

Advanced Authentication 6.4 Service Pack 3 Patch 2

August 2024

Advanced Authentication 6.4 Service Pack 3 Patch 2 resolves 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](#) 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 Patch 2, 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 2, 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 Patch 2 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 2, ensure to update the complexity values of your password to meet your requirements.

Security Improvements

This release mitigates the following security issues:

- ♦ Apache log4j Vulnerability.
- ♦ RADIUS server updates to address the security vulnerability named as BlastRadius (CVE-2024-3596). For more information, see [BlastRadius](#).
- ♦ RADIUS client updates to consistently send the Message-Authenticator (MA) attribute at the beginning of all RADIUS messages.
- ♦ **Radius Options** policy improvement to include the **Require message Auth** option to mandate the MA attribute for each configured RADIUS client during authentication.

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

BlastRadius

This section describes the following aspects of the BlastRadius attack and details on how this release addresses and mitigates the issue:

- ♦ If you use RADIUS Extensible Authentication Protocol (EAP) - Tunnelled Transport Layer Security (TTLS), BlastRadius does not affect you.
- ♦ To carry out a successful BlastRadius attack, the attacker must have physical access or have previously compromised network to read and write RADIUS messages. This makes an attacker more likely to be an insider. Other insider attacks are probably easier and less expensive to implement than the BlastRadius attack. However, this does not change the fact that modifications are required.
- ♦ The BlastRadius CVE-2024-3596 highlights that the RADIUS protocol is broken, affecting all Radius vendors. The vulnerability impact depends on the RADIUS system configuration. The system consists of every RADIUS server, RADIUS proxy, and RADIUS client.
- ♦ To resolve this vulnerability, the Advanced Authentication 6.4 Service Pack 3 Patch 2 release includes various security improvements. For more information, see [Security Improvements](#).

- ♦ If your system is configured such that there are RADIUS servers that are proxying RADIUS requests, you must immediately upgrade the proxy (as well as upgrade the application to Advanced Authentication 6.4 Pack 3 Patch 2).
- ♦ An administrators can configure Advanced Authentication 6.4 Pack 3 Patch 2 to ensure that all components of the RADIUS system use the recommended MA attribute to protect against the BlastRadius attack. After upgrading to Advanced Authentication 6.4 Pack 3 Patch 2 or later version and configuring each RADIUS client to include the MA attribute in the beginning of the Radius messages, an administrator should:
 - ♦ Verify if the RADIUS client is capable and configured to send the MA attribute.
 - ♦ Set the **Require message Auth** option to **ON** in the **RADIUS Options** policy for all RADIUS clients.

Resolved Issues

This release includes the following software fixes:

Component	Description of the Issue
Administration Portal	When an administrator configured the CEF Log Forward policy, if the external Syslog server was unavailable due to shutdown or reboot, the Advanced Authentication server did not cache event data logged during that time. When the external Syslog server was back online, it failed to send events logged during the downtime, and it stopped forwarding newly logged events.
Administration Portal	After upgrading to Advanced Authentication 6.4 Service Pack 3, the administrator was unable to access the administration portal. This was due to the host header being filtered with case sensitivity.
New Enrollment Portal	Pre-condition: ♦ Password + FIDO U2F chain was assigned to the SAML2 event. After upgrading to Advanced Authentication 6.4 Service Pack 2 Patch 1, when a user attempted to authenticate using the Password + FIDO U2F chain, the browser entered into an infinite refresh loop after the authentication process completed.
TOTP Method	When a user attempted to change the Display Name while enrolling the TOTP method, the following error message was displayed: one of the "enroll_process_id", "auth_t_id", "method_id" parameters is required
Web Authentication	When configuring the Web Authentication policy, the administrator was unable to set the Session Timeout option to less than 60 seconds.

Upgrading

You can directly upgrade to Advanced Authentication 6.4 Service Pack 3 Patch 2 from 6.4 Service Pack 3 Patch 1 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 RAM requirements for Advanced Authentication 6.4 Service Pack 3 patch 2 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 2 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>).

