

# Advanced Authentication 6.3 Service Pack 6 Release Notes

December 2021

Advanced Authentication 6.3 Service Pack 6 includes new features, 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](#) on NetIQ 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](#) 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](#) page.

## What's New?

Advanced Authentication 6.3 Service Pack 6 provides the following enhancements in this release:

Enhancement	Description
<b>Prompt to Change Expired Password</b>	<p>From this release, the Advanced Authentication Password method prompts the users to change their password when it expires. This feature is supported in Advanced Authentication portals, web integrations, and Clients.</p> <p>Also, Helpdesk Administrators can enable the <b>Password Must Be Changed</b> option. When this option is enabled, the user is prompted to change the password in the subsequent login.</p>

Enhancement	Description
<b>Allows to Change the Look and Feel of All the Advanced Authentication Portals</b>	<p>From this release, the administrator can change the look and feel of Helpdesk, Report, Tokens, and Search card portals along with the new Enrollment Portal and Administration Portal by configuring the <b>Custom Branding</b> policy.</p> <p>For more information, see <a href="#">Custom Branding</a> in the <i>Advanced Authentication - Administration</i> guide.</p>
<b>Improvements to the OTP Methods</b>	<p>This release introduces the following enhancements to the Email OTP, SMS OTP, and Voice OTP methods:</p> <ul style="list-style-type: none"> <li>◆ The maximum lifespan of an OTP token (OTP Period) now can be increased up to 86400 seconds (1 day).</li> <li>◆ The <b>Allow re-sending after (seconds)</b> option is introduced to configure the delay before the next OTP can be sent for authentication.</li> <li>◆ With OTP, the associated sequence number is sent. The sequence number is displayed in the OTP message. This number helps users identify the order of the received OTP and prevents them from specifying a wrong OTP.</li> </ul> <p>For more information, see <a href="#">Email OTP</a>, <a href="#">SMS OTP</a>, and <a href="#">Voice OTP</a> in the <i>Advanced Authentication - Administration</i> guide.</p> <ul style="list-style-type: none"> <li>◆ The administrator does not require re-entering sensitive data from this release while updating <b>Mail Sender</b>, <b>SMS Sender</b>, and <b>Voice Sender</b> policies. The administrator can keep the fields empty while modifying the previously configured policies, and sensitive data remains same.</li> </ul> <p>For more information, see <a href="#">Mail Sender</a>, <a href="#">Voice Sender</a>, and <a href="#">SMS Sender</a> in the <i>Advanced Authentication - Administration</i> guide.</p>
<b>Support for macOS Monterey</b>	<p>This release supports Mac OS Client, Device Service, and Desktop OTP Tool on macOS Monterey.</p> <p>For more information, see <a href="#">Advanced Authentication System Requirements</a>.</p>
<b>Improved User Experience with SMS OTP</b>	<p>Advanced Authentication enhances the user experience of the SMS OTP method. Now, users can tap the OTP displayed above the onscreen keyboard to copy it to the input field. On iOS, the OTP is automatically copied to the clipboard. On Android 11 and 12, the user must tap COPY &lt;OTP&gt; in the notification and tap the OTP displayed above the onscreen keyboard to copy it to the input field.</p>

Enhancement	Description
Provision to Hide the Help Icon	<p>A new policy, <b>Help Options</b>, is introduced. This policy enables you to perform the following tasks:</p> <ul style="list-style-type: none"> <li>◆ Hide the Help icon on portals, such as Administration, Self Enrollment, Helpdesk, Reporting, and Search Card.</li> <li>◆ Modify the URL of the documentation linked to the help icon.</li> </ul> <p>For more information, see <a href="#">Help Options</a> in the <i>Advanced Authentication - Administration</i> guide.</p>
Provision to Customize the Configuration of All the Database Servers	<p>A new policy, <b>Database Options</b>, is introduced to customize the configuration of all the database servers in the cluster. In this policy, the administrator can modify the parameters, such as maximum connections, cache limit, shared buffers size, WAL (Write Ahead Logging) disk use, number of workers for parallel queries and so on.</p> <p>For more information, see <a href="#">Database Options</a> in the <i>Advanced Authentication - Administration</i> guide.</p>
Support Mail Sender When SMTP Does Not Require Authorization	<p>You can configure the <b>Mail Sender</b> policy if the mail server does not require authorization.</p> <p>For more information, see <a href="#">Mail Sender</a> in the in the <i>Advanced Authentication - Administration</i> guide.</p>
Support FIDO 2.0 in Windows Logon Event	<p>Now, users can authenticate to the Windows workstation using <b>FIDO 2.0</b> method.</p> <p>For more information, see <a href="#">FIDO 2.0</a> in the <i>Advanced Authentication- User</i> guide.</p> <p>This release also supports offline login to the Windows Client by using the <b>FIDO 2.0</b> method.</p> <p>For more information, see <a href="#">Offline Support for Windows Client</a> in the <i>Advanced Authentication - Windows Client</i> guide.</p>
Provision to Add a Priority Vendor for Smartphone Method	<p>In addition to the NetIQ Advanced Authentication smartphone application, you can now add other smartphone authentication applications developed using MobileSDK by customers.</p> <p>Customers can switch from the NetIQ Advanced Authentication smartphone application to their smartphone application gradually. Earlier, using multiple applications at a time was possible with the significant restriction. The push notifications could be sent to only one vendor.</p> <p>For more information, see <a href="#">Smartphone</a> in the <i>Advanced Authentication - Administration</i> guide.</p>

Enhancement	Description
<b>A Refresh Button to View the Incoming Authentication Request in the Out-of-band Portal</b>	This release introduces a Refresh button in the Advanced Authentication Out-of-band portal. If the push notification does not appear automatically, the user can click the <b>Refresh</b> button to view the incoming authentication requests.
<b>Improved Login Performance for Helpdesk Portal and RADIUS Event</b>	In this release, the Advanced authentication improves the login performance of the RADIUS event and Helpdesk Portal for the user who is a member of dozens of nested groups. Previously, this could cause a significant delay.

## Resolved Issues

This release includes the following software fixes:

Component	Description
Administration Portal	In the <b>Local Repository</b> , the <b>Locked</b> column shows <b>X</b> for all the non-locked accounts. In this release, the <b>Locked</b> column is blank unless the account is locked.
Administration Portal	In eDirectory, when multiple values are entered for the CN attribute, the subsequent full synchronization fails.
Administration Portal	Using the SAML SP method in the appliance version is not possible. Now, some restrictions are unveiled and documented.  For more information, see <a href="#">SAML Service Provider</a> in the <i>Advanced Authentication - Administration</i> guide.
Administration Portal	The <b>Return groups on logon</b> option has been discarded from this release for the <b>OAuth 2.0/ OpenID Connect</b> event. Previously, this option was not supported.
Administration Portal	When a user selects <b>Activity Stream</b> and sets <b>Relative Time Interval</b> to <b>OFF</b> in <b>Reports</b> , the reports are not displayed.
Desktop OTP Tool	When Auto-appearance is enabled in the macOS workstation, the font in the Desktop OTP tool becomes illegible at night.
Device Service	After upgrading to Advanced Authentication Device Service 6.3.4.1, there is a significant delay when the Windows Hello chain is selected.
Device Service	Enrolling the PKI method at the terminal server is not possible, and the PKI reader gets redirected with the Citrix USB redirection functionality. The logs contain the following error:  PKCS exception, 0x00000005.
Mac OS Client	After setting the parameter <code>forceCachedLogon</code> to <code>true</code> , when a user tries to authenticate to a macOS workstation using the public or private hotspot, the authentication fails.

Component	Description
Mac OS Client	<p>When a user tries to authenticate using the Touch ID method in M1 Macbook, the authentication fails. The following is presented in the logs:</p> <pre data-bbox="683 327 1409 415">The connection on mach service named com.netiq.touchid.deviceservice from pid 727 was invalidated</pre>
Mac OS Client	<p>When a user tries to authenticate with enrolled Touch ID on another macOS workstation, the Unknown Error message is displayed instead of the following message:</p> <pre data-bbox="683 558 1349 646">TouchID is machine-specific, and the current enrollment does not match and may be from a different computer</pre>
New Enrollment Portal	<p>When a user attempts to log in to a New Enrollment Portal, an unbranded splash screen is displayed before directing the user to the login page.</p>
RADIUS Event	<p>Previously Advanced Authentication did not support &amp; character in the LDAP password for RADIUS events if the ampersand is used as a delimiter between the password and OTP. Now users whose passwords contain the ampersand can authenticate in RADIUS.</p>
Smartphone	<p>When a user tries to access the enrollment link in an iOS smartphone where the NetIQ Advanced Authentication application is not installed, the following error message is displayed:</p> <pre data-bbox="683 1062 1438 1115">Safari cannot open the page because the address is invalid.</pre>
Web Authentication	<p>After upgrading to 6.3.5.2, the SAML authentication fails if the <b>Public External URL</b> and <b>Identity provider URL</b> in the <b>Web Authentication</b> policy is different.</p>
Windows Clients	<p>When a user tries to change the password, the credential provider is not displayed after pressing Ctrl+Alt+Del and selecting <b>Change the password</b>. The user can see only the <b>Cancel</b> button.</p>
Windows Client	<p>After setting a time in skipAlreadyTriedPeriod, when a user tries to authenticate, the methods are not listed if the Advanced Authentication server is offline.</p>
Windows Client	<p>When a user tries to authenticate to a Windows workstation in the offline mode using a chain that includes the HOTP method, authentication fails after specifying HOTP, and the following error message is displayed:</p> <pre data-bbox="683 1640 1000 1665">Internal server Error</pre>

# Upgrading

You can directly upgrade to Advanced Authentication 6.3.6 from 6.3.x.

For more information about upgrading from Advanced Authentication 6.2, see “[Upgrading Advanced Authentication](#)” in the *Advanced Authentication- Server Installation and Upgrade* guide.

---

**NOTE:** If you complete the server registration before updating to Advanced Authentication 6.3 SP4, the server update to 6.3 SP4 might not be displayed. Therefore, it is required to de-register and register again to resolve this issue.

---

---

**NOTE:** The upgrade to Advanced Authentication 6.3.6 overwrites the previously customized text in **Body** of the SMS OTP, Email OTP and Voice OTP methods with the new default text. The default text includes the sequence number variable.

---

---

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

- 1 Advanced Authentication servers.
- 2 Plug-ins
- 3 Client components

Any change in the upgrade sequence is not supported.

---

## Known Issues

Advanced Authentication 6.3 Service Pack 6 includes the following known issue:

- ♦ [Web Authentication Fails Due to Using Non-Hexadecimal Color Values in the Background Color](#)
- ♦ [The SAML 2.0 and OAuth Events Do Not Display A Message When Users Attempt Logon With the Expired Password](#)
- ♦ [The Unknown Error Message is Displayed While Login With Touch ID](#)
- ♦ [Issue with OAuth Events After the Upgrade](#)
- ♦ [The Scheduled Backup to the Remote FTP Server Fails After the Upgrade](#)

### Web Authentication Fails Due to Using Non-Hexadecimal Color Values in the Background Color

The Web Authentication event fails if you use one of the following values in the background color and enable the New Enrollment portal:

- ♦ RGB values (xx, xx, xx)
- ♦ HTML color values (red, blue, black and so on)

This issue occurs because the Web Authentication event does not recognize the decimal codes of colors.

## The SAML 2.0 and OAuth Events Do Not Display A Message When Users Attempt Logon With the Expired Password

With the **Logon with expired password** set to deny for the SAML and OAuth events, if users attempt to log on with an expired password, a message instructing them to update the password is not displayed.

## The Unknown Error Message is Displayed While Login With Touch ID

In macOS Big Sur, when a user tries to authenticate using Touch ID method, an `Unknown error` message is displayed if the workstation is in non-domain mode. The issue has been fixed in macOS Monterey.

## Issue with OAuth Events After the Upgrade

**Issue:** After upgrading to Advanced Authentication 6.3 SP6, users are unable to authenticate to OAuth events. This is due to the missing trailing slash (/) in the Public External URL.

**Workaround:** Perform the following steps:

- 1 Log in to the Advanced Authentication Administration portal with the administrator credentials.
- 2 Navigate to **Policies > Public external URLs**
- 3 Add a trailing slash to the <default> URL  
For example, if the default Public external URL is `https://lb.cloudfarm.cf`, add a slash (/) to it. URL after adding the trailing slash: `https://lb.cloudfarm.cf/`.
- 4 Save the policy.

## The Scheduled Backup to the Remote FTP Server Fails After the Upgrade

**Issue:** After upgrading to Advanced Authentication 6.3 SP6, files are not backed up to the configured FTP server and the following error is displayed in the logs:

```
mirror: Login failed: 530 Login incorrect
```

**Workaround:** To reconfigure the backing up to the remote FTP server, perform the following steps:

- 1 Log in to the Advanced Authentication Administration portal with the administrator credentials.
- 2 Navigate to **Backup/Restore > Schedule Backup**.
- 3 Set the cron expression for the scheduled synchronization in the first column.
- 4 Select **Upload to FTP server** from the drop down.
- 5 Specify the required details.
- 6 Save the configuration.

## Upcoming Changes

Advanced Authentication 6.4 will introduce the following changes:

- ♦ The PPC64 version of Linux PAM Client will not be supported.

- ◆ The options, **Push salt TTL** and **Authentication salt TTL** will be removed from the **Smartphone** method settings.
- ◆ The user credentials prompt for HTTPS proxy will be removed during login and the credentials will be made available in the `config` file.

## Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email [Documentation-Feedback@netiq.com](mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the [Support Contact Information website](#).

For general corporate and product information, see the [NetIQ Corporate website](#).

For interactive conversations with your peers and NetIQ experts, become an active member of our [community](#). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

## Legal Notice

© Copyright 2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.