Advanced Authentication 6.2 Patch Update 3 Release Notes

August 2019

Advanced Authentication 6.2 Patch Update 3 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.

For more information about this release and for the latest release notes, see the 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.

IMPORTANT: Advanced Authentication 6.3 and later will not support SLES 11 Service Pack 4.

1 What's New?

Advanced Authentication 6.2 Patch Update 3 provides the following enhancements, and fixes in this release:

- Section 1.1, "Enhancements," on page 1
- Section 1.2, "Software Fixes," on page 3

1.1 Enhancements

Advanced Authentication 6.2 Patch Update 3 includes the following enhancements:

- Section 1.1.1, "Server Enhancements," on page 1
- Section 1.1.2, "Client Enhancement," on page 3

1.1.1 Server Enhancements

Advanced Authentication 6.2 Patch Update 3 includes the following enhancements on the server:

- Section 1.1.1.1, "Limit Linked Chain to the Same Endpoint," on page 2
- Section 1.1.1.2, "Improved Stability of the RADIUS Server," on page 2
- Section 1.1.1.3, "An Option to Enroll the TOTP Method during the Smartphone Enrollment," on page 2

- Section 1.1.1.4, “A Policy to Disallow Authentication from a Rooted Device,” on page 2
- Section 1.1.1.5, “Support for the Hungarian Language,” on page 2

1.1.1.1 Limit Linked Chain to the Same Endpoint

This patch introduces an option that allows a user to authenticate with the alternate linked chain during the grace period. The user must use the same device while using the linked chain to authenticate that was used in the previous successful authentication with a required chain.

Previously, if a user authenticated successfully with the required chain on a particular device (Windows, Linux, or Mac Client), then the user was able to authenticate with the linked chain on another device.

For more information, see “Linked Chains” in the *Advanced Authentication - Administration* guide.

1.1.1.2 Improved Stability of the RADIUS Server

This patch improves the stability of the built-in RADIUS server. The RADIUS authentication fails abruptly in Advanced Authentication 6.2 Patch Update 1 and 6.2 Patch Update 2.

Now, the RADIUS authentication does not cause these sudden failures.

1.1.1.3 An Option to Enroll the TOTP Method during the Smartphone Enrollment

This patch introduces a policy for the Smartphone method to enable the enrollment of the TOTP method automatically for offline usage.

For more information about this policy, see “Smartphone” in the *Advanced Authentication - Administration* guide.

1.1.1.4 A Policy to Disallow Authentication from a Rooted Device

This patch introduces the **Prevent login from a rooted device** policy for the Smartphone method to enable or disable the root check for mobile devices.

When the policy is turned **ON**, the smartphone app must detect whether the device is rooted and prevent login from that device. Rooted devices can provide administrative privileges to third-party software that is not secured and mostly not allowed by device vendors.

NOTE: This policy is supported from the NetIQ Auth app version 3.1.14 (Android) and 3.1.8 (iOS).

For more information, see “Smartphone” in the *Advanced Authentication - Administration* guide.

1.1.1.5 Support for the Hungarian Language

This patch introduces the Hungarian language support on all server portals of Advanced Authentication.

1.1.2 Client Enhancement

Advanced Authentication 6.2 Patch Update 3 includes the following enhancement on Client:

- Section 1.1.2.1, “Password Synchronization for Linked Accounts,” on page 3

1.1.2.1 Password Synchronization for Linked Accounts

This patch introduces seamless synchronization of LDAP password if the login is done with a linked account, when the **Shared Authenticator** feature is enabled.

In the earlier versions, when users logged in to a linked account with a shared authenticator, the password could not be synchronized and the following message was displayed: `This operation is not available for a linked account.`

1.2 Software Fixes

This patch includes the following software fixes:

- Section 1.2.1, “Server Fixes,” on page 3
- Section 1.2.2, “Client Fixes,” on page 3

1.2.1 Server Fixes

- Section 1.2.1.1, “An Issue with Generating Reports,” on page 3
- Section 1.2.1.2, “Intermediate Certificates from the uploaded pfx Are Lost during Translation,” on page 3
- Section 1.2.1.3, “Different Error Messages Are Displayed for Authenticating Known and Unknown Users,” on page 3
- Section 1.2.1.4, “RADIUS Logs Are Not Rotated,” on page 3

1.2.1.1 An Issue with Generating Reports

Reports for the **Authenticators** report type are not exported successfully when an enrolled authenticator is not linked to a user.

1.2.1.2 Intermediate Certificates from the uploaded pfx Are Lost during Translation

This issue occurs during the enrollment of the Smartphone authenticator.

1.2.1.3 Different Error Messages Are Displayed for Authenticating Known and Unknown Users

When a user specifies incorrect password while authenticating, the message displayed is different for known users and unknown users.

This leads to security issues when the Username disclosure option is disabled.

1.2.1.4 RADIUS Logs Are Not Rotated

Now, when the maximum log file size is 50M, the RADIUS logs are rotated and a backup of the last 10 log files is available.

1.2.2 Client Fixes

- Section 1.2.2.1, “Slow Transition to Windows Workstation After Successful Unlock,” on page 4
- Section 1.2.2.2, “A Tap of a Card Does Not Populate the User Name Automatically,” on page 4

- Section 1.2.2.3, "Cached Login with the U2F Method Displays an Error If Facets Are Activated," on page 4
- Section 1.2.2.4, "Advanced Authentication Clients Display an Error during Offline Authentication," on page 4
- Section 1.2.2.5, "Advanced Authentication Clients Display the Cannot Find Server Error," on page 4
- Section 1.2.2.6, "Offline Login with the LDAP Password Method as First Factor Authenticator Binds a Domain User to the Local User Account," on page 5
- Section 1.2.2.7, "Delay in Displaying the Authentication Chain List," on page 5
- Section 1.2.2.8, "Error Due To Inactive User IDs," on page 5

1.2.2.1 Slow Transition to Windows Workstation After Successful Unlock

This patch resolves the issue where after a user unlocks the Advanced Authentication Windows Client on Windows 10 there is a significant delay while the operating system displays a message `Please Wait` before becoming functional.

1.2.2.2 A Tap of a Card Does Not Populate the User Name Automatically

This patch resolves the issue where a tap of a card displays the login screen, and the user is required to specify the user name to log in instead of auto-populating the user name. This issue occurs on Advanced Authentication 6.2.

1.2.2.3 Cached Login with the U2F Method Displays an Error If Facets Are Activated

This patch resolves the issue where if you configure facets and when users try to perform a cached log in with the U2F method, an error message `Wrong APP-ID` is displayed.

1.2.2.4 Advanced Authentication Clients Display an Error during Offline Authentication

This patch resolves the issue where if a user tries to log in to the Advanced Authentication Linux PAM, Mac, or Windows Client in the offline mode after a successful online login, the following message is displayed:

```
Authenticators of <user name> are not cached. Please try again to log in as a local
user or cached user
```

This issue occurs when the Clients fail to retrieve the policies with the list of repositories from the server.

1.2.2.5 Advanced Authentication Clients Display the Cannot Find Server Error

This patch resolves the issue where the Advanced Authentication clients (Linux PAM, Mac, and Windows) display an error message `Cannot find the server` when a user logs in with a cached method in the authentication chain. This issue occurs, if a user restores the Clients from the sleep mode and initiates the login process.

In addition, this patch adds a parameter that enables an administrator to define a delay duration for which the Client does not search the server. Therefore, after an unsuccessful search, the Client cache does not try to search for servers during the defined delay period instead switches to the online mode.

For more information, see "Configuring Authentication Server Discovery in Client" in the *Advanced Authentication- Linux PAM Client* guide.

1.2.2.6 Offline Login with the LDAP Password Method as First Factor Authenticator Binds a Domain User to the Local User Account

This patch resolves the issue where if a domain user logs in to the Advanced Authentication client (Linux PAM, Mac, or Windows) in the offline mode using a chain with LDAP Password method as the first method, the user is mapped with the local user account. Therefore, the domain user is logged in as a local user.

1.2.2.7 Delay in Displaying the Authentication Chain List

This patch resolves the issue where if a user tries to log in or unlock the Windows Client, a message `Please wait` appears, and there is a delay of 3 seconds before listing the authentication chains.

1.2.2.8 Error Due To Inactive User IDs

This patch resolves the issue where after re-enrolling the deleted authenticators if a user logs in to Advanced Authentication Clients in the offline mode, an error `Cannot find the server` is displayed. This issue occurs, when the cache contains two users with the same name, but distinct user IDs.

2 Known Issues

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

2.1 Icons of Methods Are Not Displayed on the macOS Client in the Offline Mode

Workaround: No workaround is available.

3 Upgrading

You must start the upgrade process first from the Global Master server (GMS), then upgrade the database servers, and finally upgrade the web servers.

For more information about upgrading from 6.x, see “Upgrading Advanced Authentication” in the *Advanced Authentication- Server Installation and Upgrade* guide.

4 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.

5 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 https://www.netiq.com/company/legal/.