Advanced Authentication 6.2 Patch Update 1 Release Notes

April 2019

Advanced Authentication 6.2 Patch Update 1 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 Patch Update 1 provides the following key features, enhancements, and fixes in this release:

1.1 Enhancements

Advanced Authentication 6.2 Patch Update 1 includes the following enhancements:

1.1.1 Enhanced Logs

The following enhancements have been added to the Advanced Authentication logs:

- **Improved audit for Helpdesk**

  All of the actions of the Helpdesk administrator who logs in to the Helpdesk console are now logged, including the modification of authentication methods for a user.
- **Improved audit for Administration portal**

  Audit logs have been added to track the configuration changes (repositories, methods, chains, events, endpoints, and so on). Additionally, these logs are helpful for troubleshooting.
- **Username added to logs**

  Logs have been enhanced by adding the username of a user who performs an action.

1.1.2 Enhanced Security by Disabling Storage of the LDAP Password

Previously, the LDAP Password was stored in the Advanced Authentication server if caching was enabled. Now, the Advanced Authentication server does not store the LDAP password in the template data and in the local cache when you disable the **Save LDAP password** option (see LDAP Password method). This enhances security.

1.1.3 Customized Attribute Returned after the RADIUS Authentication

You can now specify any attribute apart from the `Filter-Id` attribute in the **Groups attribute** option of the RADIUS event, which Advanced Authentication returns after the RADIUS authentication. For example, if you want to return the `class` attribute instead of the `Filter-Id` attribute, you must specify `class` in the **Groups attribute** of the RADIUS event.

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

1.1.4 An Option to Use SSL for the DNS Discovery of Active Directory Repositories

Previously, when performing the DNS discovery for Active Directory repositories, the non-SSL mode was used on the port 389. To enable SSL, the **Manual setting** option has to be used and edit an individual LDAP server. For an enterprise with a large number of domain controllers, this causes delay and needs to be done every time the DNS discovery is performed.

Now, the **Use SSL** option has been added to use SSL for the DNS discovery on port 636. This allows Advanced Authentication to automatically discover the DNS names over SSL port 636.

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

1.1.5 Support for MySQL and PostgreSQL

This patch adds support for MySQL and PostgreSQL as repositories. The following versions are supported:

- PostgreSQL 11
- MySQL 5.5

1.1.6 Enhanced API for Enrolling HOTP and TOTP Methods with the Serial Number of a Token

Advanced Authentication allows administrators to use the `serial` attribute in the API queries for enrolling the HOTP and TOTP methods with the serial number of a token. This attribute allows the administrator to enroll numerous users to the HOTP and TOTP methods in less time.

1.1.7 Enhanced Custom Localization for RADIUS Event to Support the Non-ASCII Characters

Now, Advanced Authentication allows administrators to use the non-ASCII characters while customizing the messages related to the RADIUS event. Previously, Advanced Authentication allowed only the ASCII characters in the custom messages of the RADIUS event.

1.1.8 Web Authentication Event Display Token Status

Now, Advanced Authentication displays a valid error message when users select a chain with the RADIUS client method and log in to the Web authentication event. For example, when an incorrect PIN is specified, a new token code is expected, or a token resynchronization is required.

1.1.9 Option to Configure Facets List

You can now configure a list of Facets to be added as part of a domain. Previously, to configure facets, the main URL and prefixes had to be specified. Now, flexibility has been added to configure the facets list.

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

1.2 Software Fixes

Advanced Authentication 6.2 Patch Update 1 includes the following software fixes:

1.2.1 Server Fixes

Advanced Authentication 6.2 Patch Update 1 includes the following server fixes:

1.2.1.1 Issue with RADIUS Authentication

This patch resolves the issue where the RADIUS server stops periodically and the RADIUS authentication fails in Advanced Authentication 6.2.

1.2.1.2 Uploading the Custom ZIP File of Client Deletes the Customized Messages on the Server

This patch resolves the issue when an administrator uploads the custom `ZIP` file from the Client to the Advanced Authentication server to customize the messages on the Client, Advanced Authentication erases the existing messages on the server.

Advanced Authentication merges the messages when the administrator uploads the custom `ZIP` file.

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

1.2.1.3 Issue with Login on Helpdesk Portal

This patch resolves the issue where a user accesses `https://aa-server-name/helpdesk`, Advanced Authentication redirects user to the **Helpdesk Authenticators** page (`https://aa-server-name/helpdesk/authenticators`) instead of the login page (`https://aa-server-name/helpdesk/auth`).

Now, Advanced Authentication directs user to the login page to specify the credentials.

1.2.1.4 Issue with Fingerprint Authentication

This patch resolves the issue where in Advanced Authentication 6.1 and 6.2, the fingerprint authentication fails due to the AFIS service timeout. This issue occurs, when users initiate multiple fingerprint authentication requests simultaneously.

1.2.1.5 Unable to Unlock the Locked Users of a Repository

This patch resolves the issue where an administrator is unable to access the **Repositories > Locked Users** tab of a configured repository in the Advanced Authentication Administration portal. Therefore, an administrator is unable to unlock the locked users of the repository.

1.2.1.6 Advanced Authentication Appliance Does Not Install the Open-vm-tools

This patch resolves the issue where the Advanced Authentication appliance installer does not install the open-vm-tools and you cannot install them manually.

Now, administrators can install the open-vm-tools on the Advanced Authentication server.

1.2.1.7 Linked Authenticators Tab Is Not Visible on the Helpdesk Portal

This patch resolves the issue where the Advanced Authentication Helpdesk portal does not display the **Linked Authenticators** tab when a helpdesk administrator logs in to the Advanced Authentication Helpdesk portal, specifies a user name, and the defined policies do not require the administrator authenticate. The administrator did see the **Linked Authenticators** tab on refreshing the browser.

1.2.1.8 Windows Hello Does Not Work with Web Authentication

This patch resolves the issue when you configure Windows Hello method as second-factor authenticator (for example, PIN and Windows Hello) for web authentication. For example, if user specifies the user name and PIN in the first screen, the sub-sequent screen prompts the user to place finger on the reader. The authentication does not progress when user places their enrolled finger on the reader.

1.2.1.9 Web Authentication Event on a Smartphone Displays a Prompt to Download the NetIQ App

This patch resolves the issue where users try to access the web authentication event on an iPhone, the screen prompts the user to download the NetIQ app. This issue occurs only on the Safari browser.

The patch disables the prompt that states the user must download the NetIQ app.

1.2.1.10 Login and Navigation Processes Are Slow on the Administration Portal

This patch resolves the issue where there is a significant delay before the page returns a list of chain when a user specifies the user name on the login page of Advanced Authentication Administration portal. After the user selects a preferred chain, there is another delay before the portal displays input field. This issue occurs when you use IPv6 address format.

1.2.1.11 Issue with RADIUS Container If the RADIUS Secret Contains Prohibited Characters

This patch resolves the issue where the RADIUS container restarts constantly after upgrading to Advanced Authentication 6.2. This issue occurs, when the RADIUS secret contains the characters that are prohibited (for example, comma and space).

1.2.2 Client Fixes

Advanced Authentication 6.2 Patch Update 1 includes the following server fixes:

1.2.2.1 Issue with Resetting the Password When a User’s Account is Locked

This patch resolves the issue where users use Client Login Extension (CLE) and the users' accounts are locked. Users are unable to navigate to the **LDAP Password** page where the **Forgotten Password** link is displayed.

1.2.2.2 Error When Using Yubikey or Smartphone

This patch resolves the issue where users have issues logging in to a Windows workstation using the **PIN+Yubikey** or **Smartphone** methods, after upgrading to Advanced Authentication 6.2.

1.2.2.3 Error if the Username is Specified with the Domain Name

This patch resolves the issue were Advanced Authentication displays an **Internal server error**, if the username is specified along with the domain name (`domainname/username`) on the Windows and Mac workstation.

1.2.2.4 Mac OS X Client Displays an Internal Server Error During Offline Authentication

This patch resolves the issue where the MAC OS X Client connects to a network but is not able to reach the Advanced Authentication server or it cannot resolve the internal IP address (not connected to the VPN), the users are unable to log in and an **Internal server error** is displayed.

1.2.2.5 Login Issue with Windows Hello

This patch resolves the issues with the Windows Hello login method for the users after upgrading to Advanced Authentication 6.2.

1.2.2.6 Members of Domain and Enterprise Administrator Groups Cannot Access a Shared Folder Secured with the Logon Filter

This patch resolves the issue where the members of domain and enterprise administrator group cannot access a shared folder secured with the Logon Filter.

1.2.2.7 Issue with Unlocking Windows When the Yubikey is Used

This patch resolves the issue where Yubikey is unable to unlock user's non-domain Windows workstation. This issue happens when users incorrectly map their domain accounts to the local accounts.

Advanced Authentication contains additional checks to eliminate the chance of users creating incorrect mappings.

1.2.2.8 Issue with Initiating Authentication to Unlock a Session When OTP Methods are Used

This patch resolves the issue where users are unable to start the authentication to unlock a session (KDE) if they select the authentication chain that use the Email, SMS, or Voice OTP methods.

1.2.2.9 Local User Cannot Log In if the Tenant Name Is Not Set in the Configuration File

This patch resolves the issue where a local user is unable to log in to a Windows workstation, if the `tenant_name` parameter is not set in the `config.properties` file.

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 1 includes the following known issue:

- Section 2.1, "Configured LDAP Servers Are Unavailable When the Global Master Server is Down," on page 7
- Section 2.2, "Browser Displays an Error During SAML Authentication," on page 7

2.1 Configured LDAP Servers Are Unavailable When the Global Master Server is Down

Issue: When the Global Master server is down, the configured LDAP server is not available on both the Database and the Web servers within a site.

Workaround: Perform the following steps on the Global Master server before the Global Master server goes down to ensure that the fail over process is successful:

1. Log in to the Administration Console as an administrator.
2. Navigate to **Repositories** section.
3. Click **Edit** adjacent to the configured LDAP repository.
4. Specify the password of LDAP repository in the **Password** and save the settings.

   This initiates replication of the LDAP servers list to the database servers.

2.2 Browser Displays an Error During SAML Authentication

Issue: After upgrading to Advanced Authentication 6.2, when users try to authenticate to a third-party site with the SAML authentication, the browser displays an error: `SAML Assertion verification failed; Please contact your administrator`.

Workaround: Perform the following steps:

1. Log in to the server as `root`.
2. Run the following command:

   ```
   docker exec -ti aaf_webauth_1 /bin/bash
   ```
3. Open the following file:

   ```
   vi /usr/local/tomcat/bin/setenv.sh
   ```
4. Modify the following content in the file setenv.sh:

   ```
   export CATALINA_OPTS="$CATALINA_OPTS \
   Dinternal.osp.framework.ext-context-dir=$OSP_CONF \
   Dinternal.osp.framework.generic-properties-filename=$OSP_CONF/aa-osp-
   configuration.properties \
   Dorg.apache.el.parser.SKIP_IDENTIFIER_CHECK=true
   ```

   to

   ```
   export CATALINA_OPTS="$CATALINA_OPTS \
   -Dinternal.osp.framework.ext-context-dir=$OSP_CONF \
   -Dinternal.osp.framework.generic-properties-filename=$OSP_CONF/aa-osp-
   configuration.properties \
   -Dorg.apache.el.parser.SKIP_IDENTIFIER_CHECK=true \
   -Dorg.apache.xml.security.ignoreLineBreaks=true
   ```
5. Save and restart the webauth container with `docker restart aaf_webauth_1`.
6. Recreate the event.
7. Download the SAML 2.0 metadata from the Advanced Authentication server and update a used Service Provider with the valid certificates

3 Upgrading

You can upgrade Advanced Authentication 6.2 to 6.2 Patch Update 1. You cannot directly upgrade from Advanced Authentication 5.x to 6.2 Patch Update 1. However, you can export the database from Advanced Authentication 5.6 and after you install Advanced Authentication 6.2 Patch Update 1, you can import the database from 5.6.

For example, to upgrade from Advanced Authentication 5.5 to 6.2 Patch Update 1, you must first upgrade from Advanced Authentication 5.5 to 5.6. Next, you must install Advanced Authentication 6.2 Patch Update 1 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/.