Access Manager Appliance CE 24.2 (v5.1) Release Notes

May 2024

Access Manager Appliance 5.1 includes a new Administration Console interface. The new interface is highly intuitive and responsive built on the Angular framework. This release introduces revamped Identity Server configuration pages and auditing for the administration configuration.

Access Manager 5.1 includes new features and 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.

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:

- “Enhanced Administration Console” on page 2
- “Removal of iManager Framework” on page 2
- “Enhanced REST APIs” on page 2
- “Auditing of Configuration Changes” on page 2
- “A New Authentication Class to Encrypt the User Password” on page 3
- “Liberty Configurations Through API” on page 3
- “Updated Apache Httpd Directive” on page 3
- “Branding Updates” on page 3
- “Updates for Dependent Components” on page 3

Enhanced Administration Console

The new Administration Console home page is intuitive and highly responsive. It provides a modernized look with improved UI performance, better accessibility, and seamless configuration. The following are the benefits of the new UI:

- End-to-end application configuration workflow
- Revamp of centralized administration tasks
- Grouping of tasks
- Search by applications
- Filter by application protocols
- Pagination

Removal of iManager Framework

The iManager framework of Access Manager and its dependencies are removed from Administration Console.

Enhanced REST APIs

The Administration Console interface is built using the REST API architectural approach. You can use the REST APIs to automate the Identity Server configurations. This release also introduces the **Try it out** option with Swagger API for you to test.

The Swagger documentation is available in Administration Console. To access it, use your Administration Console hostname and port in the following format:

```
https://<admin-console-host>:<admin-console-port>/nps/swagger-ui.html
```

Auditing of Configuration Changes

This release introduces the auditing of administrator configuration changes.

A New Authentication Class to Encrypt the User Password

This release introduces a new custom authentication class, `SecureCredentialsAuthClass`. Using this class, you can encrypt the user password before sending it to Identity Server. This authentication class uses Web Crypto API for password text encryption from the front end during login.

For more information, see SecureCredentialsAuthClass.

Liberty Configurations Through API

From this release, you can perform Liberty configurations through APIs.

To access the Swagger documentation for the Liberty APIs, use your Administration Console hostname and port in the following format:

`https://<admin-console-host>:<admin-console-port>/nps/swagger-ui.html`.

NOTE: The Administration Console interface does not contain Liberty in Access Manager 5.1. You can configure Liberty only through APIs.

Updated Apache Httpd Directive

With this release, the default value of `MaxConnectionsPerChild` is updated to 2000. Setting it to a non-zero value limits the amount of memory that a child process can consume by memory leakage, if any.

Branding Updates

Micro Focus is now part of OpenText. To adhere to the OpenText brand, the name of the product, its components and user interfaces, logos, company name references, and documentation are updated. The OpenText versioning mechanism uses the CY.Q (Calendar Year.Quarter) format. Starting from the 5.1 release, Access Manager adheres to the OpenText versioning convention. Access Manager 5.1 is known as Access Manager 24.2 (v5.1).

Updates for Dependent Components

This release provides the following updated components:

- JRE 1.8.0-392
- Tomcat 9.0.87
- Activemq 5.16.7
- Apache httpd 2.4.58-510001
- eDirectory 9.2.8
- jackson-databind 2.14.1
- jsoup: 1.16.1
- xercesImpl v2.12.2
- xalan 2.7.3
- wss4j 1.6.17
- junit 4.13.2

- spring-boot 2.7.18
- tomcat-embed-core 9.0.87
- maven-core 3.8.1
- dom4j 2.1.4
- hibernate-core 5.3.20
- xmltooling v1.4.4
- opensaml 2.6.4
- common-fileupload 1.5

Security Vulnerability Fixes

Access Manager 5.1 resolves the following security issues:

- Directory traversal vulnerability in Access Manager, CVE-2024-4556.

  For more information, see KM000032782.
- User impersonation with multi-factor authentication when configured in specification, CVE-2024-4555.

  For more information, see KM000032781.
- Multiple XSS vulnerability in Access Manager, CVE-2024-4554.

  For more information, see KM000032780.

Resolved Issues

This release includes the following software fixes:

Component	Bug ID	Issue
Logging/alerting/ monitoring	493149	Audit events `002E0514` and `002E0525` do not contain User DN.
MAG-eSP	196834	When users access multiple applications or logging in through user portal, 409 error is displayed intermittently.
NIDS-Risk	196835	The evaluation is validated even if the eDirectory attribute used in the `User Profile Rule` does not exist.
NIDS-Authentication	197089	Radius Authentication logs out the user if an incorrect password is entered.
MAG-Proxy	198124	Intermittent CORS errors occur while using the AMPS web application.
Identity Server	198335	If one of the servers of an Identity Server cluster has a garbage collection issue, the service stops responding when the free memory goes below 30 percent. The service needs to be restarted.
Administration Console	211433	Use of password containing <> displays `HTTP 400 Bad Request`.
NIDS-Risk	260059	After upgrading Access Manager from 4.5 to 5.0 Service Pack 2, the Device Fingerprint rule does not send emails.

Component	Bug ID	Issue
Advanced File Configurator	302044	After upgrading to Access Manager 5.0 Service Pack 4, Advanced File Configurator does not work.
NIDS-Authentication	320017	When a user session expires, HTTP status code `200` is displayed. The user is redirected to a blank screen instead of Identity Server logout page.
NIDS-SAML 2.0	490140	The **Attribute matching** settings displays `HTTP Status 500 - Internal Server Error` during SAML 2.0 federation.

For the complete list of software fixes, see Resolved Issues.

Installing Access Manager

The following files are available:

Table 1 *Files Available for Access Manager Appliance 5.1*

Filename	Description
`AM_51_AccessManagerAppliance.iso`	Contains Access Manager Appliance .iso file.
`AM_502_AnalyticsDashboard.tar.gz`	Contains the Access Manager Analytics Server .tar file.

Verifying Version Number After Upgrading to 5.1

After upgrading to Access Manager 5.1, verify that the version number of the component is indicated as 5.1.0.0-272. To verify the version number, perform the following steps:

1. On the **Home** page, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists 5.1.0.0-272.

Accessing Administration Console

Access Manager users are required to access the Administration Console URL. The older URL of Administration Console is no longer supported.

To access the Administration Console, the users are required to use the following URL:

```
https://<Admin-Console IP/DNS>:<Port>/roma/namui
```

You must open a new browser session to access the upgraded Administration Console.

Supported Upgrade Paths

To upgrade to Access Manager Appliance 5.1, you must be on one of the following versions of Access Manager:

- 5.0 Service Pack 4
- 5.0 Service Pack 3

Supported Platforms

The following is the supported platform for Access Manager Appliance 5.1:

- SLES 12 SP5

Not In Scope

Access Manager 5.1 does not support Code Promotion. It will be supported in future releases.

Known Issues

The following issues are currently being researched for Access Manager 5.1:

- "Cluster Name Is Not Displayed on Managed Policies Page" on page 6
- "Local Attribute Type and Group Details Are Missing" on page 6
- "A Cluster or Device Requires an Update Whenever the Payload Makes a PUT Call with the Same Details" on page 6
- "Context-sensitive Help Is Not Localized" on page 6
- "Secondary Identity Server Device is in Halted State after Installing Secondary Access Manager Appliance (603253)" on page 7
- "Unable to Get Clusters in Branding Page after Installing Secondary Access Manager Appliance (604297)" on page 7
- "Issues with Advanced File Configuration After Upgrading to Access Manager 5.1" on page 7

Cluster Name Is Not Displayed on Managed Policies Page

After adding and enabling Identity Server roles, the **Used By** column in **Manage Policies** does not display the cluster name.

Local Attribute Type and Group Details Are Missing

The local attribute type and group details are unavailable in the list while creating an attribute set mapping.

A Cluster or Device Requires an Update Whenever the Payload Makes a PUT Call with the Same Details

Whenever the payload makes a PUT call with the same or updated details, the device or cluster requires an update.

Context-sensitive Help Is Not Localized

Context-sensitive help is not localized for this release.

Secondary Identity Server Device is in Halted State after Installing Secondary Access Manager Appliance (603253)

Workaround: Restart Identity Server

Unable to Get Clusters in Branding Page after Installing Secondary Access Manager Appliance (604297)

Workaround: Restart Administration Console

Issues with Advanced File Configuration After Upgrading to Access Manager 5.1

Issue: After upgrading Access Manager from 5.0 Service Pack 4 to 5.1, a few files in Advanced File Configuration are blank and unusable.

Workaround: To resolve this issue, perform the following steps:

1. Export all Access Manager 5.0 Service Pack 4 configuration before upgrading to Access Manager 5.1.
2. Remove all the configurations after upgrading.
3. Import the exported configurations and apply changes by performing send configuration.

For more information about importing and exporting configurations, see Exporting and Importing Configurations.

For more information about removing configurations, see Removing Configurations.

Planned End of Support

Analytics Dashboard

Analytics Dashboard will be deprecated, and its replacement will be introduced in the future releases. Analytics Dashboard will be supported until the replacement is introduced.

End of Support

With Access Manager 5.1 release, the following have reached end of support and will not be supported in the future releases:

- SAML 1.1
- SLES 15 SP2

Legal Notice