

# OpenText Advanced Authentication 25.1.0.3 (v6.5.0.3)

June 2025

OpenText Advanced Authentication 25.1.0.3 (v6.5.0.3) 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 [OpenText 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 [OpenText 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 [OpenText 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 OpenText Advanced Authentication, with server version 25.1.0.3 (v6.5.0.3). 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, intended only for internal processing between OpenText Advanced Authentication components. Administrators can edit it, but it has no configurable settings and does not affect user functionality.
- 

## Security Improvement

OpenText Advanced Authentication has been enhanced to prevent the exposure of excessive data in the Web Authentication HTTP Post request.

# Resolved Issues

| Component                             | Description of the Issue                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enrollment Portal and Helpdesk portal | <p>While logging into the enrollment portal, the user account is locked out after 10 consecutive failed attempts. However, once the user is locked, the OpenText Advanced Authentication allows one additional login attempt during the lockout period, with the following behavior:</p> <ul style="list-style-type: none"><li>♦ If the 11th attempt is successful, the user is unlocked automatically.</li><li>♦ If the 11th attempt fails, the user remains locked until manually unlocked.</li></ul> <p><b>NOTE:</b> This behavior occurs regardless of whether the Lockout Options policy is enabled or disabled.</p> <p>Additionally, Helpdesk users are unable to unlock accounts locked by this mechanism.</p> <p>Now, OpenText Advanced Authentication has temporarily disabled the <a href="https://www.netiq.com/documentation/advanced-authentication-65/advanced-authentication-releasenotes-6.5/data/advanced-authentication-releasenotes-6.5.html#t4ro5eofmf72">Ability to Lockout the Login Method After Multiple Authentication Failures (https://www.netiq.com/documentation/advanced-authentication-65/advanced-authentication-releasenotes-6.5/data/advanced-authentication-releasenotes-6.5.html#t4ro5eofmf72)</a> feature.</p> |

## Upgrading OpenText Advanced Authentication

You can directly upgrade from OpenText Advanced Authentication 25.1 (v6.5) and 25.1.0.2 (v6.5.0.2). However, you cannot upgrade directly from version 6.4 Service Pack 3 Patch 3 or earlier to version 25.1.0.3 (v6.5.0.3).

The recommended upgrade order from version 6.4 Service Pack 3 Patch 3 or earlier to version 25.1.0.3 (v6.5.0.3) is as follows:

- 1 Perform Online Update to apply all updates.

---

**NOTE:** Once all updates are installed, the **Product Upgrade** option becomes available in the Appliance Configuration console.

---

- 2 Perform Product Upgrade to OpenText Advanced Authentication 25.1.0.3 (v6.5.0.3). During the Product Upgrade process, the Appliance Configuration console prompts to register the appliance before proceeding.

---

**NOTE:** The following is the recommended upgrade sequence:

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

Any deviation in the upgrade sequence is not supported.

---

---

**NOTE:** The RAM requirement for OpenText Advanced Authentication 25.1.0.3 (v6.5.0.3) is 12 GB per server. For more information, see [Advanced Authentication system requirements](#).

---

## Known Issues

OpenText Advanced Authentication 25.1.0.3 (v6.5.0.3) 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 OpenText 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 OpenText 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.