Advanced Authentication 6.3 Service Pack 4 Release Notes

March 2021

Advanced Authentication 6.3 Service Pack 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 for the latest release notes, see the NetIQ Advanced Authentication Documentation 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 page.

What's New?

Advanced Authentication 6.3 Service Pack 4 provides the following enhancements and fixes in this release:

Enhancements

This release includes the following enhancements:

Enhancement	Description
Support for HANIS Method	Advanced Authentication provides the Home Affairs National Identification System (HANIS) method that facilitates citizens of South Africa to authenticate through their fingerprint that has been enrolled in the National Identification System. During authentication, the Advanced Authentication server forwards the user details to the third-party Service Provider that is integrated with National Identification System where the validation takes place. Based on the validation result, the user gets authenticated to the required resource or endpoint. For more information, see Home Affairs National Identification System (HANIS) in the *Advanced Authentication - Administration*. To support HANIS verification, the Wavelet Scalar Quantization (WSQ) algorithm-based parameter, `fingerprint.wsqBitrate` is introduced. This parameter enables to configure the amount of compression for a fingerprint scanner. For more information, see Fingerprint Settings in the *Advanced Authentication - Device Service*.
Provision to Customize the Look and Feel of the New Enrollment Portal and Administration Portal	A new policy **Custom Branding** is introduced to customize the look and feel of the new Enrollment Portal and Administration Portal. Custom Branding policy allows the administrator to customize the title, logos, and application bar colors of the new Enrollment portal and Administration portal. For more information, see Custom Branding in the *Advanced Authentication - Administration*. **NOTE:** The **Custom Branding** Policy replaces the **Logo** policy. If the administrator configured the Logo policy, then the administrator should configure the new Custom Branding Policy. To apply the new branding to the Enrollment Portal, it is required to enable the new Enrollment UI. For more information, see Enrollment Options (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/enrollment_options.html) in the *Advanced Authentication - Administration*.

Enhancement	Description
Provision to Hide the Copyright Information	A new parameter `show_copyright` is introduced to hide the copyright information on the Windows Client login screen. For more information, see Hiding the Copyright Information in the *Advanced Authentication - Windows Client*.
Provision to Configure a Port for Windows Client Cache Service	With the default settings, on Windows Server OS, Windows Client Cache Service might conflict with another third-party software like Microsoft SQL Server. With the new parameter `offline.port`, an administrator is allowed to configure the preferred port for Cache Service in Windows Client. The Windows Client Cache Service listens on the port 8082 by default. For more information, see Configuring the Port for Windows Client Cache Service in the *Advanced Authentication - Windows Client*.
Support for Windows 10 version 20H2	The following components of Advanced Authentication extends support for Windows 10 version 20H2 operating system: ◆ Windows Client ◆ Desktop OTP Tool ◆ Authentication Agent For more information, see Advanced Authentication System Requirements.
Custom Attribute in SAML Assertion	◆ A new attribute `userGroups` is added to the SAML assertion by default. This attribute retrieves the user group details of a specific user. ◆ The **Custom attributes to fetch** and **Custom attributes to return** available under **Advanced Settings** of LDAP repository are configurable for the SAML-based integration. You can define AD user attributes that matches with the corresponding LDAP attribute name. It is required to add the valid attributes in both parameters. For example, postalAddress, description, distinguishedName, and so on. These options facilitate gathering specified user attributes from the target directory. **NOTE:** If the attribute has more than one value, then first value is returned in the SAML assertion. For more information, see Custom Attributes to Fetch and Custom attributes to return in the *Advanced Authentication - Administration* guide.

Enhancement	Description
Support for macOS version 11 (Big Sur)	Advanced Authentication supports Mac OS X Client, Device Service, and Desktop OTP Tool on macOS 11 including M1 chip in the emulation mode. The emulation works imperceptibly for users.
Ability to Enable Third-party Credential Providers	The Windows Client filters out all third-party Credential Providers to enhance the security. Now, an administrator can define permitted third-party Credential Provider with the new parameter `allowedProviders`. This allows administrators to select the preferred providers that verify users' identity during the logon process and grant access. For more information, see Enabling the Third-Party Credential Provider in the *Advanced Authentication - Windows Client*.
Getting the Profiling Logs for Clients	With the new parameter `rest_profiling`, administrators can enable the profiling for Web Server logs of the Advanced Authentication server in all clients. The profiling tool helps in tracking the performance, memory allocation, and CPU utilization of each REST API calls that are processed including the background programs that are initiated by the call. In case of an issue, it facilitates in identifying the cause. For more information, see Enabling the Profiling Tool in the *Advanced Authentication - Windows Client*.
Google reCAPTCHA Support for Users Located in China	Advanced Authentication supports Google ReCaptcha for users from China.
Provision to Set the Logout URL in IIS Plug-in	Administrators can now configure the logout URL in the IIS plug-in. To allow another application to manage the logout process, set the URL related to that application. For example, to allow Outlook Web Access (OWA) to manage logout, set **Logout URL** with `/owa/logoff.owa` For more information, see Configuring the IIS Authentication Plug-in in the *Advanced Authentication - IIS Authentication Plug-in*.
Support for FIPS Compatible Encryption in Windows Client	A fresh install and upgraded version of Windows Client contains FIPS-compatible encryption for the local Cache Service.
A Setting to Configure the Authentication Protocol	A new parameter, `provider.AuthenticationProtocol` is introduced to enforce an alternate authentication protocol that the Local Security Authority applies during Windows OS logon process. For more information, see Configuring the Authentication Protocol in the *Advanced Authentication - Windows Client*.

Enhancement	Description
Ability to Apply the Logging Level to All Servers	A option **Debug logging** is introduced to generate detailed logs for each events and the logs are available in the respective tabs. After enabling the **Debug logging**, you can apply the change to other Advanced Authentication servers in a cluster with the **Apply to all Servers** option. For more information, see Logging in the *Advanced Authentication - Administration*.

Security Improvement

Advanced Authentication 6.3 Service Pack 4 resolves the broken authentication and improper session management issues. For more information, see CVE-2021-22497 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22497).

We would like to offer a special thanks to Syed Sohaib Karim (syedsohaibkarim@gmail.com) for responsible disclosure of this vulnerability.

Software Fixes

This release includes the following software fixes:

Component	Description
Administration Portal	An administrator is unable to customize some messages on the updated Advanced Authentication server. When the administrator tries to apply the changes, the following error message is displayed: `Custom message with key "method.bluetooth.waiting_for_service", locale: "hu" and category: "messages" doesn't exist (AuError).`

Administration Portal	After upgrading Advanced Authentication 6.2 to 6.3, sometimes the full synchronization for Active Directory repositories fails and the following errors messages are displayed in the logs:
	
	`socket sending error[Errno 104] Connection reset by peer; ['<ourLDAPserver>:389']`
	
	`can't unbind ldap connection: socket sending error[Errno 32] Broken pipe <class 'ldap3.core.exceptions.LDAPSocketSendError'>`
	
	`ConnectionResetError: [Errno 104] Connection reset by peer`
	
	`LDAP connect error: socket sending error[Errno 104] Connection reset by peer; ['<ourLDAPserver>:389']`

Administration Portal	The administrator is not able to export the **Authenticators** report to the CSV or JSON format.

Component	Description
Administration Portal	The Backup or Restore mirror command fails to keep the specified number of files on the remote server.
Administration Portal	The Active Directory repositories synchronization fails due to the existence of non-ASCII characters in the attributes of used service accounts and the following message is displayed: `string argument should contain only ASCII characters`.
Administration Portal	When the RADIUS policy is configured with clients and the event is secured with the LDAP password method, the authentication is successful. However, in some specific instances, the password is displayed as readable text without encryption in the **RADIUS** logs.
Administration Portal	After customizing the CSS file and uploading the same file to the **Web Authentication** policy, customization is not applied to the login page of Web Authentication events.
Administration Portal	If there is a chain with two or more methods and the second method is the OTP method that has multiple categories enrolled. During authentication with this chain, the default category of the OTP method is auto-selected without prompting a user to select the preferred category and OTP is sent to the respective device. This issue occurs on the Administration and Helpdesk portals.
Administration Portal	Advanced Authentication appliance consumes more disc space and causes space issues due to the working table and temporary data that is not purged properly.
Administration Portal	If an administrator configured the Recipient Mask in Advanced Authentication 6.3.2 (or earlier) and upgrade to Advanced Authentication 6.3.3, the Email OTP method fails and does not send OTP to the users. The same issue occurs with the SMS OTP method also.
Administration Portal	When an administrator tries to set the **Relative intervals** in the **Dashboard** to 30 days, an unknown error message is displayed.
API	Use of an empty event in API calls causes the security issues.
Clients	When an unsupported method is assigned to an event, an error message is displayed and the respective authentication chains are not displayed on the login screen of the event. Due to this, a user is unable to login. For example, if the Touch ID method that is supported for Mac OS Client is assigned to Linux Client, a user is unable to view the authentication chains while logging into Linux Client.
Device Service	After installing Device Service 6.3.3 in macOS 10.15 or 11, the RF IDeas card reader does not work. However, It was working as expected on Device Service 6.3.2.

Component	Description
Enrollment and Helpdesk Portal	When a user tries to specify a comment in **Comment** of methods in the old Enrollment Portal and Helpdesk Portal, the following error message is displayed: `AttributeError 'str' object has no attribute 'id' (Internal Server Error).`
Enrollment and Helpdesk Portal	After upgrading to Advanced Authentication 6.3.3, it is consuming a significant time to display the authenticators in the Helpdesk Portal and Enrollment Portal.
Enrollment Portal	Pre-conditions: ◆ Two local accounts have an active session ◆ Two different domain users have enrolled to the Touch ID chain With the above pre-conditions, when a user tries to log in to the new Enrollment portal using the Touch ID method and presents an incorrect finger for five times, the login screen does not respond. Also, an error message is not displayed.
Enrollment Portal	When an administrator changes an email address or a phone number for a user in eDirectory, there is a 5 minutes delay in updating the data in authenticators.
Enrollment Portal	While enrolling the **Smartphone** method, **Category** drop down is not displayed. After enrollment, the **Category** drop down is prompted, however if user selects the category following message is displayed: `The account already has enrolled authenticator`
Linux Client	When a user logs in to Linux Client without prefixing the domain name, the username without domain gets cached. Later, if the user switches to the offline mode and prefixes the domain name to username, an authentication error occurs.
Mac OS Client	The product version information is missing in the `info.plist`, and in this release, the `CFBundleVersion` and the `CFBundleShortVersionString` with product info are added on Mac OS Client, Mac OS Device Service, and Desktop OTP Tool for Mac.
Mac OS Client	Pre-conditions: ◆ Mac OS Client is installed ◆ Basic proxy is configured ◆ User has logged in using several authentication chains that can be cached for offline authentication With the above pre-conditions, when a user logs in to Mac OS Client if the network of Advanced Authentication server is turned off, an error message is displayed. In such circumstances, the cached methods must be displayed.
Mac OS Client	With the NTLM proxy method configured if you turn off the network of the server, a user is not allowed to either login or unlock the Mac OS Client, due to the HTML exception error.

Component	Description
Mac OS Client	While logging in to Mac OS Client installed on macOS 11, following visual issues are noticed: ◆ The Back and Next buttons of mac operating system are visible ◆ Login screen blinks
Mac OS Client	In domain and non-domain mode, the offline cache does not display the cached chains when the server network is down. Also, when a user tries to log in with the mobile account from the login window or through FUS actual cached chains are not displayed and users are not allowed to log in.
Mac OS Client	Previously, it was required to use `dmg` installer to uninstall the Mac OS applications. Now, the uninstall script for Mac OS Client and Device Service is available in the following folders: Mac OS: `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/Resources` Device Service: `/Library/Application Support/NetIQ/uninstall` For more information, see Uninstalling Mac OS X Client in the *Advanced Authentication - Mac OS X Client* and Uninstalling Device Service on Mac in the *Advanced Authentication - Device Service*.
Online Update	When an administrator tries to perform online update, the update fails due to a conflict in the package and returns a warning message.
Web Authentication	When a user tries to authenticate to any Web Authentication events with the HOTP or TOTP method, the **Resend** button is displayed which is not relevant to these methods.
Web Authentication	When a user tries to log in, an error message is displayed if the user specifies the incorrect password. When the user tries to log in again by specifying the correct password, the same error message is displayed.
Web Authentication	When a user tries to authenticate after setting `sign AuthnRequests` and `force authentication` to `True` in the Service Provide SAML configuration, the authentication fails.
Web Authentication	When a user tries to authenticate to ADFS, the Web Authentication service sends deformed Consent URI in the SAML response to ADFS and causes the following error: `MSIS0018: The SAML protocol message cannot be read because it contains data that is not valid.`
Windows Client	When a user tries to perform the first login to a Windows Client through RDP, the `config.properties` does not stores the Endpoint ID and secret created in the server. This causes the following error during the subsequent login: `Cannot add or change the endpoint (same name or software_name already exist?)`

Component	Description
Windows Client	When a user tries to log in to a Windows Client after setting `forceCachedLogon` to `True` and a user account is marked as disabled, expired or locked in local cache, the Cache Service tries switching to the online session and one of the following happens: ◆ The Advanced Authentication server is available, the user is allowed to login to Windows Client once. In subsequent login, after selecting the chain (before providing credentials), an error message (about the disabled account) is displayed. ◆ When the Advanced Authentication server is unavailable, the user is allowed to log in to Windows Client once. In subsequent login, after submitting the credentials, an error message is displayed. When a user account is not marked as disabled, expired, or locked in the local cache, the Cache Service processes request and starts a background task to update the user data. Therefore, when a user account is disabled on domain controller, the subsequent log on fails.
Windows Client	The Facial Recognition method is not displayed on the Windows login page even though a user has authenticated earlier using the same method.

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 6.3 Service Pack 4 includes the following known issues:

- Windows Client Does Not Respond
- Syslog is Flooded with the Health Check Messages
- Delete Button Is Not Displayed in the Enrollment Portals
- Issue with Risk Service After Upgrade
- Issue with Web Authentication

Windows Client Does Not Respond

When a user tries to authenticate to Windows Client, it freezes in the `Please wait` screen after providing the username. This happens only in Windows machines with external Nvidia Quadro graphics cards and their drivers installed.

Syslog is Flooded with the Health Check Messages

There are various messages as follows:

```
dockerd[2167]: time="2020-12-21T23:30:22.663706880Z" level=warning msg="Health
check for container
b1cc02cc52d3fe2681c9fa60abfab62aa54fa40d4d833fca4bb0fef5d0414890 error: context
deadline exceeded" in syslog.
```

These messages do not indicate any issues. This is due to the absence of the Risk Service license.

Workaround: Perform the following steps:

1. Log in to the Configuration Portal (:9443).
2. Click **System Services** and select the Risk Service then click **Action** and select **Stop**.
3. Click **Options** then select **Set as Manual** for Risk Service.

Delete Button Is Not Displayed in the Enrollment Portals

The **Delete** option for the SMS OTP and Email OTP methods is not available in the new and old Enrollment Portals.

Issue with Risk Service After Upgrade

Issue: The Risk Service does not work after upgrading to Advanced Authentication 6.3 SP4.

Workaround: Run the following commands to remove the old `rba_history` container and reboot the appliance:

1. `systemctl stop docker`
2. `systemctl start docker`
3. `docker container stop risk_rbahistory_1`
4. `docker container rm risk_rbahistory_1`
5. `docker rmi -f mfsecurity/rba_history:1.0.0.2`
6. `reboot`
7. Log in to the Administration portal and click **Logs > Clear** to clear the logs.

NOTE: If any command takes too long to respond or hangs, press Ctrl+C to stop and continue with the next step.

Issue with Web Authentication

Issue: After a user successfully authenticates to OAuth 2.0, SAML 2.0 event or new Enrollment portal, an error message `WebAuth feature is not running` is displayed.

Workaround: Perform the following:

1. Run the following commands:

   ```
   docker cp aaf_aucore_1:/opt/AuCore/static/nginx.conf.j2 /tmp/
   vi /tmp/nginx.conf.j2
   ```

2. In the `nginx.conf.j2` file, change the `proxy_buffer_size` value from 8k to 16k:

   ```
   proxy_buffer_size 16k;
   ```

3. Include the following lines:

   ```
   proxy_busy_buffers_size 24k;
   proxy_buffers 64 4k;
   ```

4 Run the following commands:

```
docker cp /tmp/nginx.conf.j2 aaf_aucore_1:/opt/AuCore/static/
systemctl restart aauth
```

Upgrading

You can update Advanced Authentication 6.3.0, 6.3.1, 6.3.2, 6.3.3 to 6.3.4.

For more information about upgrading from 6.2, see "Upgrading Advanced Authentication" in the *Advanced Authentication- Server Installation and Upgrade* guide.

NOTE: If you complete the server registration before updating to Advanced Authentication 6.3 Service Pack 4, the Server update to 6.3.4 might not display. Therefore, it is required to de-register and register again to resolve this issue.

NOTE: The recommended upgrade sequence is the upgrade of Advanced Authentication servers, followed by plug-ins and Client components. Any change in the upgrade sequence is not supported.

Upcoming Changes

The PPC64 version of Linux PAM Client will be discontinued in Advanced Authentication 6.4.

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.

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 http://www.microfocus.com/about/legal/.