# Advanced Authentication 6.3 Service Pack 5 Patch 1 Release Notes

September 2021

Advanced Authentication 6.3 Service Pack 5 Patch 1 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 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, visit 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 5 Patch 1 provides the following enhancements in this release:

| Enhancement | Description |
|---|---|
| **Support NFC Cards for Web Authentication** | Advanced Authentication extends the Card method capabilities to enable users to use Near Field Communication (NFC) cards to authenticate to OAuth 2.0/ OpenID Connect, SAML 2.0 events, and Advanced Authentication portals. |
| **A Setting to Choose the Camera for Facial Recognition Method** | A new parameter, `video.deviceId` is introduced in the Advanced Authentication Device Service. This parameter enables you to configure the camera for the Facial Recognition method enrollment and authentication.<br><br>For more information, see Facial Recognition in the *Advanced Authentication - Device Service* guide. |
| **Support for Customization and Localization of the Chain Message in the Linux PAM Client** | A new key, `client.linux.chain_number` is introduced in the `Custom Localization` file. This key enables the administrator to customize and localize the chain message, `Enter chain number` in the Linux PAM Client.<br><br>For more information, see Custom Messages in the *Advanced Authentication - Administration* guide. |
| **Setting to Use Biometrics Without PIN** | Advanced Authentication extended capabilities of the **Require biometrics** option. Using this option, you can enable biometrics without enabling the PIN request. From the next release, smartphone applications will support this enhancement.<br><br>For more information, see Smartphone in the *Advanced Authentication - Administration* guide. |
| **Enhanced Risk Service** | In this release, Advanced Authentication includes Risk Service 2.0.0.4. In the new update, Risk Service updated the third-party libraries. |

# Security Vulnerability Fixes

This release resolved several security vulnerabilities, and we strongly recommend upgrading.

Micro Focus would like to offer special thanks and appreciation to Frank Spierings of Warpnet B.V. for following responsible disclosure practices and responsibly disclosing this vulnerability to us. (CVE-2021-22509)

# Resolved Issues

This release includes the following software fixes:

| Component | Description |
|---|---|
| Administration Portal | After every successful authentication, Syslog recorded the `User was unlocked` event with the code 611. Now the event is not registered. |

| Component | Description |
|---|---|
| Administration Portal | The following warning message is displayed even though the number of users does not exceed the license limit:<br>`Number of users for the LOCAL exceed the license limit Number of users for the Repo 1 exceed the license limit.`<br>Similarly, the following warning message is displayed even though the number of users in multitenancy does not exceed the license limit:<br>`Number of users for the LOCAL will soon exceed the license limit Number of users for the Repo 1 will soon exceed the license limit.` |
| Administration Portal | Sometimes, users are accidentally removed from the Advanced Authentication database after the full or fast synchronization. |
| Device Service | When a user tries to connect a PKI token to the Ubuntu system, the Device Service does not recognize the PKI token. After restarting the Device Service, the token was recognized. |
| Enrollment Portal | When a user enrolls the U2F Yubikey by using Google Chrome on Mac or Windows workstation, the following error message is displayed when the user touches the Yubikey:<br>`Enroll failed: Device is not attested. Contact your administrator to upload your token attestation certificate.` |
| Enrollment Portal | The PKI method stopped supporting the multi-SingleResp OCSP responses after a third-party library replacement in Advanced Authentication 6.3 Service Pack 5. |
| Linux PAM Client | While activating the domain or non-domain `.sh` file, the user is not prompted to accept the license terms in SLES OS. |
| Mac OS Client | The local users are able to log in to the macOS workstation even after setting the `disable_local_accounts` parameter to `True`. |
| Mac OS Client | In the Mac OS client login page, the focus is not placed in the **Username** field and does not allow the user to type the username until the user moves focus to the username field. |
| Out-of-Band Portal | The OOB push notification stops after the session and does not send the notification again after new login from the same device. |
| Out-of-Band Portal | While receiving the push notification, the following error message is displayed if the installed authentication agent is kept unclosed, but the last session is logged out or expired:<br>`AttributeError 'NoneType' object has no attribute 'event'` |
| RADIUS Events | The users marked for removal for N days specified in the Users Synchronization Options policy cannot perform the RADIUS authentication. However, the users are automatically recovered if they perform any other authentication. |

| Component | Description |
|---|---|
| Web Authentication | When Advanced Authentication 6.3 was installed, but at least OAuth 2.0/OpenID Connect or SAML 2.0 event was not configured before upgrading to Advanced Authentication 6.3 Service Pack 5, the Web Authentication does not work. |
| Web Authentication | Users are not able to log in to Web Authentication events using the OOB method. The message `This page isn't working` with the error code `ERR_TOO_MANY_REDIRECTS` is displayed. |
| Web Authentication | While using Smartphone offline method to authenticate, there is no space between `Waiting for you to accept the authentication request in the Advanced Authentication app..` message and the **OTP** field in the Web Authentication event. |
| Web Authentication | The Web Authentication interface does not scale to the browser window size. |
| Web Authentication | While authenticating using the Smartphone method, users cannot find the **OTP** field to specify the TOTP during offline authentication. |

# Upgrading

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. You can upgrade to Advanced Authentication 6.3 Service Pack 5 Patch 1 from one of the following versions of Advanced Authentication:

- 6.3
- 6.3.1
- 6.3.2
- 6.3.3
- 6.3.4
- 6.3.5

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

**NOTE:** Since Advanced Authentication 6.3 Service Pack 5 Patch 1, the Custom Branding settings of Web Authentication events have been relocated from Web Authentication policy to Custom Branding policy.

For more information, see Customizing the Login Page of Web Authentication Events in the *Advanced Authentication - Administration* guide.

# Planned End of Support in Advanced Authentication 6.4

- 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. 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/.