Advanced Authentication 6.4 Service Pack 3 Patch 1

June 2024

Advanced Authentication 6.4 Service Pack 3 Patch 1 resolves 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).

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/) 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/) page.

IMPORTANT:

- If you use eDirectory as an LDAP repository while upgrading to Advanced Authentication 6.4 Service Pack 3 Patch 1, 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 1, 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).
- 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).

- Upgrading to Advanced Authentication 6.4 Service Pack 3 Patch 1 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 1, ensure to update the complexity values of your password to meet your requirements.

Resolved Issues

This release includes the following software fixes:

Component	Description of the Issue
Web Authentication	When users are associated with a large number of groups and contain enormous **userGroups** attributes are rejected by the Nginx reverse proxy. Therefore, users were unable to log in.
Enrollment Portal	When a user attempts to log in to the Enrollment Portal on their iPhone, user receives the `noAuthCahinFound` error message after entering their credentials and clicking the Login button. This occurs while: ◆ Accessing the New Enrollment Portal in Firefox and Safari browsers. ◆ Accessing the Old Enrollment Portal in the Chrome browser. Pre-conditions: ◆ **LDAP** + **Smartphone** chain was assigned to the **OAuth / OpenID Connect** event. ◆ Integrate Advanced Authentication with Access Manager using the **OAuth 2.0 / OpenID Connect** event. ◆ Change the language on iPhone from English to any other language.

Upgrading

You can directly upgrade to Advanced Authentication 6.4 Service Pack 3 Patch 1 from 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 RAM requirement for Advanced Authentication 6.4 Service Pack 3 patch 1 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 Patch 1 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 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).