Advanced Authentication 6.2 Patch Update 2 Release Notes

June 2019

Advanced Authentication 6.2 Patch Update 2 includes enhancements and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Advanced Authentication forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

For more information about this release and for the latest release notes, see the Advanced Authentication NetIQ Documentation page. To download this product, see the Advanced Authentication Product website.

If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of the specific page in the HTML version of the documentation posted at the Advanced Authentication NetIQ Documentation page.

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

---

1 What's New?

Advanced Authentication 6.2 Patch Update 2 provides the following enhancements, and fixes in this release:

1.1 Enhancements

Advanced Authentication 6.2 Patch Update 2 includes the following enhancements:

1.1.1 Server Enhancements

Advanced Authentication 6.2 Patch Update 2 includes the following enhancements on the server:

1.1.1.1 Integration with Office 365 Without ADFS

This patch adds support for the integration of Advanced Authentication with Office 365. With this integration, you can set up the strong multi-factor authentication to Office 365 without ADFS. This integration approach eliminates the additional configurations and expenses required to deploy and maintain the ADFS service.

Also, this patch introduces an option in the SAML event settings to allow the Advanced Authentication server to send the `ImmutableId (User objectId)` as the `NameID` element to achieve seamless authentication. This option is required for integrating Advanced Authentication with Microsoft Office 365 without ADFS.

For more information, see "Configuring Integration with Office 365 Without ADFS" in the *Advanced Authentication - Administration* guide.

1.1.1.2 Enhanced Performance for the Bulk Enrollment of Users

This patch reduces the time consumed during the bulk enrollment process of users in large environments.

1.1.1.3 Provision to Add the TOTP Authenticator Using a Seed

Now users can add the TOTP authenticator in the Desktop OTP tool manually using a seed. The seed can be generated either on the Advanced Authentication Self-Service portal or in a third-party software. To use the seed with Advanced Authentication it is required to enable the manual enrollment in the **OATH OTP** method of the Advanced Authentication Administration portal.

For more information, see "Enrolling with the Secret Key" in the *Advanced Authentication- User* guide.

1.1.2 Client Enhancement

Advanced Authentication 6.2 Patch Update 2 includes the following enhancement on Client:

- Section 1.1.2.1, "Support for Windows 10 Version 1903," on page 2

1.1.2.1 Support for Windows 10 Version 1903

This patch extends support for the Windows 10 version 1903.

1.2 Software Fixes

Advanced Authentication 6.2 Patch Update 2 includes the following software fixes:

- Section 1.2.1, "Server Fixes," on page 2
- Section 1.2.2, "Client Fixes," on page 5

1.2.1 Server Fixes

Advanced Authentication 6.2 Patch Update 2 includes the following server fixes:

- Section 1.2.1.1, "Issue with RADIUS Authentication," on page 3
- Section 1.2.1.2, "Advanced Authentication Server Does Not Send the RADIUS Challenge," on page 3
- Section 1.2.1.3, "LDAP Servers Are Unavailable When the Global Master Server Is Down," on page 3

1.2.1.1 Issue with RADIUS Authentication

During high activity with the RADIUS server, sometimes the authentication fails and users have to authenticate again. This issue occurs due to the memory corruption in the third-party component (freeradius). To overcome this issue, the RADIUS container is scheduled to restart frequently.

1.2.1.2 Advanced Authentication Server Does Not Send the RADIUS Challenge

This patch resolves the issue where the Advanced Authentication server does not send the additional challenge from the RADIUS server to a RADIUS Client. Instead, the server returns an Access-Reject packet during the RADIUS authentication. Here, the Advanced Authentication server acts as a RADIUS proxy between the third party RADIUS server and a RADIUS Client.

1.2.1.3 LDAP Servers Are Unavailable When the Global Master Server Is Down

This patch resolves the issue when the Global Master server is down, the configured LDAP server is unavailable on both the database and the web servers within a site.

1.2.1.4 Importing the Database from Advanced Authentication 6.1 to 6.2 Fails

This patch resolves the issue when the import of database from Advanced Authentication 6.1 to 6.2 fails.

1.2.1.5 Full Synchronization Removes the Enrolled Authenticators

This patch resolves the issue where the full synchronization of a repository might remove the users’ authenticators. This might happen if there are more than a thousand groups in the repository and sometimes when some users are skipped during the synchronization. In this case, the users along with their authenticators are removed from the Advanced Authentication database.

Now, Advanced Authentication does not remove the users from the database instead retains the enrolled authenticators for a specified duration. Administrators can customize the time duration. This prevents the loss of authenticators during the full synchronization.

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

1.2.1.6 Security Issue: Helpdesk Administrator Can Reset the Authentication Methods of a Full Administrator

This patch resolves the security issue where a helpdesk administrator is allowed to re-enroll the methods of a full administrator in the **Users to Manage** page of the Advanced Authentication Helpdesk portal. This might result in a helpdesk administrator misusing the administrator’s credentials.

Now, if a helpdesk administrator specifies the user name of a full administrator in the **Users to Manage** page, Advanced Authentication displays an error message `No permission to manage this user. Are you an Enroll Admin?`. This prevents the helpdesk administrator from re-enrolling the methods of a full administrator.

1.2.1.7 Issue with the Memory of Docker Container and the Portals Are Inaccessible Inconsistently

This patch resolves the issue where the docker containers run out of memory and subsequently the Advanced Authentication portals are inaccessible. This issue occurs after upgrading to Advanced Authentication 6.2 Patch Update 1.

1.2.1.8 Issue with Enrolling the Fingerprint on an Android Smartphone to the FIDO 2.0 Method

This patch resolves the issue where users are unable to enroll the fingerprint that exists on an android smartphone to the FIDO 2 method.

Now, users can utilize the fingerprint on an android smartphone to enroll and authenticate with the FIDO 2.0 method.

1.2.1.9 The Activity of Unlocking a User is Not Logged

This patch resolves the issue where the unlocking activity of a user is not logged in syslog files.

1.2.1.10 Advanced Authentication Does Not Work with Amazon Web Services

This patch resolves the issue when the Advanced Authentication server is hosted on the Amazon Web Services, the services stop after a period of about 10 minutes.

1.2.1.11 Expired Password Blocks Users from Logging into the Web Authentication Events

This patch resolves the issue where a user is not allowed to log in with an expired password. The system does not provide a mechanism to change or register a new password.

1.2.1.12 A Bad Gateway Is Displayed for the Web Authentication

This patch resolves the issue where an error `invalid request block size` is displayed on the web server during the web authentication. This issue occurs because the size of the cookie header that is sent exceeds the limit set for UWSGI.

Now, the buffer-size has been increased to 8192 bytes.

1.2.1.13 Issue with the Facet Settings

This patch resolves the issue where users cannot enroll the U2F method when **Facets primary server URL suffix** in the Facets settings contains a custom port.

1.2.1.14 The symdb.log File is not Exported Along with the Other Log Files

This patch resolves the issue where the `symdb.log` file is not generated and exported in the debug logs location (`\opt\symdb\logs`) from the Administration portal.

1.2.1.15 The symdb.log File Does not Contain Previous Logs

This patch resolves the issue where the `symdb.log` file does not contain all of the previous logs as compared to the other log files, where the older files are stored.

1.2.2 Client Fixes

Advanced Authentication 6.2 Patch Update 2 includes the following client fixes:

1.2.2.1 Domain Controller Does Not Complete the Boot Process

This patch resolves the issue where after installing the Logon filter and rebooting the server results in an infinite server reboot loop.

To fix this issue, perform one of the following actions:

- Boot the server with the last known configuration and install the Logon filter again
- Restore a VMware snapshot before installing the Logon filter

1.2.2.2 Issue in Authenticating with the Re-enrolled Methods on Windows Client When the Cached Login Is Enforced

This patch resolves the issue where if you enable the forced cached logon (`forceCachedLogon: true`) on Windows Client, you cannot authenticate with the re-enrolled methods.

Now, during the first login with the re-enrolled authenticator, the cached authenticator gets cleared. When you log in the next time, you can authenticate with the authenticator.

1.2.2.3 Issue with Enrolling the Fingerprint Method on Windows 7 Professional

This patch resolves the issue where users are unable to enroll the Fingerprint method on Windows 7 Professional.

1.2.2.4 Issue with Login on Mac OS Client

This patch resolves the issue when users try to log in to the Mac OS Client with an expired password (on the Active Directory), a message `You must change your password` is repeatedly displayed.

Now, the user login window is displayed after clicking **OK**. `You must change your password` message does not repeat.

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 Patch Update 2 includes the following known issue:

2.1 Cannot Find Server on Mac

Issue: When trying to authenticate with the second-factor authentication on Mac, sometimes an error `Cannot find the server` is displayed.

3 Upgrading

You can upgrade Advanced Authentication 6.2 to 6.2 Patch Update 2. You cannot directly upgrade from Advanced Authentication 5.x to 6.2 Patch Update 2. However, you can export the database from Advanced Authentication 5.6 and after you install Advanced Authentication 6.2 Patch Update 2, you can import the database from 5.6.

For example, to upgrade from Advanced Authentication 5.5 to 6.2 Patch Update 2, you must first upgrade from Advanced Authentication 5.5 to 5.6. Next, you must install Advanced Authentication 6.2 Patch Update 2 and import the configurations from Advanced Authentication 5.6.

For more information about migrating, see “Migrating Advanced Authentication from Version 5.x” 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/.