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).

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
Prompt to Change Expired Password	This release introduces the **Logon with Expired Password** option in each event to facilitate administrators to display a prompt to users to change LDAP Password and Password when it expires. This feature is supported in Advanced Authentication portals, web integrations, and Clients. **NOTE:** Advanced Authentication supports change in the LDAP Password if LDAP servers are added with a valid SSL certificate. For the LDAP servers configured with port 389, the LDAP Password change is not allowed and the LDAP server rejects the new password. Also, Helpdesk Administrators can enable the **Password Must Be Changed** option. When this option is enabled, the user is prompted to change the password in the subsequent login.
Allows to Change the Look and Feel of All the Advanced Authentication Portals	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 **Custom Branding** policy. For more information, see Custom Branding in the *Advanced Authentication - Administration* guide.
Improvements to the OTP Methods	This release introduces the following enhancements to the Email OTP, SMS OTP, and Voice OTP methods: ◆ The maximum lifespan of an OTP token (OTP Period) now can be increased up to 86400 seconds (1 day). ◆ The **Allow re-sending after (seconds)** option is introduced to configure the delay before the next OTP can be sent for authentication. ◆ 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. For more information, see Email OTP, SMS OTP, and Voice OTP in the *Advanced Authentication - Administration* guide. ◆ The administrator does not require re-entering sensitive data from this release while updating **Mail Sender**, **SMS Sender**, and **Voice Sender** policies. The administrator can keep the fields empty while modifying the previously configured policies, and sensitive data remains same. For more information, see Mail Sender, Voice Sender, and SMS Sender in the *Advanced Authentication - Administration* guide.

Enhancement	Description
Support for macOS Monterey	This release supports Mac OS Client, Device Service, and Desktop OTP Tool on macOS Monterey. For more information, see Advanced Authentication System Requirements.
Improved User Experience with SMS OTP	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 <OTP> in the notification and tap the OTP displayed above the onscreen keyboard to copy it to the input field.
Provision to Hide the Help Icon	A new policy, **Help Options**, is introduced. This policy enables you to perform the following tasks: ◆ Hide the Help icon on portals, such as Administration, Self Enrollment, Helpdesk, Reporting, and Search Card. ◆ Modify the URL of the documentation linked to the help icon. For more information, see Help Options in the *Advanced Authentication - Administration* guide.
Provision to Customize the Configuration of All the Database Servers	A new policy, **Database Options**, 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. For more information, see Database Options in the *Advanced Authentication - Administration* guide.
Support Mail Sender When SMTP Does Not Require Authorization	You can configure the **Mail Sender** policy if the mail server does not require authorization. For more information, see Mail Sender in the in the *Advanced Authentication - Administration* guide.
Support FIDO 2.0 in Windows Logon Event	Now, users can authenticate to the Windows workstation using **FIDO 2.0** method. For more information, see FIDO 2.0 in the *Advanced Authentication- User* guide. This release also supports offline login to the Windows Client by using the **FIDO 2.0** method. For more information, see Offline Support for Windows Client in the *Advanced Authentication - Windows Client* guide.

Enhancement	Description
Provision to Add a Priority Vendor for Smartphone Method	In addition to the NetIQ Advanced Authentication smartphone application, you can now add other smartphone authentication applications developed using MobileSDK by customers. 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. For more information, see Smartphone in the *Advanced Authentication - Administration* guide.
A Refresh Button to View the Incoming Authentication Request in the Out-of-band Portal	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 **Refresh** button to view the incoming authentication requests.
Improved Login Performance for Helpdesk Portal and RADIUS Event	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 **Local Repository**, the **Locked** column shows **X** for all the non-locked accounts. In this release, the **Locked** 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 SAML Service Provider in the *Advanced Authentication - Administration* guide.
Administration Portal	The **Return groups on logon option** has been discarded from this release for the **OAuth 2.0/ OpenID Connect** event. Previously, this option was not supported.
Administration Portal	When a user selects **Activity Stream** and sets **Relative Time Interval** to **OFF** in **Reports**, 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.

Component	Description
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 `forceCachedLogon` to `true`, when a user tries to authenticate to a macOS workstation using the public or private hotspot, the authentication fails.
Mac OS Client	When a user tries to authenticate using the Touch ID method in M1 Macbook, the authentication fails. The following is presented in the logs: `The connection on mach service named com.netiq.touchid.deviceservice from pid 727 was invalidated`
Mac OS Client	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: `TouchID is machine-specific, and the current enrollment does not match and may be from a different computer`
New Enrollment Portal	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.
RADIUS Event	Previously Advanced Authentication did not support & 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.
Smartphone	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: `Safari cannot open the page because the address is invalid.`
Web Authentication	After upgrading to 6.3.5.2, the SAML authentication fails if the **Public External URL** and **Identity provider URL** in the **Web Authentication** policy is different.
Windows Clients	When a user tries to change the password, the credential provider is not displayed after pressing Ctrl+Alt+Del and selecting **Change the password**. The user can see only the **Cancel** button.
Windows Client	After setting a time in `skipAlreadyTriedPeriod`, when a user tries to authenticate, the methods are not listed if the Advanced Authentication server is offline.

Component	Description
Windows Client	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: `Internal server Error`

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 Pubic 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 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. 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