Advanced Authentication 6.0 Release Notes

May 2018

Advanced Authentication 6.0 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 6.0 provides the following key features, enhancements, and fixes in this release:

1.1 New Features

This release introduces the following features:

1.1.1 Facial Recognition Method

Advanced Authentication introduces the Facial recognition identification to leverage the use of face biometrics as a multi-factor authentication. Users will have to present their face to the camera to get authenticated in a matter of seconds.

For more information, see “Facial Recognition” in the *Advanced Authentication - Administration* guide.

1.1.2 Google reCAPTCHA

Advanced Authentication now supports the Google reCAPTCHA as a policy. Using reCAPTCHA, you can prevent the bot attacks on Advanced Authentication web portals by confirming that the user trying to log in is a human, not a robot. This adds an additional layer of security before users perform the multi-factor authentication.

For more information, see “Google reCAPTCHA Options” in the *Advanced Authentication - Administration* guide.

1.1.3 Web Authentication Method

Advanced Authentication facilitates the use of identity providers for OAuth 2.0, SAML, and OpenID Connect for web authentication. Administrators can configure the method with any of the identity providers. Users must enroll with any of these identity providers and get authenticated through them.

For more information, see “Web Authentication Method” in the *Advanced Authentication - Administration* guide.

1.1.4 Support for Windows Hello

Advanced Authentication now supports the Windows Hello authentication with the Fingerprint authenticator on the Windows 10 machine.

For more information, see “Windows Hello” in the *Advanced Authentication - Administration* guide.

1.1.5 New Reporting Portal

Advanced Authentication now provides a new Reporting portal. Administrators can add new reports and customize the existing reports on this portal. The new reports provide information about enrolled users, authenticators, and so on with better graphical representation.

For more information, see “Reporting” in the *Advanced Authentication - Administration* guide.

1.1.6 Enhanced User Interface

Advanced Authentication user interface has been enhanced to comply with the Micro Focus standards. The base operating system has changed from Debian to SUSE.

1.1.7 Policy to Use a Customized CSS

You can now use your customized CSS for all web portals of Advanced Authentication to modify the look and feel of the user interface to comply with the corporate colors and style.

For more information, see “Custom CSS” in the *Advanced Authentication - Administration* guide.

1.1.8 Custom Branding for SAML 2.0 and OAuth 2.0 Login Pages

You can now customize the branding and display of OAuth 2.0 and SAML 2.0 login pages in the **Web Authentication** policy. For more information, see “Web Authentication” in the *Advanced Authentication - Administration* guide.

1.1.9 Support for the SQL Repository

Advanced Authentication now supports the SQL repository. You can add the Microsoft SQL Server type of SQL repository to be consumed by the Advanced Authentication server. For more information, see “Adding an SQL Database” in the *Advanced Authentication - Administration* guide.

Advanced Authentication supports the Microsoft SQL Server 2016.

1.1.10 ADFS Multi-Factor Authentication Plug-in

A new Multi-Factor Authentication (MFA) plug-in has been introduced to enable the multi-factor functionality for Active Directory Federation Services (ADFS). In comparison with the old ADFS plug-in, the new plug-in has been implemented as a standard extension for ADFS.

For more information, see the *Advanced Authentication - ADFS MFA plug-in* guide.

1.1.11 Windows Authentication Agent

Authentication Agent allows you to perform strong multi-factor authentication on one computer to get authorized access to another computer where it is not possible to display the user interface or connect any external authentication devices. You can install the Authentication Agent on a workstation or laptop. When an authentication is initiated from a computer using Authentication Agent chain, the Authentication Agent on another computer prompts a restricted browser where user must perform authentication.

For more information, see “Authentication Agent” in the *Advanced Authentication- User* guide.

1.1.12 Tokens Management Portal

Advanced Authentication introduces a new portal where a Helpdesk administrator can upload a batch file that contains multiple tokens and can assign a token to specific users for the OATH authentication method.

For more information, see “Managing Tokens” in the *Advanced Authentication - Administration* guide.

1.1.13 Swedish BankID Method

Advanced Authentication allows users to authenticate with their Swedish Personal Identification Number. Users must configure the BankID app (desktop or mobile version) with the Personal Identification Number, activation, and security code.

For more information, see “Swedish BankID” in the *Advanced Authentication - Administration* guide.

1.1.14 Custom Localization Support

Advanced Authentication allows an administrator to customize the method and chain names in a preferred language. The customized names are reflected on the Advanced Authentication portals and clients.

For more information, see “Configuring Methods” and “Creating a Chain” in the *Advanced Authentication - Administration* guide.

1.2 Enhancements

Advanced Authentication 6.0 includes the following enhancements:

1.2.1 Server Enhancements

Advanced Authentication 6.0 includes the following enhancements on the server:

1.2.1.1 Provision to Add Custom RADIUS Event for Specific RADIUS Clients

Previously, an administrator was able to add multiple RADIUS Clients to only the predefined **RADIUS Server** event and all the RADIUS Clients had to use the same set of authentication chains. Now, administrators can create a custom RADIUS event to use it for specific RADIUS Client.

For more information, see "Creating a RADIUS Event" in the *Advanced Authentication - Administration* guide.

1.2.1.2 Support for Facets in U2F

Administrators can now add a list of facets for the FIDO U2F tokens to work on multiple sub-domains of a single domain. This allows users to enroll the FIDO U2F tokens on a single domain and get authenticated on multiple sub-domains.

NOTE: The facets are supported only on the Google Chrome. The support for sub-domains is not stabilized in Chrome, so you may get an error message `The visited URL doesn't match the application ID or it is not in use` during enrollment and authentication.

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

1.2.1.3 Language Support for Canadian French

Now, Advanced Authentication supports the Canadian French language.

1.2.1.4 FIPS Enabled by Default

Now, FIPS has been enabled by default.

1.2.1.5 Integration with Citrix StoreFront, Google G Suite, and Office 365

This release adds support for integration of Advanced Authentication with the following third party solutions:

- Citrix StoreFront using SAML
- Google G Suite
- Office 365

For more information, see "Configuring Integration with Citrix StoreFront", "Configuring Integration with Google G Suite", and "Configuring Integration with Office 365" in the *Advanced Authentication - Administration* guide.

1.2.1.6 Enhanced Local Cache for the LDAP Password Method

This release introduces the **Enable cached logon** option in the **LDAP Password** method to validate the user's password with the password cached in the Advanced Authentication server.

If the password does not match with the cached password or it is not stored on the Advanced Authentication server, the following actions are performed:

- The cached value is reset
- Advanced Authentication server contacts the LDAP server to validate the user password.

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

Previously, while authenticating a user, Advanced Authentication server contacted the LDAP server to validate the user's password that caused performance issues.

1.2.1.7 New Widgets on the Dashboard

This release introduces the following widgets on the dashboard:

- **Users**
- **Authenticators**
- **Licenses**
- **Enroll Activity Stream**

These widgets help administrators to collect more information about enrolled users, authenticators, active licenses, and so on.

For more information, see “Managing Dashboard” in the *Advanced Authentication - Administration* guide.

1.2.1.8 Exporting Widgets

Now, administrators can export the dashboard widgets to CSV or JSON formats.

For more information, see “Exporting Widgets” in the *Advanced Authentication - Administration* guide.

1.2.1.9 Identify User and Authentication Method for Web Authentication

Previously, while authenticating on the web pages using SAML or OAuth, users had to specify their username twice during the multi-factor authentication. With the **Identify User and Authentication** method, users are not prompted to specify their user name for a second time.

1.2.1.10 Support for Custom Smartphone Apps

Advanced Authentication now supports third-party vendors for the Smartphone apps. The **Vendor ID** option for iOS app and **Google Project ID** option for Android app have been introduced in the Smartphone settings of the Administration portal. The push notification is sent only to the app whose **Vendor name** or **Google Project ID** matches with the app. By default, the Smartphone method works with the NetIQ Auth apps.

For more information, see “Smartphone” settings in the *Advanced Authentication - Administration* guide.

1.2.1.11 NetIQ App Support for the Google Authenticator Format

The NetIQ App can now be used to scan the QR code when the Google Authenticator format is enabled. Previously, the QR code could be scanned only with the Google Authenticator or Microsoft Authenticator apps.

This support is applicable only for the Android and iOS apps. It does not apply for the Windows Phone app.

For more information, see “OATH OTP” in the *Advanced Authentication - Administration* guide.

1.2.1.12 Enhanced Syslog to Track Events and Chain Logs

Advanced Authentication Syslog now records all the actions performed by the administrators such as adding, updating, and deletion of all events and chains in the appliance.

For more information see, “Syslog” in the *Advanced Authentication - Administration* guide.

1.2.1.13 Ability to Import the Database/New Migration Method

Advanced Authentication introduced the export database feature in 5.6 Patch Update 3. With 6.0, you can import the database. You can use this functionality to migrate from version 5 as well as migrating the database to next versions.

For more information, see “Exporting and Importing the Database” in the *Advanced Authentication - Administration* guide.

1.2.1.14 Support for Feitian U2F Tokens

By default, certified Feitian attestation certificates have been added for the FIDO U2F authentication in the Advanced Authentication appliance.

For more information, see “Configuring the Certificate Settings” settings in the *Advanced Authentication - Administration* guide.

1.2.1.15 Provision to Add the Custom Attestation Certificate for the FIDO U2F Method

Advanced Authentication now allows an administrator to delete the pre-configured attestation certificate and add the custom attestation certificate to the FIDO U2F compliant token for authentication.

For more information, see “Configuring the Certificate Settings” settings in the *Advanced Authentication - Administration* guide.

1.2.1.16 Ability to Unlock Users By the Helpdesk Administrator

An option to unlock the users who have been locked in the Advanced Authentication server local repository has been added to the Helpdesk portal. The Helpdesk administrator can unlock these users and allow them to authenticate.

For more information, see “Helpdesk Options” in the *Advanced Authentication - Administration* guide.

1.2.1.17 Policy to Hide a Required Chain

Advanced Authentication introduces the **Linked Chain** policy that allows administrators to hide the required (high security) chain after users authenticate with the required chain within a grace period. With this policy, only the linked chain is displayed to the users in place of both the required and linked chain within the grace period.

For more information, see “Linked Chains” in the *Advanced Authentication - Administration* guide.

1.2.1.18 New Fingerprint Matching Service

Advanced Authentication now uses the NBIS as a fingerprint matching engine in the server. The new engine improves the quality of fingerprint recognition, specially for inexpensive swipe sensors.

NOTE: After migrating from Advanced Authentication v5, users may need to re-enroll the Fingerprint authenticators if they have enrolled the authenticators on the WBF compliant readers. This is because, the previous authenticators may contain low quality fingerprint images. Re-enrollment for the Lumidigm and Digital Persona readers is not required.

1.2.1.19 Option to Bypass User Lockout in Repository

Previously, users locked in a repository (Active Directory) were not able to authenticate on Advanced Authentication. Now, administrator can allow users who are locked in a repository to authenticate on Advanced Authentication using the **Bypass user lockout in repository** option in Events. This option may be required for integrations such as Self Service Password Reset integration.

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

1.2.2 Client Enhancements

1.2.2.1 Support for High Resolution Display on Windows Client

Advanced Authentication now supports different resolutions of display on the Windows Client. Previously, on the Windows Client that has smaller screen with a high resolution, the window was very smaller in size. The text and controls were not readable.

1.2.2.2 Diagnostic Tool for Mac OS

Advanced Authentication provides a Diagnostic Tool that allows users to collect logs from the Mac OS X Client, and Device Service. The Diagnostic Tool also validates connection to the Advanced Authentication servers.

For more information, see "Collecting Debug Logs" in the *Advanced Authentication - Mac OS X Client* guide.

1.2.2.3 Support to Customize Login Screen Background for Windows 7

This release enables users to customize the background image of the login screen in Windows 7.

For more information, see "Customizing Logon Page Background Screen" in the *Advanced Authentication - Windows Client* guide.

1.2.2.4 Installer for Mac OS Client and Device Service

This release provides a new install package of the Device service and Mac OS client for Mac OS. The uninstaller scripts to remove these components automatically are also available. For more information, see “Installing and Uninstalling Mac OS X Client” in the *Advanced Authentication - Mac OS X Client* guide.

1.2.2.5 Customization of Logo for the Mac OS Client

Advanced Authentication now allows the administrators to change the default logo and set a customized logo in the Mac OS Client.

For more information, see “Customizing a Logo” in the *Advanced Authentication - Mac OS X Client* guide.

1.2.2.6 Support for Multiple Fingerprint Reader Modes

Now, Advanced Authentication Device Service for Windows allows you to configure multiple fingerprint reader modes to use more than one fingerprint reader mode without switching the modes in the configuration file. By default, the `fingerprint.mode` is set to `auto` that enables the Lumidigm, DigitalPersona, and WbfDirect modes.

For more information see, “Fingerprint Settings” in the *Advanced Authentication - Device Service* guide.

1.2.2.7 Enhanced Single Sign-On Behavior to Access Remote Desktop

Now, Advanced Authentication introduces an option to validate the Windows Client installation on a terminal client and allows Single Sign On (SSO) only in the situations. Previously, the SSO feature for a Remote Desktop connection overlooked the Windows Client installation on the terminal client and allowed SSO, which may not be secure.

For more information, see “Configuring Single Sign-on Support for Citrix and Remote Desktop” in the *Advanced Authentication - Windows Client* guide.

1.2.2.8 Voice OTP for Linux and Mac

Advanced Authentication now supports the Voice OTP authenticator for Linux and Mac.

For more information see, “Voice OTP” in the *Advanced Authentication- User* guide.

1.2.2.9 Support for Cisco AnyConnect Start Before Login and Microsoft VPN

Previously, the VPN icon was not being displayed on the Windows login screen. The icon was being filtered with the Windows Client Credential Provider. Now, Advanced Authentication removes the filter for Pre-Logon-Access Provider (PLAP) and displays this icon on the login screen.

1.2.2.10 Support for New Versions of Operating Systems

This release extends support to the following operating systems:

- Debian 9.4
- Ubuntu 18.04
- SUSE 11 Service Pack 3 and 4
- SUSE 12 Service Pack 3
- Mac OS High Sierra
- Red Hat Linux 7.5
- Microsoft Windows 10 v1803

1.2.2.11 Support for Multiple Discovery Hosts

When a DNS discovery for the servers is not used, Advanced Authentication allows you to specify more than one Advanced Authentication server. This is supported for Windows Client, Linux PAM Client, and Mac OS Client.

For more information, see "Using a Specific Advanced Authentication Server" in the *Advanced Authentication - Windows Client* guide.

1.2.2.12 Basic Events Logged in the Eventlog for Windows Client

All events of the Windows Client are now logged in the Application logs of **Event Viewer**. These logs provide information about login, server connections, and so on.

For more information, see "Logging for Windows Specific Advanced Authentication Events" in the *Advanced Authentication - Windows Client* guide.

1.2.2.13 Support for Card Timeout on the Mac OS Client

You can now configure the card waiting timeout for Card authentication on Mac OS Client.

For more information, see "Configuring Timeout for Card Waiting" in the *Advanced Authentication - Mac OS X Client* guide.

1.2.2.14 Support for RFIDeas Card Readers on Linux and Mac

This release extends the support for the RFIDeas card readers to Linux and Mac Clients.

1.2.2.15 Help Button for Advanced Authentication Portals

Context-sensitive help has been added to the Authenticators Management (Self-Service), Helpdesk, Search Card, and Tokens Management portals of Advanced Authentication. Users can read the related documentation, when they click the Help button on the respective portals.

1.2.2.16 Mac OS Client Is Supported for the Fast User Switching

Previously, native Mac OS authentication was used for the fast user switching. Now, Advanced Authentication uses the authentication window of the Mac OS Client for the fast user switching.

1.2.2.17 Support for Cache in Linux and Mac

Cache support has been extended to Linux and Mac Clients.

1.2.3 Security Enhancements

Advanced Authentication contains the following security enhancements in 6.0:

1.2.3.1 Windows Client Uses OpenSSL instead of DPAPI

Advanced Authentication now uses OpenSSL instead of DPAPI to comply to the FIPS standards.

1.2.3.2 Encryption of Few Parameters in the Configuration Files

The `endpoint id` and `endpoint_secret` have been encrypted in the configuration files.

1.2.3.3 XML External Entity (XXE) Injection Vulnerability in the PSKC Import

The XML External Entity (XXE) injection vulnerability has been removed during the importing of the PSKC import.

1.2.3.4 Verification of the Server Certificate in Linux and Mac

To secure connection between Linux endpoints and Advanced Authentication server, you must insert the server certificates in one of the following path:

- PAM specific
- Operating System specific

Enable the verification of a certificate after inserting the certificate in the preferred path. For more information see, "Configuration for Verification of Server Certificates" in the *Advanced Authentication-Linux PAM Client* guide.

You can also enable the verification of a certificate in Mac endpoints to secure the connection between the respective endpoint and Advanced Authentication server. For more information see, "Configuration for Verification of Server Certificates" in the *Advanced Authentication - Mac OS X Client* guide.

1.3 Software Fixes

Advanced Authentication 6.0 includes the following software fixes:

1.3.1 Appliance DNS Suffix

Issue: When users send any request with only the host name instead of Fully Qualified Domain Name (FQDN) to the server, the server does not respond. (*Bug 1020827*)

Fix: Now, users can provide only the host name to send a request to the server to receive appropriate response.

1.3.2 NetIQ Access Manager 4.4 Authentication Fails Due To URL Redirection

Issue: When users log in to NetIQ Access Manager 4.4 in path based acceleration setup, the Access Gateway forwards the request to the Self-Service portal URL (`https://<aa server>/account/`). Advanced Authentication server performs URL redirection and provides a redirect URL without trailing backslash (`https://<aa server>/account`), Access Gateway adds trailing backslash to the redirect URL, which causes a loop and the valid page is not displayed. *(Bug 1062262)*

Fix: Now, valid URLs (with or without trailing backslash) of a specific page is mapped to the relevant HTML page.

1.3.3 Password Synchronization Message Updated

When a user log in to Windows workstation using the Windows Client for the first time, a message that prompts the user to synchronize the password is updated to `Password must be synchronized`. (*Bug 1030020*)

1.3.4 Unable to View the Workstation Name on the Login Screen

In the Windows Client, when a user specifies backslash (\) in **User name**, a message `Sign in to <workstation name>` is not displayed. (*Bug 1063099*)

1.3.5 WebAuth Service Issue with Self Service Password Reset

Issue: After a successful login to the Self Service Password Reset (SSPR) service through Advanced Authentication, an idle WebAuth session is active in the background. After a duration of one hour, if a user tries to access SSPR again, the WebAuth service displays an error message `Access Denied` due to the endpoint session timeout. (*Bug 1049204*)

Fix: When users try to access Self Service Password Reset, a new WebAuth session is initiated to allow users to access the Self Service Password Reset service.

1.3.6 Issue with the OAuth 2.0 Event

Issue: When a user logs in to the OAuth 2.0 event, an error message `Invalid authentication method` is not displayed though one of the following condition is true:

- Chain is not assigned to the OAuth event.
- User has not enrolled to the method that is assigned to the OAuth event. (*Bug 1047448*)

Fix: With this release, if the method is not assigned or methods available in the chain are not enrolled, a valid message is displayed.

1.3.7 Man in the Middle (MITM) Vulnerability

This release also addresses a potential Man in the Middle (MITM) attack in the versions prior to Advanced Authentication 6.0. Special thanks to Octav Opaschi, of Detack GMBH, for responsibly disclosing this to us. *(CVE-2019-11650)*

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 6.0 includes the following known issues:

2.1 Issue with the Linux Client

Issue: When a local (non-domain) user logs in to the Linux Client, a chain that is assigned to a domain-user authentication is prompted in place of the local user name form.

2.2 Issue with Authentication Window in the Mac Client

Issue: On the Mac Client, when a user clicks the  icon in the lower-right corner of the **System Preferences** dialog box, the Mac authentication window is displayed in place of the Advanced Authentication window.

Workaround: To display the Advanced Authentication window, execute the command: `defaults write com.apple.Preferences UseSheets -bool FALSE`

2.3 Issue with the Fingerprint Method Enrollment on Mozilla Firefox Quantum Browser

Issue: When a user enrolls the Fingerprint method on the Mozilla Firefox Quantum browser, the enrollment fails and a message `Cannot reach the server` is displayed.

Workaround: To enroll the Fingerprint method on the Mozilla Firefox Quantum browser, import the `rootCA.crt` file from the `Device Service` folder to the Trusted Root Certification Authorities certificate store of the computer.

2.4 Configuration Error While Installing Advanced Authentication

Issue: When you install Advanced Authentication with Dynamic Host Configuration Protocol (DHCP), an error is displayed and the network is not configured on the server.

Reason: This error occurs because of the Yet another Setup Tool (YaST) configuration available in the Open SUSE.

2.5 Issue with Domain Joined Mac Client

Issue: On Mac 10.13.4 machine, when a domain user logs in for the first time to the domain joined Mac Client using any of the available authentication chain, the Mac machine gets stuck and a network account is not created for the new domain user. This issue happens, when one of the following condition is true:

- The user does not have a mobile account on the Mac machine.
- The **Create mobile account** is turned **OFF** during login.

2.6 Issue While Installing the Advanced Authentication Server with a Static IP

Issue: When you install the Advanced Authentication server with a static IP address, the installation gets stuck in the **Network Settings** screen in some instances.

Workaround: You must wait for few hours or try to install the server again.

3 Upgrading

Upgrading Advanced Authentication 5.6 to 6.0 is not supported. However, you can export the configurations from Advanced Authentication 5.6.341 to 6.0. After you install Advanced Authentication 6.0, you can import all the configurations from 5.6.341.

For example, to upgrade from Advanced Authentication 5.5 to 6.0, you must first upgrade from Advanced Authentication 5.5 to 5.6.341. Then, you must install 6.0 and import the configurations from 5.6.341.

For more information about upgrading, see "Migrating Advanced Authentication to 6.0" in the *Advanced Authentication- Server Installation and Upgrade* guide.

NOTE: This release discontinues the ADFS plug-in. You can configure integration with ADFS using the ADFS MFA Plug-in or through SAML. For more information, see "Configuring Integration with ADFS" in the *Advanced Authentication - Administration* guide and *Advanced Authentication - ADFS MFA plug-in* guide.

After migrating from Advanced Authentication v5, users may need to re-enroll the Fingerprint authenticators if they have enrolled the authenticators on the WBF compliant readers. This is because, the previous authenticators may contain low quality fingerprint images. Re-enrollment for the Lumidigm and Digital Persona readers is not required.

---

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/.