Advanced Authentication 6.4 Release Notes

July 2022

Advanced Authentication 6.4 includes new features, enhancements, 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. You can also post or vote for the ideas of enhancement requests in the Ideas forum (https://ideas.microfocus.com/MFI/advance-authentication).

For more information about this release and the latest release notes, see the NetIQ Advanced Authentication Documentation (https://www.netiq.com/documentation/advanced-authentication-64/) page.

If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of the specific page in the HTML version of the documentation posted at the NetIQ Advanced Authentication Documentation (https://www.netiq.com/documentation/advanced-authentication-64/) page.

What's New?

Advanced Authentication 6.4 includes the following enhancements:

Single Sign-on Support for Remote Desktop Server and Citrix for Active Directory Groups

Now, in Advanced Authentication Windows Client, you can enable single sign-on to Citrix and Remote Desktop server for a specific group of users.

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

Support for Local Users to Log in Without Endpoints

Advanced Authentication now allows local users to log in even if the specified endpoint has not been created on the Advanced Authentication server.

Extended Support for Kernel Tuning Measures

This release includes new kernel tuning measures for the base Operating System, SUSE in addition to the existing measures. This enhances the minimum protection to the Network Layer.

Improved Error Messages for Repository Synchronization

This release improves the error messages displayed for the repository synchronization issues to enhance the troubleshooting experience.

An Option to Re-use the Token

The **Allow Token Re-use** option is introduced in the existing and custom events. This option allows users to apply a single OTP more than once within the valid duration for authentication. This option is applicable for Email OTP, SMS OTP, and Voice OTP methods.

For more information, see Configuring an Existing Event in the *Advanced Authentication - Administration* guide.

Ability to Send Common Name as NameID in the SAML Response

This release introduces an option **Send CN as NameID** in the SAML event. This option must be set to ON while integrating with CyberArk. This option is also must be set to ON when eDirectory is used as a repository and service providers require Common Name (UID by default) in the SAML response.

For more details, see Creating a SAML 2.0 Event in the *Advanced Authentication - Administration* guide.

Support for Upgrading Advanced Authentication Using the Docker Image

This release provides the Docker image with Helm charts to upgrade the Advanced Authentication in the Azure Kubernetes air-gapped environment.

For more information, see Upgrading Advanced Authentication on Azure Kubernetes Services in an Air Gap Environment in the *Advanced Authentication- Server Installation and Upgrade*.

Ability to Trace the Reason for Failed Login

Now, you can determine the cause of failed login attempts in the Syslog. A parameter, `reason` is included to the Syslog code 102 that captures the actual cause for failed login. Common causes are incorrect password, user locked, and so on.

Support for New Operating Systems

This release adds support for Device Service and Linux PAM Client on SLES 12 SP5 and SLES 15 SP3.

For more information, see the Linux PAM Client and Device Service in the *Advanced Authentication System Requirements* guide.

Attribute Mapping for the SAML Events

Advanced Authentication now supports attribute mapping for the SAML events. You can map the attributes to display in the SAML assertion as follows:

- `localName="mail" samlName="e-mail address"`
- `localName="userLastName" samlName="Surname"`
- `localName="userFirstName" samlName="Given Name"`
- `localName="mobile" samlName="Telephonenumber"`

For more details, see Creating a SAML 2.0 Event in the *Advanced Authentication - Administration* guide.

Resolved Issues

This release includes the following software fixes:

Component	Description
Administration Portal	Customized messages related to any method in **Policies > Custom Messages** on the Administration Portal are not displayed on the web portals. Also, a series of errors are observed in the log file.
All clients	If an Advanced Authentication administrator deletes a workstation's endpoint from the Advanced Authentication server, users cannot log in even in the cached mode. The local administrator of the workstation can also not log in. Now, the local administrator can log in to delete the endpoint data from `C:\ProgramData\NetIQ\Windows Client\config.properties`
All clients	In Advanced Authentication 6.3.6, the cached login by PKI does not work. The following error message is displayed: `Wrong card UID`

Component	Description
All clients	HTML codes do not work in the custom messages for Advanced Authentication Clients. When you customize the font size of the message that gets displayed on Advanced Authentication Clients, the message might be invisible or not readable based on the size that you set. It is recommended to set the font size between 2 (smallest) and 9 (biggest). Sample HTML code: `[<font size="3" color="red" face="Arial"><b>Message to Display</b></font>]`
All clients	When users try to enroll the PKI method by using the Omnikey 3021 card, the device is not detected and the following error is displayed: `{ "result":"PLUGIN_NOT_INITTED" }`
API	The auto-created `EMAIL_OTP: 1` template does not include the email attribute that displays the email address used for enrollment in the API response.
Out-of-Band Portal	The time stamp of each authentication request is displayed in the UTC format instead of the local time format in the **Authentication Request History** of Out-of-Band Portal.
Configuration Portal	The Configuration Portal does not display the valid network mask and displays an incorrect IP address even though the correct details are configured in YAST.
Configuration Portal	The RPM files on upgraded Advanced Authentication Server and freshly installed server are different. If the administrator upgrades the Advanced Authentication Server from version 6.1 to 6.3, a few unused RPM files are not removed. However, freshly installed Advanced Authentication Server do not have unused RPM files.
Diagnostic Tool	On macOS 10.13.6, if a user tries to launch the Diagnostic tool and then clicks **Cancel** without specifying the password, the application gets launched even after canceling.
IIS Authentication plug-in	When a user for whom the mailbox is not configured in Exchange tries to login to the respective mailbox using the IIS Authentication plug-in, the error message `redirected you too many times` is displayed instead of redirecting to the logout page.
Linux PAM Client	Preconditions: ◆ A chain containing the **Fingerprint** method is assigned to **Linux logon** event. ◆ Device service is not installed on the Linux system. When a user tries to log in to the Linux system, the Linux PAM client displays the chain instead of hiding it.
Linux PAM Client	The Linux PAM client does not display the security questions when a user attempts to perform the SSH login using security questions.

Component	Description
Old Self-Service and Helpdesk Portals	After upgrading to Advanced Authentication 6.3 Service Pack 7, the following options are not applicable on the old Self-Service and Helpdesk portals: ◆ **Override Mobile Phone** in **SMS OTP** method ◆ **Override Email** in **Email OTP** method
Web Authentication	Use of the Web Authentication causes the following error: `Request cannot be completed at this time.` This occurs due to blank color field or use of transparent colors in the **Custom Branding** policy. Now, you must set the colors in the Hexadecimal format.
Web Portals	On macOS 11.6, Safari users cannot authenticate to any web portals using the FIDO2 technique, and the following error message is displayed: `Failed`
Windows Client	Pre-condition: User attributes are set as follows in the Active Directory: ◆ `userPrincipalName = firstname@company.com` ◆ `sAMAccountName = firstname` When a user tries to log in to Windows Client using `firstname@company.com`, the login fails and a message, `User not found` is displayed. This does not work when the **Username disclosure** option is enabled.
Windows Client	When the Advanced Authentication server is offline or unreachable, and users update their password in Active Directory, the updated password does not work.
Windows Client	On Windows 10 machines, Advanced Authentication sometimes fails to detect the PKI card and a message `Wait` is displayed. Later, a prompt to specify the PIN is not displayed.

Upgrading

You can directly upgrade to Advanced Authentication 6.4 from 6.3.

NOTE: The following is the recommended upgrade sequence:

1. Advanced Authentication servers.
2. Plug-ins
3. Client components

   Any change in the upgrade sequence is not supported.

NOTE: The RAM requirements of Advanced Authentication have been changed in 6.4 as follows:

- Minimum: 8 GB per server.
- Recommended: 16 GB per server

Before upgrading your Advanced Authentication cluster to 6.4, ensure that the environment complies with the new requirements.

For more information, see Advanced Authentication System Requirements.

Known Issue

Advanced Authentication 6.4 includes the following known issues:

- SSL Bad Handshake Error While Accessing the New Enrollment Portal
- Logout from the Active Web Authentication Event Before Logging In to Another Event

SSL Bad Handshake Error While Accessing the New Enrollment Portal

This release breaks the fix provided for the SSL `bad handshake` error while trying to access the new Enrollment Portal in Advanced Authentication 6.3 Service Pack 2.

To resolve the *SSL bad handshake* issue in Advanced Authentication 6.4, disable your proxy for internal communication between Advanced Authentication servers in the YAST proxy settings as follows:

```
"NO_PROXY=localhost,127.0.0.l,your.domain"
```

Logout from the Active Web Authentication Event Before Logging In to Another Event

When a user logs in to a Web Authentication event, New Enrollment Portal or Out-of-Band Portal and then tries to access another Web Authentication event, the message that states to logout from active Web Authentication event is displayed.

Upcoming Changes

The following options in the Smartphone method settings will be removed in Advanced Authentication 6.4 Service Pack 1:

- Push salt TTL
- Authentication salt TTL

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.

Legal Notice