Advanced Authentication 6.3 Service Pack 7 Release Notes

April 2022

Advanced Authentication 6.3 Service Pack 7 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 7 includes the following enhancements:

Enhancement	Description
An Option to Validate the OTP Methods Manually	This release introduces the following options in the respective OTP methods: ◆ **Verify email address**: This option is introduced in the Email OTP method and helps to send the verification code to a specified email address. This option allows the users to validate the email address during the manual enrollment. For more information, see Email OTP in the *Advanced Authentication - Administration* guide. ◆ **Verify phone number**: This option is introduced in the SMS OTP and Voice OTP methods to send the verification code to a specified phone number. This option lets users verify whether the phone number is valid before the manual enrollment. For more information, see SMS OTP and Voice OTP in the *Advanced Authentication - Administration* guide.
Support for HANIS Face Method	Advanced Authentication provides the Home Affairs National Identification System (HANIS) method that facilitates citizens of South Africa to authenticate using their face that has been enrolled in the National Identification System. During authentication, the Advanced Authentication server forwards the user details to the third-party service provider that is integrated with National Identification System where the validation takes place. The user gets authenticated to the required resource or endpoint based on the validation result. For more information, see HANIS Face in the *Advanced Authentication - Administration* guide.
FIDO2 Supports CCID Cards	In this release, the FIDO2 method supports CCID (chip card interface device) for authentication.
Timeout Options	This release introduces the following options in the **Login Options** policy: ◆ **Logon timeout (seconds)**: This option allows you to set the maximum duration of the logon session. The user must specify the login credentials within this duration to prevent the session termination. ◆ **Logon inactivity timeout (seconds)**: This option allows you to set the maximum inactivity timeout of the logon session, and a user can remain idle within this duration. For more information, see Login Options in the *Advanced Authentication - Administration* guide.

Enhancement	Description
Device Authentication Method Support For Web Authentication Event	Now, users can authenticate to the OAuth 2.0, OIDC, SAML 2.0 events, the New Enrollment Portal and OOB Portal using the Device Authentication method.
Ability to Retrieve the Risk Score	After integrating a product with Advanced Authentication, the administrators can use the following API call to retrieve the Risk Score of an authenticated user after successful authentication: `api/v1/logon/{{logon_process_id}}/do_logon`
Support for Installing Advanced Authentication Using the Docker Image	This release provides the Docker image with Helm charts to install the Advanced Authentication in the Azure Kubernetes air-gapped environment. For more information about installing Advanced Authentication in the air gap environment, see Deploying Advanced Authentication on Azure Kubernetes Services in an Air Gap Environment (https://www.netiq.com/documentation/advanced-authentication-63/install-upgrade-guide/data/dply_aa_on_aks_argp.html) in the *Advanced Authentication- Server Installation and Upgrade*.
Ability to Change the Locale without Changing the Operating System's Locale	This release introduces a new parameter, `locale`, to enable you to change the client locale without changing the operating system's locale. For more information, see the following guides: ◆ Changing the Locale for Windows Client in the *Advanced Authentication - Windows Client*. ◆ Changing the Locale of Linux PAM Client without Changing the Locale of the Operating System in the *Advanced Authentication- Linux PAM Client*. ◆ Changing the Locale of Mac OS Client without Changing the Locale of the Operating System in the *Advanced Authentication - Mac OS X Client*.
New Parameters for PKI Service	This release replaces the parameter, `pki.blockingMode: true` with a new parameter, `pki.detectionMode=vendor`, to detect and monitor the token connected to your system. Also, adds another parameter, `pki.reinitRequired=false`, to configure whether the PKI service reloads the PKCS#11 library after every operation, such as getting certificates, generating key pairs, and so on. For more information, see PKI Settings in the *Advanced Authentication - Device Service*.

Enhancement	Description
TLS Upgrade	In this release, Advanced Authentication switches to TLSv1.3 that the Client uses for establishing a secure connection with the Advanced Authentication server. For more information, see the following guides: - Configuring the TLS Version in the *Advanced Authentication - Mac OS X Client* guide. - Configuring the TLS Version in the *Advanced Authentication- Linux PAM Client* guide. - Configuring the TLS Version in the *Advanced Authentication - Windows Client* guide.
Renamed FIDO 2.0	In this release, the FIDO 2.0 method is renamed to FIDO2.
Support for Windows 21H2	This release adds support for Windows 21H2 for the following components: - Windows Client - Device Service - Desktop OTP Tool - Authentication Agent For more information see, Windows Client, Device Service, Desktop OTP Tool, and Windows Authentication Agent in the *Advanced Authentication System Requirements* guide.

Resolved Issues

This release includes the following software fixes:

Component	Description
Administration Portal	When an administrator tries to add a new SQL repository, the repository creation fails, and the following error message is displayed: `SQL repo connect error: (pymssql.InterfaceError).`
Administration Portal	When a user from an AD user group with administrator rights tries to access the Helpdesk report, the complete report of all the sites is not displayed. Instead, the following error message is displayed: `TypeError: a bytes-like object is required, not 'str.`
Administration Portal	When an administrator tries to change the Cache expiration time in the **Cache Options** policy, the updated expiration time is not saved, and changes are not applied.

Component	Description
All Clients	Pre-condition: ◆ Configure and enroll a chain with two methods. The first method in the chain is **LDAP Password**. ◆ Configure and enroll the **LDAP Password** only chain. The **LDAP Password** only chain is not displayed in the chain list if the client is online. When the client is offline, the chains list displays both the **LDAP Password** + other method and the **LDAP Password** only chains and allows the user to skip the second-factor method by specifying only the **LDAP Password**.
All Events	When a user tries to log in using a password that contains Non-ASCII characters, the authentication fails, and the following message appears: `TypeError: comparing strings with non-ASCII characters is not supported.`
Device Service	After enabling the system detection mode (the new parameter is `pki.detectionMode=system`, while the old one is `pki.blockingMode=false`), when a user reconnects the card, the Device Service fails to detect the card and the following message is displayed: `NO_CARD`.
Enrollment Portal	When a user tries to enroll the FIDO2 method, the enrollment fails, and the following error message is displayed. This happens if the verification signature call is sent twice. `{"status":"error","errors":[{"location":"server","name":"Unknown Error","description":"AttributeError 'NoneType' object has no attribute 'get'"}]}`
Mac OS Client	The Advanced Authentication Mac OS X client allows the users to skip multi-factor authentication and logs in by specifying `.\username`.
New Enrollment Portal	When a user tries to test the FIDO2 method in the New Enrollment portal, the test fails, and the following message is displayed: `expected 'status' to be 'string', got: error.`
Web Authentication	With the **Logon with Expired Password** option set to **Deny** in the Web Authentication event, if a user tries to log in with the expired password, the following message is not displayed: `You must change your password in order to logon.`
Web Authentication	When a user tries to authenticate to a Web Authentication event using the Denmark National ID method, the Denmark National ID portal loads, and an error appears after entering the username.

Component	Description
Web Authentication	When a user tries to authenticate to a Web Authentication event after enabling Google reCAPTCHA, the Google reCAPTCHA fails, and the following messages are displayed one after the other if the connection is via proxy: `Verification expired. Check the checkbox again` a few second later, `504 Gateway Time-out`.
Web Authentication	On the Google Chrome browser, when a user tries to authenticate to the Web authentication event with FIDO U2F token, the following error message is displayed: `The U2F Security Key API is deprecated and will be removed soon. If you have this website, please switch to the web authentication API. For more information, see https://groups.google.com/a/chromium.org/g/blink-dev/c/xHC3AtU_65A/m/yg20tsVFBAAJ`.
Web Authentication	After upgrading from Advanced Authentication 6.3.4.1 to 6.3.6.1, the Internet Explorer does not allow the users to authenticate to any web authentication events by using the Card or Bluetooth method.
Web Authentication	When a user tries to authenticate to the Web Authentication event with the incorrect password, the user is redirected to the default login page without prompting the error message, `Incorrect password`.
Web Authentication	When a user tries to authenticate to the Web Authentication event by using the FIDO2 method, the FIDO2 chain is not displayed if the FIDO2 token is not connected. The authentication fails when a user uses the FIDO2 method to authenticate to a Web Authentication event in the Safari browser.
Web Authentication Method	After upgrading from Advanced Authentication 6.3, when a user tries to authenticate with the Web Authentication method, the following error message is displayed: `Invalid redirect_URI.`

Upgrading

You can directly upgrade to Advanced Authentication 6.3.7 from 6.3.x.

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: Due to Windows limitation of 65535 as the maximum value, we changed the version number of Windows Client to 6.3.61xxx format. Before to this release, we were following the Major.Minor.Patch00BuildNumber format. For example, 6.3.61035. This restriction will be removed from Advanced Authentication 6.4.

The Device Service and the Desktop OTP Tool for Windows Client have undergone similar changes.

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 Issue

Advanced Authentication 6.3 Service Pack 7 includes the following known issues:

- "Issue with the FIDO U2F Method Enrollment on the Google Chrome Browser" on page 7
- "Issue with the FIDO2 Method on the Firefox Browser" on page 7

Issue with the FIDO U2F Method Enrollment on the Google Chrome Browser

Issue: The enrollment fails when a user tries to enroll the FIDO U2F method in the old Enrollment Portal in Google Chrome.

Workaround: To resolve this issue, use the Firefox browser to enroll FIDO U2F in the old Enrollment Portal.

Issue with the FIDO2 Method on the Firefox Browser

When you try to authenticate to any web portal using the FIDO2 method on the Firefox browser, a prompt to specify the PIN is not displayed.

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

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.