

Advanced Authentication 6.3 Patch Update 1 Release Notes

January 2020

Advanced Authentication 6.3 Patch Update 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 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 [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 Patch Update 1 provides the following enhancements, and fixes in this release:

- ◆ [“Enhancements” on page 1](#)
- ◆ [“Software Fixes” on page 2](#)

Enhancements


Advanced Authentication 6.3 Patch Update 1 includes the following enhancements:

- ◆ [“Enhanced User Interface” on page 2](#)
- ◆ [“Icons for Authentication Methods on Clients” on page 2](#)

Enhanced User Interface

This patch introduces the following enhancements on the Advanced Authentication Administration portal:

- ◆ **Dashboard Settings are hidden under the Settings icon**

To change the Dashboard settings, click the **Dashboard Settings** icon  on the upper-right corner of the dashboard. Using this option, you can update the dashboard to view the data based on the time interval.

- ◆ **Event Customization tab for the Email OTP method**

The **Event Customization** tab in the Email OTP method displays only the customized events. You can use **Add** button + to customize any default event according to the requirement.

Previously, all (default and customized) events were displayed in the **Event Customization** tab. Due to this, administrators were facing difficulty in identifying customized events.

- ◆ **Pagination links on Authentication Chains and Events screens**

The pagination links have been introduced on **Authentication Chains** and **Events** screens. When several chain or event records are available, each page display 25 records. Pagination optimizes and improves the page loading speed.

Icons for Authentication Methods on Clients

The Advanced Authentication Clients now display a new icon for each authentication method in the chain selection window. The icon is displayed based on the number of methods in the chain as follows:

- ◆ The icon of the method is displayed when a single method is associated to a chain. For example, a chain with only card method displays the Card icon.
- ◆ The NetIQ icon is displayed when multiple methods are associated to a chain.

You can update the default icon of each method in the Chain settings.

Software Fixes

Advanced Authentication 6.3 Patch Update 1 includes the following software fixes:

- ◆ [“Server Fixes” on page 2](#)
- ◆ [“Client Fixes” on page 4](#)

Server Fixes

Advanced Authentication 6.3 Patch Update 1 includes the following server fixes:

- ◆ [“Login Performance Issue” on page 3](#)
- ◆ [“Users Are Allowed to Authenticate with the Shared Authenticators of a Deleted User” on page 3](#)
- ◆ [“Database Backup Displays an Error Message” on page 3](#)
- ◆ [“Database Restoring Fails Due to a RADIUS Event” on page 3](#)
- ◆ [“Issue with the Mirror Cron Job” on page 3](#)
- ◆ [“Mirror Cron Job Execution Displays an Error” on page 3](#)
- ◆ [“The New Endpoint Button Is Not Clickable after Resizing the Browser” on page 3](#)

- ◆ [“Celery Logs Display Incorrect Timezone” on page 3](#)
- ◆ [“Issues with the Repo Agent” on page 4](#)

Login Performance Issue

This patch resolves the issue where reading of user data on LDAP servers initiates an unnecessary group membership search. This issue results in end-users experiencing some delay in the authentication. Now, the group membership search has been disabled for reading the user data.

Users Are Allowed to Authenticate with the Shared Authenticators of a Deleted User

Previously, a user can authenticate to an event with the shared authenticators of a deleted user with the following settings:

- ◆ [Allow to logon to this event by shared template](#) option is set to ON.
- ◆ [User Synchronization Options > Retain the deleted users or groups \(days\)](#) option is set (for example, 30 days) and retention period has not expired.

Now, irrespective of the value set in [Retain the deleted users or groups \(days\)](#), users are not allowed to authenticate to any event with the shared authenticators of a deleted user.

Database Backup Displays an Error Message

This patch resolves the issue when an administrator tries to backup the database, an error message `Cannot start export (AuError)` is displayed. This issue occurs when the administrator initiates the backup process for the first time after upgrading to Advanced Authentication 6.3.

Database Restoring Fails Due to a RADIUS Event

This patch resolves the issue where database restoration fails and an error message `not enough values to unpack` is displayed in Logs. This issue occurs when the role **ALL USERS** is set in the [User group whitelist](#).

Issue with the Mirror Cron Job

This patch resolves the issue when an administrator schedules the export and mirror cron expressions to run at the same time then the working folder gets uploaded to the FTP server directory in place of the `.cpt` file.

Mirror Cron Job Execution Displays an Error

This patch resolves the issue when an administrator tries to execute the mirror cron expression with valid parameters and clicks **Run Now**, the backup files (`.cpt` format) are not copied to the FTP server. Also, an error message is displayed.

The New Endpoint Button Is Not Clickable after Resizing the Browser

This patch resolves the issue where after resizing the browser window, the **New Endpoint** button is not clickable on the [Endpoints](#) page.

Celery Logs Display Incorrect Timezone

This patch resolves the issue where the Celery Logs displays the UTC timezone instead of the local timezone in the [Logs > Background tasks](#) page of the Administration portal.

Issues with the Repo Agent

This patch resolves the following issues related to the Repo Agent:

- ♦ While adding a new external repository, if an administrator specifies the repository name in the upper-case in the **External servers > URL**, the repo agent returns a 404 error.

Now administrators can define repository name using both upper and lower case text.

- ♦ The default URL format defined in **External servers** while adding a new external repository is invalid and displays an error in the Repo agent. The default URL is now updated to `https://repo-agent.net:9443/aurepa/repository_name`.

Client Fixes

Advanced Authentication 6.3 Patch Update 1 includes the following server fixes:

- ♦ [“Offline Login to Remote Desktop fails” on page 4](#)
- ♦ [“The Client Fails to Display a Message When the Advanced Authentication Server Is Unavailable” on page 4](#)
- ♦ [“User is not possible to login to Linux” on page 5](#)
- ♦ [“Chain Caching erased with update” on page 5](#)
- ♦ [“Unable to Login as a Local User When a Default Repository Is Set” on page 5](#)
- ♦ [“Device Service Crashes in RHEL during the PKI Method Enrollment” on page 5](#)
- ♦ [“Device Service Not Detect the RFIDeas Reader after Reconnection” on page 5](#)
- ♦ [“Old Digital Persona Readers Do Not Work with the New RTE” on page 5](#)
- ♦ [“Issue with Selecting the Available Devices” on page 5](#)
- ♦ [“Issue with Message Customization in the VDA Agent” on page 5](#)
- ♦ [“Issue with Launching a Selected Profile” on page 5](#)
- ♦ [“Users without Administrator Privileges Are Allowed to Launch the Manage Profiles Window” on page 6](#)
- ♦ [“Unable to Install the VDA Agent in the Silent Mode” on page 6](#)

Offline Login to Remote Desktop fails

This patch resolves the issue where, users who have not enrolled authenticators are unable to perform the offline login to a remote desktop. By default, the Windows Client does not allow non-enrolled users to do offline login to remote desktop and UAC.

To fix this issue, a parameter `allowUnknownUserOfflineCredUI` is introduced in Windows Client. Using this parameter administrators can permit the non-enrolled users to log in to remote desktop and UAC when there is no connection to the Advanced Authentication server. However, it requires to enable the **Username disclosure** option in **Policies > Login Options**.

For more information, see [Enabling Non-Enrolled Users to Log In to Remote Desktop and User Account Control through Offline Mode](#) in the *Advanced Authentication - Windows Client* guide.

The Client Fails to Display a Message When the Advanced Authentication Server Is Unavailable

This patch resolves the issue with the client. When the Advanced Authentication server became unavailable after authentication but before validating the user credentials on LDAP Servers, the client fails to display the message.

User is not possible to login to Linux

This patch resolves the issue when a domain or local user tries to log in to the Linux PAM Client, an error message `Cannot add or change the endpoint (same name or software name already exist)` is displayed. This issue repeats even after deleting the endpoint in the Administration portal.

Chain Caching erased with update

This patch resolves the issue when right after the Linux PAM Client update, the user performs an offline login, authentication fails as the cached chains have been erased.

Unable to Login as a Local User When a Default Repository Is Set

This patch resolves the issue when a local user not able to login to a Linux machine when the `defaultRepo` parameter is configured.

Device Service Crashes in RHEL during the PKI Method Enrollment

This patch resolves the issue when the user tries to enroll the PKI method, the Device Service crashes.

Device Service Not Detect the RFIdeas Reader after Reconnection

This patch resolves the issue where the Device Service fails to detect the RFIdeas card reader when the user unplugged it and then plugged in. This issue occurs in following Mac OS:

- ◆ Mac OS Mojave (through C-type adaptor)
- ◆ Mac OS Catalina (even when the reader is connected directly without adapters)

Old Digital Persona Readers Do Not Work with the New RTE

This patch resolves the issue when the user tries to log in with Digital Persona U.are.U 4500 reader, the reader does not respond and a timeout error message is displayed. This issue occurs only where the DigitalPersona RTE v3 reader is installed.

Issue with Selecting the Available Devices

This patch resolves the issue when WBF direct mode is used, Device Service detects the first available biometric device. As a result, Device Service triggers the camera instead of fingerprint device.

Issue with Message Customization in the VDA Agent

This patch resolves the issue where the VDA agent prompts the user to specify password twice instead of PIN during the in-line enrollment process. This issue occurs, when the message is not customized appropriately.

Now, an administrator can customize the messages that is displayed during the in-line enrollment along with other VDA related messages. To customize messages, first import the `aucore.custom.zip` file to **Policies > Custom messages** on the Administration portal.

Issue with Launching a Selected Profile

This patch resolves the issue where the VDA agent launches the default profile, when a user selects a profile in the **Show Profile** window and tries to launch the selected profile.

Users without Administrator Privileges Are Allowed to Launch the Manage Profiles Window

This patch resolves the issue where a user without administrator privileges can launch the **Manage Profiles** window (`AAA.VDA.Shell.exe /manageProfiles`). However, when the user tries to set a profile as default, the window closed automatically and the default profile is not set.

Now, when a user without the administrator privileges tries to launch the **Manage Profiles** window, an alert message `You should have local administrator rights in order to manager VDA profiles` is displayed.

Unable to Install the VDA Agent in the Silent Mode

This patch resolves the issue where the .msi installer of the VDA agent does not accept `/qn` command for silent installation.

Now, you can install the VDA agent using the msi installer with the following command for silent installation:

```
msiexec /i naaf-vda-x86-release-<version>.msi /qn /l*v install.log
```

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 Patch Update 1 includes the following known issue:

- ◆ [“Issue with Web Authentication” on page 6](#)
- ◆ [“Export Option Is Not Available for the Custom Reports” on page 6](#)
- ◆ [“Windows Hello for Business Accepts only Numeric PIN” on page 6](#)

Issue with Web Authentication

When a user accesses Citrix NetScaler, which is SAML Federated with Advanced Authentication, the page redirects to the Advanced Authentication’s IDP login screen. After the user specifies the username, chooses a chain, and succeeds all methods in the chain, Advanced Authentication does not redirect back to the Citrix NetScaler. In a similar way, the OAuth 2.0 based integrations such as NAM and SSPR are also broken. This issue occurs after upgrading to Advanced Authentication 6.3.

Export Option Is Not Available for the Custom Reports

The **Export** button is not available for each custom report on the [Reports](#) page.

Windows Hello for Business Accepts only Numeric PIN

Windows Hello for Business does not accept alphanumeric characters for the PIN. It accepts only numeric characters.

Upgrading

You can upgrade Advanced Authentication 6.3 to 6.3 Patch Update 1.

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/>.

© Copyright 2020 NetIQ Corporation, a Micro Focus company. All Rights Reserved.