Advanced Authentication 5.6 Patch Update 2 Release Notes

January 2018

Advanced Authentication 5.6 Patch Update 2 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.

The documentation for this product is available on the NetIQ website in HTML and PDF formats. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Advanced Authentication NetIQ Documentation page. To download this product, see the Advanced Authentication Product website.

1 What's New?

Advanced Authentication 5.6 Patch Update 2 provides the following enhancements and fixes in this release:

1.1 New Features and Enhancements

This release introduces the following features and enhancements:

1.1.1 Support for Exporting the Database

This release enables you to export the database with enrolled authenticators, endpoints, and some server configurations for further import to the upcoming Advanced Authentication 6.0 version. You must upgrade to Advanced Authentication 5.6 Patch Update 2 before migrating to 6.0 version. For more information, see "Exporting the Database" in the *Advanced Authentication - Administration* guide.

1.1.2 Options to Prevent Phone Number and Email Address Modifications

The **Allow to override phone number** and **Allow to override email address** options have been added that enables you to hide phone number and e-mail address fields on the Self Service and Helpdesk portals. Thereby, preventing users and helpdesk administrators from modifying the phone number and e-mail address that are stored in the repository attributes during an authenticator enrollment. This option is implemented for the following methods:

- **SMS OTP**
- **Email OTP**
- **Voice OTP**

These options enhance the security for enrollment of listed methods. For more information, see "SMS OTP", "Email OTP", and "Voice OTP" methods in the *Advanced Authentication - Administration* guide.

1.1.3 REST API Support to Search an Endpoint

The REST API has been extended to support for searching the endpoint functionality. Previously, to re-deploy an endpoint, an administrator had to be engaged to find the old endpoint and remove it from the Administration portal. Now, the Advanced Authentication administrators and helpdesk administrators can use the REST API calls with an endpoint name to search and remove a specific endpoint.

1.1.4 Support for Returning User Groups in an Authentication Response

Now, Advanced Authentication RADIUS server returns the `filter-id` attribute in an authentication response to a RADIUS Client. The attribute contains user groups. Therefore, a RADIUS client can configure the policy to specific user groups. For example, a user associated with the group **Night Workers** is allowed to login from 11:00 PM to 9:00 AM.

1.1.5 Support for Returning User Name After RADIUS Authentication

After successful RADIUS authentication, Advanced Authentication RADIUS server returns the `User-Name` attribute with a user name from repository to a RADIUS Client. Previously, when users try to log in to the RADIUS client by providing user name and chain name, the name validation could be failed in some RADIUS clients because the user name is specified along with chain name in the same field.

1.2 Software Fixes

Advanced Authentication 5.6 Patch Update 2 includes the following software fixes:

1.2.1 A User Locked on eDirectory Is Allowed to Log in to Advanced Authentication

Issue: A user who is locked on eDirectory is allowed to log in to Advanced Authentication by using chains that do not contain the LDAP password. This happens because of the cached password.

Fix: Now, when a user locked on eDirectory tries to log in to Advanced Authentication, an error message `The account is currently locked out` is displayed.

1.2.2 Delay in Login to the Administration Portal For Domain Users

Issue: When domain users try to log in to the Administration portal, there could be a significant delay to fetch the associated chains list.

Fix: Performance has now been improved for the domain user log in to the Administration portal without any significant delay.

1.2.3 RADIUS Server Event Login Generates Multiple Push Messages on the Smartphone App

Issue: When the phone is in the 3G mode with WIFI connection turned OFF and a user tries to log in to the RADIUS server event with the LDAP and Smartphone methods, multiple push messages are received on the Smartphone app.

Fix: Now, the user receives a single push message on the Smartphone app for each login attempt to the RADIUS server event.

1.2.4 RADIUS Client Authentication Fails With Short Chain Name

Issue: When users try to log in to the RADIUS client with `<username> <chain short name>`, the authentication fails because the Advanced Authentication built-in RADIUS server no longer supports usage of space as a separator (for example, `john password`).

Fix: Now, users must specify the chain short name and user name with an ampersand (&) as a separator (for example, `user name&chain short name`) for the RADIUS client authentication.

1.2.5 Issue With the SMS Method After Upgrade

Issue: After you upgrade to Advanced Authentication 5.6 Patch Update 1, users are not receiving the SMS with One Time Password (OTP). This happens because of the Proxy server.

Fix: This issue is resolved. Users are receiving SMS with OTP.

1.2.6 Smartphone App Fails to Receive Push Notifications After Upgrade

Issue: After you upgrade to Advanced Authentication 5.6 Patch Update 1, when users log in to Administration portal using the Smartphone method, push notifications are not sent to the NetIQ Advanced Authentication app. This happens because of the Proxy server.

Fix: This issue is resolved. Push notifications are sent to the Advanced Authentication app.

1.2.7 Meltdown and Spectre Hardware Vulnerabilities

The Meltdown and Spectre hardware vulnerabilities have been fixed in the processor.

2 Upgrading

You can upgrade to Advanced Authentication 5.6 Patch Update 2 from Advanced Authentication 5.5 and later versions.

For more information about upgrading, see “Upgrading Advanced Authentication” in the *Advanced Authentication Installation and Upgrade* guide.

3 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.

4 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/.