



Advanced Authentication as a Service Release Notes

2022

Legal Notices

© Copyright 2022 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. Micro Focus 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>).

Contents

About this Book	5
1 2022.10.1 Update	7
Enhancements	7
Repository Alias Name	7
Ability to Change the LDAP Password	7
Cloud Bridge External Repository Improvements	7
A New Custom Attribute is Added in SAML Assertion	8
Software Fixes	8
Known Issue	8
SSL Bad Handshake Error	8
Part I Previous Releases	11
2 2022.8.1 Update	13
Enhancements	13
Ability to Disable Fast Sync and Modify Fast Sync Interval for the Cloud Bridge External Repository	13
Timeout Settings Support for Web Authentication Events	13
Software Fixes	14
3 2022.5.1 Update	15
Enhancement	15
Software Fixes	16
4 2022.3.1 Update	17
Enhancements	17
Support for HANIS Face Method	17
An Option to Validate the OTP Methods Manually	17
Timeout Options	18
Renamed FIDO 2.0	18
Ability to Retrieve the Risk Score	18
Software Fixes	18

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 2022.10.1 Update

Advanced Authentication as a Service 2022.10.1 includes the following updates:

- ♦ “Enhancements” on page 7
- ♦ “Software Fixes” on page 8
- ♦ “Known Issue” on page 8

Enhancements

This release includes the following enhancements:

- ♦ “Repository Alias Name” on page 7
- ♦ “Ability to Change the LDAP Password” on page 7
- ♦ “Cloud Bridge External Repository Improvements” on page 7
- ♦ “A New Custom Attribute is Added in SAML Assertion” on page 8

Repository Alias Name

This release introduces the **User repository alias** option in the following for ease of identifying the repository when there are several repositories:


- ♦ Local Repository
- ♦ Cloud Bridge External Repository
- ♦ SCIM Managed Repository

Ability to Change the LDAP Password

This release introduces the **Change Password** button in the LDAP Password method on the Self Service Portal to allow users to change the auto-enrolled LDAP Password.

Cloud Bridge External Repository Improvements

This release includes the following improvements to the Cloud Bridge External repository:

- ♦ The **Data Source Connection credentials id** has been renamed to **Data Source Credential Unique ID**.
- ♦ A copy icon  is introduced next to the **Data Source Credential Unique ID** to copy the ID to clipboard.

A New Custom Attribute is Added in SAML Assertion

This release introduces an Active Directory attribute, **objectGUID**, to the SAML assertion for uniquely identifying an object. SAML assertion passes attributes to the Service Provider to describe the user. Users can customize the name of **objectGUID** attribute and send the SAML assertion as required.

For example, if a user's service provider does not recognize the **objectGUID** attribute but recognizes the **object_guid** attribute, then the user can change the name of attribute to meet the service provider's requirements.

Software Fixes

Component	Issue Description
Administration Portal	The Tenant export from Export/Import page fails due to the foreign key violation error.
Administration Portal	When an administrator tries to customize the look and feel of the administration portal by using the Custom Branding policy in the safari browser, color customization is not applied to the administration portal.
Administration Portal	Accessing the tenant host URL displays <code>PyoidcError provider info issuer mismatch</code> error if the tenant name contains hyphen (-).
Administration Portal	Users are unable to enroll the Smartphone method through Click to Enroll link because the link points to the TOP tenant URL instead of the respective tenant URL.
Cloud Bridge	In Cloud Bridge, the LDAP user attributes, first name and last name are not mapped appropriately with the following repository types: <ul style="list-style-type: none">◆ Active Directory◆ eDirectory Due to this incorrect mapping, the token and assertion does not display the first name and last name of the authenticated users.
Web Authentication	With one Web Authentication event active, if a user tries to log in to another Web Authentication event, an error message stating to log out from the previous event is displayed.

Known Issue

Advanced Authentication as a Service 2022.10.1 includes the following known issue:

SSL Bad Handshake Error

Issue: The Advanced Authentication Clients connected to Advanced Authentication as a Service use TLS 1.3 by default for HTTPS connection with the server. Therefore, the following error is displayed on clients due to the default TLS version:

SSL Exception: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure" or "Internal Server Error

Workaround:

1 Open the configuration file for respective client:

- ◆ Linux PAM Client: /opt/pam_aucore/etc/pam_aucore.conf
- ◆ Mac OS Client: /Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf
- ◆ Windows Client: C:\Program Data\NetIQ\Windows Client\config.properties

2 Set the parameter `tlsVersion` as follows:

`tlsVersion: TLS1.2`

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:

- ♦ [Chapter 2, “2022.8.1 Update,” on page 13](#)
- ♦ [Chapter 3, “2022.5.1 Update,” on page 15](#)
- ♦ [Chapter 4, “2022.3.1 Update,” on page 17](#)

2 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 \(https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/?page=/documentation/advanced-authentication-64/tenant-administrator-guide/data/t4donma2ncp4.html#t4duu5sbtj4f\)](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 \(https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/bookinfo.html\)](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 \(https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/web_auth.html#t4cjcywwk712\)](https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/web_auth.html#t4cjcywwk712) in the [Advanced Authentication - Administration \(https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/bookinfo.html\)](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 <code>authcfg.xml</code> 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.

3 2022.5.1 Update

Advanced Authentication as a Service 2022.5.1 includes the following updates:

- ♦ “Enhancement” on page 15
- ♦ “Software Fixes” on page 16

Enhancement

Enhancement	Description
API Support for OAuth Authentication	<p>This release introduces OAuth2 Application policy to allow the OAuth2 protocol-based applications to access the Advanced Authentication API.</p> <p>For more information, see OAuth2 Application (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/oauth-apps.html) in the <i>Advanced Authentication - Administration (https://www.netiq.com/documentation/advanced-authentication-64/tenant-administrator-guide/data/bookinfo.html)</i> guide.</p> <p>Also, introduces API calls to retrieve the following information of OAuth2 authentication:</p> <ul style="list-style-type: none">♦ Authenticated User details♦ Chain details♦ Tenant details <p>For more information, see Advanced Authentication API (https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html) guide.</p>

Software Fixes

Component	Issue Description
SAML Service Provider	<p>Pre-condition:</p> <p>Download the SAML metadata from the <code>https://<servername>/osp/a/TENANT1/auth/saml2/metadata</code> URL.</p> <p>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.</p>
Web Authentication	<p>Deleting a Web Authentication event that contains incorrect configuration does not reconfigure or restart the Web Authentication module cache.</p>

4 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 \(https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/hanis_face.html\)](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 \(https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/email_otp.html\)](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 \(https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/sms_otp.html\)](https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/sms_otp.html) and [Voice OTP \(https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/voice_otp.html\)](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 \(https://wwwtest.netiq.com/documentation/advanced-authentication-63/tenant-administrator-guide/data/login_opts.html\)](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: <code>TypeError: a bytes-like object is required, not 'str'.</code>
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: <code>SQL repo connect error: (pymssql.InterfaceError)</code>
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: <code>expected 'status' to be 'string', got: error.</code>
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. <code>{"status": "error", "errors": [{"location": "server", "name": "Unknown Error", "description": "AttributeError 'NoneType' object has no attribute 'get'"}]}</code>
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: <code>You must change your password in order to logon.</code>
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	<p data-bbox="673 222 1435 344">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:</p> <p data-bbox="673 373 1370 453">Verification expired. Check the checkbox again a few second later,</p> <p data-bbox="673 478 976 506">504 Gateway Time-out</p>
Web Authentication	<p data-bbox="673 531 1435 621">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.</p>
Web Authentication Method	<p data-bbox="673 646 1435 737">After upgrading from Advanced Authentication 6.3, when a user tries to authenticate with Web Authentication method, the following error message is displayed:</p> <p data-bbox="673 762 976 789">Invalid redirect_URI</p>