Access Manager Appliance 5.0 Service Pack 1 Release Notes

August 2021

Access Manager Appliance 5.0 Service Pack 1 (5.0.1) 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:

Risk-based Multi-factor Authentication Support for OAuth Client Applications

This release adds risk-based multi-factor authentication support for OAuth client applications. Based on the contextual information of the client application, Access Manager computes the associated risk level and prompts for multi-factor authentication if required.

You can now configure authentication contracts for a client application. To enable risk-based authentication for an OAuth application, configure a risk-based contract for the application.

For more information, see "Managing OAuth Client Application" > **Registering OAuth Client Applications** in the NetIQ Access Manager Appliance 5.0 Administration Guide

For information about configuring risk-based authentication, see Configuring Risk-based Authentication in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

When you configure an authentication contract, the server-side configuration takes precedence. After this configuration, the ACR value in the request is ignored, and the configured contracts are used for authentication.

Identity Server Configuration to Prevent Cross-Site Request Forgery Attacks

This release introduces a new filter `CSRFDetectionFilter` to detect and mitigate any Cross-Site Request Forgery (CSRF) attempts in requests. You can configure this filter in web.xml of Identity Server.

For more information, see "Preventing Cross-Site Request Forgery Attacks" in the *NetIQ Access Manager Appliance 5.0 Security Guide* .

HTTP/2 Protocol Support

Access Manager supports the HTTP/2 protocol.

The HTTP/2 protocol support helps in protecting the web application or web server which is HTTP/2 protocol enabled. This support also helps in communication with the HTTP/2 protocol using the HTTP/2 protocol - enabled browsers.

You can enable the following options:

- Browser and Access Gateway communication using the global and proxy level option named `protocols h2`.
- Access Gateway and web server communication using the proxy level option named `ProxyHTTP2 on`.

For more information, see "Configuring the HTTP/2 Protocol " and Access Gateway Advanced Options in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

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: Access Manager 5.0 Service Pack 1 onwards, 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 1onwards, 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 and Upgrading Access Manager Appliance in the *NetIQ Access Manager Appliance 5.0 Installation and Upgrade Guide*.

Enhanced WS Federation Service Provider

This release adds the following enhancements:

- Support for configuring authentication contracts for applications using WS-Federation. This feature allows configuring step-up authentication for applications that use WS-Federation protocol, such as SharePoint and Office365. For more information, see Defining Options for WS Federation Service Provider Service Provider and Managing WS Federation Providers > **Contracts Assigned to a WS Federation Service Provider** in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

- Support for entityID in the WS-Federation schema. This support enables multiple federation configurations for the WS-Federation targets. For more information, see WS Federation.
- Support for configuring virtual attributes in WS-Federation tokens.

Analytics Dashboard Enhancements

- **ElasticSearch Logstash Kibana (ELK) Version Upgrade:** The ELK version is upgraded from 7.4.2 to 7.10.2. This upgrades does not affect the behavior of Analytics Dashboard. The upgrade script handles the migration configuration. After the ELK upgrade, you can see significant performance improvement in handling number of events per sec. For more information, see Upgrading Analytics Server in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.
- **Analytics Dashboard Cluster Upgrade:** The procedure of upgrading the Analytics Dashboard cluster is updated. For more information, see Upgrade Analytics Server Cluster in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

Updates for Dependent Components

This release provides the following updated components:

- Tomcat 9.0.48
- eDirectory 9.2.4
- iMan 3.2.4

Access Manager 5.0 Changes

The Access Manager 5.0 release preceding the Access Manager Appliance 5.0 Service Pack 1 included the following new features and enhancements, and these are now available with 5.0.1 release:

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 Appliance 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 Appliance 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 and reports from Administration Console. Instead, you can access the old data using the following direct access links:

- **Dashboard:** `https://<Analytics IP>:8445/amdashboard/login`
- **Reports:** `https://<Analytics IP>:8443/sentinel`

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/angular-oauth2-oidc-error.html).

- **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 Appliance 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 Appliance 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 and later do not support the earlier version of the MobileAccess app.

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

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 Service Pack 1 fixes the following security issues:

- XML injection vulnerability could cause service. (CVE-2021-22524).

  Special thanks to Sipke Mellema for responsibly disclosing this vulnerability.
- Potential vulnerability in storing and managing confidential information that might lead to disclosing sensitive information. (CVE-2021-22525).
- Potential open redirection vulnerability when specific resources are accessed. (CVE-2021-22526).
- Information disclosure when server configuration has specific settings. (CVE-2021-22527)
- Cross-Site Scripting (XSS) Vulnerability in Access Manager Product. (CVE-2021-22528)

NOTE: Special thanks to the researcher community for reporting this to us as part of responsible disclosure, anonymously.

Resolved Issues

This release includes the following software fixes:

Component	Bug ID	Issue
NIDS-x509	219447	The cluster property has been renamed from **crlRefreshIntervalDays** to **CRL REFRESH INTERVAL DAYS**.
NIDS-OAuth2.0	218399	The Authorization Code request fails if no default authentication contract is selected for Identity Server.
Analytics Server	219101	Accessing the Analytics Server URL using 8445 port redirects the login page.

Component	Bug ID	Issue
Analytics Server	299150	Changing Administration Console password is displaying exceptions in the `catalina.out` log file.
Advanced Authentication integration	217920	An issue is detected when Identity Server sends a proxy request from one server to the other Identity Server in the `/oauth/nam/callback` page.
Access Gateway Alerts	217620	Access Gateway Service installed on Linux does not rotate the `ags_error.log` file. `logrotate` displays the `skipping "/var/opt/novell/amlogging/logs/ags_error.log` error.
Identity Server	320118	The TOTP method does not work when JSP and MainJSP properties are configured.

Deprecation of the Sample Portal

The sample portal that was part of the earlier releases is not supported in Access Manager Appliance 5.0 SP1 and later.

Installing or Upgrading Access Manager

After purchasing Access Manager Appliance 5.0.1, download the software and the license from the Software License and Download (https://sld.microfocus.com/) portal. For information about how to download the product from this portal, watch the following video:

http://www.youtube.com/watch?v=esy4PTVi4wY

Table 1 *Files Available for Access Manager Appliance 5.0.1*

Filename	Description
`AM_501_AccessManagerAppliance.iso`	Contains Access Manager Appliance .iso file.
`AM_501_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 5.0.1

After upgrading to Access Manager Appliance 5.0.1, verify that the version number of the component is indicated as **5.0.1.0-147**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **5.0.1.0-147**.

Supported Upgrade Paths

To upgrade to Access Manager Appliance 5.0.1, you must be on one of the following versions of Access Manager:

NOTE: Direct upgrade to Access Manager Appliance 5.0 Service Pack 1 is not supported. For more information, see "Access Manager Appliance Install and Upgrade Changes" on page 3.

- 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 2
- 4.5 Service Pack 3 Patch 3
- 4.5 Service Pack 4

Known Issues

The following issues are currently being researched for Access Manager 5.0.1.

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.

- Analytics Dashboard Is Not Accessible After Upgrading from 4.5.3.1 to 5.0.1
- Administration Console Might Become Slow After Upgrading to 5.0 Service Pack 1

Analytics Dashboard Is Not Accessible After Upgrading from 4.5.3.1 to 5.0.1

Workaround: Perform the following steps:

NOTE: Before generating any certificates with Administration Console CA, ensure that the time is synchronized within one minute among all Access Manager devices. If the time of Administration Console is ahead of the device for which you are creating the certificate, the device rejects the certificate.

1. Click **Security** > **Certificates** > **New**.
2. Select **Use local certificate authority**.
3. Specify a name in **Certificate name**.
4. In **Subject**, click the **Edit Subject** icon.
5. In **Common name**, specify the DNS name of Administration Console.
6. Click **OK**.
7. Click **Advanced Options**.
8. In **Alternative name(s)**, click the **Edit Subject Alternate Name(s)** icon > **New**.
9. Specify the following details:

   Name Type: IP address

   Name: IP address of Administration Console

   Name Type: DNS name

   Name: DNS of Administration Console

10 Click **OK**.

11 Click the newly added certificate > **Add Certificate to Keystores**.

12 Add the certificate to the Administration Console Keystore with alias as `tomcat`.

13 Restart Administration Console.

14 Restart the dashboard.

```
ll /etc/products.d/
total 8
-rw-r--r-- 1 root root 2912 Nov  9  2019 SLES.prod
-rwxr-xr-x 1 root root  818 Aug  4 16:39 am.prod
lrwxrwxrwx 1 root root    9 Aug  5 13:04 baseproduct -> SLES.prod
```

Administration Console Might Become Slow After Upgrading to 5.0 Service Pack 1

Workaround: Perform the following steps if you face any slowness:

1 Open the `/etc/opt/novell/tomcat9/server.xml` file using Advanced File Configurator.

For information about how to open and edit a file using Advanced File Configurator, see Modifying Configurations in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

2 Increase `acceptorThreadCount` to `2` for the Administration Console connector:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
maxHttpHeaderSize="8192" minSpareThreads="25" enableLookups="false"
disableUploadTimeout="true" acceptorThreadCount="2" acceptCount="100"
scheme="https" secure="true" keystoreType="PKCS12" keystoreFile="/var/opt/
novell/novlwww/.p12" keystorePass="changeit" clientAuth="false"
sslProtocol="TLS" sslEnabledProtocols="+TLSv1.1, +TLSv1.2"/>
```

3 Save the file.

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/.