

Advanced Authentication 6.3 Service Pack 4 Patch 1 Release Notes

April 2021

Advanced Authentication 6.3 Service Pack 4 Patch 1 includes enhancements 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 \(https://ideas.microfocus.com/MFI/advance-authentication\)](https://ideas.microfocus.com/MFI/advance-authentication).

For more information about this release and for the latest release notes, see the Documentation [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 4 Patch 1 includes the following:

- ◆ [Enhancements](#)
- ◆ [Security Improvements](#)
- ◆ [Software Fixes](#)

Enhancements

This release includes the following enhancements:

Enhancement	Description
Settings to Retrieve User Groups after Authentication	<p>The options, Return Group on Logon and Groups are introduced in all events (existing and new events). These options allow an administrator to retrieve the list of groups a user is associated with after successfully authenticating to an event.</p> <p>NOTE: The Return Group on Logon is enabled by default for all the events except the Authenticators Management, Smartphone Enrollment, OAuth 2.0, and SAML 2.0 events.</p> <p>For more information, see Configuring an Existing Event in the <i>Advanced Authentication - Administration</i> guide.</p>
Improved REST API Call to Return the DNS Name	<p>The REST API call <code>/api/v1/repositories</code> has been enhanced to return the DNS name of each repository along with the repository name and repository type.</p>

Security Improvements

Advanced Authentication 6.3 Service Pack 4 Patch 1 resolves a potential Multi-Factor Authentication (MFA) downgrade issue (CVE-2021-22515).

We would like to offer a special thanks to Julkair for responsibly disclosing this issue.

Software Fixes

This release includes the following fixes:

Component	Description
Enrollment Portal	The Delete option for the SMS OTP and Email OTP methods is not available in the old Enrollment portal.
Enrollment Portal	When a user logs in to the old Enrollment portal by performing the basic authentication and tries to enroll the TOTP method, the QR code is not displayed.
Enrollment Portal	<p>When a user connects the Spanish national identity card (Documento Nacional de identidad) and tries to enroll it using the PKI method, the certificate is not displayed in the Key field.</p> <p>However, on click of Show All, certificates are displayed. When the user selects a certificate, the following error message is displayed:</p> <p>Cannot check the revocation status.</p>
RADIUS	The RADIUS server does not return the <code>msRADIUSFramedIPAddress</code> attribute if the hexadecimal value of that attribute contains a negative value.

Component	Description
Web Authentication	<p>When the users from LDAP repositories try to log in to the Enrollment Portal, the following error message is displayed:</p> <pre>WebAuth feature is not running.</pre> <p>This issue happens only for LDAP users who are associated with many groups and many nested groups. The local users can log in without any problem.</p>

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 4 Patch 1 includes the following known issue:

- ◆ [“Windows Client Does Not Respond” on page 3](#)
- ◆ [“Syslog is Flooded with the Health Check Messages” on page 3](#)
- ◆ [“Issue with Risk Service After Upgrade” on page 3](#)

Windows Client Does Not Respond

When a user tries to authenticate to Windows Client, it freezes in the `Please wait` screen after providing the username. This happens only in Windows machines with external Nvidia Quadro graphics cards and their drivers installed.

Syslog is Flooded with the Health Check Messages

There are various messages as follows:

```
dockerd[2167]: time="2020-12-21T23:30:22.663706880Z" level=warning msg="Health
check for container
b1cc02cc52d3fe2681c9fa60abfab62aa54fa40d4d833fca4bb0fef5d0414890 error: context
deadline exceeded" in syslog.
```

These messages do not indicate any issues. This is due to the absence of the Risk Service license.

Workaround: Perform the following steps:

- 1 Log in to the Configuration Portal (:9443).
- 2 Click **System Services** and select the Risk Service then click **Action** and select **Stop**.
- 3 Click **Options** then select **Set as Manual** for Risk Service.

Issue with Risk Service After Upgrade

Issue: The Risk Service does not work after upgrading to Advanced Authentication 6.3 SP4.

Workaround: Run the following commands to remove the old `rba_history` container and reboot the appliance:

- 1 `systemctl stop docker`
- 2 `systemctl start docker`
- 3 `docker container stop risk_rbahistory_1`
- 4 `docker container rm risk_rbahistory_1`
- 5 `docker rmi -f mfsecurity/rba_history:1.0.0.2`
- 6 `reboot`
- 7 Log in to the Administration portal and click **Logs > Clear** to clear the logs.

NOTE: If any command takes too long to respond or hangs, press Ctrl+C to stop and continue with the next step.

Upgrading

You can update Advanced Authentication 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4 to Advanced Authentication 6.3.4 Patch 1.

The updated Client bundle and Helm chart are available in [Software Licenses and Downloads \(https://sld.microfocus.com\)](https://sld.microfocus.com) page.

For more information about upgrading, see [Performing an Online Update](#) in *Advanced Authentication - Administration* guide.

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

NOTE: The default value of remote access parameters has been changed in the Windows Client.

For more information, see [Configuring Single Sign-on Support for Citrix and Remote Desktop](#) and [Enabling Flexible Sign-on for Citrix VDI or Remote Desktop Login](#) in the *Advanced Authentication - Windows Client* guide.

NOTE: If you complete the server registration before updating to Advanced Authentication 6.3 Service Pack 4, the Server update to 6.3.4 might not display. Therefore, it is required to de-register and register again to resolve this issue.

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/>.

© Copyright 2021 NetIQ Corporation, a Micro Focus company. All Rights Reserved.