

Advanced Authentication 6.1 Release Notes

October 2018



Advanced Authentication 6.1 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 6.1 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 3](#)
- ♦ [Section 1.3, "Software Fixes," on page 8](#)

1.1 New Features

This release introduces the following features:

- ♦ [Section 1.1.1, "Kubernetes Support," on page 1](#)
- ♦ [Section 1.1.2, "Desktop OTP Tool," on page 2](#)
- ♦ [Section 1.1.3, "Another Way to Enroll Smartphone Method," on page 2](#)
- ♦ [Section 1.1.4, "FIDO 2.0 Method," on page 2](#)
- ♦ [Section 1.1.5, "Virtual Smartcard Support," on page 2](#)
- ♦ [Section 1.1.6, "IIS Authentication Plug-in," on page 2](#)

1.1.1 Kubernetes Support

This release supports deployment of Advanced Authentication on the Amazon Elastic Container Service for Kubernetes (Amazon EKS) and Azure Kubernetes Service (AKS).

For more information, see the ["Deploying Advanced Authentication on Amazon Web Services"](#) and ["Deploying Advanced Authentication on Azure Kubernetes Services"](#) in the [Advanced Authentication-Server Installation and Upgrade](#) guide.

1.1.2 Desktop OTP Tool

This release introduces Desktop OTP tool that enables you to generate time-based one-time password (TOTP). This tool is used for enrolling TOTP method on the Advanced Authentication server. Later, you can use the tool to generate a one-time password which can be used for authenticating to any device and service that is secured with the TOTP method of Advanced Authentication.

For more information, see the [Advanced Authentication - Desktop OTP Tool](#) guide.

1.1.3 Another Way to Enroll Smartphone Method

This release enables you to enroll the Smartphone method by using the link that has been provided by your administrator through email or SMS. Click the link on your smartphone where the NetIQ Auth app is installed to initiate the smartphone app where you can enroll and create an authenticator.

For more information, see “[Configuring Enrollment Link](#)” in the [Advanced Authentication - Administration](#) guide.

1.1.4 FIDO 2.0 Method

The FIDO 2.0 method facilitates the use of FIDO compliant devices for authenticating users to the web-based environment. The FIDO 2.0 complied devices need to register with the browser that supports web authentication. Devices can be of both types: built-in to the platform or externally connected through USB. The FIDO 2.0 method uses the Web Authentication (WebAuthn) API and Client to Authenticator Protocol (CTAP).

For more information, see “[FIDO 2.0](#)” in the [Advanced Authentication - Administration](#) guide.

1.1.5 Virtual Smartcard Support

Advanced Authentication facilitates administrators to configure virtual smartcard support for the PKI method. Users can enroll the PKI method using a virtual smartcard that is imported to the browser on the user’s system.

A virtual smartcard is a client SSL certificate that contains information such as digital signature, expiration date, name of user, name of CA (Certificate Authority), and so on. The information available in the virtual smartcard is used to authenticate the user to the web portals that are integrated with Advanced Authentication using OAuth 2.0.

For more information, see “[Virtual Smartcard](#)” in the [Advanced Authentication - Administration](#) guide.

1.1.6 IIS Authentication Plug-in

Advanced Authentication introduces IIS Authentication plug-in. Using this plug-in, users can perform the multi-factor authentication to access websites that are hosted and managed on the Microsoft IIS server.

For more information, see the [Advanced Authentication - IIS Authentication Plug-in](#) guide.

1.2 Enhancements

Advanced Authentication 6.1 includes the following enhancements:

- ♦ [Section 1.2.1, “Server Enhancements,” on page 3](#)
- ♦ [Section 1.2.2, “Client Enhancements,” on page 5](#)
- ♦ [Section 1.2.3, “Security Enhancements,” on page 7](#)

1.2.1 Server Enhancements

Advanced Authentication 6.1 includes the following enhancements on the server:

- ♦ [Section 1.2.1.1, “Customizing Authentication Request Message for the Smartphone Method,” on page 3](#)
- ♦ [Section 1.2.1.2, “Endpoint Management Support for Helpdesk Administrators,” on page 3](#)
- ♦ [Section 1.2.1.3, “Option to Add More Than One RADIUS Servers for a Specific Site,” on page 4](#)
- ♦ [Section 1.2.1.4, “Cache Time Expiration,” on page 4](#)
- ♦ [Section 1.2.1.5, “User Interface to Monitor Replication Batches,” on page 4](#)
- ♦ [Section 1.2.1.6, “Option to Disable the Offline Authentication for Smartphone Method,” on page 4](#)
- ♦ [Section 1.2.1.7, “Option to Customize the Branding of ADFS MFA Plug-in Templates,” on page 4](#)
- ♦ [Section 1.2.1.8, “Managing Reporting History,” on page 4](#)
- ♦ [Section 1.2.1.9, “General Data Protection Regulation Compliance,” on page 4](#)
- ♦ [Section 1.2.1.10, “Enhanced Syslog to Track Administrator Activities,” on page 5](#)
- ♦ [Section 1.2.1.11, “Enhanced API,” on page 5](#)
- ♦ [Section 1.2.1.12, “Option to Enable Login Using the Shared Authenticator to an Event,” on page 5](#)

1.2.1.1 Customizing Authentication Request Message for the Smartphone Method

Advanced Authentication now allows administrators to customize the authentication request message that is displayed on the NetIQ Auth app. When a user initiates Smartphone authentication to the endpoint or to the Advanced Authentication portals, the respective customized message is displayed on the latest version of NetIQ Auth app, such as 3.1.9 for Android and 3.1.4 for iOS.

For more information, see [“Customizing Authentication Request Message For Smartphone Method”](#) in the *Advanced Authentication - Administration* guide.

1.2.1.2 Endpoint Management Support for Helpdesk Administrators

This release introduces the **Allow to manage endpoints** option in the **Helpdesk Options** policy to allow a helpdesk administrator to manage the endpoints of the Advanced Authentication server. When the helpdesk administrator logs in to the Helpdesk portal, an **Endpoints** tab is displayed. The helpdesk administrator can delete preferred endpoint when there is a need to rebuild a corresponding workstation or to create a new endpoint.

For more information, see [“Helpdesk Options”](#) settings in the *Advanced Authentication - Administration* guide.

1.2.1.3 Option to Add More Than One RADIUS Servers for a Specific Site

Previously, it was possible to add only one RADIUS Server for the **RADIUS Client** method. Now, Advanced Authentication allows the administrators to configure more than one RADIUS servers for a specific site.

For more information, see “[RADIUS Client](#)” in the *Advanced Authentication - Administration* guide.

1.2.1.4 Cache Time Expiration

This release introduces the **Cache Expire Time** option in the **Cache Options** policy where you can define the expiry time of the client cache in hours. It sets the duration to store the enrolled authenticators of users in Client cache and allow offline logon to the Client. This setting is applicable for Windows and Linux Clients.

For more information, see “[Cache Options Policy](#)” in the *Advanced Authentication - Administration* guide.

1.2.1.5 User Interface to Monitor Replication Batches

You can monitor the last 200 outgoing batches that the Master server transmits to the peer servers on the same site or to the Master server on other sites in the cluster. The batches are transmitted to replicate information about the changes that are made to the database. The changes include a new entry, update, or deletion action to all DB servers in the cluster.

For more information, see “[Monitoring Replication Batches \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/t479rs4a7fuv.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/t479rs4a7fuv.html)” in the *Advanced Authentication - Administration* guide.

1.2.1.6 Option to Disable the Offline Authentication for Smartphone Method

Advanced Authentication now allows administrators to disallow users to authenticate using the Smartphone TOTP. This option prevents the use of Smartphone authenticator in offline mode which can be used when a user’s smartphone is out of networks or in Airplane mode.

For more information about the Smartphone method, see “[Smartphone](#)” in the *Advanced Authentication - Administration* guide.

1.2.1.7 Option to Customize the Branding of ADFS MFA Plug-in Templates

Advanced Authentication now allows customization of the ADFS multi-factor authentication (MFA) plug-in templates’ branding. You can customize the textual information around the variables sent by Advanced Authentication server. This information is displayed to the users.

For more information, see “[Customizing the Branding of Advanced Authentication ADFS MFA Plug-in](#)” in the *Advanced Authentication - ADFS MFA plug-in* guide.

1.2.1.8 Managing Reporting History

This release introduces the **Reporting Options** policy where you can set the number of days to record the history of users login in **History max age(days)**. By default, value is set to 30 days indicating that the login history is recorded for the past 30 days. Any data before that is reset in the server.

For more information, see “[Reporting Options](#)” in the *Advanced Authentication - Administration* guide.

1.2.1.9 General Data Protection Regulation Compliance

Advanced Authentication is now General Data Protection Regulation (GDPR) complaint. For more information about how to configure Advanced Authentication for GDPR compliance, see “[Delete Me Options](#)” in the *Advanced Authentication - Administration* guide.

1.2.1.10 Enhanced Syslog to Track Administrator Activities

Advanced Authentication Syslog now records some actions that are performed by administrators. Following are the related actions:

- ♦ Adding and removing of local users
- ♦ Granting and revoking role for all users (not only local)

1.2.1.11 Enhanced API

This release provides the following API enhancements:

- ♦ Public REST API is extended to store the registered tokens into the OATH tokens list.
- ♦ Public API is enhanced to support a TOTP or HOTP token association with a user.

1.2.1.12 Option to Enable Login Using the Shared Authenticator to an Event

In Advanced Authentication 6.0, login to the Advanced Authentication portals using the shared authenticator was disabled to enhance security. Now you can configure the **Allow to logon to this event by shared template** option to allow login using the shared authenticators. The default setting of this option is as follows:

- ♦ Disabled for the events, such as **Authenticators Management**, **Helpdesk**, **Helpdesk User**, **AdminUI**, **Search Card**, **Token Management**, and **Report Logon**.
- ♦ Enabled for all other events, such as **OS logon**, **SAML 2.0** and so on.

1.2.2 Client Enhancements

Advanced Authentication 6.1 includes the following enhancements on Clients:

- ♦ [Section 1.2.2.1, "Integration with Sophos SafeGuard Credential Provider," on page 5](#)
- ♦ [Section 1.2.2.2, "Face Recognition Support for Windows Hello," on page 6](#)
- ♦ [Section 1.2.2.3, "Support for YubiKey PKI and OpenSC," on page 6](#)
- ♦ [Section 1.2.2.4, "Operating System Support for Linux PAM Client and Device Service," on page 6](#)
- ♦ [Section 1.2.2.5, "Linked Chain Support for Cached Login," on page 6](#)
- ♦ [Section 1.2.2.6, "Enhanced Login Speed Using Logon Filter," on page 6](#)
- ♦ [Section 1.2.2.7, "Support for the ppc64le Architecture," on page 6](#)
- ♦ [Section 1.2.2.8, "Prompt to Change Domain Password in Linux," on page 6](#)
- ♦ [Section 1.2.2.9, "Enhanced Cache Login," on page 7](#)

1.2.2.1 Integration with Sophos SafeGuard Credential Provider

Advanced Authentication introduces Credential Provider Chaining to support the Sophos SafeGuard Credential Provider, which can also be used to integrate with the other third-party Credential Providers.

For more information about Sophos SafeGuard integration, see [Configuring Integration with Sophos SafeGuard 8](#).

1.2.2.2 Face Recognition Support for Windows Hello

Advanced Authentication now supports the Windows Hello authentication with the Facial Recognition authenticator on the Windows 10 workstations.

For more information, see “[Windows Hello](#)” in the [Advanced Authentication - Administration](#) guide.

1.2.2.3 Support for YubiKey PKI and OpenSC

Advanced Authentication now supports use of the YubiKey tokens with PKI and allows use of the OpenSC for any supported third-party smart cards and PKI tokens. Administrators can configure the Device Service to detect YubiKey PKI, and other PKI tokens and smart cards. With this configuration users can enroll and authenticate with the PKI method.

For more information about configuring YubiKey, see [Configuring the YubiKey PKI](#).

For more information about configuring OpenSC for PKI tokens, see [Configuring OpenSC](#).

1.2.2.4 Operating System Support for Linux PAM Client and Device Service

In addition to the existing supported platforms, this release enables you to install Linux PAM Client and Device Service on the following operating systems:

- ♦ Debian 9.5
- ♦ Red Hat Enterprise Linux Client 7.5
- ♦ Red Hat Enterprise Linux Server 7.5
- ♦ SUSE Linux Enterprise Desktop 15
- ♦ SUSE Linux Enterprise Server 15

1.2.2.5 Linked Chain Support for Cached Login

The [Hide required chain](#) option enables administrator to hide the required chain and display the linked chain after the user has authenticated once with the required chain. This release extends support of the [Hide required chain](#) option to cache login.

1.2.2.6 Enhanced Login Speed Using Logon Filter

This release introduces two new parameters for Logon Filter to improve the login speed. Configure these parameters in the configuration file of Logon Filter.

For more information, see “[Configuring the Logon Filter Parameters](#)” in the “[Advanced Authentication - Logon Filter](#)” guide.

1.2.2.7 Support for the ppc64le Architecture

Advanced Authentication now supports installing Linux PAM Client on operating systems running on the ppc64le architecture.

1.2.2.8 Prompt to Change Domain Password in Linux

Previously in Linux Client, if a user failed to update the domain password before it expired, the user was not allowed to change the password and log in to Client.

Now, any user with expired domain password tries to log in to Linux Client, the Login form prompts to update the domain password and allows to login successfully.

1.2.2.9 Enhanced Cache Login

During the user authentication, Windows Client, Mac OS X Client, and Linux PAM Client try to connect to the Advanced Authentication server, by default. When the network connection is slow or unstable, the client login and unlock processes might take several minutes (3G networks). You can enforce a cached login to overcome delayed login.

Previously, users were allowed to select **Offline logon** checkbox in Windows Client to skip the online login. If the specified credentials were incorrect, the cached data was implicitly invalidated in the background after login. The new parameter (`forceCachedLogon`) supports the background credentials validation and does not require any checkbox. In addition to Windows Client, the new parameter extends its support for Linux PAM Client and Mac OS X Client.

1.2.3 Security Enhancements

This release provides the following security enhancements:

- ♦ [Section 1.2.3.1, “Option to Disable Username Disclosure,” on page 7](#)
- ♦ [Section 1.2.3.2, “LDAP Injection Vulnerability,” on page 7](#)
- ♦ [Section 1.2.3.3, “Encryption of Passwords in Memory Cache,” on page 7](#)
- ♦ [Section 1.2.3.4, “Private Key of Device Service Is Not Accessible for Users,” on page 8](#)
- ♦ [Section 1.2.3.5, “SAML Vulnerabilities,” on page 8](#)
- ♦ [Section 1.2.3.6, “Last Logged In User Information Is Encrypted,” on page 8](#)
- ♦ [Section 1.2.3.7, “Advanced Authentication Version Disclosure,” on page 8](#)
- ♦ [Section 1.2.3.8, “Users Cannot Log in with an Expired Password,” on page 8](#)

1.2.3.1 Option to Disable Username Disclosure

This release introduces the **Username disclosure** option in the **Login Options** policy to conceal valid user names and prevent security vulnerabilities. This makes difficult for hackers to predict the valid username.

If a user specifies invalid username on the login page, the chain list is displayed instead of error message. User is then allowed to select preferred authentication chain and try to authenticate using the methods of the chain then a generic message `Invalid credentials` is displayed. This does not disclose whether username or first-factor authentication is incorrect.

1.2.3.2 LDAP Injection Vulnerability

With this release, Advanced Authentication limits the characters that can be used to customize the user and group attributes of a repository. The supported characters are: a to z, A to Z, 0-9 and a symbol hyphen (-). This is to prevent the LDAP injection and to secure the values specified in each attribute.

1.2.3.3 Encryption of Passwords in Memory Cache

Previously the passwords were stored as clear text in memory of the cache service in Windows Client, Linux PAM Client, and Mac OS X Client.

Now, Advanced Authentication encrypts the password before storing in the memory cache.

1.2.3.4 Private Key of Device Service Is Not Accessible for Users

With this release, the Private key of Device Service is not accessible for the users on all Client platforms (Linux, Mac, and Windows) for security reasons.

1.2.3.5 SAML Vulnerabilities

The SAML vulnerabilities have been fixed for the Web Authentication events.

1.2.3.6 Last Logged In User Information Is Encrypted

With this release, Advanced Authentication Windows Client encrypts the last logged in user information before saving details in the configuration file.

1.2.3.7 Advanced Authentication Version Disclosure

With this release, the Advanced Authentication version is not displayed when accessed using Advanced Authentication portals.

1.2.3.8 Users Cannot Log in with an Expired Password

Previously, domain users were able to log in to all events of Advanced Authentication with an expired password.

Now, if a user fails to update the password before it expires, the user is prevented from changing the password and therefore user will not be able to log in to any event except for the Linux, Mac OS and Windows Client logon events. While logging in to these Clients with an expired password, users are prompted to change the domain password before logging in.

1.3 Software Fixes

Advanced Authentication 6.1 includes the following software fixes:

- [Section 1.3.1, “Advanced Authentication Portals Stop Working After Update When Proxy Is Used,” on page 8](#)
- [Section 1.3.2, “Error Displayed on High Load,” on page 9](#)
- [Section 1.3.3, “Full Administrator Permission Required to Access Reporting Portal,” on page 9](#)
- [Section 1.3.4, “Report on Authentication Method Failures,” on page 9](#)
- [Section 1.3.5, “Test Button in Sender Policies Does Not Use Proxy Settings,” on page 9](#)
- [Section 1.3.6, “Limited Data Is Exported From Widgets,” on page 9](#)
- [Section 1.3.7, “Issue with Fingerprint Method,” on page 9](#)
- [Section 1.3.8, “Improved Handling of Authentication Agent Session,” on page 10](#)
- [Section 1.3.9, “Blank Login Screen Is Displayed During Windows Login,” on page 10](#)
- [Section 1.3.10, “Blank Login Screen Is Displayed During macOS Login,” on page 10](#)
- [Section 1.3.11, “An Error Message Is Displayed When Users Login In to macOS In the Offline Mode,” on page 10](#)
- [Section 1.3.12, “Blank Login Screen Is Displayed When a Laptop Is Connected to a Docking Station,” on page 10](#)
- [Section 1.3.13, “Kerberos Single Sign-on Does Not Work,” on page 10](#)

1.3.1 Advanced Authentication Portals Stop Working After Update When Proxy Is Used

Issue: After upgrading to Advanced Authentication 6.0 Patch Update 2, users are unable to access the Advanced Authentication portals except for the Configuration portal (port 9443). This issue occurs when the Docker bypasses the proxy settings.

Fix: Now, the Docker is made to go through the proxy settings and users can access the Advanced Authentication portals without any issue.

1.3.2 Error Displayed on High Load

Issue: When number of simultaneous connection to the database in Advanced Authentication site exceeds the default value set in the `max_connections` parameter of the `postgresql.conf` file, an error message `FATAL: sorry, too many clients already` is displayed.

Fix: Now, the default value for the `max_connections` parameter is set to 400 to increase maximum number of simultaneous connections to the database and to increase the limit of the possible load.

1.3.3 Full Administrator Permission Required to Access Reporting Portal

Issue: The users with only FULL ADMINS privilege are allowed to access the Reporting portal. If any user without FULL ADMINS privilege tries to access the Reporting portal, an error message `Permission Denied` is displayed. (*Bug 1038294*)

Fix: Now, all users of Advanced Authentication who can authenticate with the chain associated to the Reporting portal are allowed to access the portal without any issue.

1.3.4 Report on Authentication Method Failures

Issue: The report on failures did not work neither in the Reporting portal nor in the Dashboard.

Fix: Now, the report on failures is fixed to render actual data and display an accurate details.

1.3.5 Test Button in Sender Policies Does Not Use Proxy Settings

Issue: The **Test** button in the policies, such as Mail sender, SMS sender, and Voice sender does not use the proxy settings. Therefore, the test message of authentication methods, such as Email OTP, SMS OTP, and Voice OTP are not sent to the users.

Fix: Now, the Mail sender, SMS sender and Voice sender policies use the proxy settings. The test message of the authentication methods, such as Email OTP, SMS OTP, Voice, and Voice OTP are transmitted through the proxy server to the registered email address or phone number.

1.3.6 Limited Data Is Exported From Widgets

The administrator can now export all data available in **Users** and **Authenticators** widgets without any limit. Previously, when an administrator exported report from the **Users** and **Authenticators** widgets in the Dashboard, the report exported only 50 entries due to the configured limit.

1.3.7 Issue with Fingerprint Method

During the first attempt of enrolling and authenticating with Fingerprint method, an error message `Timeout` is displayed on Windows 10 workstation while using the fingerprint reader from Broadcom ControlVault.

Now, user can enroll and authenticate using the Fingerprint method without any error on Windows 10 workstation.

1.3.8 Improved Handling of Authentication Agent Session

Previously, user was allowed to initiate login using the Authentication Agent chain from one system even though the Authentication Agent that is installed on another system is not logged in.

Now, when a user initiates login with the Authentication Agent chain and the Agent is not active then Advanced Authentication server prompts a message `Cannot notify your Logon Agent` and prevents user from initiating login.

1.3.9 Blank Login Screen Is Displayed During Windows Login

In Windows, blank login screen is displayed to the users when the following Microsoft policies are configured:

- ♦ `Do not display last username: true`
- ♦ `Display user information when the session is locked: Display username only`

No authentication prompt is displayed.

1.3.10 Blank Login Screen Is Displayed During macOS Login

In macOS, blank login screen is displayed to the users when a custom Login window profile is used. No authentication prompt is displayed.

1.3.11 An Error Message Is Displayed When Users Login In to macOS In the Offline Mode

In the macOS offline mode, the `Internal Server Error` error message is displayed to the users.

1.3.12 Blank Login Screen Is Displayed When a Laptop Is Connected to a Docking Station

In Windows, users get the blank login screen when they try to login. No authentication prompt is displayed. This issue occurs when laptops are connected to a docking station.

1.3.13 Kerberos Single Sign-on Does Not Work

With the Kerberos single sign-on configured, when a domain user tries to log in to the Advanced Authentication Self-Service portal on the Internet Explorer or Google Chrome browsers, the user is not auto logged in.

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 6.1 includes the following known issues:

- ♦ [Section 2.1, “Issue with SAML Single Logout in Citrix StoreFront,” on page 11](#)
- ♦ [Section 2.2, “Issue with Unlocking Linux for Domain Users,” on page 11](#)
- ♦ [Section 2.3, “Issue with the Activation Script Execution,” on page 11](#)
- ♦ [Section 2.4, “Issue with Webd Container,” on page 11](#)

2.1 Issue with SAML Single Logout in Citrix StoreFront

Issue: The Citrix StoreFront supports the SAML from version 3.9. But, the previous and the latest version 3.16 do not support SAML single logout. The users who logged out from Citrix are able to log in again to Citrix on the same browser without authentication.

Workaround: The users must ensure to close the browser after they logout from Citrix to prevent any unauthorized access to the previous session.

2.2 Issue with Unlocking Linux for Domain Users

Issue: On Ubuntu 16, when a logged in domain user tries to unlock the system by selecting a chain and specifying data relevant to each method, the chains list is displayed again without unlocking the system. This issue does not occur in Ubuntu 18.

2.3 Issue with the Activation Script Execution

Issue: If a user executes the `sudo /opt/pam_aucore/bin/activate-nondomain.sh` command in a SLED 15 system that is not joined to any domain, the following errors are displayed:

```
/opt/pam_aucore/bin/activate-nondomain.sh: line 68: bc: command not found
/opt/pam_aucore/bin/activate-nondomain.sh: line 68: [: -eq: unary operator expected
```

2.4 Issue with Webd Container

Issue: After installing Advanced Authentication 6.1, users are unable to access the Advanced Authentication portals except for the Configuration portal (port :9443) though the processor with SSE 4.2 is in use. When user executes the `docker ps -a` command, a message `aaf_webd_1 container exited` is displayed. Even, rebooting does not get the results. This issue may be due to the slow hardware or a server is rebooted after the installation without the required wait of 15 minutes.

Workaround: As a solution, execute the following commands:

```
rm /var/lib/docker/volumes/aaf_webd-config/_data/dhparams.pem
systemctl restart aauth.service
```

Later, wait for few minutes.

3 Upgrading

You can upgrade Advanced Authentication 6.0 to 6.1. You cannot upgrade from Advanced Authentication v5 to 6.1. However, you can export the database from Advanced Authentication 5.6 to 6.1. After you install Advanced Authentication 6.1, you can import the database from 5.6.

For example, to upgrade from Advanced Authentication 5.5 to 6.1, you must first upgrade from Advanced Authentication 5.5 to 5.6. Then, you must install 6.1 and import the configurations from 5.6.

For more information about migrating, see [“Migrating Advanced Authentication from Version 5”](#) in the *Advanced Authentication- Server Installation and Upgrade* guide.

For more information about upgrading from 6.0, see [“Upgrading Advanced Authentication Appliance 6.0 to 6.1”](#) in the *Advanced Authentication- Server Installation and Upgrade* guide.

WARNING: The [Admin UI Whitelist \(https://www.netiq.com/documentation/advanced-authentication-60/server-administrator-guide/data/configuring_policy.html#restricting_access_to_the_administrative_portal\)](https://www.netiq.com/documentation/advanced-authentication-60/server-administrator-guide/data/configuring_policy.html#restricting_access_to_the_administrative_portal) policy is discontinued in 6.1. You must configure the settings on the reverse proxy or load balancer to secure access to the Administration portal.

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 © 2018 NetIQ Corporation, a Micro Focus company. All Rights Reserved.