

Advanced Authentication 6.4 Service Pack 3 Patch 5

July 2025

Advanced Authentication 6.4 Service Pack 3 Patch 5 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 5, 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 5, 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 5 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 5, 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.

Resolved Issues

This release includes the following software fixes:

Component	Description of the Issue
Administration Portal	When the Return groups option is set to OFF in an event configuration, the Advanced Authentication returns the groups of users authenticated to an event. This is inconsistent behavior, as user groups are returned from both the logon response and user API call.

Upgrading Advanced Authentication

You can directly upgrade to Advanced Authentication 6.4 Service Pack 3 Patch 5 from 6.4 Service Pack 3 Patch 3 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 5:

- ♦ 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 5 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 - 2025 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.