Advanced Authentication 6.2 Release Notes

February 2019

Advanced Authentication 6.2 includes new features, 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.

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.

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

1 What's New?

Advanced Authentication 6.2 provides the following key features, enhancements, and fixes in this release:

- Section 1.1, "New Features," on page 1
- Section 1.2, "Enhancements," on page 3
- Section 1.3, "Software Fixes," on page 8

1.1 New Features

This release introduces the following features:

- Section 1.1.1, "Repo Agent," on page 2
- Section 1.1.2, "Offline Updates," on page 2
- Section 1.1.3, "Support for Windows Server 2019," on page 2
- Section 1.1.4, "Support for the CN UA550II Card Reader," on page 2
- Section 1.1.5, "Support for Multi-Finger Reader," on page 2
- Section 1.1.6, "Ability to Enable Duress Finger," on page 3

1.1.1 Repo Agent

Advanced Authentication introduces Repo Agent. It acts as a middleware between the LDAP repository and Advanced Authentication. This Repo Agent retrieves users' data from the LDAP repository, stores it in a database, and sends it to Advanced Authentication for authentication.

This prevents operational delays caused due to direct interaction of Advanced Authentication with the LDAP repository. The Repo Agent is recommended to be used in cloud-based environments with on-premise LDAP repositories. In addition, it enhances security because customers may not want to publish LDAP servers on the internet.

For more information, see the *Advanced Authentication - Repo Agent* guide.

1.1.2 Offline Updates

This release provides an option to perform offline updates for the operating system. This is in addition to the online updates.

For more information, see the "Performing the Offline Updates" in the *Advanced Authentication-Server Installation and Upgrade* guide.

1.1.3 Support for Windows Server 2019

In addition to the existing supported platforms, this release adds support for Windows Server 2019 for the following components:

- Windows Client
- Authentication Agent
- Device Service
- RDG Plug-in
- Logon Filter

1.1.4 Support for the CN UA550II Card Reader

This release adds support for the CN UA550II type of card reader.

For more information, see "Card Settings" in the *Advanced Authentication - Device Service* guide.

1.1.5 Support for Multi-Finger Reader

Advanced Authentication now supports the multi-finger reader `Green Bit DactyScan84c` for enrolling the Fingerprint method. This reader enables users to enroll more than one finger together. The Green Bit DactyScan84c has capability to capture one of the following fingers combination at a time:

- Four fingers of the left hand
- Four fingers of the right hand
- Two thumbs

For more information, see "Fingerprint" in the *Advanced Authentication - Administration* guide.

1.1.6 Ability to Enable Duress Finger

This release introduces an option to enable users to assign one of the enrolled fingers as duress. Using the duress finger, users can authenticate to any device or application in case of a threat or emergency. Authentication with the duress finger triggers an alert notification to the configured recipient. This helps in securing the device or application without compromising the safety of the user.

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

1.2 Enhancements

Advanced Authentication 6.2 includes the following enhancements:

- Section 1.2.1, “Server Enhancements,” on page 3
- Section 1.2.2, “Client Enhancements,” on page 6
- Section 1.2.3, “API Enhancements,” on page 6
- Section 1.2.4, “Security Enhancements,” on page 7

1.2.1 Server Enhancements

- Section 1.2.1.1, “Improved Database Export and Import for a Cluster,” on page 3
- Section 1.2.1.2, “An Option to Configure the Whitelist IP Address for Endpoint Registration,” on page 4
- Section 1.2.1.3, “An Option to Disable the LDAP Cache,” on page 4
- Section 1.2.1.4, “Customized Permissions for Sharing the Authenticators,” on page 4
- Section 1.2.1.5, “An Option to Use Repositories Instead of Groups,” on page 4
- Section 1.2.1.6, “An Option to Migrate a Repository,” on page 4
- Section 1.2.1.7, “Improved RADIUS Authentication,” on page 4
- Section 1.2.1.8, “An Option to Send SamAccountName in the SAML Response,” on page 5
- Section 1.2.1.9, “New Widgets,” on page 5
- Section 1.2.1.10, “Customizing the Prompts of Authentication Method Required for RADIUS Client,” on page 5
- Section 1.2.1.11, “Log Level of the SQL Alchemy Are Revised,” on page 5
- Section 1.2.1.12, “An Option to Display the Serial Number of an Enrolled Token,” on page 5
- Section 1.2.1.13, “Pre-installed Netcat,” on page 5
- Section 1.2.1.14, “Resend OTP Option Added to the Web Authentication for All the OTP Based Methods,” on page 6

1.2.1.1 Improved Database Export and Import for a Cluster

The database export and import process has been improved to keep the cluster configuration intact while importing the database.

You can refer to the Disaster Recovery procedure if the cluster is lost while importing the database. For more information, see “Recovering from a Disaster” in the *Advanced Authentication - Administration* guide.

1.2.1.2 An Option to Configure the Whitelist IP Address for Endpoint Registration

Advanced Authentication facilitates an administrator to add a preferred IP addresses to the **Whitelist IP Address**. This helps to register a trusted endpoint from these IP addresses with the administrator's credentials.

The endpoint registration request from any other IP address that is not included in the whitelist are blocked automatically.

For more information, see the "Endpoint Management Options" policy in the *Advanced Authentication - Administration* guide.

1.2.1.3 An Option to Disable the LDAP Cache

In one of the previous versions, a 5 minute LDAP caching on the server was implemented. This increased performance and solved issues for environments where the connection to LDAP servers was unstable or slow. However, the caching opened a security issue because within these 5 minutes a locked or a deleted user, or a user with an expired password was able to authenticate.

In this release, the LDAP caching is disabled by default to enhance security but introduces an option **LDAP caching,** which allows you to enable the LDAP caching to improve performance.

For more information, see the "Login Options" policy in the *Advanced Authentication - Administration* guide.

1.2.1.4 Customized Permissions for Sharing the Authenticators

Previously, a Helpdesk administrator was allowed to share authenticators by default. This resulted in security issues because the helpdesk administrator can misuse the authenticators of users.

Now, only when assigned as a member in the **SHAREAUTH ADMINS** role, a Helpdesk administrator can share the authenticators.

For more information, see "Local Repository" in the *Advanced Authentication - Administration* guide.

1.2.1.5 An Option to Use Repositories Instead of Groups

This release introduces an option that allows you to use repositories in place of groups. You can use a group of users in a specific repository or all the users of the repository.

For more information, see "Creating a Chain" in the *Advanced Authentication - Administration* guide.

1.2.1.6 An Option to Migrate a Repository

This release introduces the command line migration tool `RepoMigrationtool` that allows you to migrate user's data from a repository to another repository. This helps customers who plan for migrating one repository to another to retain authenticators and avoid re-enrollment.

For more information, see "Migrating the Repositories" in the *Advanced Authentication - Repo Agent* guide.

1.2.1.7 Improved RADIUS Authentication

The RADIUS logic has been changed from Freeradius plug-in to AuCore REST API. In addition, the RADIUS logs have been enhanced.

1.2.1.8 An Option to Send SamAccountName in the SAML Response

The samAccountName attribute can now be sent as a NameID element in the SAML response from the Advanced Authentication server. This option has been added for the integration with CyberArk when Advanced Authentication is used as the SAML identity provider.

For more information, see "Creating a SAML 2.0 Event" in the *Advanced Authentication - Administration* guide.

1.2.1.9 New Widgets

This release introduces the following widgets on the dashboard:

- **Total Users**
- **Total Users Per Event**

These widgets help administrators to analyze information about the number of logged in users for each event.

For more information, see "Total Users" and "Total Users Per Event" in the *Advanced Authentication - Administration* guide.

1.2.1.10 Customizing the Prompts of Authentication Method Required for RADIUS Client

Advanced Authentication now allows customization of the prompt message specific to the authentication method that is displayed on the RADIUS Client.

For example, In **Custom Messages** policy, the administrator customizes the prompt message for SMS OTP method that is mapped to the RADIUS event. When a user initiates authentication to a RADIUS event using the SMS OTP method, the customized prompt message is displayed on the RADIUS Client.

For more information, see "Customizing Prompt Messages of the Authentication Methods for RADIUS Event" in the *Advanced Authentication - Administration* guide.

IMPORTANT: Only ASCII symbols are supported for the customized messages of the RADIUS event.

1.2.1.11 Log Level of the SQL Alchemy Are Revised

Previously, in the **Background tasks** tab of **Logs**, an enormous number of log entries are stored for the SQL alchemy commit and new transactions.

Log level of SQL alchemy transactions have been revised so that the debug transactions are not stored in the **Background tasks**.

1.2.1.12 An Option to Display the Serial Number of an Enrolled Token

This release introduces an option to allow users to view the serial number of an enrolled token for the HOTP and TOTP methods on the Self-Service portal.

1.2.1.13 Pre-installed Netcat

With this release, a fresh installation of Advanced Authentication appliance includes the Netcat pre-installed for resolving the possible network connectivity issues.

The Netcat package is not available when you upgrade Advanced Authentication from version 6.1 or earlier versions.

1.2.1.14 Resend OTP Option Added to the Web Authentication for All the OTP Based Methods

In the Web authentication, a **Resend OTP** button has been added to allow users to resend OTP for all the OTP based methods such as SMS, Voice, and so on.

1.2.2 Client Enhancements

- Section 1.2.2.1, “1:N Support for Mac,” on page 6
- Section 1.2.2.2, “Username Disclosure Support for Cached Login,” on page 6
- Section 1.2.2.3, “Enhanced Logging for Windows Client,” on page 6
- Section 1.2.2.4, “An Option for U2F Timeout,” on page 6
- Section 1.2.2.5, “Ability to Configure Timeout for the Authentication Agent Window After Successful Authentication,” on page 6

1.2.2.1 1:N Support for Mac

Now, Advanced Authentication supports the 1:N feature on the macOS. It allows to automatically detect the username when user presents an enrolled card or PKI token.

For more information, see “Disabling 1:N” in the *Advanced Authentication - Mac OS X Client* guide.

1.2.2.2 Username Disclosure Support for Cached Login

This release extends support to the **Username disclosure** option for a Client cache login. The **Username disclosure** option allows administrators to conceal the valid user names and prevents security vulnerabilities.

1.2.2.3 Enhanced Logging for Windows Client

Now, along with the details for the successful login attempts, log files include details for failed login attempts.

For more information, see “Logging for Windows Specific Advanced Authentication Events” in the *Advanced Authentication - Windows Client* guide.

1.2.2.4 An Option for U2F Timeout

An option has been added to configure the U2F timeout for authentication on all the Clients.

For more information, see “Configuring Timeout for the U2F Authentication” in the *Advanced Authentication - Windows Client* guide.

1.2.2.5 Ability to Configure Timeout for the Authentication Agent Window After Successful Authentication

Now, Advanced Authentication administrators can set the duration of the Authentication Agent window display after a user authenticates using the Authentication Agent.

For more information, see “Configuring Time to Close the Restricted Browser” in the *Advanced Authentication - Windows Authentication Agent* guide.

1.2.3 API Enhancements

- Section 1.2.3.1, “Support for Synchronizing the HOTP Token Counter,” on page 7
- Section 1.2.3.2, “REST API to Clone Users,” on page 7

1.2.3.1 Support for Synchronizing the HOTP Token Counter

With this release, Public API has been enhanced to provide an ability to synchronize the HOTP token counter during the enrollment of HOTP authenticator.

1.2.3.2 REST API to Clone Users

With this release, REST API has been enhanced to provide an ability to migrate users of an existing LDAP repository to an another repository (LDAP or External repository for Repo Agent).

1.2.4 Security Enhancements

This release provides the following security enhancements:

- Section 1.2.4.1, "XSS Vulnerability in React Router Fixed," on page 7
- Section 1.2.4.2, "Slow HTTP POST Vulnerability Fixed," on page 7
- Section 1.2.4.3, "Ability to Disable the Key-Pair Generation for PKI Authentication," on page 7
- Section 1.2.4.4, "Permissions Added to Access Cache Files by the System Account Only," on page 7
- Section 1.2.4.5, "Settings to Secure Digital Certificate of the PKI Authenticator," on page 7
- Section 1.2.4.6, "Write Permission Removed for the Configuration File of Linux PAM Client," on page 7

1.2.4.1 XSS Vulnerability in React Router Fixed

XSS vulnerabilities in the react router have been fixed.

1.2.4.2 Slow HTTP POST Vulnerability Fixed

The Slow HTTP POST vulnerability for the Denial of Service (DoS) attack has been fixed.

1.2.4.3 Ability to Disable the Key-Pair Generation for PKI Authentication

You can now disable the key-pair based enrollment of the PKI device and enforce the PKI enrollment using only a user certificate issued by the CA.

For more information, see "Disabling the Key-Pair Option" in the *Advanced Authentication - Administration* guide.

1.2.4.4 Permissions Added to Access Cache Files by the System Account Only

Permission have been added to access the Cache Files by the System account only.

1.2.4.5 Settings to Secure Digital Certificate of the PKI Authenticator

This release introduces two security settings on the Device Service that prevents access to the digital certificates of a PKI authenticator. This enhances the security by protecting the digital certificates.

For more information, see "Configuring the Security Settings" in the *Advanced Authentication - Device Service* guide.

1.2.4.6 Write Permission Removed for the Configuration File of Linux PAM Client

The write permission has been removed for the configuration file `pam_aucore.conf` of the Linux PAM Client.

1.3 Software Fixes

Advanced Authentication 6.2 includes the following software fixes:

- Section 1.3.1, “Server Fixes,” on page 8
- Section 1.3.2, “Client Fixes,” on page 10

1.3.1 Server Fixes

Advanced Authentication 6.2 includes the following server fixes:

- Section 1.3.1.1, “Database Migration from Version 5.x Stopped Working With 5.6 Patch Update 7,” on page 8
- Section 1.3.1.2, “The Advanced Authentication Server Does Not Return Available Authenticators for Clients,” on page 8
- Section 1.3.1.3, “Phone Numbers and Emails of Users for the Web Authentication Events Are Not Masked,” on page 8
- Section 1.3.1.4, “Web Servers Not Able to Communicate with the Database Servers,” on page 9
- Section 1.3.1.5, “An Error Occurs When Logging In to the Administration Portal After Updating,” on page 9
- Section 1.3.1.6, “Heartbeat or Replication Issues,” on page 9
- Section 1.3.1.7, “Customized Chain Names Are Not Applicable for Web Authentication,” on page 9
- Section 1.3.1.8, “Filters Do Not Work Appropriately for Widgets in the Dashboard,” on page 9
- Section 1.3.1.9, “A Repository Sync Updates the Login Options Policy,” on page 9
- Section 1.3.1.10, “No Response Received After Authentication in the Advanced Authentication - NetIQ Access Manager Integration,” on page 9
- Section 1.3.1.11, “An Error is Displayed in the User Report Section of the Helpdesk Portal,” on page 9
- Section 1.3.1.12, “Addition of two eDirectory Repositories with the Same Base DN Fails,” on page 9
- Section 1.3.1.13, “Short Names of the Chains Are Displayed Instead of Custom Names for Web Authentication,” on page 10
- Section 1.3.1.14, “RADIUS Authentication Does Not Work When Username Contains Spaces,” on page 10

1.3.1.1 Database Migration from Version 5.x Stopped Working With 5.6 Patch Update 7

Importing the database from Advanced Authentication 5.6 Patch Update 7 to version 6 does not work. The migration has been fixed and this will work from Advanced Authentication 5.6 Patch Update 8 to 6.2.

1.3.1.2 The Advanced Authentication Server Does Not Return Available Authenticators for Clients

There are specific conditions that involve the offline login and use of more than one user on a workstation. In these conditions, the server does not return the available authenticators for Clients and login or unlocking the operating system is not possible.

1.3.1.3 Phone Numbers and Emails of Users for the Web Authentication Events Are Not Masked

Issue: The phone numbers and emails of the users are not masked on the authentication page for the Web authentication method.

Fix: The option **Recipient Mask** has been added for the Mail Sender, SMS Sender, and Voice Sender policies that allow to mask the phone numbers and email address. For more information, see “Mail Sender”, “SMS Sender”, and “Voice Sender” policies in the *Advanced Authentication - Administration* guide.

1.3.1.4 Web Servers Not Able to Communicate with the Database Servers

Issue: When a Database Master server is rebooted, the Web servers of the same site do not switch to the secondary Database server and this causes a delay of 15 minutes. Even after the Database Master server comes up again, the web servers display errors until those web servers are rebooted.

Fix: A 2-minute timeout has been added to fix the issue.

1.3.1.5 An Error Occurs When Logging In to the Administration Portal After Updating

An error `TypeError NoneType object is not iterable (Unknown Error)` is displayed after installing the patch while logging in to the Administration portal. The issue does not occur after up to 30 minutes.

1.3.1.6 Heartbeat or Replication Issues

Issue: In a clustered environment with several sites, the Global Master server experiences issues with the heartbeat and replication. When a conflict is detected, the system must automatically ignore the incoming change. However, the system ignores the entire batch.

Fix: Now, Advanced Authentication controls whether the entire batch or just the row in conflict must be ignored.

1.3.1.7 Customized Chain Names Are Not Applicable for Web Authentication

Custom localization of method and chain names does not work in the Web Authentication.

1.3.1.8 Filters Do Not Work Appropriately for Widgets in the Dashboard

When you apply filters for Widgets on Dashboard, sometimes the filters are not reflected, and the Dashboard fails to display the information according to the configured filters.

1.3.1.9 A Repository Sync Updates the Login Options Policy

When a full synchronization or a quick synchronization is done for a repository, the repository name gets updated in the **Logins Options** policy.

1.3.1.10 No Response Received After Authentication in the Advanced Authentication - NetIQ Access Manager Integration

After authentication, NetIQ Access Manager does not get a proper JSON response back from Advanced Authentication to indicate that the user is authenticated. *(Bug 1109606)*

1.3.1.11 An Error is Displayed in the User Report Section of the Helpdesk Portal

A 503 error is displayed when navigating to the **User Report** tab of the Helpdesk portal on a web server.

1.3.1.12 Addition of two eDirectory Repositories with the Same Base DN Fails

In an Advanced Authentication server repository configuration, addition of two eDirectory repositories with the same admin base DN does not work.

1.3.1.13 Short Names of the Chains Are Displayed Instead of Custom Names for Web Authentication

When custom names are used for chains in the Web authentication, the short names of the chains are displayed in place of the custom names during authentication.

1.3.1.14 RADIUS Authentication Does Not Work When Username Contains Spaces

When the username contains spaces, the RADIUS authentication does not work.

1.3.2 Client Fixes

Advanced Authentication 6.2 includes the following Client fixes:

- Section 1.3.2.1, “A Blank Screen Is Displayed While Unlocking a Windows Client,” on page 11
- Section 1.3.2.2, “Login to Windows Clients Fails If the Domain Password Is Expired,” on page 11
- Section 1.3.2.3, “Keystrokes Delay In the Password Field,” on page 11
- Section 1.3.2.4, “Unable to Unlock the Client Workstation If Verification of Certificate Is Enabled,” on page 11
- Section 1.3.2.5, “Sign-In Button Is Displayed After Tapping the Card During Windows Login,” on page 11
- Section 1.3.2.6, “Windows Sign-In Text Is Displayed on Background of the Lock Screen,” on page 11
- Section 1.3.2.7, “An Error Message Is Displayed During Windows Login,” on page 11
- Section 1.3.2.8, “Users Cannot Change the Login Credentials on a Terminal Client for a Remote Session,” on page 12
- Section 1.3.2.9, “The U2F Method Does Not Work When Used In a Second Factor Authentication,” on page 12
- Section 1.3.2.10, “Switch User with the Card,” on page 12
- Section 1.3.2.11, “Show Password Icon Is Not Displayed on the Login Screen,” on page 12
- Section 1.3.2.12, “Mac OS Does Not Cache the Repository Name of the Last Logged In User,” on page 12
- Section 1.3.2.13, “Caps Lock Notification Is Not Displayed on Mac OS,” on page 12
- Section 1.3.2.14, “Uninstalling a Client Does Not Remove Respective Endpoint from the Server,” on page 12
- Section 1.3.2.15, “Customized Messages Are Not Displayed on Mac OS,” on page 12
- Section 1.3.2.16, “Customized Messages Are Not Displayed on the Linux Terminal,” on page 12
- Section 1.3.2.17, “Unable to Authenticate with the Face Recognition Method on a Terminal Client,” on page 12
- Section 1.3.2.18, “Unable to Enroll the FIDO 2.0 Method on the Microsoft Edge Browser,” on page 13
- Section 1.3.2.19, “DigitalPersona Reader Not Accessible for a Third Party Application,” on page 13
- Section 1.3.2.20, “Fingerprint Authentication Fails After a Migration from Version 5,” on page 13
- Section 1.3.2.21, “Sometimes the Device Service May Hang or Crash After a Restart,” on page 13
- Section 1.3.2.22, “Issue with the PKI Plug-in After Upgrading Device Service,” on page 13
- Section 1.3.2.23, “The Backspace Key Does Not Work If the Language Is Hebrew,” on page 13

1.3.2.1 A Blank Screen Is Displayed While Unlocking a Windows Client

A blank screen is displayed without any controls when users try to unlock a workstation if some combination of the following Microsoft policies are used:

- **Interactive logon: Display user information when the session is locked**
- **Interactive logon: Do not display last user name**

1.3.2.2 Login to Windows Clients Fails If the Domain Password Is Expired

Issue: With the user switching disabled, when users try to log in to Windows Client with the expired domain password, a prompt to change the password is displayed. However, the prompt does not contain the password change form. Therefore, users are allowed neither to change password nor log in to the Windows Client.

1.3.2.3 Keystrokes Delay In the Password Field

Issue: In Windows Client login screen, when a user specifies the LDAP password or Password, the specified characters appear in the **Password** field after a significant delay. This happens for a screen with high resolution.

Fix: Now, the keystroke delay has been optimized.

1.3.2.4 Unable to Unlock the Client Workstation If Verification of Certificate Is Enabled

Issue: If the Client workstation contains a valid certificate and the parameter `verifyServerCertificate` is set to `true`, the domain users are unable to log in since November 14, 2018.

Fix: Now, the CA certificate is bundled with the Client distributive packages and validity has been extended for 5 years.

1.3.2.5 Sign-In Button Is Displayed After Tapping the Card During Windows Login

Issue: Previously, to log in to a Windows workstation with the Card method, a user had tap the card on the reader, and click **Sign in**.

Fix: Now, the user can tap the card the reader and log in successfully.

1.3.2.6 Windows Sign-In Text Is Displayed on Background of the Lock Screen

While unlocking a Windows workstation, if users delay in selecting the authentication chain, a `Windows sign-in text` is displayed when the Microsoft Interactive logon policy is configured as follows:

- `Display user information when session is locked: Do not displayed user information`
- `Do not require CTRL+ALT+DEL: Not Defined`
- `Don't display last signed-in: Enabled`
- `Don't display username at sign-in: Enabled`

1.3.2.7 An Error Message Is Displayed During Windows Login

When users try to log in to the Windows Client for the first time, an error message `Internal Server Error` is displayed. This is due to the Firewall settings that blocks all outbound connections.

Now, the Cache Service creates the required records in the Windows firewall.

1.3.2.8 Users Cannot Change the Login Credentials on a Terminal Client for a Remote Session

Issue: When a user initiates a terminal session, a prompt to select the chain is displayed. However, an auto-selected user is a currently logged in instead of the Remote Desktop application saved user and users are not allowed to change it.

Fix: Now, the Remote Desktop application saved user can log in to a terminal session by default. This complies with the Microsoft Windows behavior. Moreover, an administrator can set the parameter `select_terminal_client_user: false` (default value is true) to allow the users to change the login credentials on the terminal client during remote login.

1.3.2.9 The U2F Method Does Not Work When Used In a Second Factor Authentication

When the U2F method is used along with another method (for example, Password and U2F), the login screen does not respond after a user authenticates to the first method.

1.3.2.10 Switch User with the Card

Issue: Previously, to log in to a Windows workstation that has been locked, the user had to click **Switch user**, tap the relevant card, and proceed authentication with the other methods of the assigned chain.

Fix: Now, irrespective of whether Windows is locked or not, the user can tap the card on the reader and proceed authentication with the other methods of the assigned chain.

1.3.2.11 Show Password Icon Is Not Displayed on the Login Screen

Sometimes, in the Windows Client login and unlock screen, the show password icon 👁 is not displayed when a user specifies the password in the **Password** field. This icon helps users to validate the specified password.

1.3.2.12 Mac OS Does Not Cache the Repository Name of the Last Logged In User

Mac OS does not cache the repository name of the last logged in user.

1.3.2.13 Caps Lock Notification Is Not Displayed on Mac OS

The Mac OS login page does not display the notification when **Caps Lock** in on.

1.3.2.14 Uninstalling a Client Does Not Remove Respective Endpoint from the Server

When a Client is uninstalled, the respective endpoint is not removed from the Advanced Authentication server. This issue happens because of the Firewall settings that blocks all outbound connections.

1.3.2.15 Customized Messages Are Not Displayed on Mac OS

when an administrator customizes a message in **Custom Messages** policy, the customized messages are not displayed on Mac OS Client.

1.3.2.16 Customized Messages Are Not Displayed on the Linux Terminal

When an administrator customized a message in the **Custom Messages** policy, the customized messages are not displayed on the Linux Terminal.

1.3.2.17 Unable to Authenticate with the Face Recognition Method on a Terminal Client

When users try to log in to the terminal client with Face Recognition method for a remote session, an error message `face service is not available` is displayed.

1.3.2.18 Unable to Enroll the FIDO 2.0 Method on the Microsoft Edge Browser

Issue: On Self-Service portal, when users try to enroll the FIDO 2.0 method using the U2F device, an error message `Web authentication is not supported in this browser` is displayed.

Reason: Users can enroll the FIDO 2.0 method on Microsoft Edge 17 or further supported versions.

1.3.2.19 DigitalPersona Reader Not Accessible for a Third Party Application

Issue: When a third-party application requires to use the DigitalPersona reader, but the reader is busy with the Advanced Authentication Device Service that is installed on the workstation.

Fix: By default, Device Service now uses a cooperative mode and the DigitalPersona reader is not locked for exclusive use by the Device Service. The mode is customizable.

1.3.2.20 Fingerprint Authentication Fails After a Migration from Version 5

Issue: After migrating from Advanced Authentication 5.6 to version 6.1, when users authenticate on Windows Client with the Fingerprint method using the Secugen Hamster Pro 20, an error message `mismatch` is displayed.

Reason: In version 6, another fingerprint engine is available and the old engine which handled the enrollment in version 5 saved the fingerprints with a very low quality.

Fix: An option is included to configure the Device Service to use the old fingerprint engine. For more information, see Mismatch Error After Migrating from Advanced Authentication 5.6 to 6.0.

1.3.2.21 Sometimes the Device Service May Hang or Crash After a Restart

Sometimes Advanced Authentication Device Service may hang or crash when an administrator restarts the service.

1.3.2.22 Issue with the PKI Plug-in After Upgrading Device Service

In Windows, after upgrading Advanced Authentication Device Service 6.0 to version 6.1, the PKI plug-in with card reader does not work.

1.3.2.23 The Backspace Key Does Not Work If the Language Is Hebrew

In Windows, users are unable to delete the incorrect password with the **Backspace** key when the language is set to **Hebrew**.

2 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 6.2 includes the following known issues:

2.1 Issue With Syncing Data for the Repo Agent

Issue: The Repo Agent fails to sync data with Advanced Authentication server when the **Repo Name** contains spaces.

2.2 Some of the Customized Messages Are Not Displayed on the Server

Previously, there was an issue where uploading a localization package from the Client to the server rewrote the localization messages used by the server.

This issue was fixed by merging the server and Client localization packages. However, after this change some of the messages are still not localized on the server.

2.3 Authentication Window Does Not Appear After the Sleep Mode

Issue: On macOS 10.14.2, when the Client goes in the sleep mode and a user tries to log in, the authentication window does not appear.

Reason: This issue is related to Apple and a fix should be provided in the forthcoming macOS release.

2.4 Issue With the Helpdesk Portal Login

Issue: When a user specifies `<aa-server-name>/helpdesk` in a browser to access the Advanced Authentication Helpdesk portal, the user is redirected to the Helpdesk Authenticators page (`/helpdesk/authenticators`) instead of the login page of the Helpdesk portal (`/helpdesk/auth`).

Workaround: Users can either append `/auth` as a suffix to the URL `<aa-server-name>/helpdesk` or click the User icon 👤 > **Log Out** on the Helpdesk Authenticators page to navigate to the login page of the Helpdesk portal.

3 Upgrading

You can upgrade Advanced Authentication 6.1 to 6.2. You cannot directly upgrade from Advanced Authentication 5.x to 6.2. However, you can export the database from Advanced Authentication 5.6 to 6.2. After you install Advanced Authentication 6.2, you can import the database from 5.6.

For example, to upgrade from Advanced Authentication 5.5 to 6.2, you must first upgrade from Advanced Authentication 5.5 to 5.6. Then, you must install 6.2 and import the configurations from 5.6.

For more information about migrating, see “” in the *Advanced Authentication- Server Installation and Upgrade* guide.

For more information about upgrading from 6.0, 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/.