Access Manager 5.0 Release Notes

March 2021

Access Manager 5.0 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.

Access Manager 5.0 Overview

Access Manager 5.0 includes significant improvements in deployment, administration, and automation of the product. This release introduces several features for easing installation, upgrade, and monitoring processes. These features help customers in reducing the total cost of ownership of the product. This release also addresses many long-pending operational challenges.

The product now has a modernized distribution with Docker images and is optimized to run on the Kubernetes platform. As a result, the installation and upgrades are significantly fast. The in-built scaling functionality of the Kubernetes helps with optimizing the cost of running the servers.

Channel-based software distribution is also enhanced. The existing deployments will now get notifications whenever an update to the product is available.

This release also addresses several concerns on handling customization. Using an Advanced File Configurator, you can centrally manage all configuration files. The tool will take care of customized files in future upgrades automatically.

Enhanced Analytics Dashboard offers modernized and customizable graphs, a smaller footprint, and an easier way to manage upgrades. It is delivered as a service, which makes it available for cloud deployments as well.

In addition to these, this release includes many enhancements around OAuth and OIDC. This provides better application interoperability, flexibility, and improved security.

For more information about Access Manager, see *Access Manager Overview*.

For system requirements, see *NetIQ Access Manager System Requirements*.

What's New?

This release includes the following new features and enhancements:

Support for Docker Deployment

Access Manager now supports Docker for deploying the containers. Access Manager components are delivered as Docker images and are self-sufficient to run on their own.

Access Manager Docker images are optimized to run on Kubernetes, a popular container orchestration engine for Docker. Kubernetes simplifies deploying, running, scaling, and upgrading Access Manager Docker images. Access Manager Docker images are cloud-native applications and can run in Kubernetes environments deployed on Linux servers and cloud.

The following are some of the noteworthy advantages while deploying the Docker images in Kubernetes:

- Significantly reduced installation and upgrade time, thereby reducing the maintenance cost.
- Decreased downtime and reduced manual intervention for upkeep. Kubernetes constantly monitors the health of the Access Manager pods. If a pod stops working, Kubernetes automatically starts a new one.
- Kubernetes offers a built-in fault-tolerant environment and therefore has no service interruption. This Kubernetes has built-in isolation mechanisms, such as namespaces. It allows you to group container resources using access permissions, thereby enhancing security.
- Orchestrate and manage all container resources from a single control plane. This helps optimize the networking, load-balancing, security, and scaling across all Kubernetes nodes.
- Access Manager components can be easily scaled up to meet high demands.
- Support for deploying in cloud environments; Amazon EKS and Microsoft Azure AKS.

For more information, see "Installing Access Manager Containers" in the *NetIQ Access Manager 5.0 Installation and Upgrade Guide*.

NOTE: Access Manager Docker images are supported only on a Kubernetes environment.

Online Update Service and Upgrade Assistant

Online Update Service enables you to get the latest Access Manager product updates through the service channel. The Upgrade Assistant feature simplifies the usage of Online Service Update. Using this feature, you can perform the following actions on Administration Console:

- Register to Online Service Update for all devices
- View notifications on Administration Console Dashboard when a release update is available
- View the list of all devices, their versions, and registration status
- View available updates and status of devices
- Invoke the channel registration for an individual device

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

Advanced File Configurator

Access Manager supports many advanced configurations through files, such as `server.xml` and `tomcat.conf`. Using these files, you can perform various customizations for your Access Manager setup. Access Manager also supports customization and extensions of the product through JSP files and authentication classes. In the earlier releases, customers managed these custom files manually during an

upgrade. Besides, system configuration files, such as `server.xml` and `tomcat.conf`, were overwritten with the default values during the upgrade. Access Manager introduces Advanced File Configurator to address these challenges.

Advanced File Configurator helps with the centralized management of configuration files. Using this feature, you can retrieve a configuration file from a specific device, customize it, upload it, and apply the changes to all clusters or a specific cluster.

Advanced File Configurator provides the following features:

- **Manage Configuration:** Manages all configuration files for Administration Consoles, Identity Server, Access Gateway, and ESP.
  - Provides the capability to add, fetch, upload, compare, merge, send to all, and remove configurations. You can also compare files and folders.
  - Provides an option to fetch multiple files from a cluster, modify them, and add them as configuration files in Administration Console.
  - Provides an option to download a specific file or all files related to a device.
  - Provides an option to send configuration changes to all devices together.
  - Maintains a list of all configuration files with the customization details.
- **Export and Import Configuration:** Provides options to export and import the Access Manager configuration across different clusters of the same or different Access Manager setups. The setups must have the same version of Access Manager.
- **Auto-apply Configuration to a New Node:** When a new instance is added to a cluster, all configurations are automatically applied to that instance. No need to manually apply or revert any change to each device.
- **Persist Configuration Across Releases:** Eases restoring customizations after the product upgrade.

For more information, see "Advanced File Configurator" in the *NetIQ Access Manager 5.0 Administration Guide*.

Enhanced Analytics Dashboard

This release introduces a significantly enhanced Analytics Dashboard built on top of the latest Elasticsearch, Logstash, and Kibana (ELK) components. The Dashboard offers significant advantages over the previous versions, including a smaller footprint, better manageability, ease of upgrade, and maintenance.

The following are some of the significant updates included in this release:

- Significantly reduced hardware requirements:

For the Demonstration Purpose	For a Production Environment
◆ CPU: 2 Cores ◆ Memory: 4 GB ◆ Hard disk: 50 GB	◆ CPU: 4 Cores ◆ Memory: 16 GB ◆ Depends on the Access Manager login pattern for a day. For more information, see "Sizing Guidelines".

- Built on top of the latest ELK stack and uses most of the Kibana functions including search, visualizations, custom graphs, and more.
- Built-in geo-location identification.

- To create a custom dashboard using the existing data.
- Customized view of the graphs.
- Significant performance improvement. Supports 600 logins/sec.
- Enhanced security with updated libraries.
- Flexibility to install on SLES and RHEL.
- Clustering for high availability.
- Eliminates dependency on Sentinel for the storage and processing of events.

NOTE: Access Manager still supports sending the Audit events to Sentinel, which works as an independent SIEM system.

For more information, see "Analytics Dashboard" in the "*NetIQ Access Manager 5.0 Administration Guide*".

IMPORTANT: Before installing the new Analytics Dashboard, ensure to delete Analytics Server nodes of the earlier version from Administration Console.

The latest version is independent of the SIEM server and uses logstash that acts as the aggregator and replaces the Analytic Server aggregator. The events are processed by ELK. Therefore, reports and offline Analytics Dashboard are not supported, and the existing events cannot be migrated.

However, you can use the new Analytics Dashboard along with the earlier Sentinel-based Analytics Dashboard to capture events in both until all the data become available in the new dashboard. To achieve this, you must configure two target servers, one for the old and one for the new Analytics Dashboard. For more information, see Setting Up Logging Server and Console Events.

However, you cannot launch the old Analytics Dashboard from Administration Console. Instead, you can access the old data using the following direct access link:

- **Dashboard:** `https://<Analytics IP>:8445/amdashboard/login`

OAuth Enhancements

Access Manager provides the following enhancements to the OAuth support for better application interoperability, flexibility, and improved security:

- **Default Resource Server Configuration:** You can choose a resource server to make it the default resource server. All the new tokens are then issued and encrypted by the default resource server keys.
- **Support to Choose the Resource Server for Token Encryption:** While configuring an Access Gateway Identity Injection policy, you can choose the resource server for encrypting tokens.
- **OIDC Front-Channel Logout Support:** This feature supports the following two forms of logout request:
  - Identity Provider initiated logout request: Allows a user to log out from all client applications when the user logs out from Identity Server.
  - Relying Party (client application) initiated logout request: When a user initiates logout from one client application, the user can authorize to log out from Identify Server and other logged-in applications.

NOTE: The OIDC specification does not mandate that the OIDC endpoints must start with the issuer URL. Therefore, the OAuth client applications that use the `angular-oauth2-oidc` third-party OAuth library might not be functional and display errors after upgrading to Access Manager 5.0. For more information and to rectify the issue, see OAuth Client Application Returns an Error Message (https://www.microfocus.com/documentation/access-manager/5.0/admin/b1cgrlhj.html#angular-oauth2-oidc-error).

- **Support for Multi-Factor Authentication (Resource Owner Credential Grant):** You can now invoke multi-factor authentication for the resource owner credential flow. It supports Smartphone and Voice Call methods.
- **Support to Disable OAuth Client Application:** Access Manager now supports disabling OAuth client applications. Deleting and re-creating a client application can be a hassle, and it also removes the Client ID and Secret. Hence, if you do not need to use a client application temporarily, you can disable it.
- **Performance Improvement of the Client Applications Page:** The Client Applications page is enhanced to:
  - Load thousands of registered client applications instantaneously.
  - Support faster registration and management of client applications.

For more information, see "OAuth and OpenID Connect" in the *NetIQ Access Manager 5.0 Administration Guide*.

Access Manager License

This release introduces an Access Manager licensing solution for better manageability of the product license.

The following three types of licenses are available for Access Manager:

- **Evaluation or Trial License:** This is a free license for evaluating Access Manager. This license is available with Access Manager 5.0 and subsequent releases. Uploading a full license overwrites this evaluation license.

  NOTE: Extension of the Evaluation license is not supported.

- **Permanent or Full License:** This is a paid license and without any expiration date. Customers must procure it from Software Licenses and Downloads. The customers who are upgrading to Access Manager 5.0 do not need to add this license. It will be installed as part of the upgrade process.
- **Subscription License** This license allows users to purchase the product for various time periods, and the users are entitled to use the software during the agreed upon time period. The subscription license includes software license, access to support service, and new versions of the software as they are released. This license is similar to the full license, except that there is an expiration date, whereas full license is a perpetual or permanent license without any expiry period. Customers must procure it from Software Licenses and Downloads.

For more information, see "Access Manager Licensing" in the *NetIQ Access Manager 5.0 Administration Guide*.

NOTE: Secure API Manager licensing is an add-on solution that Micro Focus offers to customers along with Access Manager.

NetIQ MobileAccess 2 App

This release provides the enhanced MobileAccess 2 app. The following are the key features and functions of NetIQ MobileAccess 2:

- Updates to the supporting libraries
- Role-based mobile view of corporate and SaaS applications
- Single Sign-on to the resources, such as federated applications
- Support for the auto-updated view
- Enhanced device registration and deregistration management
- Reduced access-related risk of lost or stolen devices
- Additional passcode protection when enforced by the MobileAccess administrator
- Support for the face identification
- Support for registering of devices using a QR code
- Support for the latest versions of iOS

NOTE: Access Manager 5.0 does not support the earlier version of the MobileAccess app. This release supports only MobileAccess 2.

For more information about MobileAccess, see Enabling Mobile Access in the *NetIQ Access Manager 5.0 Administration Guide* and *Access Manager 5.0 MobileAccess Quick Start*.

Operating System Support

See *NetIQ Access Manager System Requirements*.

Updates for Dependent Components

This release provides the following updated components:

- Tomcat 9.0.41
- eDirectory 9.2.3
- iMan 3.2.3
- OpenSSL 1.0.2x
- Apache 2.4.46

Videos

This release includes the following videos:

- Access Manager Advanced File Configurator: Modifying Session Timeout


http://www.youtube.com/watch?v=JZpu3KnMqXA

- Using Access Manager Analytics Dashboard


http://www.youtube.com/watch?v=dyBBPr6myqE

Security Vulnerability Fixes

Access Manager 5.0 fixes the following security issues:

- The SAML service provider redirection issue when Assertion Consumer Service URL is used (CVE-2021-22506).
- The XSS vulnerability in Administration Console. (CVE-2020-25840)
- An authentication bypass issue. (CVE-2021-22496).

  Special thanks to Tom de Haas of Utrecht University for responsibly disclosing this vulnerability.

Resolved Issues

This release includes the following software fixes:

Component	Bug ID	Issue
Identity Server	284106	Users experience slow login and the number of connections from Identity Server to the active user stores increases. This issue occurs when the following conditions are true: - Identity Server failover is enabled - The user session limit is enabled - One of the Identity Server nodes is down
Identity Server	219348	Updating the Identity Server cluster nodes fails during business hours.
OAuth	218305	When the OAuth prompt parameter is set as `prompt=none` and the **Require user permission** option is disabled, an error message is returned in the authorization endpoint request.
Access Gateway	286173	When protected behind Access Gateway, the SharePoint applications fail to start on Internet Explorer 11. This issue occurs when the Protected Mode is enabled in Internet Explorer.
Access Gateway	218496	Support for the `SameSite` cookie does not work with some user agents, such as the Safari browser.
Access Gateway	216195	Cannot disable cookie mangling for specific cookies.

Deprecation of Support

Support for the following features is deprecated starting this release:

- **Kerberos Constrained Delegation (KCD) support:** Access Manager 5.0 will no longer support Kerberos Constrained delegation (KCD). For more information, see Access Manager Community announcement.
- **Windows Installer Support:** Access Manager 5.0 will no longer support `.exe` based Windows installation. Access Manager 4.5.x will continue to support Windows installers under general support till March, 2022. For more information, see Access Manager Community announcement.

Installing or Upgrading Access Manager

After purchasing Access Manager 5.0, download the software and the license from the Software License and Download (https://sld.microfocus.com/) portal.

The following files are available:

Table 1 *Files Available for Access Manager 5.0*

Filename	Description
`AM_50_AccessManagerService_Linux64.tar.gz`	Contains the Identity Server and Administration Console .tar file.
`AM_50_AccessGatewayAppliance_OVF.tar.gz`	Contains the Access Gateway Appliance OVF template.
`AM_50_AccessGatewayAppliance.tar.gz`	Contains the Access Gateway Appliance .tar file.
`AM_50_AccessGatewayService_Linux64.tar.gz`	Contains the Access Gateway Service .tar file for Linux.
`AM_50_HelmChart-1.0.0.tgz`	Contains the Access Manager Helm Chart 1.0.0.
`AM_50_AnalyticsDashboard.tar.gz`	Contains the Access Manager Analytics Server .tar file.
`AM_50_Containers.tar.gz`	Contains the .tar file of all the images for Docker deployment.
`Dashboard_50_HelmChart-1.0.0.tgz`	Contains the Analytics Dashboard Helm Chart 1.0.0.

NOTE: The Access Manager Appliance installer is not available for this release.

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

IMPORTANT: If you have configured the risk-based authentication, perform the following actions after the upgrade:

1. Copy all custom rules and database-connector jars from `/opt/novell/nids/lib/webapp/WEB-INF/lib` to `/opt/novell/rba-core/lib/webapp/WEB-INF/lib`.
2. (Conditional) Upgrade the Database Schema for Risk Service. For more information, see "(Conditional) Upgrading the Database Schema for Risk Service" in the *NetIQ Access Manager 5.0 Installation and Upgrade Guide*.

Verifying Version Number After Upgrading to 5.0

After upgrading to Access Manager 5.0, verify that the version number of the component is indicated as **5.0.0.0-760**. To verify the version number, perform the following steps:

1 In Administration Console Dashboard, click **Troubleshooting > Version**.

2 Verify that the **Version** field lists **5.0.0.0-760**.

Supported Upgrade Paths

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

- 4.4 Service Pack 4
- 4.4 Service Pack 4 Hotfix 1
- 4.5 Service Pack 2
- 4.5 Service Pack 2 Hotfix 1
- 4.5 Service Pack 2 Hotfix 2
- 4.5 Service Pack 3
- 4.5 Service Pack 3 Hotfix 1
- 4.5 Service Pack 3 Patch 3
- 5.0 Early Access <Only for Analytics Dashboard>

Known Issues

The following issues are currently being researched for Access Manager 5.0.

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.

New or Existing SLES Channel Registration is Disrupted With Installation or Upgrade of Access Manager

Issue: Installing Access Manager 5.0 before registering for SLES channel updates fails to populate the SLES channel updates. You might see the following error message: `Warning: The /etc/products.d/baseproduct symlink is dangling or missing! (Bug 337039)`

Workaround:

- To avoid this issue, register to SLES channel updates before installing or upgrading Access Manager 5.0 and then register to Access Manager 5.0 product channel.
- After registering at Access Manager 5.0 product channel, if you still see issues with registered SLES channel, then change the `/etc/products.d/baseproduct` symbolic link to point to SLES.prod file.

(Docker) Changing the Administration Console Administrator Password Fails

Issue: After changing the administrator password from the Administrator Console, logging in to Access Manager with the new password shows an error stating that the account is locked because of intruder detection. This issue occurs because the password does not get updated in the `values.yaml` file.(Bug 286128)

Workaround:

1. Open the `access-manager/values.yaml` file.
2. Update the new password and save the file.
3. Perform a helm upgrade on the same helm release with the Access Manager helm chart. Use the `helm upgrade <release-name> access-manager -n <name-of-the-namespace>` command.
4. Delete all pods and wait until the `StatefulSets` bring up the pods again.
5. Log in to Administration Console using the new password.

The `amdiagcfg` Script Does Not Work

The `amdiagcfg.sh` script utility does not work in Access Manager 5.0.(Bug 302076)

The `ambkup` Script Does Not Work in the Access Manager Docker Environment

The `ambkup.sh` script does not work in the Access Manager 5.0 Docker environment. (Bug 267085)

Misleading Warning Message When Performing Backup While Running Upgrade Script

Issue: The upgrade script displays the following message while performing backup and restore.(Bug 317328)

```
zip warning: name not matched: /opt/novell/nam/adminconsole/data/NAMLicFile.txt
```

Workaround: Ignore this error and proceed with the upgrade.

Upgrading Access Manager from Version 4.5.3 Patch 3 to 5.0 Fails

Workaround: Perform the following steps:

1. After downloading the Access Manager 5.0 installer, open `common_scripts/upgrade_utility_functions.sh` script.
2. Search for the `checkVersion()` function. You would find the following details:

   ```
   supportedVersions="4.4.4.0\|4.4.4.1\|4.4.4.2\|4.4.4.3\|4.5.2.0\|4.5.2.1\|4.5.2.2\|4.5.3.0\|4.5.3.1\|5.0.0.0"
   ```

3. Add 4.5.3.3 in `supportedVersions`. After adding, it would look similar to the following:

   ```
   supportedVersions="4.4.4.0\|4.4.4.1\|4.4.4.2\|4.4.4.3\|4.5.2.0\|4.5.2.1\|4.5.2.2\|4.5.3.0\|4.5.3.1\|4.5.3.3\|5.0.0.0
   ```

4. Upgrade Access Manager.

(Docker) The Primary and Secondary Administration Console Pod Restarts Multiple Times

Issue: The primary and secondary Administration Console pod restarts multiple times because the hostname, release name, and namespace combination of the IP address is exceeding 54 characters as illustrated in the following example: (Bug 319212)

`mf-access-am-idp-0.mf-access-am-idp.nam-742.svc.cluster.local.`

Workaround: A long host name causes an issue during the creation of encryption certificates. Use characters limiting to 54 before proceeding with the installation. You can confirm this issue using log located at `/tmp/novell-access-manager log`.

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/.