Advanced Authentication 6.3 Service Pack 1 Release Notes

March 2020

Advanced Authentication 6.3 Service Pack 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).

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 Service Pack 1 provides the following enhancements, and fixes in this release:

- "New Features" on page 1
- "Enhancements" on page 2
- "Software Fixes" on page 4

New Features

This release introduces the following features:

- "Preview New User Interface for Self-Service Portal" on page 2
- "Flex OTP" on page 2
- "EAP-TTLS-PAP Support for RADIUS Authentication" on page 2

Preview New User Interface for Self-Service Portal

Advanced Authentication introduces a new User Interface in Self-Service Portal with updated method icons for better usability. The new self enrollment UI enables the user to enroll the methods individually in **Your Enrolled Single Methods for sign in** or in sequence in **Your Enrolled Sequence for sign in**. Currently, new Self-Service portal UI does not support Multitenancy, Event categories, Basic authentication, UI customizations, disabling the chain selection, and auto-enrollment of methods.

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

Flex OTP

Advanced Authentication introduces a new method **Flex OTP**. The Flex OTP method enables the users to authenticate by using one-time password from any of HOTP, TOTP, and Smartphone (OTP) methods. When users tries to authenticate to any place, they need to specify the OTP generated in any of HOTP, TOTP, and Smartphone (OTP) methods to authenticate.

For more information, see the Flex OTP in the *Advanced Authentication- User* guide.

EAP-TTLS-PAP Support for RADIUS Authentication

Advanced Authentication introduces a new policy, **RADIUS EAP-TTLS-PAP Options**. With this policy, you can configure the Advanced Authentication server to support the secure EAP-TTLS/PAP communication for RADIUS authentication.

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

Enhancements

Advanced Authentication 6.3 Service Pack 1 includes the following enhancements:

- “A Policy to Prevent the DoS Attack” on page 2
- “The Ability to Restore Database from a Backup File Located on the Local Drive” on page 3
- “A Provision to Hide the User Report on the Helpdesk Portal” on page 3
- “An Option to Disable Chain Selection for Web Authentication” on page 3
- “Support RADIUS Client for Sharing Authenticators” on page 3
- “Support for Debugging Risk Service Logs” on page 3
- “The Ability to Re-Create an Endpoint Though Another Endpoint with Same Name Exists” on page 3
- “Provision to Use Two Factors in One Request for the RADIUS Authentication without Separators” on page 4

A Policy to Prevent the DoS Attack

Advanced Authentication introduces a new policy, **Rate Limiting Options**. You can configure this policy to enhance the security of the server, prevent DoS attacks by limiting the incoming requests.

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

The Ability to Restore Database from a Backup File Located on the Local Drive

In addition to restoring the database from the appliance and an external server, Advanced Authentication now allows you to import the database from the local file.

For more information, see “Restoring the Database from Local File” in the *Advanced Authentication - Administration* guide.

A Provision to Hide the User Report on the Helpdesk Portal

Advanced Authentication introduces an option, **Allow to view user report** in the **Helpdesk Options** policy. Using this option you can hide the **User Report** tab on the Helpdesk portal so that a helpdesk administrator cannot view the user’s login report.

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

An Option to Disable Chain Selection for Web Authentication

Advanced Authentication introduces an option, **Enable chain selection** in the **Web Authentication** policy. With this option, you can hide the chain selection list, and display only a high priority chain with enrolled methods to users for authentication in the SAML 2.0 and OAuth 2.0 events.

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

Support RADIUS Client for Sharing Authenticators

In addition to existing supported methods that can be shared, this release supports the RADIUS client method for sharing authenticators.

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

Support for Debugging Risk Service Logs

This release adds support for displaying debug logs for Risk Service in the Advanced Authentication server. You can set the debug level in **Logs** of the Administration portal.

The Ability to Re-Create an Endpoint Though Another Endpoint with Same Name Exists

Advanced Authentication introduces an option, **Allow unprivileged user to re-register an endpoint or workstation** in the **Endpoint management options** policy. With this option set to ON, administrators can allow all users to re-register an endpoint that already exists in the endpoint list. The user is required to specify user name and password to re-register the endpoint.

This option is set to OFF by default. When set to **OFF**, users with ENROLL ADMIN or FULL ADMIN privileges are allowed to re-register an endpoint.

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

Provision to Use Two Factors in One Request for the RADIUS Authentication without Separators

Previously, in Advanced Authentication 6.2 and prior versions, users were allowed use the ampersand (&) as a delimiter between the password and OTP for RADIUS authentication. Later, in Advanced Authentication 6.3, with the **RADIUS Options** policy, it is possible to customize the delimiter.

In this release, a custom RADIUS attribute, `User-OTP` is added. With this attribute, you can configure a rule to extract specific number of characters from the user-specified password. In this way, Advanced Authentication separates the OTP from the password.

For more information on the `User-OTP` attribute, see "Input Rule" in the *Advanced Authentication - Administration* guide.

Software Fixes

Advanced Authentication 6.3 Service Pack 1 includes the following software fixes:

- "Server Fixes" on page 4
- "Client Fixes" on page 6

Server Fixes

Advanced Authentication 6.3 Service Pack 1 includes the following server fixes:

- "Web Authentication Does Not Work in Advanced Authentication 6.3 with the SSPR Link Configured" on page 4
- "Configuration Portal Is Not Accessible When Using Proxy" on page 5
- "Export Button Is Not Visible for the Custom Reports" on page 5
- "Unnecessary Screen with Next button on Advanced Authentication 6.3 Portals" on page 5
- "Web Authentication Certificates Reset to Default after Uploading the Customer Certificates" on page 5
- "Information Exposure through the Log Files" on page 5
- "Error While Exporting Logs in Advanced Authentication 6.3" on page 5
- "Search Guard Not Initialized Error in Advanced Authentication Server" on page 5
- "Web Authentication Fails When a Secondary Tenant Uses the PIN Method" on page 5
- "PKI Enrollment Does Not Display the Enrollment Status to Users" on page 5
- "Log Files Contain Warnings About the Health Check of the Risk Service Containers" on page 6
- "Numerous 520 Unknown Server Error Messages in the uwsgi.log File" on page 6
- "IP Address Rule Does Not Pass After Adding the Actual Client IP Address" on page 6
- "A Cookie Is Not Managed in the Browser After Risk Evaluation" on page 6
- "Tomcat Version Disclosure" on page 6
- "Localization of Chain Name is Not Supported in the Web Authentication Event" on page 6

Web Authentication Does Not Work in Advanced Authentication 6.3 with the SSPR Link Configured

This release resolves the issue where the chain selection page appears even after a user succeeds with all methods in the chain. This issue occurs in Advanced Authentication 6.3 with the SAML 2.0 and OAuth 2.0 integrations if the SSPR URL has been set in **LDAP Password** method on the Administration portal.

Configuration Portal Is Not Accessible When Using Proxy

This release resolves the issue where the Configuration portal (:9443) is not accessible and displays an exception after upgrade to Advanced Authentication 6.3 with the proxy already configured.

Export Button Is Not Visible for the Custom Reports

This release resolves the issue where the **Export** button is not visible for a custom report in **Reports** of the Administration portal. After adding a custom report, the administrator is unable to export the report to the preferred format.

Unnecessary Screen with Next button on Advanced Authentication 6.3 Portals

This release removes the unnecessary screen that gets displayed with the **Next** button after a use methods, such as Email OTP, Bluetooth, Smartphone and so on, on Advanced Authentication 6.3 portals. User is required to click **Next** to proceed with the authentication.

For example, there is a chain with LDAP password and Smartphone methods. To authenticate with this chain, a user must specify LDAP password, click **Next** and then tap **Accept** in the push notification on the Advanced Authentication app. Later, the user is expected to click **Next** to log in.

Web Authentication Certificates Reset to Default after Uploading the Customer Certificates

This release resolves the issue when an administrator imports new OSP certificates for signing in **Server options** of the Administration portal, the certificates reset to default after few minutes. This interrupts or fails the existing SAML integrations.

Information Exposure through the Log Files

This release resolves the issue where the log files are accessible to unauthorized users, resulting in information exposure. Now, the log rotate removes the logs within 24 hours and blocks access to sensitive data.

Error While Exporting Logs in Advanced Authentication 6.3

This release resolves the issue when an administrator tries to export logs, an error message `File not found` is displayed. This error occurs due to the missing Risk Service logs.

Search Guard Not Initialized Error in Advanced Authentication Server

This release resolves the issue where an error message `Search guard not initialized` is displayed in Notifications of the Administration portal. Also, the Dashboard displays empty widgets with an error message stating an unknown server.

Web Authentication Fails When a Secondary Tenant Uses the PIN Method

This release resolves the issue when a secondary tenant tries to authenticate to the Web authentication event, using the PIN method, an error message `Authentication failed` is displayed. This issue occurs, if a user initiates the authentication request after the Advanced Authentication server is restarted. Also, an error message `Endpoint address is not allowed` is displayed in logs.

PKI Enrollment Does Not Display the Enrollment Status to Users

This release resolves the issue when a user is enrolling the PKI method on the Self-Service portal, it might take about a minute based on the used card and its security algorithms. However, the status of enrollment is not displaying to users. Due to this, the user is uncertain whether the method is still enrolling or the process has hanged. This issue has been fixed in the new user interface of the Self-Service portal.

Log Files Contain Warnings About the Health Check of the Risk Service Containers

This release resolves the issue where the Risk Service containers are marked as unhealthy, and this causes a warning message in the server logs.

Numerous 520 Unknown Server Error Messages in the uwsgi.log File

This release resolves the issue where, in the clustered environment, an error message `520 Unknown Server Error` is logged numerous times in the Web server logs (`uwsgi.log`).

IP Address Rule Does Not Pass After Adding the Actual Client IP Address

This release resolves the issue where **IP Address Rule** fails as the client IP address was not forwarded to Risk Service for evaluation in the federated environment.

Now, the client IP address is forwarded to Risk Service to evaluate the defined IP address rule.

A Cookie Is Not Managed in the Browser After Risk Evaluation

This release resolves the issue when a user succeeds the chain mapped to medium risk level for the federated authentication, the cookie is not handled in the browser for further authentication. In the subsequent login, the user is prompted with the same chain to authenticate.

Tomcat Version Disclosure

From this release, the Advanced Authentication server does not disclose the Tomcat version on the screen that appears in case of an HTTP error, which might cause a security vulnerability.

Localization of Chain Name is Not Supported in the Web Authentication Event

Previously, an administrator was unable to localize the chain name displayed on the Login page of the Web Authentication events (SAML 2.0 and OAuth 2.0).

Now, the administrator can localize the chain name for Web Authentication events. However, the changes will reflect after approximate delay of 1 hour.

Client Fixes

Advanced Authentication 6.3 Service Pack 1 includes the following client fixes:

- "Advance Authentication Selects Last Used Chain Automatically for Authentication" on page 7
- "Users Cannot Log in to Windows Client in the Offline Mode After Installation" on page 7
- "RF IDeas Card Reader Does Not Work on MacOS Catalina" on page 7
- "Single Sign-On Does Not Work on Citrix Virtual Desktop Infrastructure Session" on page 7
- "RDP Session is Terminated When a User Clicks Back on the Chain Selection Screen" on page 7
- "Single Sign-On Does Not Work in a Remote Session" on page 7
- "Device Service Does Not Boot Automatically in RHEL 7.1" on page 7
- "User Not Logged Out of an Active VDA Session After Tapping the Card" on page 7
- "Users Cannot Log In to VDA Agent When the Password Needs to be Changed or Has Expired" on page 7
- "Users without Administrator Privileges Are Allowed to Close the VDA Shell Using the Quit Hotkey" on page 8

- "Specifying an Incorrect PIN Prompts the User to Specify the User Name Again" on page 8
- "Bypassing the Step to Select Single Desktop Hosted on the VMware Horizon Client" on page 8

Advance Authentication Selects Last Used Chain Automatically for Authentication

This release resolves the issue when the user tries to log in to a Windows workstation with Windows Client 6.3 installed, the Advance Authentication selects the last used chain automatically for authentication, now this feature is disabled by default. A new parameter introduced to enable the automatic chain selection.

For more information, see Enabling Last Logged In Authentication Chain for Login in the *Advanced Authentication - Windows Client* guide.

Users Cannot Log in to Windows Client in the Offline Mode After Installation

This release resolves the issue when a user tries log in to Windows Client in the offline mode after installation, the login fails.

RF IDeas Card Reader Does Not Work on MacOS Catalina

This release resolves the issue where users were not able to use RF Ideas card readers in MacOS Catalina. The issue can be fixed by adding Device Service to **Input Monitoring** policy.

Single Sign-On Does Not Work on Citrix Virtual Desktop Infrastructure Session

This release resolves the issue with Citrix Virtual Desktop Infrastructure. When the user tries to authenticate in Citrix VDI, Single Sign-On does not work, and Advance Authentication request for the credentials again.

RDP Session is Terminated When a User Clicks Back on the Chain Selection Screen

This release resolves the issue when the user tries to connect a workstation through RDP, the RDP session terminates if the user clicks the Back button on the chain selection screen.

Single Sign-On Does Not Work in a Remote Session

This release resolves the issue when a user tries to connect to a workstation from remote workstation, Single Sign-On does not work, and Advance Authentication request for user credentials again.

Device Service Does Not Boot Automatically in RHEL 7.1

This release resolves the issue with the Device Service installed in RHEL 7.1. The Device Service does not boot automatically right after the installation, boot-up, or reboot.

User Not Logged Out of an Active VDA Session After Tapping the Card

This release resolves the issue when a user taps the card within a logged in VDA session, the user is redirected to the selection screen instead of logging out of the active session. This issue occurs, when the user has privilege to access more than one desktop virtualization clients.

Users Cannot Log In to VDA Agent When the Password Needs to be Changed or Has Expired

This release resolves the issue when a user tries to enroll the card using VDA agent, a message `you have to change your password` is displayed. However, when the user specifies the user name and password, a message, `Your password must be changed before logging on` is displayed. Therefore, the user is unable to log in to VDA agent. This issue occurs if the administrator has enabled the **Change password on next logon** option in Active Directory.

Users without Administrator Privileges Are Allowed to Close the VDA Shell Using the Quit Hotkey

From this release, a user without administrator privileges is not allowed to close the VDA shell and remote VDI session using the quit hotkey.

Specifying an Incorrect PIN Prompts the User to Specify the User Name Again

This release resolves the issue where if a chain contains Card and PIN methods to authenticate to VDA Agent, a user specifies user name, taps the card, and specifies incorrect PIN, a message `Wrong PIN` is displayed. When user clicks **OK**, the user is prompted to specify the user name instead of PIN.

Bypassing the Step to Select Single Desktop Hosted on the VMware Horizon Client

Previously, after authenticating to VDA agent, if a single desktop is published on VMware Horizon Client, a user is required to select the desktop to launch it from the VMware Horizon dashboard.

Now, a new parameter vmware.singleAutoConnect to forbid auto-selection of a single desktop that is published on VMware Horizon Client.

For more information, see "Disabling the Direct Launching of Single Entitlement. " in the *Advanced Authentication - Virtual Desktop Authentication Agent* 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 Service Pack 1 includes the following known issue:

- "The Configuration Portal Displays the IPv6 address" on page 8
- "OAuth 2.0 or SAML 2.0 Not Working in All Tenants" on page 8

The Configuration Portal Displays the IPv6 address

Issue: The Configuration portal displays the IPv6 address though IPv4 address was specified during the Advanced Authentication server installation.

Workaround: Perform the following steps:

1. Run **yast lan**.
2. Select **Global Options**.
3. Under **IPv6 Protocol Settings**, uncheck **Enable IPv6**, and reboot.

OAuth 2.0 or SAML 2.0 Not Working in All Tenants

In Multi-tenancy mode, when the administrator creates a new tenant, OAuth 2.0 or SAML 2.0 integrations do not work in tenants except in the TOP tenant.

Upgrading

You can upgrade Advanced Authentication 6.3 to 6.3 Service Pack 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.

NOTE: In this release, the **RADIUS Clients** section in the **RADIUS Events** page has been relocated to the **RADIUS Options** policy.

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

NOTE: In this release, the location of configuration file in Device Service for Mac has been changed to `/Library/Application Support/NetIQ/DeviceServiceTool.app/Contents/Resources/config.properties`.

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/.