Advanced Authentication 5.5 Patch Update 1 Release Notes

February 2017

Advanced Authentication 5.5 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.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. 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 5.5 Patch Update 1 provides the following key features, enhancements, and fixes in this release:

1.1 New Features

This release introduces the following new features:

1.1.1 Disabling Self-Enrollment

Administrators can now restrict users from self-enrollment and enable enrollment only through a Helpdesk officer. For more information, see "Helpdesk User" in the *Advanced Authentication - Administration* guide.

1.1.2 Support for Pooling in Twilio

Advanced Authentication introduces support for pooling of phone numbers in Twilio. This feature improves the SMS delivery to phone numbers, as Twilio selects the best phone number from the pool of numbers for sending every message.

1.1.3 Option to Customize Logo

Advanced Authentication introduces a functionality where the administrators can change the default logo and set a customized logo in the Windows Client. For more information, see "Customizing a Logo" in the *Advanced Authentication - Windows Client* guide.

Also, administrators can set a logo with an image for the Administration and Self-Service portal. Alternatively, you can also set a text as a logo. For more information, see "Logo" in the *Advanced Authentication - Administration* guide.

1.2 Enhancements

Advanced Authentication 5.5 Patch Update 1 includes the following enhancements:

- Section 1.2.1, "Protection from MITM Vulnerability," on page 2
- Section 1.2.2, "Improved Security During New Server Deployment," on page 2
- Section 1.2.3, "Option to Disable Paged Search," on page 2
- Section 1.2.4, "Usage of LDAP Password Method Does Not Consume a License," on page 3
- Section 1.2.5, "Different Attributes for Voice OTP, Voice Call, and SMS," on page 3
- Section 1.2.6, "Option to Restrict Re-enrolling and Deleting Authenticators by Users," on page 3
- Section 1.2.7, "Option to Clear Logs," on page 3
- Section 1.2.8, "Improved Communication with LDAP Servers," on page 3

1.2.1 Protection from MITM Vulnerability

Administrators can now enable the **Verify SSL Certificate** option to ensure that the LDAP connection to appliance is secured with a valid self-signed SSL certificate. This helps in preventing security attacks on the LDAP connection and ensures safe authentication. For more information, see "Verify SSL Certificate" in the *Advanced Authentication - Administration* guide. Also, now it is possible to configure a certificate check between a Windows based workstation and Advanced Authentication Server. For more information, see "Configuring for Verification of Server Certificates" in the *Advanced Authentication - Windows Client* guide.

1.2.2 Improved Security During New Server Deployment

Security is enhanced during deployment of a new server. Now administrators have to enter the password of local\admin account of the cluster while configuring a new server in the cluster, which enhances the security.

1.2.3 Option to Disable Paged Search

Administrators now have the option to disable paged search. This option is useful in scenarios where paged search option stops working. For example, after upgrading of NetIQ eDirectory to version 9.0. Also, this option is required for repositories with file-based backend such as openLDAP. For more information, see, "Enable paged search" in the *Advanced Authentication - Administration* guide.

1.2.4 Usage of LDAP Password Method Does Not Consume a License

Now if a user uses a chain with only the LDAP Password method, it does not consume a license.

1.2.5 Different Attributes for Voice OTP, Voice Call, and SMS

Advanced Authentication now offers administrators to configure a phone number from different repository attributes of the Voice Call, Voice OTP, and SMS methods. Previously, a single phone number was configured for all the methods. For more information, see, "User cell phone attributes" in the *Advanced Authentication - Administration* guide.

1.2.6 Option to Restrict Re-enrolling and Deleting Authenticators by Users

Administrators can now restrict users from re-enrolling and deleting authenticators in the Self-Service portal. For more information, see **Disable re-enrollment** section in "Authenticator management options" of the *Advanced Authentication - Administration* guide.

1.2.7 Option to Clear Logs

Administrators can now clear the logs on a server that they are currently working on from the Advanced Authentication Administrative portal. For more information, see "Logging" in the *Advanced Authentication - Administration* guide.

1.2.8 Improved Communication with LDAP Servers

The communication between Advanced Authentication servers and LDAP servers can be improved by disabling nested groups support. This enables Advanced Authentication to authenticate users only from a specified group, excluding its nested groups. For more information, see "Enable Nested Groups Support" in the *Advanced Authentication - Administration* guide.

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.

2.1 Issue With Voice or Voice OTP Method Enrollment of Users by a Helpdesk Administrator

Issue: When the Helpdesk administrator assists a user in enrolling Voice or Voice OTP method, an infinite loop is created.

Workaround: Presently, there is no workaround for this.

2.2 Issue in the Administration Portal After Upgrade

Issue: When you upgrade Advanced Authentication, an error `UnpicklingError invalid load key, 'W'. (Internal Server Error)` occurs in the Advanced Authentication Administrative Portal due to expired cookies.

Workaround: Clear the browser's cookies and try again.

3   Upgrading

You can upgrade to Advanced Authentication 5.5 Patch Update 1 from Advanced Authentication 5.3 and newer versions. To upgrade from 5.2 and prior versions, contact NetIQ Technical Support.

For more information about upgrading from Advanced Authentication 5.3 and newer versions, see "Upgrading Advanced Authentication" in the *Advanced Authentication - Administration* 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/.