

Advanced Authentication 6.4 Service Pack 3 Patch 3

January 2025

Advanced Authentication 6.4 Service Pack 3 Patch 3 resolves a security vulnerability and 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 \(https://community.opentext.com/cyberres/access-management/adv-auth\)](https://community.opentext.com/cyberres/access-management/adv-auth) on 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 \(https://community.opentext.com/cyberres/access-management/adv-auth/i/ideas\)](https://community.opentext.com/cyberres/access-management/adv-auth/i/ideas).

For more information about this release and the latest release notes, see the [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 Patch 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 Patch 3, if the full synchronization between the Advanced Authentication and eDirectory LDAP server fails, perform one of the following actions:

- ♦ Change the certificate used by eDirectory to SSL EC CertificateDNS in the Identity Console. 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, see [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 Patch 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 Patch 3, ensure to update the complexity values of your password to meet your requirements.

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

What's New?

- ♦ [“Enhancements” on page 2](#)
- ♦ [“Security Improvement” on page 3](#)
- ♦ [“Technical Preview” on page 3](#)

Enhancements

This release includes the following enhancements:

A Setting to Add the Alternative Load Balancer Hostnames

This release introduces the **Alternative Load Balancer Hostnames** setting in the **Public External URL (Load Balancer)** policy. This setting enables you to add any hostname or URL that does not directly point to the load balancer.

This setting contains the **DNS Host Check** option to disable the validation of incoming requests based on the host header.

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

Ability to Cancel the Multiple Method Authentication Chain

This release introduces the **Cancel** button on the second factor input form of the login page.

Now, users can cancel the multiple method authentication process at any point and return to the **Chain Selection** page. This enhancement helps prevent users from getting locked in the authentication process and enables them to choose a different authentication chain.

Security Improvement

This release resolves a security issue in the administration portal. To mitigate this issue, Advanced Authentication sends a Content-Security-Policy response header.

For more information, see [KM000031745 \(https://portal.microfocus.com/s/article/KM000031745?language=en_US\)](https://portal.microfocus.com/s/article/KM000031745?language=en_US).

Technical Preview

The features in the technical preview are available for testing and providing feedback. The technical preview features are not fully supported and may change significantly based on your feedback and ongoing development. We recommend that you try these features and provide your feedback to aafeedback@opentext.com.

IMPORTANT: It is recommended to deploy or configure the technical preview features only in the staging environment.

The following are technical preview features in this release:

- ♦ **Support for macOS 14 Operating System**

Mac OS X Client, Device Service, and Desktop OTP Tool are available for installation on macOS Sonoma.

- ♦ **Support for the Bluetooth eSec Method for Linux and MacOS Clients**

Advanced Authentication facilitates contactless authentication with the Bluetooth eSec method. Users can authenticate to Linux and macOS Clients using the Bluetooth-supported device within the discoverable range.

Resolved Issues

This release includes the following software fixes:

Component	Description of the Issue
Administration Portal	During cluster synchronization, Advanced Authentication failed to remove the cluster nodes that had been inactive or out-of-sync for more than six months.
	The Advanced Authentication failed to sync the out-of-sync node automatically.
	Additionally, nodes were forced out-of-sync.

Component	Description of the Issue
Administration and Old Enrollment Portal	After upgrading to Advanced Authentication 6.4 Service Pack 3 Patch 2, users were unable to access the old Enrollment Portal and Administration Portal through the load balancer. The portals failed to load and displayed the following error message in the Web Server logs: Request for domain {Domain name} not in valid host list
Administration Portal	After upgrading to Advanced Authentication 6.4 Service Pack 3 or Advanced Authentication 6.4 Service Pack 3 Patch 1, the administrator was unable to access the Administration Portal.
Administration Portal	When the Global Master was down, it remained offline during the entire downtime and the following error message was displayed during client authentication: ConnectionError(: Failed to establish a new connection: [Errno 113] No Route to Host) caused by: NewConnectionError(: Failed to establish a new connection: [Errno 113] No Route to Host)
Device Service	Pre-condition: ◆ Upgraded to Device Service 6.4.3 ◆ Configured a chain with methods requiring device service ◆ Established the Remote Desktop session between two machines. After disconnecting the Remote Desktop session, the device service crashed. When attempting remote or local login on the host machine, the available authentication methods were limited to methods that did not require the device service.
Device Service	When the user attempted to log in to the local console after disconnecting the Remote Desktop session, the device service continued the redirected authentication requests to the disconnected remote service. As a result, all redirected authentication methods failed.
Device Service	Pre-condition: ◆ Upgraded to Device Service 6.4.3 ◆ Configured a chain with methods requiring device service ◆ Established the Remote Desktop Protocol (RDP) connection between two machines. After disconnecting the RDP session and attempting local login on the same machine, the device service crashed and displayed authentication methods that did not require the device service.

Component	Description of the Issue
Device Service	When the user attempted to log in to the Windows machine using the CARD method through a 1:N user lookup, the authentication was occasionally rejected. This was because the PKI method was being processed instead of the CARD method. If the user attempted to log in using the CARD method and if its token was not enrolled in the PKI method, the following error message was displayed: There is no template for the PKI
Device Service	Pre-condition: Configured multiple PKCS#11 provider libraries in the Device Service. When the user attempted to enroll the card method through PKCS#11 libraries, the device service failed to direct the card to an appropriate provider.
FIDO U2F	After upgrading to the Device Service 6.4 Service Pack 3 Patch x, if an administrator configured the Facets Setting option in the U2F method, the U2F method failed.
macOS Client	When the user attempted to log in to the macOS 14 system and accidentally closed the Advanced Authentication credential provider, the user was unable to re-open the credential provider for authentication. The user must reboot the system to regain access.
macOS Client	If a user accidentally closed the Advanced Authentication credential provider while logging into macOS 14, they could not reopen it for authentication and had to reboot the system to regain access.
New Enrollment Portal	Pre-condition: ♦ Installed Advanced Authentication 6.4 server ♦ Configured the SMS Sender policy and created a chain containing the SMS OTP method After upgrading to Advanced Authentication 6.4 Service Pack 3 Patch 2, the users were unable to access the New Enrollment portal, and the following error message was displayed: AttributeError 'NoneType' object has no attribute 'strip'
SAML Event	Pre-condition: Users were associated with a large number of group memberships (typically hundreds of group memberships). When Advanced Authentication was integrated with Office 365 using SAML 2.0 without ADFS, the following error message was displayed in the error log files when the user was authenticating to Office 365: upstream sent too big header
Web Authentication	When the user attempted to log in to an event that did not have any chains assigned to it, the username prompt was displayed in an indefinite loop until the portal times out.

Component	Description of the Issue
Web Authentication	When users were associated with a large number of groups and contained enormous userGroups attributes, they were unable to log in. This was due to different issues depending on the authentication methods used.
Web Authentication	The administrator was unable to set the Session Timeout value to less than one minute in the Web Authentication policy.
Web Portals	When a developer attempted API calls against the Helpdesk event to manage the users, the web server logs displayed the following error: No space left on device
Windows Client	Pre-condition: ♦ Installed Windows Client 6.4.3.x ♦ Configured the allowedProviders parameter for the third-party credential provider in the config.properties file of the Windows Client When users attempted to authenticate to the Windows Client, the configured third-party credential provider was unavailable to authenticate them.
Windows Client	Pre-condition: ♦ The user configured Windows Hello on the Windows workstation ♦ Chain with Windows Hello was assigned to the Windows Logon event ♦ The Windows Client was upgraded to Advanced Authentication Windows Client 6.4 Service Pack 2 When the user changed the Windows Hello password and attempted to log in to the Windows using the Windows Hello method for the first time after changing the password, the following message was displayed: The PIN has to be synchronized
Windows Client	When an administrator set the disable_local_accounts parameter to true in the Windows client's config.properties file, the user was allowed to authenticate to the Windows client with the wrong domain name, bypassing the multi-factor authentication without any errors.
Windows Client	Pre-condition: ♦ Users had never logged in with an LDAP password ♦ Users were selecting chains that did not include the LDAP method When the users attempted to authenticate to the Windows Client, the configured third-party credential provider was unavailable to authenticate them.

Component	Description of the Issue
Windows Client	Pre-condition: ♦ Installed Advanced Authentication Windows Client 6.4 Service Pack 2 on the local machine ♦ The remote machine was part of an Entra-managed environment When the user attempted to establish a Remote Desktop connection to an Entra-joined machine, the authentication through the Windows Client failed.

Upgrading Advanced Authentication

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

NOTE: The following is the recommended upgrade sequence:

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

Any deviation in the upgrade sequence is not supported.

NOTE: The following are the RAM requirements for Advanced Authentication 6.4 Service Pack 3 patch 3:

- ♦ 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 Patch 3 does not have any known issues.

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 are implemented only in the New Enrollment Portal.
 - ♦ Starting with the Advanced Authentication 6.4 Service Pack 2 release, the New Enrollment Portal is 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 the Advanced Authentication 6.4 Service Pack 3 release.
 - ♦ The configuration details related to Repo Agent are 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 used 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 [opentext support \(https://www.microfocus.com/support-and-services/\)](https://www.microfocus.com/support-and-services/).

Additional technical information or advice is available from several sources:

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

Legal Notice

Copyright 2014 - 2024 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.