Advanced Authentication 6.3 Service Pack 2 Release Notes

June 2020

Advanced Authentication 6.3 Service Pack 2 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 2 provides the following enhancements, and fixes in this release:

New Features

This release introduces the following features:

Apple Touch ID for Mac

Advanced Authentication introduces a new authenticator **Apple Touch ID**. Apple Touch ID is an electronic fingerprint recognition feature available in the Mac operating system. This feature allows users to authenticate to Mac.

For more information about Apple Touch ID, see Apple Touch ID, in the *Advanced Authentication- User* guide.

Support for Custom Language

Advanced Authentication introduces a new feature to localize error messages, method message, and prompt message displayed to an unsupported language for all the portals of Advanced Authentication, integrated third party products, and Windows Client.

For more information about custom localization for server side, see Localizing the Web UI and Messages in the *Advanced Authentication - Administration* guide.

For more information about the custom localization for Windows Client, see Localizing the Messages for Clients in the *Advanced Authentication - Windows Client* guide.

Flexible Single Sign- On for Remote Desktop/Citrix

In this release, Advanced Authentication introduces a new feature to enable flexible single sign-on (SSO) to connect to RDP or Citrix ICA. When a user tries to connect to a remote machine launched via Citrix StoreFront or Microsoft Remote Desktop and the user has to enter a LDAP password as a part of the used authentication chain, the LDAP password prompt is skipped when the Flexible sign-on is enabled. The user has to authenticate using rest authentication methods of the used chain.

For more information, see Enabling Flexible Sign-on for Citrix VDI or Remote Desktop Login in the *Advanced Authentication - Windows Client* guide.

Enhancements

Advanced Authentication 6.3 Service Pack 2 includes the following enhancements:

Server Enhancements

This release includes the following Server enhancements:

Option to Hide TOTP on Smartphone

Advanced Authentication allows the users to hide TOTP on rooted smartphones for OATH TOTP authenticators. This feature will be available from the following releases of mobile applications:

- iOS app v3.1.10
- Android app v3.1.16

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

Support for Event Categories on the New Enrollment Portal

In the new Enrollment portal, Advanced Authentication allows a user to enroll or delete authenticators or chains that are enrolled for any event category.

Improved Complexity Requirements for the Password Method

Advanced Authentication improves the complexity requirements of a password when the **Complexity requirements** option in **Password** method settings is enabled. Now, the password specified by the user must meet at least three of the complexity requirements.

New Timeout Settings for Web Authentication

Advanced Authentication introduces a new enhancement in **Web Authentication** policy to enable the Administrator to change both **Session Timeout** and **Authorization Code Timeout** values.

For more information about the timeout settings, see Configuring Timeout in the *Advanced Authentication - Administration* guide.

Flex OTP Improvements

Advanced Authentication now supports Flex OTP as a shared authenticator. Users can use shared TOTP, Smartphone OTP, and HOTP methods as Flex OTP to authenticate.

Now it is possible to use Flex OTP for authentication in SAML 2.0 and OAuth 2.0 integrations.

Improved Compatibly to AdminByRequest

Advanced Authentication is now compatible to AdminByRequest. Now, `login failed` message is not displayed when a user tries to run a program as an administrator.

RADIUS Enhancements

This release includes the following RADIUS enhancements:

Per Event Configuration of RADIUS Rules

Advanced Authentication introduces the following rules in the RADIUS event:

- Input rule
- Chain selection rule
- Result specification rule

Now, it is possible to specify the rules not only in the **RADIUS Options** policy, but also per Event. For more information, see RADIUS Server in the *Advanced Authentication - Administration* guide.

Improved Multi-Factor Possibilities with Flex OTP

In this release, Advanced Authentication improves Flex OTP to work in one line with LDAP Password and Password for RADIUS.

Improved Error Messages for RADIUS

In this release, Advanced Authentication improves the error messages for RADIUS authentication for users and in logs.

Software Fixes

Advanced Authentication 6.3 Service Pack 2 includes the following software fixes:

Server Fixes

Advanced Authentication 6.3 Service Pack 2 includes the following Server fixes:

Common issues

This release includes the following fixes:

User Reporting does Not Work in Helpdesk

When a user clicks the **User report** in the Helpdesk portal, the following message is displayed:

```
TypeError Object of type user is not json serializable (unknown error)
```

This release resolves one more issue with User report. When the proxy is configured and a user clicks the **User report** in the Helpdesk portal, an SSL `bad handshake` error message is displayed.

Not Able to Perform MFA Login When Active Directory Password Expires

When the Active Directory password expired, users cannot log in SAML 2.0 and OAuth 2.0 integrations and the following message is displayed:

```
Your authentication password has expired.
```

Now, users are redirected to Self Service Password Reset to change the password.

New Site Registration Fails

Registration of a new site fails. This happens due to the failure of copying database from the Global Master Server to a DB Master server of a new site due to the slow and unstable network connection. Now, it is possible to deploy a new server without copying the database. Later, the Administrator can import the data manually from the .cpt file or copy through the copy-db script.

For more information, see Registering a New Site (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/register_new_site.html) in the *Advanced Authentication - Administration*guide.

Smartphone Application Displays Default Message

When a user tries to authenticate via smartphone method, NetIQ mobile application displays the default push notification message instead of the custom push notification message that is set in **Custom messages** policy.

Smartphone Does Not Work After Repository Migration

When a user tries to authenticate via smartphone authentication method after repository migration using the RepoMigration tool, the user receives the push notification without accept/decline options in it.

Web Authentication Does Not Display Custom Branding and Custom Messages

The web authentication session does not display the customized branding and customized messages.

Not Able to Install Open VM Tools

While installing open VMware tools with zypper, the following error message is displayed.

```
Problem: nothing provides libmspack.so.0()(64bit) needed by libvmtools0-11.0.5-260.1.x86_64
```

```
Solution 1: do not install open-vm-tools-11.0.5-260.1.x86_64
```

```
Solution 2: break libvmtools0-11.0.5-260.1.x86_64 by ignoring some of its dependencies.
```

Postgres:10-alpine Container Restarts

After repository agent installation, when a user tries to start up containers, container postgres:10-alpine restarts automatically. This is due to the AAF docker containers are incompatible with postgres:10-alpine.

New Enrollment Portal Issues

This release includes the following fixes:

Not Able to Open the New Enrollment Portal

When the proxy is configured and a user tries to open the new Enrollment portal, an SSL `bad handshake` error message is displayed. Now, none of the internal traffic will be redirected through the proxy.

New Enrollment Portal Exposes the Direct Servers

When users access the new Enrollment portal through the load balancer, the portal shows the name of the server instead of the name of the load balancer.

Error While Opening Help Page

An `404, Object not found` error message is displayed when users click the Help icon on the Enrollment portal.

Error While Opening the New Enrollment Portal in the Safari

When a user tries to open the new Enrollment portal in the Safari, an error message `Safari Can't Open the Page` is displayed.

Error While Enrolling the U2F in New Enrollment Portal

When a user tries to enroll the U2F authenticator in the new Enrollment portal, after clicking **Detect U2F Device**, an error message `Unknown error` is displayed.

Error While Testing the U2F in Firefox

When a user tries to test the U2F authenticator in the Firefox, after clicking **Test Method**, an error message Bad `request` is displayed.

Upgrade Issues

This release includes the following fixes:

Not Able to Upgrade Underlying OS

When the users try to upgrade the Advanced Authentication Appliances from 6.2 to 6.3, the users not able to upgrade expected SUSE version.

Not Able to Install Packages

It's not possible to get the package updates during update in Configuration Portal.

Not Able to Update

When a user tries to update the Advanced Authentication Server from version 6.3 Patch Update 1 to 6.3 Service Pack 1, upgrading fails and a warning message is displayed.

RADIUS Issues

This release includes the following fixes:

A Reply-Message for Flex OTP

Advanced Authentication enhances Flex OTP to display the following message to users before they enter the OTP code in a Flex OTP authenticator chain: `Please enter the OTP code`. The message can be customized.

Database Deadlocks Cause RADIUS Authentication Issues

After upgrading to Advanced Authentication 6.3 Service Pack 1, RADIUS stop serving authentication requests due to the database deadlocks.

Back up Files Do Not Show RADIUS Client IP

When a user tries to import the backup `.cpt` file from the previous versions of Advanced Authentication to Advanced Authentication Service Pack 1, it does not display the RADIUS client IP in **Policies > RADIUS Options**.

Error While Adding New RADIUS Clients

When a user tries to add a new radius client in **Policies > RADIUS Options** after upgrading to Advanced Authentication 6.3 Service Pack 1, an error message `Secrets do not match` is displayed.

Error While Using a Three-Factors Chain

When a user tries to authenticate using a chain of three authenticators (LDAP Password + TOTP + Smartphone), the authentication fails after successful LDAP Password authentication with the following error message:

```
Unhandled exception: 'dict' object has no attribute 'get_attr.
```

No Timestamps in RADIUS Logs

When the debug mode is enabled, RADIUS logs do not display the timestamps.

Vulnerability Issues

This release includes the following fixes:

RADIUS Logs Display Passwords in Clear Text

In the Debug mode, the RADIUS logs display the passwords in clear text.

The Allow Logon to This Event by Shared Authenticator Option Does Not Work Properly

The user can authenticate using the Flex OTP method even after disabling **Allow logon to this event by shared authenticator** in the **Cache Options** policy. After the fix, the user cannot authenticate using Flex OTP if **Allow logon to this event by shared authenticator** is disabled.

Upgraded pyrad Version

In this release, Advanced Authentication upgrades the pyrad version from pyrad 2.0 to pyrad 2.1. The pyrad version upgrade resolves the vulnerability CVE-2013-0294.

Unsecured Password for Database

The passwords of some servers in the cluster are not secure. After this fix, there will not be any unsecured passwords for any database.

Security Scan Report Displays Wrong TLS Version

Security scan report displays the TLS 1.1 instead of TLS 1.2. In this release, the Security scan report does not display any version of TLS.

Multitenancy Mode Issues

This release includes the following fixes:

Web Authentication Does Not Work in Tenants

When a user tries to authenticate in multi-tenancy, OAuth2.0 and SAML does not work for tenants other than TOP tenants.

SMS and Email Authenticators Do Not Work in Tenants

When the TOP tenant enforces the policies from TOP tenant to sub tenant, SMS and Email Method do not work due to insufficient input validation.

Client Fixes

Advanced Authentication 6.3 Service Pack 2 includes the following client fixes:

Common Issues

This release includes the following fixes:

Not Able to Perform Offline Login After Windows Client Upgrade to Service Pack 1

After upgrading to Advanced Authentication 6.3 Service Pack 1, when a user tries to authenticate to Windows Client in the offline mode, the cache does not work, and login fails.

Not Able to Perform Single Sign-On to VDI

When a user tries to connect to a remote VDI, single sign-on fails if the Citrix storefront is SAML federated to Advanced Authentication via ADFS.

Event Information Is Missing in Cached Chains

When the chains are cached for offline logon, event details are missed. In this release, the details of respective events are cached for each chain.

Issues with chain selection

This release resolves the following issues with chain selection:

- When a user clicks the **Cancel** button during authentication, the user is redirected to the chains selection screen and navigation using arrow buttons does not work if the `enable_last_chain_selection` parameter is enabled.
- When a user clicks the **Cancel** button during authentication, the user is redirected to the chains selection screen and hitting the Enter key to select the first chain triggers a `Wrong chain` error message.

Chains Page Displayed After Successful Authentication

The chain selection page is displayed again after successful authentication when a user tries to connect to Windows Client installed on a remote machine after rebooting.

Canceling the Bluetooth Chain Navigates to Lock Screen

When a user clicks the **Cancel** button while connecting to a Bluetooth device in Windows client, the user is redirected to the initial Username screen instead of the chain selection screen.

Not Able to Install Device Service 6.3 SP1 in Mac OS

When the user tries to install Advanced Authentication 6.3 Service Pack 1 Device Service on Mac OS 10.13.6, the installation fails and displays the following error message:

```
The installer encountered an error that caused the installation to fail.  Contact the software manufacture for assistance.
```

Device Service Does Not Recognize PKI Token

When a user tries to plug in the PKI token on Ubuntu, Device Service does not recognize the token until the user restarts the Device Service.

LDAP Password Is Required for Offline Login

LDAP password is required for authentication when a user tries to authenticate as a domain user in offline mode.

Authentication Fails in Domain Joined Linux PAM Client

When a user tries to log in to a domain joined Linux workstation, the login fails, and an error message is displayed.

Error While Authenticating PKI Authenticator

When a user tries to authenticate via PKI authenticator, the Linux Device Service displays the following error message:

```
Not found: SHA256. Error code: 0.
```

Wrong Chain Listing in Linux PAM

If a user fails to bind a domain user with a local user in the Linux PAM client, domain user chains are shown to the local user when the local user tries to login.

Authentication Agent Does Not Start Automatically

After installing, the Authentication Agent does not start automatically.

Authentication Agent Shows a Blank Restricted Browser Window

When a user tries authentication using the Authentication Agent, it does not load the event login page in the restricted browser.

VDA Issues

This release includes the following fixes:

- “Disconnecting the Remote Session Redirects the User to Desktop Selection Page” on page 11
- “Error While Re-registering the Endpoint” on page 11
- “Delay After Tapping Card” on page 11

Disconnecting the Remote Session Redirects the User to Desktop Selection Page

When a user disconnects or log off from the VMware View or VMware Horizon remote desktop, the user is redirected to the desktop selection page instead of logging out the user from the VDA session.

Error While Re-registering the Endpoint

When a user tries to re-register the endpoint, the following error message is displayed:

`Exception: Cannot add or change the endpoint` (`same name or software_name already exist?`).

Delay After Tapping Card

When the user tries to re-initiate a VDA session by taping the RFID card on the reader, it takes 5-8 seconds to prompt for the second factor of authentication.

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 2 includes the following known issue:

- “The Used Methods Are Not Cached in Domain Mode for MacOS Client” on page 11
- “Issue With Logon Filter After Upgrading to Windows 10, Version 2004” on page 11

The Used Methods Are Not Cached in Domain Mode for MacOS Client

When a domain user tries to authenticate to Mac OS in offline mode, wrong chains are displayed for authentication as the used methods aren't cached properly in domain mode for Mac OS client.

Issue With Logon Filter After Upgrading to Windows 10, Version 2004

After upgrading to Windows 10 version 2004, the Logon Filter functionality does not work properly.

Upgrading

You can upgrade Advanced Authentication 6.3 or 6.3 Service Pack 1 to 6.3 Service Pack 2.

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: It's required to re-bind a domain user to a local user after upgrade of Linux PAM Client to 6.3 Service Pack 2 on CentOS and RHEL in case when a non-domain mode is used.

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/.