Advanced Authentication 5.4 Release Notes

September 2016

Advanced Authentication 5.4 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 5.4 provides the following key features, enhancements, and fixes in this release:

1.1 New Features

This release introduces the following new features:

- Section 1.1.8, "Cached Login Support for Mac and Linux," on page 3
- Section 1.1.9, "Swisscom Mobile ID Method," on page 3

1.1.1 Multitenancy

Advanced Authentication introduces an ability to support multiple tenants on a single Advanced Authentication solution. Multitenancy allows administrators to use a single instance of Advanced Authentication solution to serve multiple customers with different environments. Tenants are given the ability to customize some application configuration settings while other remain universal.For more information, see "Adding a Tenant" in the *Advanced Authentication - Administration* guide.

1.1.2 Geo-fencing

Advanced Authentication introduces the geo-fencing feature that allows administrators to create authentication zones by defining boundaries within a geographical location. When administrators enable geo-fencing, users can authenticate with Smartphone from only allowed geographical locations. For more information, see "Smartphone " in the *Advanced Authentication - Administration* guide.

1.1.3 Logon Filter

Advanced Authentication now provides an ability to restrict access for the Windows workstations that do not have the NetIQ Windows Client installed. For more information, see" Logon Filter for AD " in the *Advanced Authentication - Administration* guide.

1.1.4 Linked Authenticators

Advanced Authentication now provides the shared authentication feature that allows a user to authenticate with his/her authenticator to another user's account. The helpdesk administrator links an authenticator of one user to another user. For more information, see "Sharing authenticators" policy in the *Advanced Authentication - Administration* guide.

1.1.5 Support for HTTP Proxy Server

Administrators can now configure the Advanced Authentication Server appliance to work through an HTTP proxy server in the configuration console. This helps to support the secure environments that restrict direct access to the internet. For more information, see "Configuring HTTP Proxy Server" in the *Advanced Authentication - Administration* guide.

1.1.6 Non-Domain Joined Client Support

Administrators can now install and run Windows Client, Mac OS X Client, and Linux PAM Client on machines that are not joined to a domain. When users authenticate with the domain account on a non-domain machine, they must specify the local account credentials to map their domain account to the local one. For more information, see the *Advanced Authentication- Linux PAM Client*, *Advanced Authentication - Mac OS X Client*, and *Advanced Authentication - Windows Client* guides.

1.1.7 Event for OAuth 2

Advanced Authentication introduces an ability to enable multifactor authentication for users who need to access third party consumer web applications. For more information, see "Configuring Events" in the *Advanced Authentication - Administration* guide.

1.1.8 Cached Login Support for Mac and Linux

Advanced Authentication now provides cached login support for Mac and Linux for the following methods: **LDAP Password, Password, TOTP, HOTP, Smartphone, FIDO U2F, Card**, and **PKI**. This helps users to authenticate outside the domain (for example, working from home or on a business trip) after the users have performed authentication in the online mode (when the Advanced Authentication server is available).

1.1.9 Swisscom Mobile ID Method

Advanced Authentication introduces the Swisscom Mobile ID method that allow users to authenticate on a phone with a Swisscom SIM card. For more information on configuring the method, see "Swisscom Mobile ID" in the *Advanced Authentication - Administration* guide.

1.2 Enhancements

Advanced Authentication 5.4 includes the following enhancements:

- Section 1.2.1, "Support for Windows 10 Anniversary Update," on page 3
- Section 1.2.2, "Support for Multiple Fingerprints," on page 3
- Section 1.2.3, "Enhanced Fingerprint Recognition," on page 3
- Section 1.2.4, "Support for Additional Operating Systems," on page 4
- Section 1.2.5, "Chain Selection in the Self-Service Portal," on page 4
- Section 1.2.6, "Certificate Management for PKI Method," on page 4
- Section 1.2.7, "Cached Login Support for PKI Method," on page 4
- Section 1.2.8, "New Charts in the Reporting Portal," on page 4
- Section 1.2.9, "Disabling 1:N," on page 4
- Section 1.2.10, "DigitalPersona Readers Support," on page 4
- Section 1.2.11, "Support for DESFire Cards," on page 4
- Section 1.2.12, "Elatec RFID Reader Support," on page 4
- Section 1.2.13, "Autodetection for Supported PKCS#11 Modules," on page 5
- Section 1.2.14, "Random Card ID Generation for LEGIC Readers," on page 5
- Section 1.2.15, "Support for Microsoft Authenticator," on page 5

1.2.1 Support for Windows 10 Anniversary Update

Advanced Authentication Windows Client now supports Windows 10 version 1607.

1.2.2 Support for Multiple Fingerprints

Users can now enroll multiple fingers for authentication that allows users to authenticate with another finger in case of injuries or minor cuts. For more information, see "Fingerprint" in the *Advanced Authentication - Administration* guide.

1.2.3 Enhanced Fingerprint Recognition

Advanced Authentication now provides an ability to record multiple captures of each fingerprint to improve the quality of fingerprint recognition. For more information, see "Fingerprint" in the *Advanced Authentication - Administration* guide.

1.2.4 Support for Additional Operating Systems

Advanced Authentication now supports the following operating systems:

- SUSE Linux Enterprise Server 12 Service Pack 1
- Red Hat Enterprise Linux Client 7.2
- Red Hat Enterprise Linux Server 7.2

1.2.5 Chain Selection in the Self-Service Portal

Administrators can now configure the **Authenticators Management** event to display the available methods in the login form. This helps users to select and use any of the enrolled chains to authenticate to the Self-Service Portal. For more information, see the event Authenticators Management in "Configuring Events" of the *Advanced Authentication - Administration* guide.

1.2.6 Certificate Management for PKI Method

Advanced Authentication now provides an ability to manage the trusted root certificates that are added for the PKI method. For more information, see "PKI" in the *Advanced Authentication - Administration* guide.

1.2.7 Cached Login Support for PKI Method

Advanced Authentication now provides support for cached login on the PKI method.

1.2.8 New Charts in the Reporting Portal

Advanced Authentication now contains new charts in the Reporting portal: **CPU load** and **Memory load**. This helps users to analyze the load on processor and memory.

1.2.9 Disabling 1:N

Administrators can now disable the `1:N` feature that allows to detect the user name automatically when authenticating with the Card and PKI methods. For more information, see the *Advanced Authentication - Windows Client* guide.

1.2.10 DigitalPersona Readers Support

Advanced Authentication now provides support for the DigitalPersona U.are.U fingerprint readers. For more information, see "Fingerprint Settings" in the *Advanced Authentication - Device Service* guide.

1.2.11 Support for DESFire Cards

Advanced Authentication now provides support for the DESfire cards.

1.2.12 Elatec RFID Reader Support

Advanced Authentication now provides support for the Elatec RFID reader with the Card plug-in of Device Service. For more information, see the *Advanced Authentication - Device Service* guide.

1.2.13 Autodetection for Supported PKCS#11 Modules

PKI plug-in of the Device Service now supports the automatic mode, where the known vendor modules are detected automatically. For more information, see the *Advanced Authentication - Device Service* guide.

1.2.14 Random Card ID Generation for LEGIC Readers

For the LEGIC readers that use the Smarfid plug-in of Device Service, administrators can now set an option to generate a random Card Identifier during an authenticator's enrollment. For more information, see the *Advanced Authentication - Device Service* guide.

1.2.15 Support for Microsoft Authenticator

Advanced Authentication now supports Microsoft Authenticator along with the Google Authenticator.

1.3 Software Fix

1.3.1 Support for 6 Digit HOTPs

Issue: You can now use 6-digit HOTPs for authentication. Previously, only 8-digit HOTPs were supported. `(Bug 949581)`

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.

- Section 2.1, "Issue With On-Screen Keyboard on Windows Tablet," on page 5
- Section 2.2, "Issue With Password Change in Card or PKI Authentication," on page 5
- Section 2.3, "Windows 10 Displays a Blank Screen After it Resumes from Sleep Mode," on page 6

2.1 Issue With On-Screen Keyboard on Windows Tablet

Issue: Sometimes the on-screen keyboard is not displayed to specify the user credentials on a Windows tablet.

Workaround: Restart your tablet.

2.2 Issue With Password Change in Card or PKI Authentication

Issue: Users are not able to change the password from the `Ctrl+Alt+Delete` menu, when using Card or PKI authentication and **Interactive login: Smartcard removal behavior** policy is enabled. When a user taps the card to authenticate to change the password, the **Interactive logon: Smartcard removal behavior** policy is initiated and the session is locked or logged off.

Workaround: Contact your administrator to reset the password and select the option **User must change password at next logon.**

2.3 Windows 10 Displays a Blank Screen After it Resumes from Sleep Mode

Issue: When resuming Windows 10 from sleep mode, sometimes a blank screen is displayed with buttons on the lower right side of the screen.

Workaround: Restart the operating system.

3 Upgrading

You can upgrade to Advanced Authentication 5.4 from Advanced Authentication 5.3, Advanced Authentication 5.3 Hotfix1 and 5.2.

For more information about upgrading, 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/.