Advanced Authentication 6.3 Service Pack 5 Release Notes

July 2021

Advanced Authentication 6.3 Service Pack 5 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 5 provides the following enhancements and fixes in this release:

New Features

This release introduces the following features:

- Support for Out-of-Band Method
- Support for Denmark National ID
- Device Authentication Method Support for Linux PAM and Mac OS X Clients

Support for Out-of-Band Method

Advanced Authentication introduces the Out-of-band method to facilitate users to authenticate through the OOB portal or a new Authentication Agent for Web application. During authentication, the authentication request is sent to the OOB portal, Authentication Agent for Web, or Authentication Agent for Windows. Users are required to log in to the portal, Authentication Agent for Web, or Authentication Agent for Windows, and accept the request to authenticate successfully.

For more information, see "Out-of-band" in the *Advanced Authentication - Administration* guide.

Users can access the OOB portal using the URL: `https://<AdvancedAuthenticationServerdomainname>/oob/ui` and succeed the authentication chain to log in to the portal. You can install the Authentication Agent for Web application from the OOB portal by using Google Chrome on a computer, laptop, tablet, or smartphone. You can also use any other browser that supports Progressive Web applications (https://en.wikipedia.org/wiki/Progressive_web_application#Browser_support).

For more information, see "Logging In to Out-of-Band Portal" in the *Advanced Authentication- User* guide.

Support for Denmark National ID

Advanced Authentication introduces the Denmark National ID method to facilitate citizens of Denmark to authenticate using their CPR (Danish social security number), a password, and the PIN which is provided during the enrollment of Denmark National ID.

For more information, see "Denmark National ID" in the *Advanced Authentication - Administration* guide.

Device Authentication Method Support for Linux PAM and Mac OS X Clients

In addition to Windows Client support in the Trusted Platform Module (TPM) mode, the Device Authentication method supports the non-TPM mode in the following clients:

- Linux PAM
- Mac OS X
- Windows

In the non-TPM mode, a key pair is generated during enrollment and is stored in the file system of the workstation or laptop. The key pair is secured using the PIN.

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

By default, the non-TPM mode is enabled on Linux and macOS workstations. However, you can disable the TPM chip in the Windows workstation by using the `deviceAuth.tpmEnabled` parameter.

For more information, see "Device Authentication Setting" in the *Advanced Authentication - Device Service* guide.

Enhancements

This release includes the following enhancements:

Enhancement	Description
Improved the forceCachedLogon Behavior for Linux	When a user tries to log in to a Linux PAM 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: ◆ If Advanced Authentication server is available, the user is allowed to login to Linux PAM Client once. In subsequent login, after selecting the chain (before providing credentials), an error message (about the disabled account) is displayed. ◆ If the Advanced Authentication server is unavailable, the user is allowed to log in to Linux PAM 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. For more information, see "Configuring the Enforced Cached Login" in the *Advanced Authentication- Linux PAM Client* guide.
Settings to Allow Third-Party SAML Service Providers to Select the Authentication Chain	The option, **Enable chain selection** is introduced in the **Web Authentication** policy. This option allows third-party SAML service providers to select the preferred authentication chain with which users can authenticate. For more information, see "Disabling the Authentication Chain Selection" policy in the *Advanced Authentication - Administration* guide.
Support for Emergency Password in the Offline Mode	The Emergency Password method now supports the offline mode to authenticate to the Linux PAM, Mac OS X, and Windows clients.
Option to Lock Users Who Fail While Testing the Enrolled Methods	The **Lock if authenticator test was failed** option is introduced in the **Lockout Options** policy. This option enables you to lock the users who have failed the authenticator test in the Self-Enrollment portal for the number of attempts specified in **Attempts failed**. For more information, see "Lockout Options" in the *Advanced Authentication - Administration* guide.

Enhancement	Description
Provision to Select the Type of Backup Schedule	A list is introduced in the **Backup Schedule** screen to select the type of backup schedule. Earlier, administrator had to specify the command to schedule the backup or to perform a backup. **NOTE:** It is required to re-configure the backup as per your requirement after upgrading to Advanced Authentication 6.3 SP5. For more information, see "Scheduling Backup" in the *Advanced Authentication - Administration* guide.
Enhanced VDA Profile Editor	This release introduces the following enhancements in the VDA: ◆ Ability to debug logs for VDA Profile Editor. ◆ Default focus is provided on **OK** button on the VDA Profiles list to select a profile from the list. ◆ In the case of a single profile, the profile is launched automatically instead of the VDA Profiles list.

Security Improvements

This release resolves the following security issues:

- Potential information leakage (CVE-2021-22529)
- Potential Brute Force attack (CVE-2021-22530)

Software Fixes

This release includes the following software fixes:

Component	Description
Administration Portal	When an administrator tries to delete the existing groups in a chain, the following error message is displayed: `AttributeError 'LogonChainGroup' object has no attribute 'obj_id' (Internal Server Error)`
Administration Portal	The Advanced Authentication log contains many instances of the following message: `level=error msg="Failed to log msg \"\" for logger fluentd: fluent#appendBuffer: Buffer full, limit 1048576`

Component	Description
Administration Portal	The Syslog contains many instances of the following health check messages: `dockerd[2167]: time="2020-12-21T23:30:22.663706880Z" level=warning msg="Health check for container b1cc02cc52d3fe2681c9fa60abfab62aa54fa40d4d833fca4bb0fef5d0414890 error: context deadline exceeded" in syslog.`
Administration Portal	After upgrading to Advanced Authentication 6.3 SP4, the administrators encounter the following error in the **Dashboard** and **Reports** on the servers of the secondary sites: `400 search_phrase_execution_exception.` For more information about fixing the index which is already broken, see TID 7025148.
Administration Portal	When a full synchronization is running for an eDirectory repository, which has a vast number of users and all users have enrolled methods to their respective chains, after three to four hours, the following error message is displayed: `psycopg2.errors.OutOfMemory: out of memory.`
Administration Portal	During backup schedule configuration, both the `celery_long.log` and `celery_long_beat.log` store the passwords in plain text.
Administration Portal	Pre-conditions: ◆ The **Enroll TOTP method when enrolling Smartphone** option is enabled in the **Smartphone** method ◆ The chain with Smartphone method is assigned to an event With these pre-conditions, when a user enrolls the **Smartphone** method on the Enrollment portal using the NetIQ Advanced Authentication app, the TOTP method is not enrolled automatically. Therefore, users are unable to use the OTP displayed in the app for authentication.
Administration Portal	Advanced Authentication integration with MSS (Host Access Management and Security Server) that is based on REST API, is broken and the authentication fails. This issue occurs after upgrading to Advanced Authentication 6.3 SP4.
Administration Portal	When an administrator updates the **Identity provider URL** in the **Web Authentication** policy, the URL is not reflecting in the SAML metadata used for integration.

Component	Description
Administration Portal	During massive use of the fingerprint method, the fingerprint authentication begins to fail after some hours, and the following error recorder in the logs: `ERROR [aucore.views] Public HTTP error: status = 400 Bad Request, title = AuError, description = Timeout (AFIS service), path = /api/v1/logon/{}/do_logon.` This issue happens due to the memory leak.
Administration Portal	After upgrading to Advanced Authentication 6.3 SP4 Patch1 in a clustered environment, the Advanced Authentication appliance displays the following error: `Appliance is under maintenance` The `aucore` container exits automatically. In this release, the database network clients have been disabled during upgrade to avoid any database locks. For more information, see TID 7025121.
Administrative Portal	The aucore container cannot start due to "Elasticsearch is not ready". The logs of the aucore container contain the following warning: `WARNI [aucore.scripts.wait_elastic] ConnectionTimeout caused by - ReadTimeoutError(HTTPSConnectionPool(host='127.0.0.1', port=9200): Read timed out. (read timeout=1))` For more information, see TID 7025172.
Clients	During offline logon to clients, the HOTP counter was not synchronized in the cache. Therefore, after some time, users might encounter the `Counter must sync` error.
Configuration Portal	During upgrade to 6.3.4.1, when the Docker service is updating, it stops all the running dockers and does not start them after the update.
Desktop OTP Tool	OTP tool icon is not removed from the system tray after uninstalling the Desktop OTP tool.
Device Service	After booting, there is a delay of 10 seconds to process the first request of Device Service. This issue occurs in Advanced Authentication 6.3 SP3 and 6.3 SP4.
Device Service	The users are unable to enroll the Fingerprint method using the Lumidigm reader because of the following error: `Unable to detect the fingers.`
Enrollment Portal	When a user tries to enroll the TOTP authenticator and chooses manual TOTP, the TOTP secret field is blank instead of populating the auto-generated secret.

Component	Description
Enrollment Portal	The users are unable to enroll the PKI method when the digital certificate is based on the Online Certificate Status Protocol (OCSP) protocol and HTTP proxy is in use.
Enrollment Portal	The New Enrollment Portal does not open behind the load balancer, and the following error message is displayed: `Error: An OAuth2 application was not specified by the client.`
Enrollment Portal	Pre-conditions in the SMS method: ◆ **Allow overriding phone number** is set to **OFF** ◆ **Allow user enrollment without a phone** is set to **ON** With the above pre-conditions, when a user enrolls the SMS method, the field to specify the phone number is not available. However, when the user saves the enrollment without a phone number and clicks the method again, the following message is displayed: `There is no available category for the required method.` Also, there is no way to remove or re-enroll the enrolled authenticator.
Linux PAM Client	Preconditions: ◆ The Linux client is installed ◆ Logs are available in the `/opt/pam_aucore/var/log` folder When the users uninstall the Linux PAM Client and try to install it again, an error message that states, file content for the log are already defined is displayed. This error occurs in CentOS 7 and Ubuntu 18 environments.
Linux PAM Client	Preconditions: ◆ Configured the proxy settings ◆ The `discovery.dnsTimeout` parameter is set with a higher value With these preconditions, while logging in to the Linux PAM client for the first time, an error message `Cannot find server` is displayed. However, the authentication chains are displayed after some delay.
NPS plug-in	The NPS plug-in fails to establish a connection with the server and due to this the RADIUS authentication is rejected. The NPS logs display the following errors: `Failed to establish connection with server. Message: Exception: Invalid JSON: 'utf-8' co-dec can't decode byte 0xb0 in position 75: in-valid start byte, code: 499.`
RADIUS	The **Result Specification** rule configured for a RADIUS event does not apply if the **Result Specification** rule in the **RADIUS Options** policy is empty.

Component	Description

RDP	Precondition:
	The `card.forceVirtualChannels` is set to `true`.
	In the RDP session when a user tries to authenticate, after clicking OK, instead of displaying proper error message, the following error message was displayed:
	`Exception`
	Now the following error is displayed:
	`Device cannot be redirected via VirtualChannel.`

Risk Service	After upgrading to Advanced Authentication 6.3 SP3 and SP4, the Risk Service Settings page is blank.

Risk Service	On an Advanced Authentication appliance where the Risk Service related license is not applied, every second, the following log messages are shown:
	`rbacollector`
	`RiskService collector Waiting for Riskservice dataservice container to be ready`
	`rbanotification`
	`RiskService notification Waiting or RiskService dataservice container to be ready`
	`rbainterset`
	`RiskService interset Waiting for RiskService dataservice container to be ready`
	`rbacore`
	`RiskService core Waiting or RiskService dataservice container to be ready`
	`rbaui`
	`RiskService Waiting for RiskService dataservice container to be ready`

Risk Service	When Risk Service is enabled and configured, we are getting the continuous replication conflicts: `Could not find the target table 'risk_configuration'.`
Smartphone Authentication	After upgrading to Advanced Authentication 6.3 SP4, while logging in to Advanced Authentication portals, the Smartphone authentication does not initiate the push notification automatically. It requires the user to click **Next**. Also, if you expand the Offline OTP section the LDAP password is pre-filled in the respective field. This issue occurs on the Firefox browser.

Component	Description
Web Authentication	When opening an OAuth 2.0 event the following error message is displayed: `{"status":"error","errors":[{"location":"server","name":"Internal Server Error","description":"PyoidcError provider info issuer mismatch 'https://164.99.162.233/osp/a/TOP/auth/oauth2' != 'https://localhost/osp/a/TOP/auth/oauth2'"}]}` **NOTE:** If you specify **Identity provider URL** in the **Web Authentication** policy, ensure to use the same URL to access the server.
Web Authentication	When users try to authenticate using SAML, the authentication fails. This issue occurs because the Advanced Authentication replaces the space character in the SAML assertion with `question mark(?)`.
Windows Client	Windows Client does not properly display the Application logs in the Windows Event Viewer.
Windows Client	When a user tries to authenticate to Windows Client, it freezes in the `Please wait` screen after providing the username. This issue happens only in Windows machines with external Nvidia Quadro graphics cards and their drivers installed. For more information, see Windows Client Freezes When A User Authenticates to an Application with UAC in the Advanced Authentication - Windows Client guide.
Windows Client	After setting `forceCachedLogon` to `True`. When a user uses 1:N, and after taping the card, the following error message is displayed: `Internal Server Error`

Upgrading

You can upgrade to Advanced Authentication 6.3.5 from one of the following versions of Advanced Authentication:

- 6.3
- 6.3.1
- 6.3.2
- 6.3.3
- 6.3.4

For more information about upgrading from Advanced Authentication 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 SP4, the server update to 6.3 SP4 might not be displayed. 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.

Known Issues

Advanced Authentication 6.3 Service Pack 5 includes the following known issue:

An Error Message While Enrolling FIDO U2F

Issue: During the FIDO U2F enrollment, the following error message is displayed when the user touches the FIDO U2F button:

```
Enroll failed: Device is not attested. Contact your administrator to upload your token attestation certificate
```

Upcoming Changes

The Advanced Authentication 6.4 will include the following changes:

- The PPC64 version of Linux PAM Client will not be supported.
- The options, **Push salt TTL** and **Authentication salt TTL** will be removed from the **Smartphone** method settings.
- The user credentials prompt for HTTPS proxy will be removed during logon and the credentials will be made available in the `config` file.

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/.

© Copyright 2021 NetIQ Corporation, a Micro Focus company. All Rights Reserved.