

OpenText Advanced Authentication 25.1 (v6.5)

April 2025

Advanced Authentication 25.1 (v6.5) 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 \(https://community.opentext.com/cyberres/access-management/adv-auth\)](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 \(https://www.netiq.com/documentation/advanced-authentication-65/\)](https://www.netiq.com/documentation/advanced-authentication-65/) 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 [Advanced Authentication Documentation \(https://www.netiq.com/documentation/advanced-authentication-65/\)](https://www.netiq.com/documentation/advanced-authentication-65/) page.

IMPORTANT:

- ♦ This release includes only server-side updates for Advanced Authentication, with server version 25.1(v6.5). Ensure that no client-side updates are included in this release, so the corresponding client version remains at 6.4 Service Pack 3 Patch 3.
- ♦ The administration portal displays the **Verification** method without any icon, intended only for internal processing between Advanced Authentication components. Administrators can edit it, but it has no configurable settings and does not affect user functionality.
- ♦ Upgrading to Advanced Authentication 25.1 (v6.5) ignores the `allowedproviders` parameter in the Windows client's `config.properties` file. This prevents the Windows client from prompting the previously configured primary or third-party credential provider during logon process.

After the upgrade, you must manually configure the **Windows Credential Provider** policy to restore the values defined in the `allowedproviders` parameter in the `config.properties` file.

For more information, see [Windows Credential Providers](#).

What's New?

Advanced Authentication 25.1 (v6.5) provides the following features and enhancements:

- ♦ [“Ability to Lockout the Login Method After Multiple Authentication Failures” on page 2](#)
- ♦ [“Branding Updates” on page 2](#)
- ♦ [“Enhanced User Interface for Administration Portal and Enrollment Portal” on page 2](#)
- ♦ [“Enhanced Username-less FIDO2 Login Process for Web Authentication Events” on page 3](#)
- ♦ [“Extended NFC Support for Android Tablets” on page 3](#)
- ♦ [“New Windows Credential Providers Policy” on page 3](#)
- ♦ [“Option to Block API Requests with Sensitive Parameter in the URL” on page 3](#)
- ♦ [“Options to Reorder and Remove the Methods and Chains” on page 4](#)
- ♦ [“Simplified FIDO2 Login Experience” on page 4](#)
- ♦ [“Support for New Versions of Operating” on page 4](#)

Ability to Lockout the Login Method After Multiple Authentication Failures

If a specific authentication method fails 10 times during authentication, regardless of the chain used, that method will be temporarily locked for one hour. During the lockout, the user cannot use any authentication chain that includes the locked method and will receive a `User is locked` error.

After the lockout period, if the user fails again (11th time) using the same method, an additional one-hour lockout will be triggered.

NOTE: This enhancement does not apply to the **SMS OTP** and **Email OTP** methods and will be included in the next upcoming release.

Branding Updates

Micro Focus is now part of OpenText. To adhere to the OpenText brand, the name of the product, its components and user interfaces, logos, company name references, and documentation are updated. The OpenText versioning mechanism uses the CY.Q (Calendar Year.Quarter) format. Starting from the 6.5 release, Advanced Authentication adheres to the OpenText versioning convention. Advanced Authentication 6.5 is known as OpenText Advanced Authentication 25.1 (v6.5).

Enhanced User Interface for Administration Portal and Enrollment Portal

This release improves the user interface of the administration and enrollment portal for the TOTP method, making it more user-friendly and efficient. The updated interface includes the following:

- ♦ The **Google Authenticator format of QR code (Key URI)** option is renamed to **Google Authenticator QR code (Key URI)** in the **OATH** method.
- ♦ The **Hide TOTP on a rooted smartphones** option is renamed to **Hide TOTP on rooted smartphones** in the **OATH** method.
- ♦ The OATH token section on the **TOTP** enrollment portal is enhanced to provide a better user experience for the **TOTP** method.

Enhanced Username-less FIDO2 Login Process for Web Authentication Events

This update introduces a new **FIDO** button and a [Click here to login with another method](#) link on the Web authentication event login page.

This enhancement allows users to log in to web authentication events using the **FIDO2** method without entering a username at any point during the login process.

These options are available only when:

- ♦ The **Username-less login enabled** option is set to **ON**
- ♦ The Event is configured to have at least one chain containing the FIDO2 method, and the user is enrolled their FIDO2 card
- ♦ A user is executing the Web Authentication event

Use Case 1:

If a user has multiple chains assigned, then the user is prompted with a new dialog box with the **FIDO2** button and the [Click here to login with another method](#) link on the login page. Clicking **FIDO** initiates a FIDO2 username-less login prompting the user to provide their FIDO2 key.

Alternatively, clicking [Click here to login with another method](#) allows the user to log in by specifying their username and selecting their chain.

Use Case 2: If a user has a single chain assigned with the **FIDO2** method, the user can directly provide their FIDO2 key, bypassing the dialog box.

Extended NFC Support for Android Tablets

This release extends the NFC functionality to include support for Android tablets, ensuring compatibility with larger screen sizes but not workstations. This enhancement enables users to seamlessly interact with the NFC feature on tablets with a more versatile experience.

New Windows Credential Providers Policy

This release introduces the **Windows Credential Providers** policy. This policy allows you to configure the settings that enable a third-party credential provider to confirm the user's identity and authentication on Windows Client.

For more information, see [Windows Credential Providers](#).

Option to Block API Requests with Sensitive Parameter in the URL

This release introduces the **Refuse Process IDs in URL** option in the **HTTPS options** policy. The **Refuse Process IDs in URL** option allows administrators to block the API requests containing sensitive parameters such as `login_session_id`, `endpoint_session_id`, and so on.

If Refuse Process IDs in URL option is set to **OFF**, API requests with these parameters returns an error until the parameters are removed from the request.

NOTE: It is recommended to upgrade all clients to version 6.4 Service Pack 3 Patch 3 and set this option to **ON** for secure connection between clients and server.

Options to Reorder and Remove the Methods and Chains

This release introduces the **Move up**, **Move down**, and **Remove** buttons next to the **Used** list under **Chains** and **Events**. These options allow you to reorder and remove methods within the chains, and to reorder and remove chains within the events.

For more information, see [Creating a chain](#) and [Configuring events](#) in [Advanced Authentication - administration](#).

Simplified FIDO2 Login Experience

This release introduces the **USB Transport**, **NFC Transport**, and **BLE Transport** settings in the **FIDO2** method. These setting enables administrators to restrict FIDO2 authentication to specific device types, such as USB, NFC, or Bluetooth devices.

This enhancement simplifies the user experience. Users do not need to select their device type during authentication. With this update, users can seamlessly authenticate using the FIDO2 key with their configured device type.

NOTE: If the **Username-less login enabled** option is set to **ON**, then the **USB Transport**, **NFC Transport**, and **BLE Transport** options must be set to **OFF**. You must set either Username-less login enabled or any transport option, but not both.

For more information, see [FIDO2](#) in the [Advanced Authentication - administration](#) guide.

Support for New Versions of Operating

In addition to the existing supported platforms, this release adds support for the following operating systems for the respective Advanced Authentication 6.4 Service Pack 3 Patch 3 client components as follows:

Components	Windows 11 24H2	Microsoft Windows Server 2022	Red Hat Enterprise Linux 8.10 and 9.4	Red Hat Enterprise Linux Workstation 9.2 and 9.3	Ubuntu 22.04 LTS and 24.04 LTS	SUSE Linux Enterprise Server 15 Service Pack6	macOS 14 (Sonoma) and 15 (Sequoia)
ADFS MFA plug-in	NA	Yes	NA	NA	NA	NA	NA
Desktop OTP Tool	Yes	Yes	NA	NA	NA	NA	Yes
Device Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IIS Authentication plug-in	NA	Yes	NA	NA	NA	NA	NA
Linux PAM Client	NA	NA	Yes	Yes	Yes	Yes	NA
Ligon Filter	NA	Yes	NA	NA	NA	NA	NA
macOS Client	NA	NA	NA	NA	NA	NA	Yes

Components	Windows 11 24H2	Microsoft Windows Server 2022	Red Hat Enterprise Linux 8.10 and 9.4	Red Hat Enterprise Linux Workstation 9.2 and 9.3	Ubuntu 22.04 LTS and 24.04 LTS	SUSE Linux Enterprise Server 15 Service Pack6	macOS 14 (Sonoma) and 15 (Sequoia)
Remote Desktop Gateway	NA	Yes	NA	NA	NA	NA	NA
Windows Authentication Agent	Yes	NA	NA	NA	NA	NA	NA
Windows Client	Yes	Yes	NA	NA	NA	NA	NA
Virtual Desktop Authentication Agent	Yes	NA	NA	NA	NA	NA	NA

Security Improvement

This release provides the following enhancements to mitigate security issues:

- The Advanced Authentication server now validates data to prevent potential SQL Injection while adding the SQL database.
- The Advanced Authentication backup field functionality has been updated to enhance input validation during backups, preventing potential shell injection during an administrator session.
- Session management has been improved to track and reject invalidated sessions after logout.
- Apache Tomcat has been upgraded to address [CVE-2025-24813](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-24813) (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-24813>).
- The Advanced Authentication administration portal is enhanced to prevent Cross-Site Scripting (XSS) attacks.
- Nginx security has been enhanced to prevent the exposure of excessive error details.

Technical Preview

The features in the technical preview are available for testing and feedback. These 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 feedback to aafeedback@opentext.com.

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

Twilio Verify Support

Advanced Authentication now supports Twilio Verify for enhanced user verification.

Twilio Verify is a turnkey API service that sends an OTP to user's SMS to enhance user account security and prevent fraud. It sends SMS from phone numbers selected from the sender's pool configured in the Twilio account, rather than using a specific phone number.

To configure the Twilio Verify, three options have been introduced in the **SMS Sender** policy.

For more information, see [SMS sender](#) in the [Advanced Authentication - administration](#) guide.

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 stopped forwarding newly logged events.
Administration Portal	When an administrator saved a report with any chart type and later accessed the Reports on the Administration portal to view the saved report, the Event Court Line Chart failed to load and displayed the Loading message.
Administration Portal	When an administrator attempted repository synchronization, the following message was displayed: LDAP connect error: socket ssl wrapping error: [Errno 104] Connection reset by peer
Card	When a user was attempting to authenticate using the CARD method: ♦ The card reader failed to change color to indicate that the user should present their card. ♦ The card reader took longer than expected to detect the card, and during this delay, the Card reader not detected error message was displayed.
FIDO2	When the Username-less login enabled option was set to ON in the FIDO2 method, it disrupted the authentication process and displayed the following error message during authentication: Authentication Failed. Contact the administrator.

Component	Description of the Issue
Web Authentication	After upgrading to Advanced Authentication 6.4 Service Pack 2, when a user attempted to log in to the web authentication events, the system failed to retrieve the group details of users who authenticated to the event. As a result, the following error message was displayed in the logs: Error contacting Advanced Authentication server while searching: <code>internal.atlaslite.jcce.exception.CoreCommunicationException: Error communicating with NAAF server during user lookup.</code>

Upgrading Advanced Authentication

You cannot directly upgrade from version 6.4 Service Pack 3 Patch 3 or earlier to version 25.1 (v6.5).

The recommended upgrade order from version 6.4 Service Pack 3 Patch 3 or earlier to version 25.1 (v6.5) is as follows:

- 1 Perform Online upgrade to Advanced Authentication 6.4 Service Pack 3 Patch 4.
- 2 Perform Product upgrade and then Online upgrade to Advanced Authentication 25.1 (v6.5).

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 25.1 (v6.5) is 12 GB per server. For more information, see [Advanced Authentication system requirements](#).

Advanced Authentication Upgrade Consideration for Public Cloud and Azure Kubernetes Services

You cannot directly upgrade the Advanced Authentication from version 6.4 Service Pack 3 Patch 3 or earlier to version 25.1 (v6.5) using the Helm chart. You must first upgrade to version 6.4 Service Pack 3 Patch 4.

The recommended upgrade order from version 6.4 Service Pack 3 Patch 4 to version 25.1 (v6.5) is as follows:

- ♦ Perform online upgrade to Advanced Authentication 6.4 Service Pack 3 Patch 4 using `aaF-1.18.6-helm-chart.zip`.
- ♦ Perform product upgrade to Advanced Authentication 25.1 (v6.5) using `aaF-1.20.19-helm-chart.zip`.

For more information on upgrade steps using Helm charts, refer [Upgrading Advanced Authentication on public cloud using Kubernetes](#) and [Upgrading Advanced Authentication on Azure Kubernetes services in an Air Gap Environment](#) in the [Advanced Authentication- server installation and upgrade guide](#).

Known Issues

Advanced Authentication 25.1 (v6.5) have the following known issues:

Logon Filter Issue on Windows 11

Issue: When the Local Security Authority (LSA) protection is enabled on Windows 11, the user group remains unchanged with the Logon filter.

Workaround: Disable LSA protection.

To disable LSA protection, follow the steps in the [Disable LSA protection \(https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection#disable-lsa-protection\)](https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection#disable-lsa-protection)

Bluetooth Method is Not Working on macOS 14 and macOS 15

The Bluetooth eSec method does not work on macOS14 and macOS15 due to permission issues. The following error message will be displayed:

The Bluetooth device is incorrect

Issue with Pie Chart Widget

When the data is below 5% of the threshold, the data is hidden in the **Pie Chart** Widget on the dashboard.

Deprecated Options

The following options are deprecated in this release and will not be available in the upcoming 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. 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

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.

