Advanced Authentication 5.6 Release Notes

June 2017

Advanced Authentication 5.6 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 5.6 provides the following key features, enhancements, and fixes in this release:

1.1 New Features

This release introduces the following features:

1.1.1 Dashboard for the Administration Console

Administrators can now view a Dashboard that displays the graphical representation of data in the Administration console. Graphs in the form of widgets display information such as system metrics, tenant information, login status that helps administrators to track memory utilization, tenant information, successful or failed logins and so on. You can customize the widgets according to your requirement and view the graphs based on specific intervals or previous data. For more information, see "Managing Dashboard" in the *Advanced Authentication - Administration* guide.

1.1.2 Enforced Configurations in Multitenancy

The top tenant administrator can now enforce the configurations of specific policies, methods, chains, and events for particular tenants. These enforced settings are either disabled or hidden on the tenant administration console.

Some additional settings of methods are enforced completely such as the secondary tenant administrator will be unable to add new U2F or PKI certificates, or geo-zones. The top administrator cannot enforce the settings for ADFS partners, OATH Tokens, Authenticator Categories, Radius server, and Endpoints. For more information, see "Configuring Methods", "Configuring Events", "Creating a Chain", and "Configuring Policies" in the *Advanced Authentication - Administration* guide.

1.1.3 Enhanced Policies for the Smartphone Application

Administrators can now set the policies for **PIN** and **Fingerprint** and then enforce these configurations for the smartphones. Users will not be able to edit these settings. You can customize the minimum pin length and specify a custom logo for the About screen of the smartphone application.

For more information, see "Smartphone" in the *Advanced Authentication - Administration* guide.

1.1.4 Search Card Portal

Advanced Authentication introduces a portal to find out the user of an enrolled card. Information such as name of the card holder, repository information, email address, and mobile number of the user can be obtained by inserting the card in the card reader. For more information, see "Searching a Card Holder's Information" in the *Advanced Authentication - Administration* guide.

1.1.5 Client Login Extension Support for Windows Client

Windows Client is now integrated with Client Login Extension that facilitates password self-service by adding a link to the Windows login screen.

For more information, see "Client Login Extension Support for Windows Client" in the *Advanced Authentication - Windows Client* guide.

1.1.6 Single Sign-on Support for Remote Desktop and Citrix in Windows Client

Single sign-on support has been introduced for Microsoft and Citrix terminal servers. To achieve this, you must have the latest Windows Client installed on the terminal server. You can disable the single sign-on functionality by editing the configuration file. For more information, see "Configuring Single Sign-on Support for Citrix and Remote Desktop" in the *Advanced Authentication - Windows Client* guide.

1.1.7 Card Redirection

Device Service for Windows now supports Card and PKI redirection to Remote Desktop terminal sessions. You must install the new version of Device Service on terminal server.

1.2 Enhancements

Advanced Authentication 5.6 includes the following enhancements:

1.2.1 Extended Details for Windows Client Endpoints

You can now view the operating system version, Windows Client version, last session time, and time zone in the **Endpoints** section for the machines on which the new Windows Client is installed. For more information, see "Managing Endpoints" in the *Advanced Authentication - Administration* guide.

1.2.2 Enhanced Logon Filter

Previously, when the Logon Filter was configured and used, users who logged in to Windows Client were automatically moved from Legacy group to MFA group. Now administrators can configure the MFA group per chain to help sort users by corresponding groups according to the chain they use. For more information, see the *Advanced Authentication - Logon Filter* guide.

1.2.3 Improved Performance

Performance has been improved between Windows Client and Advanced Authentication server interaction and fingerprint use.

1.2.4 Logs for WebAuth

Advanced Authentication introduces logs for SAML 2.0 and OAuth 2.0 integrations. These logs are available in the **Logs** section and can be exported. For more information, see "Logging" in the *Advanced Authentication - Administration* guide.

1.3 Software Fixes

Advanced Authentication 5.6 includes the following software fixes:

1.3.1 Delayed Login on Windows Client

Issue: When users login to Windows Client, there might be a delay of several minutes because Windows Client tries to reach Advanced Authentication server each time when it gets a list of available chains for the user and when the network connection is slow. (`Bug 1028954`)

Fix: You can now enforce offline logon manually so that Windows Client does not try to reach an Advanced Authentication server but goes directly to cache. For more information, see "Configuring to Force Offline Login Manually" in the *Advanced Authentication - Windows Client* 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.

Advanced Authentication 5.6 includes the following known issues:

2.1 Issue With Advanced Authentication Deployment

Issue: You may not be able to deploy Advanced Authentication in environment where the NETBIOS name of repository is `LOCAL`.

3 Upgrading

You can upgrade to Advanced Authentication 5.6 from Advanced Authentication 5.3 and above. To upgrade from 5.2 and prior versions, contact NetIQ Technical Support.

For more information about upgrading, see “Upgrading Advanced Authentication” in the *Advanced Authentication Administration Guide*.

NOTE: ADFS plug-in will be discontinued with the Advanced Authentication 6.0 release. You can configure integration with ADFS through SAML. For more information, see “Configuring Integration with ADFS” in the *Advanced Authentication - Administration* guide.

You must now install Microsoft .NET Framework 4.0 to use fingerprint with Device Service 5.6 or you must set the parameter `fingerprint.isoSupported` to `false`.

Separate License for Multitenancy

You can now enable multitenancy through a license. Contact sales to get a new license if you use multitenancy and want to upgrade from a previous version.

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/.