Advanced Authentication 5.6 Patch Update 1 Release Notes

August 2017

Advanced Authentication 5.6 Patch Update 1 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 Patch Update 1 provides the following enhancements and fixes in this release:

1.1 Enhancements

Advanced Authentication 5.6 Patch Update 1 includes the following enhancements:

1.1.1 Virtual Channel Support

Advanced Authentication Device Service for Windows now supports virtual channel. You must install Device Service on both terminal client and terminal server to perform the redirection of the device that is used for authentication (for example, a fingerprint reader) into the terminal session.

1.1.2 Advanced Authentication Integration with Google G Suite

You can now integrate Advanced Authentication with the Google G Suite by using SAML 2.0. For more information, see "Configuring Integration with Google G Suite" in the *Advanced Authentication - Administration* guide.

1.1.3 Session Lock on U2F Removal

The Advanced Authentication FIDO U2F method now supports the standard Microsoft policy **Interactive logon: Smart card removal behavior**. Administrators can now configure settings to perform a force log off or automatically lock a session when a user removes the U2F device from the computer. For more information, see "FIDO U2F" in the *Advanced Authentication - Administration* guide.

1.1.4 Card Redirection Support in Device Service

Advanced Authentication Device Service for Windows now supports Card and PKI redirection to Citrix terminal sessions. You must install Device Service on the terminal server to perform the redirection.

1.1.5 Password Change for Users Who Are Not Logged In

Previously, on a Windows machine that has the Windows Client installed, the password could be changed only for the logged in users. Now, users can change the password for other accounts after authentication is done in another account.

1.1.6 Support for Access-Challenge in RADIUS Authentication Provider

When the Advanced Authentication server acts as a RADIUS Client and the RADIUS server sends an **Access-Challenge** request (for example, a request to the user to change the password, to provide a second-factor authentication), the Advanced Authentication server forwards this request to the client.

1.1.7 Framed IPv4 Address Attribute

The **Framed IPv4 Address Attribute** has been introduced in the Administration portal for the **RADIUS server** event. When the attribute is not specified, the value of `msRADIUSFramedIPAddress` for Active Directory and `radiusFramedIPAddress` attribute for other LDAP repositories is returned as `Framed-IP-Address`.

You can specify any other attribute in **Framed IPv4 Address attribute** to return the value of the specified attribute as the `Framed-IP-Address` instead of the `msRADIUSFramedIPAddress` and `radiusFramedIPAddress` attributes. For more information, see "Framed IPv4 Address Attribute" in the *Advanced Authentication - Administration* guide.

1.1.8 Support for NXP PR533

This release adds support for the **NXP PR533** reader.

1.1.9 Test Option for SMS, Email, and Voice in Administration Portal

Administrators can now test the configuration settings for **Mail sender**, **SMS sender,** and **Voice sender** policies in the Administration portal. For more information, see "Mail Sender", "SMS Sender", and "Voice Sender" policies in the *Advanced Authentication - Administration* guide.

1.1.10 Enhanced API

This release provides the following API enhancements:

- Public API has been added to the **Delete Me** feature.
- Public REST API has been added to the event creation.
- Status API has been enhanced.
- Support for the OAuth 2 authentication provider has been added to support login to the REST API through the OAuth 2 access token.

1.1.11 Free Space Indicator in Dashboard

The **Server** widget has been added to Dashboard in the Administration portal as an indicator to display the free space available in the appliance and provides a way to monitor CPU and memory usage. This is helpful when you want to perform an upgrade. Also, you can check the free space in the **Updates** tab.

1.2 Software Fixes

Advanced Authentication 5.6 Patch Update 1 includes the following software fixes:

1.2.1 Smartphone Does Not Work in Secondary Sites

Issue: When you use Smartphone authentication in a multi-site infrastructure and configure Smartphone in a primary site, users are not able to authenticate on servers from the other sites.

Fix: The Smartphone configuration is now stored per site and you must configure the Smartphone URL for each site. For more information, see the policy " Public External URLs (Load Balancers)" in the *Advanced Authentication - Administration*.

1.2.2 RADIUS Configuration Does Not Sync Between the Sites

Issue: When you configure RADIUS Clients on an Advanced Authentication server in site A and it shows the servers in Site B, but the configuration does not work. This is because Advanced Authentication Administration portal displays the settings stored in the database, however, the settings are missed in a RADIUS configuration file on other servers. You have to apply the settings on each server.

1.2.3 Performance Issue With RADIUS Server

Issue: When the Advanced Authentication server is used as a RADIUS proxy, sometimes the Advanced Authentication server throws an error: `Discarding duplicate request from client` into the logs.

Fix: The performance of RADIUS server has been increased in high-load scenarios.

1.2.4 Issue with a Proxy Server

Issue: You cannot perform an upgrade if the proxy server uses authentication.

1.2.5 All Advanced Authentication Portals Require Access to /admin/api

Issue: `/admin/api` is used to access all portals and if you prohibit access to `/admin`, you will not be able to login to the Self-Service portal.

Fix: The Advanced Authentication server now uses `/user/api` to access the portals.

1.2.6 The 1:N Feature Does Not Work in RDP

Issue: The 1:N feature does not work when you initiate authentication with a card after connecting to a remote desktop connection to a server where the single sign-on is disabled.

1.2.7 WebAuth Logs Are Not Limited in Space

Issue: Previously, the WebAuth logs had no space limit in size. When logging was enabled, error occurred due to the nonavailability of free space in the Administration portal.

Now, the WebAuth log's size is limited.

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 Patch Update 1 includes the following known issues:

2.1 DigitalPersona Readers Do Not Work for SAML 2.0 and OAuth 2.0 Integrations

Issue: When you place your finger on the reader, the screen redirects to the chain selection screen without any errors.

2.2 Error in Dashboard After Upgrade

Issue: After upgrading from Advanced Authentication 5.6 to 5.6 Patch Update 1, an error `Access was denied to this resource.(AuError)` is displayed in the **Dashboard** page and an error `Error Bad Request` is displayed in the **Tenants** widget. This error happens because from 5.6 Patch Update 1, the tenant information is available only in the Multitenancy mode.

Workaround: Remove the **Tenants** widget.

2.3 Error While Setting Up a Global Master

Issue: While setting up a Global Master server in the **Cluster** section, you may get an error `Replica operation is already in progress (updates the status?), please retry (AUError).`

Workaround: You can ignore the error. The Global Master server will be set up without any issues even with the error.

2.4 Issue with Voice Method After Upgrade

Issue: After upgrading to Advanced Authentication 5.6 Patch Update 1, the Voice method stops working and the **Server URL** field in the **Voice Sender** policy changes to https://global.sol. This issue happens because of the "Public External URLs (Load Balancers)" in the *Advanced Authentication Administration Guide*.

Workaround: You must configure the URL again.

3 Upgrading

You can upgrade to Advanced Authentication 5.6 Patch Update 1 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*.

IMPORTANT: If you use Advanced Authentication server as a RADIUS server and have configured different RADIUS clients in different Advanced Authentication sites, then after upgrading to 5.6 Patch Update 1, the RADIUS configuration will be synchronized between the sites. You must add all the RADIUS clients in a single site. The configuration will be replicated to the servers in other sites.

WARNING: If you deny access to some of the Advanced Authentication server URLs with firewall, you must update rules because of the fix All Advanced Authentication Portals Require Access to /admin/api. Advanced Authentication no longer requires `/admin/api` to access the Advanced Authentication portal. Instead, the server uses `/user/api`.

---

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/.