

Advanced Authentication 6.4 Service Pack 3

May 2024

Advanced Authentication 6.4 Service Pack 3 includes enhancements, improves usability, and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the [Advanced Authentication forum](#) on NetIQ as part of OpenText Cybersecurity Communities, our online community that also includes product information, blogs, and links to helpful resources. You can also post or vote for the ideas of enhancement requests in the [Ideas forum \(https://ideas.microfocus.com/MFI/advance-authentication\)](https://ideas.microfocus.com/MFI/advance-authentication).

For more information about this release and the latest release notes, see the [NetIQ Advanced Authentication Documentation \(https://www.netiq.com/documentation/advanced-authentication-64/\)](https://www.netiq.com/documentation/advanced-authentication-64/) page.

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 [NetIQ Advanced Authentication Documentation \(https://www.netiq.com/documentation/advanced-authentication-64/\)](https://www.netiq.com/documentation/advanced-authentication-64/) page.

IMPORTANT:

- ♦ If you use eDirectory as an LDAP repository while upgrading to Advanced Authentication 6.4 Service Pack 3, note that LDAP uses the cipher suite that is configured in the **Policies > HTTPS Options > Advanced SSL Settings > Pre-defined SSL ciphersuite** options.

After upgrading to Advanced Authentication 6.4 Service Pack 3, if the full synchronization between the Advanced Authentication and eDirectory LDAP server fails, perform one of the following:

- ♦ Change the certificate used by eDirectory to SSL EC CertificateDNS in the iManager. For more information about how to make the changes, see [TID KM000029147 \(https://portal.microfocus.com/s/article/KM000029147?language=en_US\)](https://portal.microfocus.com/s/article/KM000029147?language=en_US).
- ♦ Set the **Policies > HTTPS Options > Advanced SSL Settings > Pre-defined SSL ciphersuite** option to either **Less restrictive ciphers for backward compatibility** or **Custom** to create a ciphersuite that works for their system. For more information, refer to [HTTPS Options \(https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/https_opts.html\)](https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/https_opts.html).
- ♦ Upgrading to Advanced Authentication 6.4 Service Pack 3 overwrites the previously customized default password complexity settings of the **Password** method, **Emergency Password** method, and **Lockout Options** policy with the default values. For more information about default password complexity settings, see [Password](#), [Emergency Password](#), and [Lockout Options](#) in the [Advanced Authentication - Administration](#) guide.

After upgrading to Advanced Authentication 6.4 Service Pack 3, ensure to update the complexity values of your password to meet your requirements.

What's New?

Advanced Authentication 6.4 Service Pack 3 provides the following:

- ♦ [“Enhancements” on page 2](#)
- ♦ [“Security Improvements” on page 5](#)

Enhancements

This release includes the following enhancements:

Enable Chain Selection by Event

This release introduces the **Enable Chain Selection** option to enable chain selection per event basis. This option is only applicable the **Authenticators Management**, **OOB UI Logon**, **Smartphone Enrollment**, **OAuth2 / OpenID Connect**, and **SAML 2** events.

This feature allows administrators to choose the below options per event basis to display the chain selection list while authentication:

- ♦ **ON**: Allows users to select their preferred authentication chain from all the chains that are available to them.
- ♦ **OFF**: Disables the chain selection for the selected event and forces users to execute the highest priority chain for authentication.
- ♦ **OPTIONAL**: It displays the chain with the highest priority along with the Select Chain button that allows users to select the required chain from the list.

Configure this option for users to view the chain selection list, only a high-priority chain with the enrolled methods, or a high-priority chain with the ability to select the other chains from the list.

For more information, see [Configuring an Existing Event](#), [Creating an OAuth 2.0 / OpenID Connect Event](#), and [Creating a SAML 2.0 Event](#) in the [Advanced Authentication - Administration](#) guide.

Migration to New Enrollment Portal

Enable New Enrollment UI is set to **ON** as the default setting in the **Enrollment options** policy. This allows users to access the New Enrollment Portal post upgrade to Advanced Authentication 6.4 Service Pack 2.

NOTE: The administrator is required to validate and replace **Public External URLs (load balancers)** with a valid DNS name instead of the default URL, `https://global.sol`.

Support for a Smart Card with an Integrated Token Adhering PKCS#11 Library

Advanced Authentication extends the Card method capabilities to enable users to use the smart card that has an integrated token supporting PKCS#11 library to authenticate to **Windows Logon Event** and Advanced Authentication portals.

NOTE: The authentication using this type of card is supported only on Windows Client.

For more information, see [Card](#) in the [Advanced Authentication - Administration](#) guide.

Additionally, this release extends support for card readers that adhere to the PKCS#11 standards. The `card.pkcs11Enabled` parameter in the device service configuration has been added to use the supported card readers.

For more information about the supported cards, card readers, and parameter configuration, see [Supported Card Readers and Cards](#) and [Card Settings](#) in the [Advanced Authentication - Device Service](#) guide.

Secure the TLS Connection For CEF Log Forwarding Using the TCP with TLS Transport

This release introduces the ability to choose the CA certificate while using the **TCP with TLS** transfer protocol from the **Transport** list in the **CEF log forward** policy.

To enhance the security of the TLS connection between the Advanced Authentication Server and the external Syslog server, select the **TCP with TLS** transfer protocol, set the **Ignore Cert** toggle to **OFF**, choose the valid CA certificate, and upload the certificate.

For more information, see [CEF Log Forward Policy \(https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/config_log_forward_policy.html\)](https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/config_log_forward_policy.html) in the [Advanced Authentication - Administration](#) guide.

Enhanced Default Security Settings

This release introduces the password complexity improvements for the following methods and policy to enhance the default security:

- ♦ **Password** method:
 - ♦ **Complexity requirements:** Set to **ON** by default.
 - ♦ **Minimum password length:** Set to **10** by default.
 - ♦ **Maximum Password Age:** Restricted to 999 days. The default value is 42.
- ♦ **Emergency Password** method:
 - ♦ **Complexity requirements:** Set to **ON** by default.
 - ♦ **Minimum password length:** Set to **10** by default.

- ♦ **Password Age (minutes):** Restricted to 7200 minutes. The default value is 4320 minutes.
- ♦ **Maximum logins:** Restricted to 100 logins. The default value is 10.
- ♦ **Lockout Options** policy:
 - ♦ **Lockout period:** Set to **900** seconds by default.

For more information, see [Password](#), [Emergency Password](#), and [Lockout Options](#) in the [Advanced Authentication - Administration](#) guide.

Improved IIS Authentication Plug-in

The **Administration Tool** is enhanced to allow the application of the IIS Authentication Plug-in to an application running in the **Application Pool Identity** that uses a specified user or principal.

For more information, see [Modifying Identity for an Application Pool](#) in the [Advanced Authentication - IIS Authentication Plug-in](#) guide.

An Option to Hide the OATH Token List on the Enrollment Portal

This release introduces the **Display Rule** option in the **OATH OTP** method.

Using this option, you can configure the enrollment options for users to view and select accordingly. You can configure this option for users to enroll the **TOTP** method by scanning the QR code, entering the OATH Token details, or using both options.

For more information, see [TOTP](#) in the [Advanced Authentication - Administration](#) guide.

Support for the JSON Content-Type for HTTP Request

This release introduces the **HTTP request content type** option in the **SMS Sender** policy.

This option allows administrators to select the required content type to send the HTTP request to the service provider. This feature supports only the **Generic** sender service.

For more information, see [Generic](#) in the [Advanced Authentication - Administration](#) guide.

Support for New Versions of Operating Systems

In addition to the existing supported platforms, this release adds support for the following operating systems for the respective client components as follows:

Components	Windows 10 22H2 and Windows 11 23H2	MacOS 13 (Ventura)	Red Hat Enterprise Linux Server 9.2 and 9.3	Red Hat Enterprise Linux Workstation 9.2 and 9.3	Ubuntu 20.04 LTS
Desktop OTP Tool	Yes	Yes	NA	NA	NA
Device Service	Yes	Yes	Yes	Yes	Yes
Linux PAM Client	NA	NA	Yes	Yes	Yes
Mac OS X Client	NA	Yes	NA	NA	NA
Virtual Desktop Authentication Agent	Yes	NA	NA	NA	NA
Windows Authentication Agent	Yes	NA	NA	NA	NA
Windows Client	Yes	NA	NA	NA	NA

Server Messages Widget

This release introduces the **Server Messages** widget on the dashboard. This widget displays a message describing the low disk space condition along with the severity. For more information, see [Server Messages in Advanced Authentication - Administration](#).

Service Name and Account Name for the TOTP Method

Advanced Authentication introduces **Service Name** and **Account Name** fields for the **TOTP** method on the New Enrollment Portal. These fields are used while enrolling the **TOTP** method using third-party applications, such as Google Authenticator and Microsoft Authenticator.

For more information, see the [Google Authenticator App](#) in [Advanced Authentication- User](#) guide.

Improved Error Message

This release improves the error message that is displayed on all Advanced Authentication web portals, **New Enrollment UI**, and **Old Enrollment UI** when a user attempts to log in without specifying a password or PIN.

Security Improvements

This release includes security updates and improvements.

Resolved Issues

This release includes the following software fixes:

Component	Description of the Issue
Administration Portal	When an administrator exported a report from the Advanced Authentication server, the exported file was stored only on the server from where it was exported. However, the option to download the file was available on all servers in the cluster. On servers where the exported report did not exist, the download link appeared black, and the report could not be downloaded. Now, Advanced Authentication displays the option to download the produced report on the server where the file exists.
Administration Portal	Previously, the User Name attributes and User Lookup attributes included the otherMailbox attribute as default in a LDAP Repository. This attribute was not indexed by Active Directory and was causing performance issues. Now, when you create a new LDAP Repository, the otherMailbox attribute is not included as a default value in User Name attributes and User Lookup attributes. NOTE: For the existing Active Directory LDAP Repositories, remove the otherMailbox attribute from User Name attributes and User Lookup attributes. Removing this attribute enhances search and performance of the repository. To remove otherMailbox attribute, perform the following steps: 1. Log in as a customer administrator to the Advanced Authentication Administration Portal. 2. Edit the existing Active Directory repository and expand Advanced Settings. 3. Delete otherMailbox from the User lookup attributes and User name attributes. 4. Save the changes.
Administration Portal	The Event_name parameter was not present in the Syslog record for codes 102, 103, 104, 106, and 107.
Administration Portal	When an administrator attempted repository synchronization, the following message was displayed: <pre>ERROR ForkPoolWorker-1863400 [aucore.scripts.celery_tasks.sync_all_ldap_repos] Sync error</pre>
Administration Portal	When an administrator attempted to enable the Bypass user lockout in repository setting while configuring the Event, the change to this setting was not saved.

Component	Description of the Issue
Administration Portal	When an administrator attempted to delete the English language locale file from the Custom Locales under the Policies and replace it with another file, the locale disappeared and the following error message was displayed: <pre>No such file or directory: '/opt/AuCore/../../webui/static/locale/webui.en.json'</pre> The local appears again after refreshing the page.
Administration Portal	After upgrading to Advanced Authentication 6.4 Service Pack 2, an extra docker network named aaf_default was added without any container reference.
Administration Portal	After upgrading to Advanced Authentication 6.4 Service Pack 2, the dashboard occasionally failed to load the data and displayed the following error: <pre>Transport Error(503, 'Search Guard not initialized (SG11). See https://docs.search-guard.com/latest/sgadmin')(Internal Server Error)</pre> This is due to the corrupted Elasticsearch configuration on an Advanced Authentication appliance.
Administration Portal	After scheduling the removal of old backup files in Advanced Authentication, the old backup files were not being removed, and the log files were displaying the FileNotFoundException message.
Administration Portal	When an administrator enabled the Show chain selection option in the Authenticators Management Event, then the user was unable to see all the chains with the enrolled methods on the New Enrollment portal.
Administration Portal	When an administrator made any changes to the setting while Scheduling Synchronization of Backups to an FTP Server, and clicked the Save button, the following error message was displayed: <pre>script failed with "mirror: Login failed: 530 Login incorrect."</pre>
Administration Portal	When an administrator attempted to add the Active Directory LDAP repository on the 636 port with the Verify the SSL Certificate option enabled, the certificate validation failed. As a result, the addition of the AD LDAP repository was unsuccessful, and the following error message was displayed: <pre>Cannot bind to LDAP. LDAP connect error</pre>
FIDO U2F	When a user attempted to test the FIDO2 U2F method with the unregistered U2F device, the enrollment portal displayed the following message: <pre>This device is already registered</pre> Now, the following error message is displayed when the user uses the unregistered U2F device: <pre>Unregistered U2F device detected</pre>

Component	Description of the Issue
Enrollment Portal	Pre-conditions: ♦ Availability of a specific value in the <code>altSecurityIdentities</code> attribute of the LDAP repository ♦ The chain with PKI method is assigned to an event When a user logged in to the enrollment portal first time, the PKI method was not enrolled automatically.
New Enrollment Portal	When the Allow user enrollment without a phone option under the SMS OTP method was set to OFF, the user was able to enroll the SMS OTP method without a phone number in the repository.
OATH OTP	When an administrator attempted to delete the OATH Tokens in the OATH OTP for a user who has been deleted from the repository, it failed to delete the token and displayed the following message: User not found in repository (AuError)
Web Authentication	When an administrator configured any Web Authentication event with the HOTP method in the associated chain and enabled the Use Custom Messages option in the Web Authentication policy, then the HOTP method on the login page displayed incorrect messages in the English, Japanese and German languages.
Web Authentication	When an administrator enabled the Lockout Options policy and configured the limit of failure attempts of authentication in the Attempts failed option, the New Enrollment portal allowed the user to authenticate without any error after reaching the configured maximum number of failed login attempts.
Web Authentication	When an administrator configured the Google reCAPTCHA Options policy and enabled it on an event while simultaneously enabling the Enable Content Security Policy for WebAuth Service option in the HTTPS Options policy, then the user failed to login to an Event and received the Login failed, please try again error message. Additionally, the web authentication logs displayed the below error message: A CAPTCHA was required for login but the CAPTCHA data was not available.
Web Authentication	Pre-conditions: ♦ FIDO U2F + Password chain was assigned to the Windows Authentication events. ♦ Lockout Options policy was enabled. When a user attempted to enter the password without inserting the U2F device into the computer during authentication, the authentication screen refreshed repeatedly. Advanced Authentication considered this a failed login attempt. As a result, the user account got locked after reaching the configured maximum number of failed authentication attempts.

Component	Description of the Issue
Web Authentication	After upgrading to Advanced Authentication 6.4 Service Pack 2 Patch1, if the user attempted to log in to the new enrollment portal when their browser was set to a non-English language, the following error message was displayed: No authentication chains found
Web Authentication	After upgrading to Advanced Authentication 6.4 Pack 2 Patch 1, when an administrator enabled the Username-less login enabled option in the FIDO2 method, the user failed to log in the New Enrollment portal and the following message was displayed: <pre>{ "status": "error", "errors": [{ "location": "server", "name": "AuError", "msgid": "AUCORE-3057", "description": "Login failed" }], "reason": "UNKNOWN_FAILURE" }</pre>
Windows Client	If a user logged in using any method that requires a USB token while the Lockout policy was enabled, then any addition or removal of other USB devices or network changes like a VPN connection disrupted the post-log tracking. This disruption caused the loss of the USB token's presence and the Windows client initiated a forced log off and displayed the following error message: Windows Screen is locked because of unknown reasons
Windows Client	Pre-conditions: • The user configured Windows Hello (excluding Windows Hello for Business) on the Windows workstation. • The user updated their LDAP director password externally and desynchronized Windows Hello. When a user attempted to authenticate to the Windows client, then the Windows client displayed the following message after AA completes the authentication: Your password was changed on a different device. You must sign in to this device once with your new password, and then you can sign in with your PIN When a user clicked the Sign in button and then clicked the sync password to finish logon button, the log in completed successfully. However, when the user attempted to login to the Windows Client again, then Windows Hello will continue to display the above error message.
Windows Logon	When the user attempted to enroll multiple FIDO 2 devices by selecting different categories, the enrollment was successful. However, only the default or first enrolled FIDO 2 device worked while authenticating Windows Logon event. For the remaining enrolled FIDO 2 devices, it displayed the below error message: This security key doesn't look familiar. Please try a different one.

Upgrading

You can directly upgrade to Advanced Authentication 6.4 Service Pack 3 from 6.4 Service Pack 2 Patch 1.

NOTE: The following is the recommended upgrade sequence:

1. Advanced Authentication servers
2. Plugins
3. Client components

Any change in the upgrade sequence is not supported.

NOTE: The RAM requirement for Advanced Authentication 6.4 Service Pack 3 is:

- ♦ Minimum: 8 GB per server
- ♦ Recommended: 12 GB per server

For more information, see [Advanced Authentication System Requirements](#).

Known Issues

Advanced Authentication 6.4 Service Pack 3 includes the following known issue:

The U2F Method Is Not Working on Linux

Issue: Users are unable to enroll the U2F method on a Linux machine and an error message, Cannot reach the local FIDO U2F service. Contact your administrator to enable the service is displayed. This occurs as Device Service is unable to detect the device.

If users have enrolled the U2F method before upgrading to Advanced Authentication 6.4 Service Pack 3, then testing the method and authentication attempt using the U2F method will fail.

Workaround: Do not upgrade Device Service to Advanced Authentication 6.4 Service Pack 3 to use the U2F method. Instead, use Advanced Authentication 6.4 Service Pack 2.

Deprecated Options

The following options are deprecated in this release and will not be available in the upcoming Advanced Authentication release:

- ♦ Old Enrollment Portal
 - ♦ The Old Enrollment Portal is deprecated.
 - ♦ The new features and functionalities will be implemented only in the New Enrollment Portal.
 - ♦ Starting with the Advanced Authentication 6.4 Service Pack 2 release, the New Enrollment Portal is set as the default enrollment option (**Enable New Enrollment Options** in the **Enrollment Options** policy is set to **ON**).

- ♦ Repo Agent
 - ♦ The Repo Agent is deprecated starting with Advanced Authentication 6.4 Service Pack 3 release.
 - ♦ The configuration details related to Repo Agent will not be available and the administrator cannot add new external repo details on the Administration Portal.

NOTE: There is no equivalent replacement for the Repo Agent. If you were using the Repo Agent previously, you must configure a VPN to ensure connectivity between your datacenter and cloud infrastructure.

Planned End of Support

Support for the following Operating Systems will be deprecated in the upcoming release:

- ♦ CentOS 7
- ♦ Debian 10
- ♦ Microsoft Windows 10 21H2
- ♦ Microsoft Windows 11 21H2

For more information about the supported Operating Systems, see [Advanced Authentication System Requirements](#).

Contacting Open Text

For specific product issues, contact Open Text Support at <https://www.microfocus.com/support-and-services/> (<https://www.microfocus.com/support-and-services/>).

Additional technical information or advice is available from several sources:

- ♦ Product documentation, Knowledge Base articles, and videos: <https://www.microfocus.com/support-and-services/> (<https://www.microfocus.com/support-and-services/>)
- ♦ The Open Text Community pages: <https://www.microfocus.com/communities/> (<https://community.microfocus.com/>)

Legal Notice

Copyright 2014 - 2023 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see <https://www.microfocus.com/en-us/legal> (<https://www.microfocus.com/en-us/legal>).

