

Advanced Authentication 5.3 Release Notes

April 2016



Advanced Authentication 5.3 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.

- ♦ [Section 1, "What's New?," on page 1](#)
- ♦ [Section 2, "Known Issues," on page 6](#)
- ♦ [Section 3, "Upgrading," on page 7](#)
- ♦ [Section 4, "Contact Information," on page 7](#)
- ♦ [Section 5, "Legal Notice," on page 7](#)

1 What's New?

Advanced Authentication 5.3 provides the following key features, enhancements, and fixes in this release:

- ♦ [Section 1.1, "New Features," on page 1](#)
- ♦ [Section 1.2, "Enhancements," on page 5](#)
- ♦ [Section 1.3, "Software Fixes," on page 5](#)

1.1 New Features

This release introduces the following new features:

- ♦ [Section 1.1.1, "Multisite Support," on page 2](#)
- ♦ [Section 1.1.2, "Device Service," on page 2](#)
- ♦ [Section 1.1.3, "Active Directory Federation Services Integration," on page 2](#)
- ♦ [Section 1.1.4, "Enhanced Windows Client and OS X Client," on page 2](#)
- ♦ [Section 1.1.5, "Offline Login Support for Windows Client," on page 2](#)
- ♦ [Section 1.1.6, "Second Factor Skipping," on page 3](#)
- ♦ [Section 1.1.7, "PKI Support," on page 3](#)

- ♦ [Section 1.1.8, “Localization,” on page 3](#)
- ♦ [Section 1.1.9, “Native LDAP Repository Support,” on page 4](#)
- ♦ [Section 1.1.10, “Reporting,” on page 4](#)
- ♦ [Section 1.1.11, “FIPS 140-2 Compliant Encryption,” on page 4](#)
- ♦ [Section 1.1.12, “Linux PAM Client,” on page 4](#)
- ♦ [Section 1.1.13, “User Data Migration Tool,” on page 4](#)
- ♦ [Section 1.1.14, “Multifactor Authentication in NAM,” on page 4](#)
- ♦ [Section 1.1.15, “NotarisID Support,” on page 4](#)

1.1.1 Multisite Support

This release introduces an ability to create sites that are based on the geographical position. Each site can include one DB Master server, two DB servers for backup and fail-over, and unlimited number of web servers to serve the workload.

1.1.2 Device Service

This release introduces the Device Service feature that helps you to combine and replace the following three separate services introduced in Advanced Authentication 5.2:

- ♦ Card Service
- ♦ FIDO U2F Service
- ♦ WBF Capture Service

Device Service is also supported on extensions such as PKI support for PKCS#11 compliant devices, Lumidigm fingerprint readers support, and LEGIC readers support.

This release introduces card support for Apple Mac OS X and Linux (except LEGIC readers).

1.1.3 Active Directory Federation Services Integration

This release introduces the ADFS plug-in component to integrate Advanced Authentication with Active Directory Federation Services 3 (ADFS 3). This integration enables you to perform strong authentication and access the systems more securely.

You must install the ADFS plug-in on each ADFS server in the ADFS farm. Each ADFS plug-in must be configured to work with the same Microsoft SQL database to share the internal state between different servers in the farm.

1.1.4 Enhanced Windows Client and OS X Client

In this release, Windows client and Mac OS X client have been redesigned and the user interface has been enhanced to support the different authentication methods with which you can perform strong authentication.

1.1.5 Offline Login Support for Windows Client

In this release, a new version of Windows client has been introduced. This Windows client supports caching of authenticators for authentication in the offline mode.

Offline login supports the following methods:

- ♦ Card

- ♦ Fingerprint
- ♦ FIDO U2F
- ♦ LDAP Password
- ♦ Password
- ♦ OATH TOTP and OATH HOTP
- ♦ Smartphone (offline mode)

1.1.6 Second Factor Skipping

You can now skip the second factor authentication for high security chains. You can configure a simple chain that can be used within a specified time frame, after the successful authentication with a high security chain.

For example, when a user has been authorized with the `LDAP Password+Card` method, which is a high-security chain, for next eight hours the user can use only the `Card` authentication and skip the `LDAP Password` authentication.

1.1.7 PKI Support

This release introduces support for Full PKI for PKCS#11 devices. The new method is implemented and supported for Microsoft Windows, Linux, Mac OS X, and NetIQ Access Manager.

1.1.8 Localization

This release introduces localization for Advanced Authentication Administrative portal, Helpdesk portal, Self Service portal, Windows client, and Mac OS X client.

The following are the supported languages:

- ♦ Arabic
- ♦ Chinese Simplified
- ♦ Chinese Traditional
- ♦ Danish
- ♦ Dutch
- ♦ French
- ♦ German
- ♦ Hebrew
- ♦ Italian
- ♦ Japanese
- ♦ Polish
- ♦ Portuguese (Brazilian)
- ♦ Russian
- ♦ Spanish
- ♦ Swedish

1.1.9 Native LDAP Repository Support

This release introduces support for RFC 2307 and RFC 2307 bis compliant LDAP repositories. You can use any LDAP as a user repository.

1.1.10 Reporting

This release introduces the reporting functionality. You can now access different security reports on the new Reporting portal.

1.1.11 FIPS 140-2 Compliant Encryption

In this release, you can enable FIPS 140-2 compliant encryption that is supported for new installations.

1.1.12 Linux PAM Client

This release introduces support for Linux with the pluggable authentication module. You can perform strong authentication on the following Linux distributive: CentOS 7 and SUSE Linux Enterprise Desktop 12.

1.1.13 User Data Migration Tool

This release introduces a new tool to migrate the existing customers from Advanced Authentication 4.x to 5.x by moving the existing authenticators to Advanced Authentication appliance database.

Advanced Authentication 5.3 supports the following authentication providers for migration:

- ♦ Lumidigm Authentication Provider (AP)
- ♦ OATH OTP AP
- ♦ Smartphone AP
- ♦ Universal Card AP
- ♦ Voice Call AP

1.1.14 Multifactor Authentication in NAM

This release allows you to configure the dynamic configuration, which is a universal configuration, on NetIQ Access Manager (NAM) only once. The dynamic configuration reads the configured chains for a NAM event from the Advanced Authentication Server. After you authenticate with a password in NAM, you can access a list of chains that you can use for further authentication. This helps you to authenticate with any of the authentication methods with the help of a single chain configuration.

Fingerprint and PKI authentication methods are now supported with the multifactor authentication.

1.1.15 NotarisID Support

This release introduces a new authentication method for Dutch notaries that is supported only for Windows login. Advanced Authentication sends a request to the NotarisID app on a notary's smartphone and the notary signs the authentication request.

1.2 Enhancements

Advanced Authentication 5.3 includes the following enhancements:

- ♦ [Section 1.2.1, “Exclude Crashed Servers from Future LDAP Requests,” on page 5](#)
- ♦ [Section 1.2.2, “Option to Manually Create Endpoint,” on page 5](#)
- ♦ [Section 1.2.3, “Option to Uninstall the NAM AA Plug-in,” on page 5](#)
- ♦ [Section 1.2.4, “HTML Support for Email Method,” on page 5](#)

1.2.1 Exclude Crashed Servers from Future LDAP Requests

In this release, if an LDAP server is unavailable, Advanced Authentication excludes the LDAP server from LDAP requests within 2.5 seconds for another 3 minutes.

1.2.2 Option to Manually Create Endpoint

You can now create an endpoint manually through the Advanced Authentication Administrative Portal. This can be used for the third-party applications that do not support creation of endpoints.

1.2.3 Option to Uninstall the NAM AA Plug-in

An option to uninstall the NAM plug-in has been introduced in this release.

1.2.4 HTML Support for Email Method

In this release, you can add a custom HTML code for the Email OTP method. This allows you to add a company's logo or custom markup for the emails containing OTP.

1.3 Software Fixes

Advanced Authentication 5.3 includes the following software fixes:

- ♦ [Section 1.3.1, “In Step-up Authentication, Ubikey Fails with NAM when Used as a Single Factor,” on page 5](#)
- ♦ [Section 1.3.2, “Last Login Name Display Issue with Advanced Authentication Windows Login Client,” on page 5](#)
- ♦ [Section 1.3.3, “Issue in Configuring Time Zone in the Administrative Portal,” on page 6](#)
- ♦ [Section 1.3.4, “Issue with the Locking Capability of a User Account,” on page 6](#)

1.3.1 In Step-up Authentication, Ubikey Fails with NAM when Used as a Single Factor

Issue: After a user authenticates with a standard method and then authenticates again with the U2F method, the authentication does not work. The U2F page prompts the user to press a button on the token, but does not blink. (Bug 970107)

1.3.2 Last Login Name Display Issue with Advanced Authentication Windows Login Client

Issue: In Windows Login client, an administrator is not able to hide the last login name when a machine starts because the Windows client does not support the **Interactive logon: Do not display last username** policy. (Bug 963045)

Fix: The **Interactive logon: Do not display last username** policy is now supported.

1.3.3 Issue in Configuring Time Zone in the Administrative Portal

Issue: Administrators are not able to change the time zone and time servers in the Administrative portal. (Bug 944048)

Fix: In the **Logs** section of the Administrative portal, a drop-down list with the time zones has been added. When an administrator changes a time zone, the logs on the section are displayed for the specified time zone.

1.3.4 Issue with the Locking Capability of a User Account

Issue: When a user specifies an incorrect SMS OTP or Email OTP for more than the specified number of failed attempts, the user account does not get locked. (Bug 946757)

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, “YubiKey with a 6 Digit HOTP Does Not Sync with a Token Counter,” on page 6](#)
- [Section 2.2, “Input Language Cannot be Changed on Windows Client Login,” on page 6](#)
- [Section 2.3, “Issue with Re-starting the Installation on Hyper-V,” on page 6](#)
- [Section 2.4, “Previous User Enrollments Are Displayed in the Helpdesk Module,” on page 6](#)

2.1 YubiKey with a 6 Digit HOTP Does Not Sync with a Token Counter

Issue: When a user synchronizes a YubiKey's counter or enrolls a YubiKey that contains a 6-digit OTP on the Advanced Authentication Enrollment Portal, an error is displayed.

Workaround: You must personalize (or flash) the YubiKey tokens to contain 8-digit OTPs. YubiKey with 6 digit OTPs are not supported.

2.2 Input Language Cannot be Changed on Windows Client Login

Issue: The option to change the input language on the Windows client login page is not available on the page.

Workaround: You can use a configured hot key to change the language.

2.3 Issue with Re-starting the Installation on Hyper-V

Issue: On Hyper-V, after the installation, an issue may occur with re-starting the installation.

Workaround: You must unmount the ISO image and restart the server.

2.4 Previous User Enrollments Are Displayed in the Helpdesk Module

Issue: While accessing a user's enrollments through the Helpdesk module, each time you access an additional user, the previous enrollments of the user, which must be hidden, are displayed before the current enrollments. (Bug 964054)

3 Upgrading

You can upgrade to Advanced Authentication 5.3 from Advanced Authentication 5.2.

For more information about upgrading, see “[Advanced Authentication 5.2-5.3 Upgrade](#)” in the *Advanced Authentication Server 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/>.

Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

