollment Portal Login Page	This release enhances the login page of the new Enrollment Portal to support the custom branding and localization settings.

Software Fixes

Advanced Authentication as a Service includes the following software fixes:

Component	Issue
Administration Portal	When an administrator tries to delete the groups added to the chains, following error message is displayed: `AttributeError 'LogonChainGroup' object has no attribute 'obj_id' (Internal Server Error)`

Component	Issue
Administration Portal	While configuring the Active Directory repository, if you provide space with the value in the **Base DN**, **Users**, and **Group DN**, an exception error occurs.
Administration Portal	The login operation takes longer than the expected time due to the `/api/v1/list` call.

Administration and New Enrollment portals	The Cloud Bridge repository related error messages that are displayed in the following scenarios are handled appropriately:
	◆ When the Cloud Bridge agent is misconfigured (value in the required fields is empty) or when the agent is not responding.
	◆ When the Cloud Bridge agent or client is down, the following latest message is displayed on the new Enrollment portal:
	`Login failed. An external service is not available. Try again later or contact your system administrator.`
	◆ When users of the disabled directory try to log in, the following message is displayed:
	`The user account is disabled.`

Enrollment Portal	When users configure the browser to remember credentials and try to enroll **HOTP** or **TOTP** method in new Enrollment Portal, the browser auto-fills **OATH Token Serial** and **OTP** using the available data.
Enrollment Portal	When a user connects the Spanish national identity card (Documento Nacional de identidad) and tries to enroll it using the PKI method, the certificate is not displayed in the **Key** field. However, on click of **Show All**, certificates are displayed. When the user selects a certificate, the following error message is displayed: `Cannot check the revocation status.`
RADIUS	The RADIUS server does not return the `msRADIUSFramedIPAddress` attribute if the hexadecimal value of that attribute contains a negative value.

2021.4.1 Update

Advanced Authentication as a Service 2021.4.1 update includes the following:

- Enhancements
- Software Fixes

Enhancements

This release provides the following enhancement:

Enhancement	Description
Provision to Restore the Default Branding	The **Restore** button is introduced in **Custom Branding** policy to reset customized the user interface settings and revert to default settings. For more information, see Custom Branding in the *Advanced Authentication - Administration* guide.

Software Fixes

Advanced Authentication as a Service includes the following software fixes:

Component	Issue
Administration Portal	When an administrator refreshes the **Methods** page in Administration Portal, the method images are not displayed and if the administrator opens the **Security questions** method, the **Add question** button blends in with the background and does not work.
Administration Portal	When an administrator tries to configure the **Custom Branding** policy, the **Collapsed App Bar Logo** does not work. In this release, the **Collapsed App Bar Logo** option is removed.
Administration Portal	While configuring a repository, after an administrator adds an external server with an SSL certificate, the **LDAP SSL** setting in the **Current configuration** section is not identical to the SSL setting under External servers.
Administration Portal	When an administrator tries to search the users in SCIM repository using `"filter=(emails eq "<theid>" or userName eq "<theid>") and active eq true or active eq false` syntax, following error message is displayed: `"status_code\": 400, \"status\": \"Bad Request\", \"detail\": \"Request is unparsable, syntactically incorrect, or violates schema.\"` The same issue happens when the administrator uses `filter=emails eq "<email>` syntax.
Enrollment Portal	Pre-conditions in the SMS method: ◆ **Allow overriding phone number** is set to **OFF** ◆ **Allow user enrollment without a phone** is set to **ON** With the above pre-conditions, when a user enrolls the SMS method, a field to specify a phone number is not available. However, the user saves the enrollment without a phone number and the following message is displayed: `There is no available category for the required method.`
Enrollment Portal	The **Delete** option for the SMS OTP and Email OTP methods is not available in the new and old Enrollment portals.

Component	Issue
Web Authentication	When an administrator tries to customize the Web Authentication page, the changes made in JAR file are not reflected in the Web Authentication pages.

2021.3.1 Update

Advanced Authentication as a Service 2021.3.1 update includes the following:

- "Enhancements" on page 12
- "Software Fixes" on page 13

Enhancements

This release provides the following enhancements:

Enhancement	Description
Fast Synchronization for eDirectory	Administrators can achieve fast synchronization for eDirectory with the assistance of the Change-log module. For more information, see Enabling Fast Synchronization for eDirectory Repository (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/t4donma2ncp4.html#t4f218l2ztzh) in the *Advanced Authentication - Tenant Administration (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)*.
Provision to Reset the Password	While logging in, if password is expired, a link is displayed along with the message to reset the password: `Password has expired, Login by this link to reset your password.`
New Position for LDAP CA Certificate	The **LDAP CA Certificate** field in Cloud Bridge External repository to upload SSL certificate has been placed outside of **Advanced Settings**. For more information, see Adding a Cloud Bridge External Repository (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/t4donma2ncp4.html) in the *Advanced Authentication - Tenant Administration (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)*.
Ability to Reset the Password on SCIM Client	With the new API call, administrators and helpdesk administrators are allowed to reset their forgotten password.

Enhancement	Description
Support for Filters in SCIM Endpoint	SCIM endpoint supports the following filters with the respective attributes and operations to retrieve appropriate details: ◆ Users filter ◆ Attributes: externalId, email address, and username ◆ Operations: eq, and ◆ Groups filter ◆ Attributes: member, externalId, and displayname ◆ Operations: eq, and

Software Fixes

Advanced Authentication as a Service includes the following software fixes:

Component	Issue Description
Administration Portal	If there is a chain with two or more methods and the second method is the OTP method that has multiple categories enrolled. During authentication with this chain, the default category of the OTP method is auto-selected without prompting a user to select the preferred category and OTP is sent to the respective device. This issue occurs on the Administration and Helpdesk portals.
Administration Portal	While adding a LDAP repository, an administrator sets **Verify SSL Certificate** to **ON** and saves the configuration. Later, on the **Edit Repository** page, the **Verify SSL Certificate** is disabled without any manual intervention.
Cloud Bridge	When an administrator changes the repository settings in Cloud Bridge External repository, such as Base DN, the changes are not updated even after saving the changes.
Cloud Bridge	After configuring Cloud Bridge with eDirectory, the full synchronization is not initiated automatically.
Enrollment Portal	If a user tries to log in to the new Enrollment Portal when the LDAP repository is down, the following incorrect error message is displayed: `This Page isn't working.`
Enrollment Portal	If a user tries to log in to the new Enrollment Portal when the Cloud Bridge External repository is down, error message is not displayed.
Enrollment Portal	When a user tries to enroll any method, such as Smartphone, U2F, and so on, the **Categories** drop down is not available on the new Enrollment portal. However, the category is selected by default without allowing the user to select the preferred category. This issue occurs when the administrator adds more than one category.

Component	Issue Description
Enrollment Portal	Pre-conditions in the SMS method on the administration portal: ◆ **Allow overriding phone number** is set to **OFF** ◆ **Allow user enrollment without a phone** is set to **ON** With the above pre-conditions, when a user enrolls the SMS method, a field to specify a phone number is not available. However, if the user tries to save the enrollment without a phone number, the following message is displayed: `There is no available category for the required method.`
Enrollment Portal	The method names in new Enrollment Portal are not displayed in localized language.
Enrollment Portal	When a user tries to log in to the new Enrollment Portal, if the Touch ID is locked or Touch ID is not available, the login page refreshes automatically and **Cancel** button does not work.
Enrollment Portal	After deleting and recreating a tenant, when a tenant administrator tries to log in to new Enrollment Portal, the authentication fails and an error message is displayed.
RADIUS	During RADIUS authentication with the Smartphone method, if a user does not accept the push notification on the NetIQ Advanced Authentication app, multiple push messages are sent before the timeout period.
SCIM repository	When an administrator adds one thousand users to SCIM repository, only ten users are displayed. Later, if the administrator adds thousand users, twenty users are displayed. For each thousand user entries, only ten user entries are processed and returned.
SCIM repository	When a customer tries to do a SCIM call, it fails because of excess count of user data available in the repository.
Web Authentication	Web authentication Password page displays Micro Focus Access instead of the product name Advanced Authentication and does not match with new Enrollment portal login pages. This is misleading users.
Web Authentication	When Advanced Authentication is integrated with ADFS using the SAML protocol, after a user succeeds authentication, an error is displayed on the ADFS page.

2021.2.1 Update

Advanced Authentication as a Service 2021.2.1 update includes the following:

- "Enhancements" on page 14
- "Software Fixes" on page 15

Enhancements

This release provides the following enhancements:

Enhancement	Description
Option to Hide the Left Navigation Pane	This release introduces a hamburger menu  option in the Administration Portal to hide or display the left navigation pane.
Provision to Download the SAML Metadata	The tenant administrators without the TOP privileges can download the SAML Metadata using **Download IdP SAML 2.0 Metadata** button in the **Web Authentication** policy. For more information, see Web Authentication (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/web_auth.html) policy in the *Advanced Authentication - Tenant Administration (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.
Updated the Easy Button Script	The easy button script that assists in installing the Cloud Bridge is updated to store data in the `.evn` file instead of the `data.cfg` file.
SCIM Enhancements	This release includes the following API updates related to SCIM: ◆ Except for the `givenName`, the GET API call returns other values from the name attribute. ◆ The POST response is updated to return the metadata according to the SCIM v2 specification. ◆ POST call supports the custom attribute and custom value in the `myCustomAttr` and `myCustomValue` attributes, respectively.

Software Fixes

Advanced Authentication as a Service includes the following software fixes:

Component	Issue Description
Administration Portal	When an administrator tries to delete a repository, the following error message is displayed: `ValueError PEM certificate was invalid (Internal Server Error)`
Administration Portal	When an administrator tries to create a repository using a certificate file that passes the `openssl x509`'s decode information, the following error message is displayed: `ValueError PEM certificate was invalid (Internal Server Error)`
Administration Portal	When an administrator sets the Expires or Max-Age attribute in cookies, the browser does not remove the cookies after closing the browser.
Cloud Bridge	When an administrator changes the repository settings in Cloud Bridge External repository. such as Base DN, the changes are not updated.

Component	Issue Description
Cloud Bridge	Rebooting the host operating system that contains the Cloud Bridge agent fails to initiate the container.
Cloud Bridge	After an administrator restarts the host operating system, the Cloud Bridge agent fails to initiate.
Enrollment Portal	Using the Internet Explorer 11 browser, when a user accesses the Enrollment portal and edits the enrolled methods related to Device Service, the browser does not respond. This issue occurs after updating to Advanced Authentication 6.3 Service Pack 3.
Risk Service	The User Last Login Rule and Cookie Rule of Risk Service fails with Advanced Authentication as a Service. Therefore, the risk is not evaluated appropriately based on the conditions defined in these rules.

2021.1.1 Update

Advanced Authentication as a Service 2021.1.1 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 Agentin 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.`
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.

Component	Issue Description
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/.