Advanced Authentication as a Service

Release Notes

May 2022

Legal Notices

Contents

About this Book

Advanced Authentication as a Service Release Notes includes enhancements and fixes of each release update.

Intended Audience

This book provides information for individuals responsible for understanding user interface changes, new settings and fixed issues.

1 2022.8.1 Update

Advanced Authentication as a Service 2022.8.1 includes the following updates:

- Enhancements
- Software Fixes

Enhancements

This release includes the following enhancements:

- Ability to Disable Fast Sync and Modify Fast Sync Interval for the Cloud Bridge External Repository
- Timeout Settings Support for Web Authentication Events

Ability to Disable Fast Sync and Modify Fast Sync Interval for the Cloud Bridge External Repository

This release introduces the following options in the Cloud Bridge External repository on the Administration Portal:

- **Fast sync enabled**: This option allows you to disable the automatic fast sync initialization of the repository and this might impact the functioning of other dependent components.
- **Time between fast syncs**: Select the required synchronization interval between the fast syncs from the list. By default, the interval is set to 5 minutes.

For more information, see Advanced Settings (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/?page=/documentation/advanced-authentication-64/tenant-administrator-guide/data/t4donma2ncp4.html#t4duu5sbtj4f) in the Advanced Authentication - Administration (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/bookinfo.html) guide.

Timeout Settings Support for Web Authentication Events

From this release, tenant administrators are allowed to configure the following timeout settings in Web Authentication events:

- Session Timeout
- Authorization Code Timeout
- Access Token Timeout
- Refresh Token Timeout
- Public Refresh Token Timeout
- Session Token Revocation Timeout

For more information, see Configuring Timeout (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/web_auth.html#t4cjcywwk7l2) in the Advanced Authentication - Administration (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/bookinfo.html) guide.

Software Fixes

Component	Issue Description
Administration Portal	The OAuth2 event that is created using an API call is not displayed in the `authcfg.xml` for the tenant. Therefore, it is not possible to issue an access or refresh token.
Administration Portal	The fast synchronization process of the Cloud Bridge repository takes more than five minutes later display some errors in the logs.
Administration Portal	Unable to initiate the full synchronization process after changing **Advanced Settings** of the Cloud Bridge repository.
Cloud Bridge Repository	On large Cloud Bridge repositories, with 10K user records, the full synchronization process suspends automatically and the synchronization fails.
OAuth2/ OpenID Connect	When users select the **SAML SP** method to access the **OAuth2/ OpenID** Connect events, the field to specify the password is not displayed. However, users are granted access without the password.
Web Authentication	The Facial Recognition method does not work in the Web Authentication events.

Previous Releases

This section includes previous Release Notes of Advanced Authentication as a Service.

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

Advanced Authentication provides the following authenticators:

2 2022.5.1 Update

Advanced Authentication as a Service 2022.5.1 includes the following updates:

Enhancement

Enhancement	Description
API Support for OAuth Authentication	This release introduces OAuth2 Application policy to allow the OAuth2 protocol-based applications to access the Advanced Authentication API. For more information, see OAuth2 Application (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/oauth-apps.html) in the *Advanced Authentication - Administration (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/bookinfo.html)* guide. Also, introduces API calls to retrieve the following information of OAuth2 authentication: ◆ Authenticated User details ◆ Chain details ◆ Tenant details For more information, see Advanced Authentication API (https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html) guide.

Software Fixes

Component	Issue Description
SAML Service Provider	Pre-condition: Download the SAML metadata from the `https://<servername>/osp/a/TENANT1/auth/saml2/metadata` URL. Uploading Identity Provider with the above metadata in the SAML Service Provider method causes configuration error in the web authentication of corresponding tenants. Removing the Identity Provider is not restoring the default identity provider settings and the web authentication is not accessible.
Web Authentication	Deleting a Web Authentication event that contains incorrect configuration does not reconfigure or restart the Web Authentication module cache.

3 2022.3.1 Update

Advanced Authentication as a Service 2022.3.1 includes the following updates:

- Enhancements
- Software Fixes

Enhancements

- Support for HANIS Face Method
- An Option to Validate the OTP Methods Manually
- Timeout Options
- Renamed FIDO 2.0
- Ability to Retrieve the Risk Score

Support for HANIS Face Method

Advanced Authentication provides the Home Affairs National Identification System (HANIS) method that facilitates citizens of South Africa to authenticate using their face that has been enrolled in the National Identification System. During authentication, the Advanced Authentication server forwards the user details to the third-party service provider that is integrated with National Identification System where the validation takes place. The user gets authenticated to the required resource or endpoint based on the validation result.

For more information, see HANIS Face (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/hanis_face.html) in the *Advanced Authentication - Tenant (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.

An Option to Validate the OTP Methods Manually

This release introduces the following options in the respective OTP methods:

- **Verify email address**: This option is introduced in the Email OTP method and helps to send the verification code to a specified email address. This option allows the users to validate the email address during the manual enrollment.

  For more information, see Email OTP (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/email_otp.html) in the *Advanced Authentication - Tenant (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.

- **Verify phone number**: This option is introduced in the SMS OTP and Voice OTP methods to send the verification code to a specified phone number. This option lets users verify whether the phone number is valid before the manual enrollment.

  For more information, see SMS OTP (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/sms_otp.html) and Voice OTP (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/voice_otp.html) in the *Advanced Authentication - Tenant (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.

Timeout Options

This release introduces the following options in the Login Options policy:

- **Logon timeout (seconds)**: This option allows you to set the maximum duration of the logon session. The user must specify the login credentials within this duration to prevent the session termination.
- **Logon inactivity timeout (seconds)**: This option allows you to set the maximum inactivity timeout of the logon session, and a user can remain idle within this duration.

  For more information, see Login Options (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/login_opts.html) in the *Advanced Authentication - Tenant (https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html)* guide.

Renamed FIDO 2.0

In this release, the FIDO 2.0 method is renamed to FIDO2.

Ability to Retrieve the Risk Score

After integrating a product with Advanced Authentication, the administrators can use the following API call to retrieve the Risk Score of an authenticated user after successful authentication:

```
api/v1/logon/{{logon_process_id}}/do_logon
```

Software Fixes

Component	Issue Description
Administration Portal	After the full synchronization of the Cloud Bridge External repository, an error message is displayed.
Administration Portal	When the Datacenter file is unavailable and the administrator launches the **Quick Start** wizard to add the Cloud Bridge external repository, an error is displayed. This prevent administrator from proceeding the configuration further.

Component	Issue Description
Administration Portal	When eDirectory is configured as the external repository in Advanced Authentication, and the user entries include multiple CN values, then synchronization fails and displays an error message.
Administration Portal	When a user from an AD user group with administrator rights tries to access the Helpdesk report, the complete report of all the sites is not displayed. Instead, the following error message is displayed: `TypeError: a bytes-like object is required, not 'str.`
Administration Portal	When an administrator tries to change the Cache expiration time in the Cache Options policy, the updated expiration time is not saved, and changes are not applied.
Administration Portal	When an administrator tries to add a new SQL repository, the repository creation fails, and the following error message is displayed: `SQL repo connect error: (pymssql.InterfaceError)`
Administration Portal	When the Cloud Bridge Agent is down and the administrator tries to verify the configuration using the **Test Configuration** button, an invalid message is displayed without stating the cause.
Administration Portal	The Licensed users count does not display accurate values in the **Tenants** widget of the Dashboard. Now, the Licensed users count is renamed to enrolled users count.
Administration Portal	When the full synchronization on the Web server is in progress and if the fast synchronization is initiated on the Master server simultaneously, the full synchronization fails and results in an error.
Enrollment Portal	When a user tries to test the FIDO2 method in the Enrollment portal, the test fails, and the following message is displayed: `expected 'status' to be 'string', got: error.`
Enrollment Portal	When a user tries to enroll the FIDO2 method, the enrollment fails, and the following error message is displayed. This happens if the verification signature call is sent twice. `{"status":"error","errors":[{"location":"server","name":"Unknown Error","description":"AttributeError 'NoneType' object has no attribute 'get'"}]}`
Web Authentication	With the Logon with Expired Password option set to Deny in the Web Authentication event, if a user tries to log in with the expired password, the following message is not displayed: `You must change your password in order to logon.`
Web Authentication	When a user tries to authenticate to a Web Authentication event using the Denmark National ID method, the Denmark National ID portal loads, and an error appears after specifying the username.

Component	Issue Description

Web Authentication	When a user tries to authenticate to a Web Authentication event after enabling Google reCAPTCHA, the Google reCAPTCHA fails. If the connection is via proxy, the following messages are displayed one after the other:
	`Verification expired. Check the checkbox again`
	a few second later,
	`504 Gateway Time-out`

Web Authentication	After upgrading to Advanced Authentication 6.3.6.1, users are unable to authenticate to the web authentication events using the Card and Bluetooth methods on Internet Explorer 11 browser.
Web Authentication Method	After upgrading from Advanced Authentication 6.3, when a user tries to authenticate with Web Authentication method, the following error message is displayed: `Invalid redirect_URI`

4 2021.10.1 Update

Advanced Authentication as a Service 2021.10.1 includes the following updates:

- Enhancements
- Software Fixes

Enhancements

This release includes the following enhancements:

- Support NFC Cards for Web Authentication
- Setting to Use Biometrics Without PIN
- Cloud Bridge Repository Improvements

Support NFC Cards for Web Authentication

Advanced Authentication extends the Card method capabilities to enable users to use Near Field Communication (NFC) cards to authenticate to OAuth 2.0/ OpenID Connect, SAML 2.0 events, and Advanced Authentication portals.

Setting to Use Biometrics Without PIN

Advanced Authentication extends the capability of the Require biometrics option. Using this option, you can enable biometrics without enabling the PIN. The upcoming release of smartphone application supports this enhancement.

For more information, see Password (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/?page=/documentation/advanced-authentication-63/tenant-administrator-guide/data/smartphone.html) in the Advanced Authentication - Tenant guide (https://www.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/bookinfo.html).

Cloud Bridge Repository Improvements

Following are the user interface changes related to the Cloud Bridge external repository:

- The **Agent** drop-down is renamed to **Data Center**. The drop-down lists the data center name instead on unique ID for usability.
- The **Data Center** drop-down is introduced in the Quick Start wizard of the Cloud Bridge external repository.

Software Fixes

Component	Issue Description
RADIUS	The RADIUS authentication fails intermittently.

5 2021.9.1 Update

Advanced Authentication as a Service 2021.9.1 includes the following updates:

- Enhancement
- Security Improvements
- Software Fixes

Enhancement

This release includes the following enhancement:

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.

Component	Issue Description
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.

6 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:

- Cloud Bridge Repository Setup Wizard
- Enhanced Custom Branding to Customize the Helpdesk Portal
- Custom Branding Settings of Web Authentication Events in the Custom Branding Policy
- Provision to Select the Agent
- Support for Out-of-Band Method

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.

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.

7 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:

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.

8 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:

- Support for Installing the Cloud Bridge Agent on RedHat
- Support for Denmark National ID
- Option to Lock Users Who Fail While Testing the Enrolled Methods

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.

Component	Issue
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.