Access Manager Appliance 5.0 Service Pack 2 Release Notes

April, 2022

Access Manager Appliance 5.0 Service Pack 2 (5.0.2) 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.

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:

Identity Server Authentication APIs

This release introduces Identity Server authentication APIs. These APIs enable you to build your own end-to-end login experience replacing the built-in user portal login experience. You can use these APIs in the following scenarios:

Primary Authentication: Verifies the end-users' credentials using one of the following methods:

- Name/Password - Basic
- Name/Password - Form
- Secure Name/Password - Basic
- Secure Name/Password - Form

Multi-factor Authentication: When Access Manager is integrated with Advanced Authentication through the plug-in approach, the API supports multi-factor authentication for the following methods:

- Smartphone
- Voice call

For more information about these APIs, see Identity Server Authentication API.

You can also configure the default user attributes that you want in the authentication response.

For information about configuring the attributes list, see Identity Server Authentication APIs (https://www.microfocus.com/documentation/access-manager/appliance-5.0/admin/b13e0zob.html#authentication_api) in the NetIQ Access Manager Appliance 5.0 Administration Guide.

Integration of Microsoft Windows Autopilot with Access Manager

Microsoft Windows Autopilot is an end-to-end Windows device management solution. Irrespective of the locations, users can log in to the device using their email ID. When integrated with Microsoft Azure, Access Manager supports the Windows Autopilot feature.

For more information about Windows Autopilot, see “Overview of Windows Autopilot”.

For more information about how to use this feature in Access Manager, see Enabling Access Manager with Microsoft Windows Autopilot in the NetIQ Access Manager Appliance 5.0 Administration Guide.

Support for Specifying Scopes for a Client Application

Access Manager now provides an option to specify scopes for a client application. The application can use only the configured scopes instead of using all scopes available in the resource server.

For more information, see Registering OAuth Client Applications (https://www.microfocus.com/documentation/access-manager/appliance-5.0/admin/b1dj6b2f.html#oauth_client_reg) in the NetIQ Access Manager Appliance 5.0 Administration Guide.

Integration with Itsme

Access Manager now supports authentication through external OAuth provider Itsme. Itsme is Belgium's official mobile identity. It is a digital identity provider, which provides a platform to quickly and effortlessly identify a user on a website or an application.

For more information, see Configuring the Social Authentication Class (https://www.microfocus.com/documentation/access-manager/appliance-5.0/admin/b1ac07ic.html#socialauthproperties) in the NetIQ Access Manager Appliance 5.0 Administration Guide.

Analytics Dashboard Plug-in Support

This release introduces Analytics Dashboard plug-in for the following products: NetIQ SecureLogin.

- NetIQ SecureLogin

  For more information, see Analytics Dashboard in the NetIQ SecureLogin 9.0 Administration Guide.
- NetIQ Secure API Manager

  For more information, see Configure Analytics in the NetIQ Secure API Manager 2.0 Administration Guide.

NOTE: The plug-in is not supported with Access Manager container deployment.

Enhanced WS-Federation Service Provider

Access Manager introduces a new option Token Lifetime for WS-Federation. Using this option, you can configure the validity duration of the authentication token.

For more information, see Modifying the Authentication Response (https://www.microfocus.com/documentation/access-manager/appliance-5.0/admin/wsfed.html#wsfedauthresp) in the NetIQ Access Manager Appliance 5.0 Administration Guide.

Support for Integration with Advanced Authentication as a Service

In addition to the integration with on-premises Advanced Authentication, Access Manager now supports integration with the Advanced Authentication as a Service.

For more information about how to integrate, see Multi-Factor Authentication Using Advanced Authentication (https://www.microfocus.com/documentation/access-manager/5.0/nam_aa_integration_guide/nam_aa_integration_guide.html).

Enhanced UserInfo Endpoint to Decrypt Tokens Encrypted Using Custom Keys

With this release, when JWT is encrypted using custom keys provided in the resource server, user info endpoint is able to decrypt the JWT and provide valid user info details in response.

Access Manager Appliance Install and Upgrade Changes

The following are the changes for Access Manager Appliance installation and upgrade:

- Access Manager Appliance installation is a two-step process.
  1. Deploying the Access Manager Appliance ISO. For more information, see Installation Using the Access Manager Appliance ISO.
  2. Configuring Access Manager Appliance using Common Framework Appliance (CAF) user interface. For more information, see Configure Access Manager Appliance Using Common Appliance Framework User Interface.

  NOTE: You must be on VMWare ESXi 6.0 version or later to deploy Access Manager Appliance.

  NOTE: From Access Manager 5.0 Service Pack 1, operating system and product upgrades will be done using CAF. Therefore, the Upgrade Assistant feature will not be available in Access Manager Appliance.

- The Access Manager Appliance upgrade has been done using the .tar file in the releases earlier than 5.0. Access Manager Appliance 5.0 Service Pack 1 onwards, it is CAF-based. Therefore, to support upgrading of Access Manager 4.5x versions to this CAF-based approach, a migration process has been introduced. This migration involves the following process:
  1. Install 5.0.1 Access Manager Appliance (CAF) as a secondary appliance and point to the 4.5.x appliance.
  2. When the device is imported, convert the 5.0.1 secondary appliance to the primary appliance.
  3. After this conversion is successful, delete the 4.5.x Access Manager Appliance.
  4. Add other nodes by performing a fresh installation of Access Manager Appliance 5.0.1.

For more information, see Migrating Access Manager Appliance in the *NetIQ Access Manager Appliance 5.0 Installation and Upgrade Guide*.

Updates for Dependent Components

This release provides the following updated components:

- Tomcat 9.0.55
- Apache 2.4.53
- Log4j 2.17.1
- JDK 1.8.0_312
- OpenSSL 1.0.2zd

Videos

This release includes the following video:

- Integrating Access Manager with Itsme

 http://www.youtube.com/watch?v=r3LyoSekQmw

Security Vulnerability Fixes

Access Manager 5.0 Service Pack 2 resolves the following security issues:

- The cache-control headers for Identity Server and ESP URL
- Generic XSS validation filter to disable scanning specific directories
- XSS vulnerability fixes in Identity Server. (CVE-2021-22531)
- XSS vulnerability in the Access Manager Administration Console (CVE-2022-26325)
- Redirection Issue with customized URL (CVE-2022-26326)

NOTE: We appreciate Stefan Stojanovski, penetration tester at Viris d. o. o. for finding and responsibly disclosing the vulnerability that is listed as CVE-2021-22531.

NOTE: We also appreciate the researcher community for anonymously notifying other vulnerabilities to us as part of the Responsible Disclosure process.

Resolved Issues

This release includes the following software fixes:

Component	Bug ID	Issue
Identity Server	218333	Swap files are not deleted after the session expires and IDP disk space is consumed by the swap files.
NIDS-Risk	218415	Calculated Risk Score value does not get passed to Virtual Attribute.
Access Gateway	328380	409-esp errors for users having French characters in their name.
NIDS-Risk	329512	IP based rule fails after upgrade to Access Manager 5.0.
NIDS-SAML 2.0	329580	SAML Attribute Matching lookup automatically sets filter to mandate `objectclass=user`.
NIDS-SAML 2.0	329605	Approval Request Link is not working when user is not logged into ServiceNow already.
OAuth	356026	In a client credentials flow, the OAuth grant does not return the scope name.
Admin Console	357126	Admin Console service is not coming up after system reboot on RHEL 8.3 and SLES 15SP3.
OAuth	367068	OAuth logout does not direct you to the default login contract unless you close the browser or try more than once.

Component	Bug ID	Issue
Admin Console	395034	Advance File Configuration Management does not restore original shipping files.
NIDS-OAuth 2.0	414186	Request for authorization code generates a 404 code when `response_mode=form_post` is used.
OAUth	419007	OAuth Redirect URI does not accept special characters.
Admin Console	419013	Brokering groups are missing after upgrading the Admin Console to 5.0.1.
Admin Console	421011	After upgrading to Access Manager 5.0.1 it is not possible to add a Page Matching Criteria which includes double quotes.
NIDS-Risk	432055	User profile rule fails in case of missing user attributes after upgrade from Access Manager 4.5.x to 5.0.1.
OAuth	434011	OAuth login redirect URI is not validated correctly.
OAuth	432131	OAuth client configuration replicated across clusters and deleted when accessed from second cluster.
NIDS-Authentication	458035	DynamicAuthentication not working after update to Access Manager 5.0.1
Admin Console	476028	Upgrade from 4.5.3 to 5.0.1 hangs at Upgrading Novell Identity Server Admin Plug-in.
OAuth	478008	Request all roles attributes in the access token does not work as expected.
Admin Console	483082	ambkup not backing up trusted roots container.
OAuth	479127	OAuth Resource Owner flow using OTP fails.
OAuth	489272	New OAuth resource servers lost from configuration.
Admin Console	425159	Migration of Access Manager 4.5 running on Windows to Access Manager 5.x on Linux fails.

Installing or Upgrading Access Manager

After purchasing Access Manager Appliance 5.0.2, 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 5.0.2*

Filename	Description
`AM_502_AccessManagerAppliance.iso`	Contains Access Manager Appliance .iso file.
`AM_502_AccessManagerAppliance.tar.gz`	Contains 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 5.0.2

After upgrading to Access Manager Appliance 5.0.2, verify that the version number of the component is indicated as **5.0.2.0-309**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **5.0.2.0-309**.

Supported Upgrade Paths

To upgrade to Access Manager Appliance 5.0.2, you must be on one of the following versions of Access Manager:

NOTE: Direct upgrade to Access Manager Appliance 5.0 Service Pack 2 is not supported. For more information, see "Access Manager Appliance Install and Upgrade Changes" on page 4.

- 4.5 Service Pack 3 Patch 2
- 4.5 Service Pack 4
- 4.5 Service Pack 5
- 4.5 Service Pack 5 Patch 1 (Log4j)
- 4.5. Service Pack 5 Patch 2 (OpenSSL)
- 5.0 Service Pack 1 Patch 1 (Log4j)
- 5.0 Service Pack 1
- 5.0 Service Pack 1 Patch 2
- 5.0 Service Pack 1 Patch 3 (OpenSSL)

To upgrade to Analytics Server 5.0.2, you must be on one of the following versions of Analytics Server:

- Analytics Server 5.0
- Analytics Server 5.0 Service Pack 1

Known Issues

The following issues are currently being researched for Access Manager 5.0.2.

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.

Rollback to Default User Attributes Is Not Possible if the Administrator Has Saved Any Other Attribute Set

Issue: You can only modify or change attribute sets to different attribute sets. After the attribute set is updated for Authentication API, it cannot be rolled back to the default settings

Workaround: Do not add any attributes in the **Selected Attribute** field. By default, Authentication API responds with given_name, family_name, and email attributes when no attribute set is configured.

Returned Attribute for an Authenticated User Does Not Contain the Required Value for Authentication API

Workaround: Clear the session cookie if the first user has not logged out.

Authentication API Is Not Picking Up the Properties for the LDAP Search

Workaround: There is no workaround for the issue.

Third Factor of Advanced Authentication Server Is Not Executed Even When IDP Logs State that Contract is Supported

Workaround: Do not use third factor of Advanced Authentication Server.

After Upgrading to Access Manager 5.0.2, OAuth Clients' Authorization Code Requests Fail

Workaround: Install Access Manager 5.0.2.1. For more information about the patch, see Access Manager Appliance 5.0 Service Pack 2 Patch 1 Release Notes.

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/.