Access Manager Appliance 5.0 Service Pack 3 Release Notes

September, 2022

Access Manager Appliance 5.0 Service Pack 3 (5.0.3) 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 Access Manager forum on Micro Focus Forums, our online community that also includes product information, blogs, and links to helpful resources. You can also share your ideas for improving the product in the Ideas Portal.

For more information about this release and the latest release notes, see the Documentation page. Note that we have moved Access Manager 5.0 documentation from the NetIQ domain to Micro Focus. For Access Manager documentation versions prior to 5.0, see Documentation.

For a list of all issues resolved in NetIQ Access Manager 5.x, including patch and service pack releases, see List of fixed issues in Access Manager 5.x.

If you have suggestions for documentation improvements, click **comment on this topic** at the top or bottom of the specific page in the HTML version of the documentation posted on the Documentation page.

For information about the Access Manager support life cycle, see the Product Support Life Cycle page.

What's New?

This release includes the following new features and enhancements:

Kerberos Privileged Attribute Certificate Support

Access Manager adds the Privileged Attribute Certificate (PAC) validation support for Kerberos authentication. PAC contains the information about a user's privileges. Domain controllers add this information to Kerberos tickets when the user authenticates within an Active Directory domain.

When users use their Kerberos tickets to authenticate to other systems, the PAC can be read and utilized to identify their level of rights without contacting the domain controller to request that information.

To support the PAC, Access Manager introduces the following three new properties for the Kerberos class:

- PacAvailable
- ResolvedGroupNames
- ExtendedParameter

For more information about these properties, see Kerberos Privileged Attribute Certificate .

User Auto Provisioning Support for Itsme

With this release, Itsme is enhanced to support the **Auto Provision User** option. Enabling this option allows to map an incoming user-specified attribute to an existing user in the local user store.

For more information, see Social Authentication in the NetIQ Access Manager Appliance 5.0 Administration Guide.

Custom Attribute Support for Itsme

This release introduces **Custom Attribute** option for Itsme. This options allows you to add additional attribute defined by Itsme that is not part of Access Manager's social attribute list.

For more information, see Social Authentication in the NetIQ Access Manager Appliance 5.0 Administration Guide.

New Access Gateway Advanced Option for Certificate Security

This release introduces a new option `SSLPassPhraseDialog` in Access Gateway Advanced Option to enhance proxy services certificate security.

NOTE: The `SSLPassPhraseDialog` option must not be updated or deleted. For more information, see Configuring Global Advanced Options in NetIQ Access Manager Appliance 5.0 Administration Guide.

OAuth Sample Client Applications

OAuth sample client applications help both web and mobile OAuth Client application developers with information about how to integrate with Access Manager as an OAuth Server and protect the client application API and resource servers.

For more information, see OAuth Sample Client Application.

Updates for Dependent Components

This release provides the following updated components:

- Tomcat 9.0.65
- Apache 2.4.54
- Log4j 2.17.1
- JDK 1.8.0-342
- OpenSSL-1.0.2zf

Videos

This release includes the following videos:

- Integrating Access Manager with Itsme Using Auto User Provisioning

 http://www.youtube.com/watch?v=EtNw7Wvk_5g

- IDP Authentication APIs

 http://www.youtube.com/watch?v=qwtTW2EpGwo

Security Vulnerability Fixes

Access Manager 5.0 Service Pack 3 resolves the following vulnerability issues:

- Fix for the Log4j vulnerability (Log4j library migration)
- Fix for vulnerabilities in third-party component libraries
- Fix for Multiple XSS vulnerabilities in Administration Console CVE-2022-26325.

Resolved Issues

This release includes the following software fixes:

Component	Bug ID	Issue
OAuth	534075	The JSON response contains Boolean values as a String for attributes received from LDAP, such as email_verified.
OAuth	547044	In Access Manager 5.0 Service Pack 2, the OAuth Client credential flow does not return any scopes or claims in the access token.
OAuth	512050	OAuth clients' authorization code requests fail after upgrading to Access Manager 5.0 Service Pack 2.
Administration Console	508008	When the `novell-tomcat9-service.service` is loaded, it is reported as `failed.failed IManager Tomcat9 service` by Administration Console.
Advanced Authentication	549175	While configuring Advanced Authentication, the users are unable to enter the domain name in the **Server Domain** field.
Identity Server	436019	SAML 2.0 with X509 is not working after upgrading to Access Manager 5.0 Service Pack 1.
Identity Server	479253	When users try to cancel the Advanced Authentication-based second factor screen, the authentication fails.
Logging/alerting/ monitoring	496309	Inconsistent `timestamp` field format is displayed in syslog messages.
Identity Server	510015	When users try to upgrade to Access Manager 5.0 Service Pack 1, the validation of service pack fails intermittently.
Identity Server	481024	An invalid signature is displayed while validating the KeyInfo in signature.
Access Gateway	515101	Invalid redirection of the reverse proxy service request occurs after upgrading to Access Manager 5.0 Service Pack 2.
Policy Authorization	328506	The query string has to be added from the original request to the redirect URL in the authorization policy.
Identity Server	337063	Azure multi-factor authentication does not work as expected due to a federation issue in the hybrid domain.
Access Gateway	495347	While upgrading to Access Manager 5.0 Service Pack 1, the following error is displayed: `Blocked potentially malicious Reference URI in incoming authn request signature (possible DOS attack)`.
Identity Server	501185	SAML authentication fails when the signed request contains an AssertionConsumerService (ACS) URL.
Identity Server	516068	The LDAP search context does not work for a few users.
Identity Server	507011	Users were not able to log in to Access Manager as SAML 2 service provider as there was a mismatch of the allowable class on the contract.

Component	Bug ID	Issue
Identity Server	582014	After upgrading to 5.0 Service Pack 2, details of Identity Server and Access Gateway clusters on Administration Console are not accessible, and the HTTP 400 Bad Request error is displayed.
Identity Server	567071	Whenever a user has two Common Names (CNs), the user sessions cannot be terminated from Administration Console.
Access Manager	217508	A reverse proxy cannot be defined for a secondary IP address on Access Manager Appliance.
Identity Server	487149	Device FingerPrint SQL script error is displayed for Oracle database.
Identity Server	319143	If the metadata of the SAML 2 service provider has an expiry date greater than 2038, it is reported as expired.
Identity Server	440068	The SAML service provider authentication request fails, and a warning message is displayed as `Invalid resource key: ACS URL in unsigned request could not be verified. since upgrading to NAM 4.5.3.`

Installing or Upgrading Access Manager

After purchasing Access Manager Appliance 5.0.3, download the software and the license from the Software License and Download (https://sld.microfocus.com/) portal.

Table 1 *Files Available for Access Manager Appliance 5.0.3*

Filename	Description
`AM_503_AccessManagerAppliance.iso`	Contains the Access Manager Appliance .iso file
`AM_503_AccessManagerAppliance.tar.gz`	Contains the Access Manager Appliance .tar file
`AM_502_AnalyticsDashboard.tar.gz`	Contains the Access Manager Analytics Server .tar file

For information about the upgrade paths, see Supported Upgrade Paths. For more information about installing and upgrading, see the NetIQ Access Manager Appliance 5.0 Installation and Upgrade Guide.

Verifying Version Number After Upgrading to 5.0 Service Pack 3

After upgrading to Access Manager Appliance 5.0.3, verify that the version number of the component is indicated as **5.0.3.0-126**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **5.0.3.0-126**.

Supported Upgrade Paths

To upgrade to Access Manager Appliance 5.0 Service Pack 3, you must be on one of the following versions of Access Manager:

- 4.5 Service Pack 5
- 4.5 Service Pack 5 Patch 1 (Log4j)
- 4.5. Service Pack 5 Patch 2 (OpenSSL)
- 4.5 Service Pack 6
- 5.0 Service Pack 1
- 5.0 Service Pack 1 Patch 1 (Log4j)
- 5.0 Service Pack 1 Patch 2 (OpenSSL)
- 5.0 Service Pack 2
- 5.0 Service Pack 2 Patch 1

Known Issue

The following issue is currently being researched for Access Manager 5.0 Service Pack 3.

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit Micro Focus Support (https://www.microfocus.com/support-and-services/), then select the appropriate product category.

- "Risk-Based Policies Are Evaluated Incorrectly When The User Attribute Does Not Exist" on page 6

Risk-Based Policies Are Evaluated Incorrectly When The User Attribute Does Not Exist

Issue: If an eDirectory attribute used in a User Profile Rule does not exist, the risk-based policies are not evaluated correctly and the rule is triggered at the wrong time.

Workaround: A patch to fix this issue is available in defect 196835. Please contact Support and provide the defect ID. They will assist with applying the patch and configuring the attributes to ignore the missing attributes.

Planned End of Support

SecretStore will be deprecated in the next release of eDirectory. For more information about SecretStore, see, Configuring a User Store for Secrets.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/

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.microfocus.com/about/legal/.