Advanced Authentication 5.5 Release Notes

December 2016

Advanced Authentication 5.5 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 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 Per-site Configuration for LDAP Servers

It is now possible to customize LDAP servers per site. This helps the Advanced Authentication server to connect to LDAP servers from its own site.

1.1.2 Support for Multiple Enrollments

Advanced Authentication introduces authentication categories to support multiple enrollments. You can assign each category to a specific event. Users can enroll one authenticator of each type for every category. For more information, see “Event categories” in the *Advanced Authentication - Administration* guide.

1.1.3 Bluetooth Method

Advanced Authentication introduces an authentication method that allows you to use a Bluetooth device that is within range. With this feature, it is possible to automatically lock the Windows machine, if the Bluetooth device goes out of range. For more information, see “Bluetooth” in the *Advanced Authentication - Administration* guide.

1.1.4 Support for SAML 2.0

Advanced Authentication introduces support for the SAML 2.0 event. Using the SAML 2.0 event, you can enable multifactor authentication for users accessing third-party consumer web applications. For more information, see“SAML 2.0 options” in the *Advanced Authentication - Administration* guide.

1.1.5 Kerberos Single-Sign On for Advanced Authentication Web Portals

Advanced Authentication now supports integration with Kerberos. You can perform a single-sign on authentication to access the Advanced Authentication portals: Administrative portal, Self-Service portal, Helpdesk portal, and Reporting portal. For more information, see “Kerberos SSO Options” in the *Advanced Authentication - Administration* guide.

1.1.6 Password Filter

Advanced Authentication has extended the Logon Filter component with the Password Filter functionality. Password Filter allows administrators to perform automatic synchronization of password between the Advanced Authentication server and Active Directory, when a user changes password or an administrator resets a user’s password. For more information, see “ Configuring Password Filter” in the *Advanced Authentication - Logon Filter* guide.

1.1.7 Integration with Remote Desktop Gateway

Advanced Authentication introduces a plug-in that enables secured access of Remote Desktop Gateway by enforcing the multi-factor authentication. The plug-in must be installed on Remote Desktop Gateway and allows to add an advanced protection for the remote connection. You can authenticate to the Remote Desktop Gateway only with the out-of-band methods such as Smartphone, Voice Call, or Swisscom methods. For more information, see the *Advanced Authentication- Remote Desktop Gateway Integration* guide.

1.1.8 Support for Removal of User Authentication Data

Advanced Authentication administrators can now configure a policy called **Delete me options** that helps users to delete all their enrolled authenticators through the Self-Service Portal. For more information, see “Delete me options” in the *Advanced Authentication - Administration* guide.

1.1.9 Support for PKCS#7

Advanced Authentication now supports p7b format of parent certificates for the PKI method. For more information, see “PKI” in the *Advanced Authentication - Administration* guide.

1.1.10 Voice OTP Method

Advanced Authentication introduces the Voice OTP method that sends a One-Time Password (OTP) to your mobile through a voice call. For more information about configuring this method, see “Voice OTP” in the *Advanced Authentication - Administration* guide.

1.2 Enhancements

Advanced Authentication 5.5 includes the following enhancements:

1.2.1 Static IP Address

Administrators can now specify an IP address, subnet mask, gateway, and DNS servers during the installation of appliance instead of specifying in the Configuration Console. For more information, see ““Installing and Upgrading Advanced Authentication”” in the *Advanced Authentication - Administration* guide.

1.2.2 Normalization of Phone Numbers

Advanced Authentication now automatically trims hyphens, spaces, and non-numeric characters from the telephone numbers obtained from a user’s profile.

1.2.3 Phone Extension Support in the Voice Call

Now, the organizations that use phone numbers with extensions can configure the Voice Call method for authentication. For more information, see “Voice ” in the *Advanced Authentication - Administration* guide.

1.2.4 Web Authentication is Disabled by Default

The strong Web Authentication (used for OAuth2 and SAML2 events) is now disabled by default. This reduces RAM usage on the Advanced Authentication servers. (However, you can enable it when needed). For more information, see“Enabling Web Authentication” in the *Advanced Authentication - Administration* guide.

1.2.5 Card Waiting Timeout

Advanced Authentication introduces a timeout for the card waiting dialog of the Windows Client. By default, the timeout is 60 seconds and you can customize it. You can also configure an option that enables logon failure after the timeout. For more information, see “Configuring Timeout for Card Waiting” and “Enabling Logon Failure after Card Timeout”in the *Advanced Authentication - Windows Client* guide.

1.2.6 Support for Windows Server 2016

Logon Filter and Windows Client now support Windows Server 2016.

1.2.7 Option to Disable Built-in Certificate Check for FIDO U2F

You can now use your own attestation certificate instead of the built-in Yubico certificate for the U2F authentication. For more information, see “FIDO U2F” in the *Advanced Authentication - Administration* guide.

1.2.8 Yubico Format of Configuration File Supported for Yubico’s HOTP Tokens

Advanced Authentication now supports Yubico’s format of configuration file for Yubico’s HOTP tokens. Previously, only traditional format was supported.

1.2.9 Improved Authentication Speed With eDirectory

The authentication speed of eDirectory with Advanced Authentication has been increased.

1.3 Software Fixes

Advanced Authentication 5.5 includes the following software fixes:

- Section 1.3.1, “Cursor Focus on the Text Field and Buttons Is Lost in Windows,” on page 4
- Section 1.3.2, “Normalization of Phone Numbers,” on page 4
- Section 1.3.3, “Login Issue With the Self-Service Portal When Email Address Is Specified,” on page 5

1.3.1 Cursor Focus on the Text Field and Buttons Is Lost in Windows

Issue: If you try to enter a pin or OTP as part of your chain, the cursor loses its focus on the Text field and buttons. `(Bug 1000884)`

1.3.2 Normalization of Phone Numbers

Issue: In the SMS method, phone numbers are retrieved or read from a field in the Active Directory. This field may contain spaces, round brackets, and hyphens in the phone numbers and hence an SMS cannot be sent. `(Bug 1004512)`

1.3.3 Login Issue With the Self-Service Portal When Email Address Is Specified

Issue: When you specify the **mail** attribute in **User lookup attributes** of the **Advanced settings** in a user repository, then you cannot login to the Self-Service portal by specifying the email address in **user name**. `(Bug 1010603)`

Fix: Users can now log in to the Self-Service portal with an email address only when the Multitenancy option is disabled.

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, "The Workstation Gets Locked if a Bluetooth Device Is Locked," on page 5
- Section 2.2, "Issue With the Domain Users Group," on page 5
- Section 2.3, "Issue With Tenancy in Radius Clients," on page 5
- Section 2.4, "Incorrect Username Saved by Remote Desktop Connection," on page 5
- Section 2.5, "Linux and Mac OS X Clients Do Not Support Multiple Enrollment Per Method," on page 6

2.1 The Workstation Gets Locked if a Bluetooth Device Is Locked

Issue: When a Bluetooth device is locked after logging in to the operating system, the workstation also gets locked automatically.

Workaround: Ensure that each of the two devices, the device on which you authenticate and the device with which you authenticate, must have at least one pairing with any Bluetooth device.

2.2 Issue With the Domain Users Group

Issue: When users from the Domain Users group log in to the Self-Service Portal, the `Access denied` message appears.

Workaround: Ensure that you specify **AD** as **LDAP type** in the Repository configuration.

2.3 Issue With Tenancy in Radius Clients

Issue: Clients of the Radius server configured for one tenant can be used on other tenants.

Workaround: Presently, there is no workaround for this.

2.4 Incorrect Username Saved by Remote Desktop Connection

Issue: When the Logon Filter is used and if a user selects **Remember my credentials** while connecting to a terminal server with the Remote Desktop Connection, a wrong username is saved. When the user tries to login the next time, the wrong username is prompted.

Workaround: Do not select the option **Remember my credentials** while connecting to Remote Desktop.

2.5 Linux and Mac OS X Clients Do Not Support Multiple Enrollment Per Method

Issue: Linux PAM Client and Mac OS X Client are not updated in Advanced Authentication 5.5. The 5.4 version does not support multiple enrollments per method.

Workaround: Do not select the categories for the **Linux logon** and **Mac OS logon** events.

3 Upgrading

You can upgrade to Advanced Authentication 5.5 only from Advanced Authentication 5.4. To upgrade from 5.3 Hotfix1 and prior versions, contact NetIQ Technical Support.

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

NOTE: The components Linux PAM Client and Mac OS X Client have not been updated in this 5.5 release.

With Advanced Authentication 5.5, the **NotarisID** method has been removed because the Notaris service is no longer available.

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/.