Advanced Authentication 6.3 Release Notes

December 2019

Advanced Authentication 6.3 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.

What's New?

Advanced Authentication 6.3 provides the following key features, enhancements, and fixes in this release:

New Features

This release introduces the following features:

- “Support for Windows Hello for Business” on page 3
- “Desktop OTP Tool for macOS” on page 3
- “Support for Virtual Smartcard (TPM)” on page 3

Risk Service Integration

In this release, Advanced Authentication is integrated with Risk Service. Risk Service evaluates the level of risk during each login attempt using the contextual information, such as IP address, HTTP header, and so on without influencing the end-user experience. It helps in preventing fraudulent access to the secured web application or workstation.

With Risk Service, Advanced Authentication controls access to a protected resource based on the risk level. An administrator can define an appropriate action for the defined risk levels.

NOTE: The Advanced Authentication server deployed on the public cloud does not support Risk Service.

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

Multi-Enrollment Support

Advanced Authentication introduces **All Categories** option that enables users to enroll authentication methods with multiple devices. However, each device is enrolled to a specific category as defined by the administrator. Authentication methods that support multi-enrollment are Card, Fingerprint, Password, FIDO U2F, and TOTP. This option helps users to register both personal and corporate devices and then authenticate with one of the devices.

For more information, see the “Configuring an Existing Event” in the *Advanced Authentication- Server Installation and Upgrade* guide.

RADIUS Rules Engine

This release introduces a policy, **RADIUS Options**. This policy facilitates administrators to define rules using regular expression to accomplish the following actions if the condition specified in the rule is true:

- Select an appropriate chain for authenticating users to the RADIUS client
- Authenticate users to a specific event when multiple RADIUS events are available
- Display associated user groups in the authentication response after a successful authentication to the RADIUS client
- Select a particular chain based on the information that the user specifies on the RADIUS client
- Define a specific authentication chain for various RADIUS clients that are mapped to the same RADIUS event

The **RADIUS Options** policy replaced the NAS ID, Return user groups, User groups white list, and Groups attribute options for RADIUS events and the Short name option for Chains.

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

Ability to Disable Portals of a Server

Advanced Authentication allows an administrator to disable the Self-Service, Administration, Helpdesk, Report, Search-card, and Tokens web portals of a server. This helps administrators to restrict access and secure the web portals on a specific Advanced Authentication server.

For more information, see "Managing Access to the Advanced Authentication Web Portals" in the *Advanced Authentication - Administration* guide.

Virtual Desktop Authentication Agent

Advanced Authentication introduces the Virtual Desktop Authentication (VDA) Agent. Using this agent, users can perform the pre-session multi-factor authentication to get authorized access to the following shared virtual desktops and applications:

- Citrix XenDesktop or XenApp
- VMware Horizon
- Microsoft Remote Desktop

Administrators can manage VDA profiles which can start virtual desktop or shared application automatically after multi-factor authentication. Also, the kiosk mode provides an ability to launch VDA on an isolated desktop.

For more information, see the Advanced Authentication - Virtual Desktop Authentication Agent guide.

Support for Windows Hello for Business

Advanced Authentication now allows to enhance security on the domain-joined Windows 10 workstations by providing an additional request for the Windows Hello authentication with PIN. It is required to have the Windows Hello for Business configured in the domain to allow users to authenticate with Windows Hello PIN.

Desktop OTP Tool for macOS

This release adds support for the Desktop OTP tool on macOS Mojave and Catalina. You can use the Desktop OTP tool for enrolling the TOTP method and further generating one-time password on macOS.

Support for Virtual Smartcard (TPM)

Advanced Authentication adds support for Windows TPM (Trusted Platform Module) based on the virtual smart card for authentication, rather than using a physical smart card with a reader. The information available in the virtual smart card is used to authenticate the users.

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

Enhancements

Advanced Authentication 6.3 includes the following enhancements:

- "Server Enhancements" on page 4
- "Client Enhancements" on page 5

Server Enhancements

Provision for Scheduling Export

Advanced Authentication allows administrators to automate the backup of configurations at a specific time. Also, override the scheduled backup process to initiate backup at any given time as per the requirement. In addition to this, you can delete old backup files while retaining a specific set of files.

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

Enhanced User Interface for Administration Portal

This release enhances the user interface of the administration portal to make user interaction effective and for ease of use. New user interface includes the following:

- New icon for methods and redesigned controls.
- Methods are displayed in the Tile view.
- Space between entries is reduced in Chains, Events, Policies, and Endpoints page.
- Policies are sorted alphabetically.

Support for Citrix Hypervisor and Citrix XenServer

This release adds support for installing the Advanced Authentication appliance on the following server virtualization platforms:

- Citrix Hypervisor 7.1, 7.5
- Citrix XenServer 8.0

The standard ISO image is used for deploying appliance on these hypervisors.

Provision to Disable Manual Enrollment of the TOTP Method

This release introduces **Disable self enrollment** option in the **OATH OTP** method. This option enables administrators to prevent users enrolling the TOTP method manually in the Self-Service portal.

For more information, see the "OATH OTP" method in the *Advanced Authentication - Administration* guide.

Ability to Disable Enrollment of the Smartphone Method Without QR code

Advanced Authentication introduces a new event, **Smartphone Enrollment**. Administrators can disable this event to prevent users from enrolling the Smartphone method using a link without scanning the QR code.

For more information, see the "Smartphone Enrollment Event" method in the *Advanced Authentication - Administration* guide.

Pre-Installed SNMP Package

With this release, a fresh installation of the Advanced Authentication appliance includes the SNMP package pre-installed for monitoring the health of Advanced Authentication server.

The SNMP package is not available when you upgrade Advanced Authentication from version 6.2 or earlier versions.

Ability to Send All Logged Events to the Syslog Server

In addition to forwarding logs from the **Syslog** section, now the **CEF Log Forward** policy enables the Advanced Authentication server to forward all logged events details to the external Syslog server. However, logs related to the NGINX error and WebAuth are not forwarded to the Syslog server.

Provision to Configure Proxy Settings on the Configuration Portal

Advanced Authentication introduces the proxy configuration on the Configuration portal (:9443). Now administrators can configure without the use of command line with YaST.

For more information, see "Configuring the Proxy Settings" in the *Advanced Authentication - Administration* guide.

Support for Windows Server 2019 for ADFS MFA Plug-in

This release adds support for installing ADFS Plug-in on Windows Server 2019.

Optimization of Repository Synchronization

The LDAP page size has been increased to optimize the repository synchronization. However, Advanced Authentication might require few seconds to load all groups of the repository after the synchronization.

Enhanced Security

Advanced Authentication introduces **Advanced SSL settings** in the **HTTPS Options** policy to enable administrators to configure the preferred DH group and SSL cipher suites for exchanging data over a secured connection.

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

Client Enhancements

- "Auto-Populate User Name After the Client Installation" on page 7
- "Support for Defining Multiple Hosts in the discovery.hosts Parameter for the Linux PAM Client" on page 7

Support for Newer Versions of Operating System

In addition to the existing supported platforms, this release adds support for the following operating systems for the respective client components as follows:

	Windows 10 v1909	CentOS 8	Debian 10	macOS Catalina
Desktop OTP Tool	Yes	NA	NA	Yes
Device Service	Yes	Yes	Yes	Yes
Linux PAM Client	NA	Yes	Yes	NA
Mac OS X Client	NA	NA	NA	Yes
Virtual Desktop Authentication Agent	Yes	NA	NA	NA
Windows Authentication Agent	Yes	NA	NA	NA
Windows Client	Yes	NA	NA	NA

To know issues related to macOS Catalina, see Known Issues.

Ability to Disable Linked Chains for Offline Login

This release introduces a new parameter `enableLinkedChainsOffline` in Clients. With this parameter administrator can prevent use of linked chains for offline login.

For more information, see "Disabling Linked Chains for Offline Login" in the *Advanced Authentication - Mac OS X Client* guide.

Renamed the Install Wizard of Client Components

Previously, there was no standard guidelines for naming the Advanced Authentication client components.

Now, the install wizard is renamed to display the brand, product, and component name (for example, NetIQ AA Device Service).

Ability to Cache Shared Authenticators

Advanced Authentication introduces an option, **Allow Local caching for logons by shared templates** in **Cache Options** policy. This option enables administrators to cache shared authenticators in Clients and use the cached details for validation during the offline authentication.

Previously, it was not possible to use shared authenticators for the offline login.

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

Provision to Configure the TLS Version for Clients

Now, Advanced Authentication administrators can configure the TLS version used for establishing a HTTPS connection on all the Clients.

For more information, see "Configuring the TLS Version" in the *Advanced Authentication - Windows Client* guide.

Customizing Look and Feel of Messages on Clients

Advanced Authentication allows administrators to customize the font size, color, and font family of notifications on Clients using the HTML tag.

For example, it is possible to customize the font, font size and color of the Caps lock indicator.

For more information, see "Customizing the Messages for Clients" in the *Advanced Authentication - Administration* guide.

Auto-Populate User Name After the Client Installation

During the first login attempt, the user name is populated from the last user used in Microsoft Windows before the Windows Client installation.

Support for Defining Multiple Hosts in the discovery.hosts Parameter for the Linux PAM Client

The Advanced Authentication Linux PAM Client allows you to configure more than one Advanced Authentication servers in the `discovery.hosts` parameter of the configuration file.

For more information, see "Using a Specific Advanced Authentication Server in Non-DNS Mode" in the *Advanced Authentication- Linux PAM Client* guide.

Software Fixes

Advanced Authentication 6.3 includes the following software fixes:

Server Fixes

Advanced Authentication 6.3 includes the following server fixes:

Security Vulnerability Due to Built-in SAML Signing and SAML Encryption Certificate

The built-in SAML Signing and SAML Encryption certificates (not HTTPS certificate) available in the Advanced Authentication server by default. The certificates are same on every Advanced Authentication appliance, rather than uniquely generated per customer.

Now, the fresh installation and upgraded Advanced Authentication server (without SAML2.0 or OATH 2.0 events) have new certificates. However, the upgraded server with SAML 2.0 or OATH 2.0 events will retain the old signing and encryption certificate for an uninterrupted SAML assertion.

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

No Disk Space Check before the Upgrade

Now, before upgrading the Advanced Authentication server, the available disk space is scanned for a successful upgrade.

Issue with the IIS Plug-in

This release resolves the issue, where the IIS plug-in displays an error message `Failed to process request` during the web authentication to RDWeb. This issue occurs, when the web authentication server fails to share the User Principal Name (UPN) of a user with the IIS plug-in.

The Dashboard Does Not Save Relative Time

This release resolves the issue when the **Relative interval** value reverts to default value (Last 15 minutes) automatically after an administrator saves the changes.

Unclear Error Message When the Enroll Activity Stream Report Contains More Than 10000 Results

This release resolves the issue where the Enroll Activity Stream report displays an unclear error message `Result window is too large` when the report has more than 10000 results.

Now, the error message states that the behavior is intended and guides to save the report. Also, allows administrators to explore the report manually to avoid performance issues.

The Context Sensitive Help Does Not Go to the Specific Page

This release resolves the issue when clicking the **Help** icon opens the front page of the guide instead of opening the context-specific information page.

The Smartphone Notification Displays the Docker Container IP Address as the Source IP Address

This release resolves the issue where the Smartphone notification displays the docker container IP address instead of the IP address of the source from where the request originates.

The Syslog and Fingerprint Log Files Are Not Exported

This release resolves the issue where the following log files are not exported to the respective debug logs location from the Administration portal:

- `syslog.log`: `/var/log/host/messages`
- `nbisd.log`: `/var/log/nbisd/`

A Syslog Entry for the User Removed Event

This release introduces an event in the `Syslog.log` file that logs when users delete all their enrolled methods on the Self-Service portal.

Repo Agent Saves User Names from an External Repository in the Case-Sensitive Format

Previously, the Repo Agent stores the user name in case-sensitive format (for example: Sussane) after synchronizing the user details from an external repository. Therefore, user was unable to log in with the user name (for example: sussane) in case-insensitive format.

Now, the Repo agent stores user names in case-insensitive format.

Repo Agent Displays Deleted Users of a Repository After Synchronization

This release resolves the issue, where after the synchronization, the Repo Agent displays deleted users of the repository.

The Advanced Authentication Server Does Not Respond to RADIUS Requests

This release resolves the issue where the Advanced Authentication server does not respond to RADIUS requests if the **Return user groups** is set to **ON**, and more than five user groups are white-listed for a RADIUS event. However, the server responds to requests after a while without any intervention.

Enroll Unlimited Emergency Password Using REST API

This release resolves the security issue where a user is allowed to enroll Emergency Password without limiting the login count.

Now, the API call includes parameters to achieve the following:

- Allow users who have access to the Helpdesk event to enroll the Emergency Password.
- Limit the login count after enrollment.

Issue with Email OTP and SMS OTP Methods in the Danish Language

This release resolves the issue when a user authenticated with the Email OTP or SMS OTP method, the prompt message did not display the email address or the phone number where the OTP was sent.

Cannot Save the Web Authentication Method if the IDP Metadata Contains Non-ASCII Characters

This release resolves the issue when an administrator tries to add a SAML IDP in the Administration portal using a metadata file that contains non-ASCII characters, an error message that states Unicode strings with encoding declaration are not supported is displayed.

Few CEF Headers Display Obsolete Value

This release resolves the issue where the CEF Headers (Device Vendor and Device Product) display obsolete value AAA, and `Core` respectively.

Now, the CEF Headers display the following value:

- Device Vendor: NetIQ
- Device Product: AA

Login to the Advanced Authentication Administration Portal is Slow

This release resolves the issue when a user specifies username to log in to the Administration portal, there is a significant delay to display the relevant authentication chains.

Now, IPv6 is properly configured in the dockerized environment.

Database Garbage Collector Consumes High CPU

The database garbage collector query is optimized to reduce CPU usage.

Client Fixes

Advanced Authentication 6.3 includes the following Client fixes:

Blank Screen While Unlocking the Mac OS Client

This release resolves the issue where a blank screen appears in the following scenario:

A user selects a chain. But, fails to specify data related to selected chain within 30 seconds on the Unlock screen of the Mac OS Client.

To fix this issue, a parameter `keep_window_on_unlock` is introduced in the Mac OS Client. This parameter displays the authentication window on lock or sleep mode until the user closes it manually.

For more information, see Displaying the Authentication Window on Unlock Screen in the *Advanced Authentication - Mac OS X Client* guide.

Prefixing Domain Name with Username Displays an Error Message

This release resolves the issue where an error message `Internal server error` is displayed on the Windows Client if you prefix the domain name with the user name while logging in to the client.

Enrolled Authenticators Are Persistent After Uninstalling the Desktop OTP Tool

This release resolves the issue where if you re-install Desktop OTP Tool, the tool displays previously enrolled authenticators.

Issue with RDP Authentication

This release resolves the issue where from Advanced Authentication clients, users are unable to authenticate to a remote workstation connected to another domain through RDP.

For example, consider workstations with Advanced Authentication client are connected to Domain A. Workstations without the client are connected to Domain B. Users cannot authenticate from a workstation of Domain A (with the Client) through RDP to a workstation in domain B.

The Linux PAM Client Displays Repeated Prompt Message During Login

This release resolves the issue where the Linux PAM Client displays some prompt messages repeatedly during login.

To fix this issue, a parameter `less_verbose_services` is introduced in the Linux PAM Client. Using this parameter the administrator can disable messages that display more than once on the login screen.

For more information, see Configuring Less Verbose Services in the *Advanced Authentication- Linux PAM Client* guide.

User Cannot Login to UAC In Offline Mode If the Username is Specified without the Repository Name

This release resolves the issue where an error message `User not cached` is displayed on Windows workstation if a user tries to authenticate to an application that requires administrator privileges. This message displays when the user specifies the user name without prefixing the repository name in the UAC (User Access Control) window.

Mac OS X Client Disables Touch ID to Improve Security

This release resolves the issue when you activate the Mac workstation from the sleep mode and unlock using Touch ID, the Net IQ window appears. You are required to pass two-factor authentication to dismiss the window. Now, the Mac OS client disables Touch ID automatically.

User Cannot Use the Enter Key for Chain Selection on the Mac OS Client

This release resolves the issue where a user cannot select a chain on the Mac OS Client using the **Enter** key from an extended keyboard. This issue occurs when the Mac OS Client is unable to identify the keystroke of the Enter key from the numerical keypad of the extended keyboard.

The Mac OS Client Displays an Error Message during Offline Authentication

This release resolves the issue where the Mac OS Client displays an error message `Internal Server error` and does not allow users to log in. This issue occurs when a user authenticates with a chain that contains PIN and Smartphone methods. The client is unable to resolve the hostname to the IP address of the Advanced Authentication server.

The Windows Client Displays the Cannot Find Server Error

This release resolves the issue where the Windows Client displays an error message `Cannot find server` when authenticating with a chain that consists of PIN and PKI methods. This issue occurs when the Windows workstation in on the public network and unable to reach the Advanced Authentication server.

The UAC Prompt Does Not Gather the Domain Name of Workstation and User

This release resolves the issue where the UAC window does not gather the domain name of the workstation and user, instead seeks a user to specify the domain name.

A User Cannot Log In to the Linux PAM Client without Specifying the Repository Name

This release resolves the issue where a user cannot log in to Linux PAM client without specifying the repository name before the user name. This issue occurs when multiple repositories are available.

Now, in multiple repositories environment, you can configure a repository as default irrespective of the order of repositories configured in the **Login Options** policy on the Administration portal. With a default repository, users can log in to the Linux Client without prefixing the repository name before the user name.

For more information, see Configuring a Default Repository on Linux PAM Client in the *Advanced Authentication- Linux PAM Client* guide.

Device Service Vulnerability

With this release, Advanced Authentication supports the content security policy and blocks embedding a page using <frame> or <iframe> in the PKI related web pages. This prevents Cross-site Scripting (XSS) vulnerabilities.

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

PKI Authentication Displays an Error Message If the Password or PIN of Token Is Expired

This release resolves the issue where the following message is displayed if a user specifies an expired PIN or password while logging in to the Windows Client with the PKI method:

```
Protocol violation, send signature
```

Now, Advanced Authentication prompts a user to set a new PIN or Password without the help of a helpdesk administrator.

Customized Messages Are Not Reflecting on RHEL

This release resolves the issue where the messages specific to the Linux Client are not displayed on RHEL after customizing a message in the **Custom Messages** policy.

Mac OS Client Does Not Mask User Specified One-Time-Password and Security Answers

This release resolves the issue where a user-specified OTP and security answer are not masked on the Mac OS Client. Now, specified OTP or any input data changes to dots immediately.

User Binding Is Required Again

This release resolves the issue where a user who is bound as a local user tries to log in as a domain user, the Mac OS client binds the user as the local user again.

Upgrading

You can upgrade Advanced Authentication 6.1 or 6.2 to 6.3. You must start the upgrade process first from the Global Master server (GMS), then upgrade the database servers, and finally upgrade the web servers.

IMPORTANT: In this release, there is a significant change in the hardware minimum and recommended requirements of the appliance. Therefore, you must change the hardware configuration before upgrading Advanced Authentication.

For more information, see "Appliance Requirements (https://www.netiq.com/documentation/advanced-authentication-63/advanced-authentication-6-3-system-requirements/data/advanced-authentication-6-3-system-requirements.html#t49ibi6auxd8)" in the *Advanced Authentication System Requirements*.

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

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 includes the following known issues:

The Login Screen Freezes on Mac OS Catalina

Issue: On macOS 10.15 (Catalina) with the Mac OS client, the login screen freezes or restarts. This issue occurs in the following scenarios:

- When a user selects the authentication chain and specifies data related to methods in the chain to log in.
- When selecting a user while logging in.

Workaround: This issue is related to Apple. The fix for this issue is expected in the forthcoming macOS release.

The Authentication Window Disappears on Mac OS Catalina

Issue: On macOS 10.15, when a user performs an action (fast user switching, unlock screen saver, unlock preference settings, and so on) that requires user credentials and the authentication window is displayed. Again, when the user initiates any action that requires user credentials, the authentication window appears. However, it disappears within 30 seconds from opening the first authentication window. The issue occurs, for all authentications except for the authentication on the login screen.

Workaround: This issue is related to Apple. The fix for this issue is expected in the forthcoming macOS release.

Domain Users Cannot Unlock Mac OS Catalina

Issue: On macOS 10.15 and 10.15.1, the domain bound users are unable to unlock the mac workstation from the sleep and screen saver mode.

Workaround: When users unlock from the sleep or screen saver mode, the screen is redirected to the login screen.

An Issue with User Switching on Ubuntu 18

Issue: On Ubuntu 18, a logged-in domain user (user1) cannot unlock the workstation due to an error message that states the user is not logged in. This issue occurs when the domain user selects his profile from the list of users and authenticates with all authentication methods in a chain.

Workaround: This issue is related to Ubuntu and it is expected to be solved in the further OS updates.

An Issue with the Web Authentication Login Page

Issue: When a user tries to authenticate to the Web authentication page, the category selection prompt is not displayed for few methods on the login page. This issue occurs when the user tries to log in with methods (SMS OTP, Smartphone, Email OTP, and so on) that do not support authenticating with one of the enrolled authenticators.

Workaround: This issue is related to Apple. The fix for this issue is expected in the forthcoming macOS release.

RF IDeas Reader Does Not Work When Reconnected on Mac OS Catalina

Issue: On macOS 10.15, when a user unplugs the RF IDeas reader and connects again, the reader does not work.

Inconsistent Behavior of the Authentication Window

Issue: On macOS 10.14.5, when a user sets the **Require password after sleep or screen saver begins** to any duration, such as 5 or 10 minutes in the **Security & Privacy Settings**. With this setting, when a logged-in user tries to wake the system from sleep or screensaver mode, the authentication windows appear. In some instances, either a black screen is displayed or desktop is available without prompting for authentication.

Risk Containers Are Marked as Unhealthy And Displays an Error in Logs

Issue: The Risk containers are marked as unhealthy and this causes a warning message in the server logs. To view the status of container, run the `docker ps` command in the command line of appliance.

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/.