Advanced Authentication 6.3 Service Pack 3 Release Notes

October 2020

Advanced Authentication 6.3 Service Pack 3 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 the ideas of enhancement requests in the Ideas forum (https://ideas.microfocus.com/MFI/advance-authentication).

For more information about this release and for the latest release notes, see the Documentation Advanced Authentication NetIQ Documentation page. To download this product, see the Advanced Authentication Product website.

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 NetIQ Documentation page.

What's New?

Advanced Authentication 6.3 Service Pack 3 provides the following new features, enhancements, and fixes in this release:

New Features

This section provides details of features by category:

Advanced Authentication Server

This release introduces the following feature:

NPS Plug-in for Microsoft Network Policy Server

In this release, Advanced Authentication introduces a new feature to configure multi-factor authentication for RADIUS clients in Microsoft operating system. The NPS Plug-in can be installed and configured to work with Microsoft NPS and brings the multifactor authentication for RADIUS Client configured on the Network Policy Server.

For more information, see Advanced Authentication - NPS Plug-in Guide.

Advanced Authentication Client

This release introduces the following features:

Support Assisted Logon for Windows Client

In this release, Advanced Authentication introduces a new feature called Support Assisted Logon. The Support Assisted Logon feature is for users who do not use the multi-factor authentication and forgot the password. Using Support Assisted Logon, the Helpdesk Administrator can access the Windows workstation with the Helpdesk Administrator’s credentials.

Later, the feature will be improved to bring the Support Assisted Logon for the users who use the multifactor authentication and can't login because they forgot their card or lost authenticators.

For more information, see Support Assisted Logon in the *Advanced Authentication - Windows Client* guide.

Enhancements

This release includes the following enhancements:

Server Enhancements

This release includes the following Server enhancements:

- “Emergency Password Expiration in Minutes” on page 4
- “New Way to Limit the Use of SMS OTP, Email OTP, Voice OTP, and Smartphone Methods” on page 4

Risk Service 2.0

In this release, Advanced Authentication includes Risk Service 2.0. NetIQ Risk Service protects against high-risk authentication and application access requests. It evaluates the level of risk during each access attempt by using contextual information without influencing the end-user experience. This prevents fraudulent access to secured web resources.

For more details, see Risk Service 2.0 (https://www.netiq.com/documentation/risk-service-2.0/admin/data/bookinfo.html).

Supports Federal PKI Certificates

In this release, Advanced Authentication allows the administrator to upload the intermediate certificate in .p7b format for PKI method enrollment.

For more information, see PKI in the *Advanced Authentication - Administration* guide.

Improves the Speed of Repository Full Synchronization

In this release, Advanced Authentication improves the speed of full synchronization with eDirectory repository.

Enhanced Web Authentication Capabilities

In this release, Advanced Authentication enhances the capabilities of Web Authentication. Following are the major capability changes for Web Authentication:

- OAuth 2.0 event supports integration with OpenID connect.
- New advanced settings for OAuth 2.0/OpenID connect. For more information, see Creating an OAuth 2.0/ OpenID Connect Event in the *Advanced Authentication - Administration* guide.
- Added timeout configuration per event. For more information, see Creating an OAuth 2.0/ OpenID Connect Event in the *Advanced Authentication - Administration* guide.
- Additional timeout options in Web Authentication policy. For more information, see Web Authentication in the *Advanced Authentication - Administration* guide.
- Ability to reset Client secret for OAuth 2 events. The new capability enables the administrator to reset the client secret when needed. For more information, OAuth Event in the *Advanced Authentication - Administration* guide.
- Introduces a new SAML Service Provider method. For more information, see SAML Service Provider in the *Advanced Authentication - Administration* guide.
- Added text customization capability for OAuth 2.0 and SAML 2.0 events. For more information, see Customizing the Login Page of Web Authentication Events in the *Advanced Authentication - Administration* guide.

Improved Certificate Selection for PKI Method Enrollment

In this release, the **Key** field in the PKI authenticator enrollment portal populates only the certificates with the authentication key and its expiry date.

It is possible to click the button **Show All** to show all the certificates.

For more information, see PKI in the *Advanced Authentication- User*.

Emergency Password Expiration in Minutes

In this release, Advanced Authentication allows the Help Desk Administrator to set the Emergency password expiration time in minutes. The time is specified based on the local time of the browser.

For more information, see Emergency Password in the *Advanced Authentication - Administration* guide.

New Way to Limit the Use of SMS OTP, Email OTP, Voice OTP, and Smartphone Methods

In this release, Advanced Authentication introduces a new option called **Allow as a first authentication method** to limit the amount of SMS OTP, Email OTP, Smartphone, and Voice OTP authentications. The new option prevents the user from authenticating using a chain where SMS, Email, Smartphone, and Voice OTP authenticator is the first authentication method.

For more information, see SMS OTP, Email OTP, Smartphone, Voice OTP in the *Advanced Authentication - Administration* guide.

New Enrollment Portal Enhancements

This release includes the following New Enrollment Portal enhancements:

- "Supports Flex OTP" on page 4
- "Removed Version Information" on page 4
- "Supports Multiple Enrollment" on page 4
- "Supports Legal Notice Localization" on page 4

Supports Flex OTP

In this release, the New Enrollment portal supports Flex OTP.

For more information see Flex OTP in the *Advanced Authentication- User*.

Removed Version Information

In this release, Advanced Authentication stops displaying version number and the product name in the New Enrollment portal.

Supports Multiple Enrollment

In this release, Advanced Authentication supports multiple enrollments of the same authenticator in the New Enrollment portal.

Supports Legal Notice Localization

In this release, Advanced Authentication displays the legal notice in the browser language.

Security Enhancements

This release includes the following security enhancements:

- "Third Party Components are Updated" on page 5
- "Does Not Support Weak Cipher" on page 5
- "Stop Supporting Insecure Cookie" on page 5

Third Party Components are Updated

In this release, Advanced Authentication upgrades the third-party components to address vulnerabilities reported against them. Since those vulnerabilities were non-impacting on the product, the upgrade is being done for forward continuity.

Does Not Support Weak Cipher

In this release, Advanced Authentication stops supporting weak ciphers `diffie-hellman-group14-sha1`.

Stop Supporting Insecure Cookie

In this release, use of cookies with SameSite set to None (`sameSite=none`) is no longer supported. For more information, see Deprecations and removals in Chrome (https://developers.google.com/web/updates/2020/07/chrome-85-deps-rems#:~:text=Use%20of%20cookies%20with%20SameSite,a%20full%20timeline%20and%20details).

Smartphone Enhancements

This release includes the following Smartphone enhancements:

- "Supports Multi-Factor Authentication to Enroll the Smartphone Method" on page 5
- "Removed Tenant Name from the Default Authentication Request Message" on page 5

Supports Multi-Factor Authentication to Enroll the Smartphone Method

In this release, Advanced Authentication supports multi-factor authentication when the user enrolls the Smartphone authenticator using the enrollment link if a multi-factor chain is added to the Smartphone Enrollment event.

Removed Tenant Name from the Default Authentication Request Message

In this release, Advanced Authentication removes the tenant name from the NetIQ mobile application's authentication request description when the user logs in using the Smartphone method.

Client Enhancements

This release includes the following client enhancements:

- "Live Face Detection" on page 5
- "Support for Background Photo for Windows 10" on page 6
- "Automatically filter the chains that cannot be used" on page 6
- "Support for Facial Recognition Method on Mac OS" on page 6
- "Custom Language Support for Linux Client and Mac OS Client" on page 6

Live Face Detection

Previously, face biometric could be spoofed with a printed picture or picture on a mobile device. In this release, Advanced Authentication uses blink detection to differentiate live face and photos. You can configure Device Service to enable blink detection. After configuring, the user needs to blink to get authenticated. You can configure the number of blinks in service settings.

For more information, see Facial Recognition in the *Advanced Authentication - Device Service* guide.

Support for Background Photo for Windows 10

In this release, Advanced Authentication allows the users to customize the background image of the login page in Windows 10. Perform the following steps to customize the background image:

1. Open **Start > Personalization > Lock screen**.
2. In the **Background** section, select **Picture**.
3. Click **Browse** and select the image to set.

NOTE: Advanced Authentication does not support **Windows Spotlight** or **Slideshow** to set as background.

Automatically filter the chains that cannot be used

In this release, Advanced Authentication automatically hides the methods which cannot be used at the specific moment. Following are the situations when Advanced Authentication hides the chains.

- Bluetooth containing chains will not be shown when Bluetooth is not available or the Device Service is not installed.
- Card, PKI, u2f containing chains will not be shown when the Device Service is not installed.
- Touch ID containing chains will not be shown when Touch ID is locked / not enrolled / unavailable or the Device Service is not installed.
- Windows hello containing chains will not be shown when devices are not available or the Device Service is not installed.
- Face containing chains will not be shown when the Device Service is not installed.

Support for Facial Recognition Method on Mac OS

In this release, Advanced Authentication fixes the issues with the Facial Recognition method in Mac OS. Mac OS users can use Facial Recognition for unlocking the operating system, FUS (fast user switching), authentication for operating system setting change, etc.

The Facial recognition cannot be used for login after boot.

Custom Language Support for Linux Client and Mac OS Client

Advanced Authentication allows administrators to localize error messages, method messages, and prompt messages displayed on endpoints to an unsupported language.

For more information, see Localizing the Messages for Clients in the *Advanced Authentication- Linux PAM Client* or Localizing the Messages for Clients in the *Advanced Authentication - Mac OS X Client*.

Software Fixes

This release includes the following software fixes:

Advanced Authentication Server Fixes

This release includes the following Server fixes:

Advanced Authentication Server Does Not Check All LDAP Servers During Binding

When the administrator tries to add some LDAP Servers in the repository configuration, Advanced Authentication does not check whether the added LDAP servers are valid and reachable or not.

Able to Add the RADIUS Client Duplicates

Since Advanced Authentication 6.3 Service Pack 1, it was possible to add the same RADIUS Clients many times. Due to that issue, the RADIUS configuration file lost RADIUS secrets. It caused the authentication issues after upgrading to Advanced Authentication 6.3. Service Pack 2. Those duplicate RADIUS Clients need to be removed manually. After this release, it is not possible to add the duplicate RADIUS Client entries.

RADIUS Logs Display Passwords in Clear Text

When the user uses some special characters in the password, the RADIUS logs display the passwords in clear text in Debug mode. After this release, passwords that contain all the possible characters are masked.

Not Able to Enter Smartphone OTP in Portals

When the user tries to authenticate using the Smartphone method, the login screen keeps refreshing, and the user cannot enter the OTP to authenticate.

Administration Portal Does Not Show Any Contents

After updating to Advanced Authentication 6.3 Service Pack 2, the administrator is not able to see the web portals of Advanced Authentication when **Kerberos SSO** is enabled.

Administrator is Unable to Update

When the administrator uses an activation key to get access to the Advanced Authentication update channel, it fails and the following error message is displayed.

```
Query installed language failed. (134) No matching items found.
```

Able to Re-enroll with the Current Password

When the user tries to enroll the **Password Only** authenticator with the current password, it gets enrolled. After this release, the enrollment checks the password for uniqueness.

Phone Numbers and Email Addresses are Not Displayed in the Customized Web Authentication Dialogs

When the administrator enables **Use Custom Messages** in the Web Authentication policy, the message is displayed without phone numbers or Email address. It's not possible to customize the messages to have the phone numbers and email addresses shown in the Web Authentication dialogs.

Advanced Authentication no longer has the Recipient mask policy. Advanced Authentication 6.3 Service Pack 3 and newer versions always mask the phone numbers or Email address and the text containing the masked value is shown on the Clients, portals and Web Authentication.

The Resend Button is Displayed while Using the TOTP Method

When users perform authenticating Web Authentication with the TOTP method, **Resend** option is displayed.

Delay in Start-up

When an administrator tries to boot up or restart the Advanced Authentication server, there is a delay and a `Appliance is under maintenance / starting up` message is displayed in the browsers. Also, the client devices display server error messages to the users during OS logins.

Custom Messages Do Not Update as Per Locale

In Custom messages policy, the inputs for each locale's custom messages are displayed right-to-left despite the locale that is selected for.

Labels in Web Portal Login Page Do Not Update the Language

English is not set as the default language on the browser. However, the labels on the login page are displayed in English. The labels are updated to the default language only when the user starts typing the user information.

Client Fixes

Advanced Authentication 6.3 Service Pack 3 includes the following client fixes:

User from a Huge Repository is Not Able to Authenticate

If a user is a member of a repository of a hundred thousands of users and the **Enable nested groups support** option is enabled for the repository and tries to authenticate, a `Please wait message` is displayed. After some time, a `Server not found` message is displayed even if the server is reachable.

Solution : The fix is only for Active Directory repositories. If a user experiences the issue with the eDirectory repository, disable **Enabled nested groups support** option in repository's **Advanced Settings**.

Linked Chain Does Not Selected Automatically

When the settings are configured to automatically select the last used chain and the linked chains are used, every time the user has to select the linked chain manually once the grace period expires. However, for the required chain, it works as expected.

Bluetooth Method Does Not Work in Linux Platform

When a user tries to enroll or test the Bluetooth authenticator, Bluetooth device driver fails to detect the Bluetooth devices present around and a `not found SHA 256 error code 0` message is displayed in the logs.

Mac OS Client

This release includes the following Mac OS Client fixes:

Caching Does Not Work Properly

In domain mode, some of the used methods are not cached in Mac OS X Client. Hence, in offline mode, all the chains are not displayed. After this release, the used methods cached properly.

The Login Window Displays the Chains Selected by the Previous User

When the user tries to log in, instead of the actual list of enrolled chains, the login window displays the chains which were available for the previous user.

User Not Able to Unlock OS

When a user tries to unlock OS in offline mode, sometimes a `Chains not found` message is displayed when the user is already logged on before.

Input Field is Not In Correct Location

When the user tries to unlock an existing session, the input field is not correctly placed until the user clicks the input field.

Windows Client

Advanced Authentication 6.3 Service Pack 3 includes the following Windows Client fixes:

Configured Logon Filter Does Not Work with the User with Windows 10 v2004 Log in

After Windows 10 2004 update, the Windows Client does not correctly apply the Multi-Factor Authentication logon tag group.

Operating System Getting Locked When Remote Desktop is Used

When the user is in a Remote Desktop session, and inserts a U2F token or taps a card, the system locks automatically.

Corrupting the Configuration File

When a user's laptop run out of battery or the user switched it off, the `config.properties` file gets corrupted.

RDP Login Window Stays Open When User Decides to Cancel the Login

When the user tries to cancel a Remote Desktop Protocol (RDP) login, Windows Client window is closed but the RDP screen appears to stay open with a new login screen and it allows the user to enter their username.

The Arrow Down Button Does Not Work

When the user needs to select the chains while accessing the Windows tablet, the arrow down button does not work. This issue happens only on the devices with a touch screen.

Windows Hello Does Not Accept Alphanumeric Characters in PIN

When the user sets the Windows Hello Pin using alphanumeric characters and tries to authenticate, the authentication fails and a `The PIN is incorrect` message is displayed.

Windows Hello Requests the PIN Twice

When the user tries to unlock a Windows workstation, it requests the user to specify the Windows Hello PIN twice to authenticate.

Second User is Unable to Login

A second user is not able to login to Windows as the Windows Hello PIN is prompted for the last logged on user.

Windows Hello PIN is Prompted for Non-Enrolled Users

Windows Hello PIN is prompted to all the users irrespective of whether the users have enrolled the authenticators or not.

VDA

Advanced Authentication 6.3 Service Pack 3 includes the following VDA fix:

Nested Group Does not Work

In kiosk mode settings, when the configured user group is assigned to another user group as its member, the functionality does not work as expected and the user is not able to quit from the VDA shell.

Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

Advanced Authentication 6.3 Service Pack 2 includes the following known issue:

Full Synchronization Failed for Active Directory Repository

A full synchronization of the Active Directory repository may be failed to unknown reason. In the logs, administrators may see the following error:

```
socket sending error [Errno 104] Connection reset by peer.
```

Probably, this is a defect in the updated third-party module.

Delay in Updating the Authenticator

When administrator updated email address or phone number for a user in eDirectory, there is a 5 minutes delay in updating the information in the user's authenticator.

Upgrading

You can update Advanced Authentication 6.3.0, 6.3.1, 6.3.2 to 6.3.3.

The Repo Agent will be discontinued in Advanced Authentication 6.4. It is replaced in Advanced Authentication as a Service (SaaS) by the Cloud Bridge integration.

For more information about upgrading from 6.2, see "Upgrading Advanced Authentication" in the *Advanced Authentication- Server Installation and Upgrade* guide.

NOTE: The recommended upgrade sequence is the upgrade of Advanced Authentication servers, followed by plug-ins and Client components. Any change in the upgrade sequence is not supported.

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

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see http://www.microfocus.com/about/legal/.