Access Manager 5.0 Service Pack 1 Release Notes

August 2021

Access Manager 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 Applications" > **Registering OAuth Client Applications** in the *NetIQ Access Manager 5.0 Administration Guide*.

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

Access Manager Migration from Windows to RHEL

Access Manager 5.0 and later versions do not provide Windows-based installers. To leverage the latest features and functionalities available with version 5.0 Service Pack 1 or later, you can migrate Access Manager from Windows to RHEL.

For more information, see "Migrating Access Manager from Windows to RHEL" in the *NetIQ Access Manager 5.0 Installation and Upgrade Guide*.

Identity Server Configuration to Prevent Cross-Site Request Forgery Attacks

This release introduces a new filter CSRF`DetectionFilter` 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 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 5.0 Administration 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 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 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 5.0 Administration Guide*.

Upgrade Service Changes

You can now upgrade Access Manager through Upgrade Service. This upgrade supports both SLES and RHEL operating systems. For more information, see Upgrading Access Manager through Upgrade Assistant in the *NetIQ Access Manager 5.0 Installation and Upgrade Guide*. In subsequent releases of Access Manager, Update Service will be enabled through Administration Console.

Operating System Support

See *NetIQ Access Manager System Requirements*.

Updates for Dependent Components

This release provides the following updated components:

- Tomcat 9.0.48

- eDirectory 9.2.4
- iMan 3.2.4

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.
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.

Installing or Upgrading Access Manager

After purchasing Access Manager 5.0.1, download the software and the license from the Software License and Download (https://sld.microfocus.com/) portal.

Table 1 *Files Available for Access Manager 5.0.1*

Filename	Description
AM_501_AccessManagerService_Linux64.tar.gz	Contains the Identity Server and Administration Console .tar file.
AM_501_AccessGatewayAppliance_OVF.tar.gz	Contains the Access Gateway Appliance OVF template.
AM_501_AccessGatewayService_Linux64.tar.gz	Contains the Access Gateway Service .tar file for Linux.
AM_501_AccessGatewayAppliance.tar.gz	Contains the Access Gateway Service .tar file.
AM_501_Dashboard_HelmChart-1.0.1.tgz	Contains the Analytics Dashboard Helm Chart 1.0.1.
AM_501_AnalyticsDashboard.tar.gz	Contains the Access Manager Analytics Server .tar file.
AM_501_Containers.tar.gz	Contains the .tar file of all the images for Docker deployment.
AM_501_HelmChart-1.0.1.tgz	Contains the Access Manager Helm Chart 1.0.1.

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.

To upgrade Access Manager on Docker, see Helm Charts in the *NetIQ Access Manager 5.0 Installation and Upgrade Guide*.

Verifying Version Number After Upgrading to 5.0.1

After upgrading to Access Manager 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 5.0.1, you must be on one of the following versions of Access Manager:

- 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
- 4.5 Service Pack 4
- Access Manager 5.0

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.

- An Issue with Access Manager 5.0 Service Pack 1 Helm Rollback
- Upgrading Kubernetes Cluster Server to a Later Version Disrupts the Installed Access Manager Setup
- An Issue with the Advanced Authentication Integration Configuration After Migrating Access Manager from Windows to RHEL
- Analytics Dashboard Is Not Accessible After Upgrading from 4.5.3.1 to 5.0.1
- An Issue with SLES Registration and Updates After Installing or Upgrading Access Manager
- Upgrading the Secondary Administration Console from 4.5 Service Pack 4 to 5.0 Service Pack 1 Fails
- Administration Console Might Become Slow After Upgrading to 5.0 Service Pack 1

An Issue with Access Manager 5.0 Service Pack 1 Helm Rollback

Workaround: No workaround is available.

Upgrading Kubernetes Cluster Server to a Later Version Disrupts the Installed Access Manager Setup

Workaround: This Kubernetes upgrade approach is recommended when Access Manager is deployed.

Before Upgrade:

1. Scale down the Identity Server and Access Gateway pods to zero. A sample format is provided:
   - `kubectl scale statefulset access-manager-am-idp --namespace automation --replicas=0`
   - `kubectl scale statefulset access-manager-am-ag --namespace automation --replicas=0`

     This step prevents scheduling of Identity Server and Access Gateway nodes to other nodes during the Kubernetes upgrade.
2. Upgrade the Kubernetes cluster to the desired version.
3. **Post Upgrade**:

   Scale up the Identity Server and Access Gateway pods to the original count.
4. Log in to the Administration Console and check if the newly scheduled Identity Server and Access Gateway nodes are scheduled on the nodes on which they were scheduled before the upgrade. If not, then perform the following actions:
   - In the Identity Server cluster, remove the non-reporting Identity Server nodes and add the newly imported nodes.
   - In the Access Gateway cluster, add the newly imported Access Gateway nodes to the cluster and turn one of the new nodes as the primary member and delete all the non-reporting nodes.

NOTE: This is applicable to the manual Kubernetes upgrade process.

An Issue with the Advanced Authentication Integration Configuration After Migrating Access Manager from Windows to RHEL

After migration, the backup of config.xml does not contain endpoint details.

Workaround: Re-create the endpoints.

1. Click **Devices** > **Identity Servers** > **Shared Settings** > **Advanced Authentication**.
2. Delete the domain name or IP address of the Advanced Authentication server, specify a dummy IP address, and click **Apply**. For example, `10.10.10.11`
3. Remove the `/opt/novell/nam/idp/plugins/aa/config.xml` file from all Identity Servers of the cluster.
4. Go to the Advanced Authentication administration portal and delete the endpoints.
5. At Access Manager, navigate to **Devices** > **Identity Servers** > **Shared Settings** > **Advanced Authentication** and specify the domain name or IP address of the Advanced Authentication server.
6. Click **Apply**.
7. Verify that the endpoint's ID and secret key are generated in the `config.xml` file.

   Verify that the endpoint has been created in the Advanced Authentication server. Go to the Advanced Authentication administration portal and verify that the hostname or domain name of the Identity Server cluster is displayed as the endpoint under **Endpoints**. If the cluster has only one Identity Server, the endpoint name is the DNS of Identity Server's base URL.

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
```

An Issue with SLES Registration and Updates After Installing or Upgrading Access Manager

Installing or upgrading to Access Manager 5.0 Service Pack 1 might hinder fetching updates from the SLES updates channel.

This issue might occur if `/etc/products.d/baseproduct` is symbolically linked to the `/etc/products.d/am.prod` file instead of the `/etc/products.d/SLES.prod` file. For example,

```
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 -> /etc/products.d/am.prod
```

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

1 Register to the SLES updates channel before installing or upgrading Access Manager 5.0 Service Pack 1 and ensure that SLES updates are being fetched as expected.

2 Before installing and upgrading to Access Manager 5.0 Service Pack 1, ensure that the `/etc/products.d/baseproduct` file is symbolically linked to `/etc/products.d/SLES.prod` file. For example,

```
ll /etc/products.d/

total 8

-rw-r--r-- 1 root root 2912 Nov  9  2019 SLES.prod

lrwxrwxrwx 1 root root    9 Aug  5 13:04 baseproduct -> SLES.prod
```

3 If a symbolic link is not present between `/etc/products.d/baseproduct` and `SLES.prod`, then run the following commands:

```
cd /etc/products.d
```

`rm baseproduct` command removes the symbolic link from baseproduct.

`ln –s SLES.prod baseproduct command` creates a symbolic link between baseproduct and SLES.prod.

4 Install or upgrade to Access Manager 5.0.x.

5 Ensure that a symbolic link between `/etc/products.d/baseproduct` and `SLES.prod` exists post-install or upgrade. Run the following command to validate:

```
ll /etc/products.d
```

Example result:

```
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
```

To use Upgrade Assistant:

Change the `/etc/products.d/baseproduct` symbolic link from `SLES.prod` file to `/etc/products.d/am.prod`:

Commands:

```
cd /etc/products.d/
```

Verify the baseproduct symbolic link before changing it using the following command:

```
ll
```

Remove the symbolic link from baseproduct using the following command:

```
rm baseproduct
```

```
ln -s /etc/products.d/am.prod baseproduct
```

Verify the baseproduct symbolic link is now pointing to the `am.prod` file.

```
ll
```

Example output:

```
ll
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   23 Aug  5 14:24 baseproduct -> /etc/products.d/am.prod
```

NOTE: ◆If you are already registered then change the symbolic link to `am.prod` file and enable the AM-5.0-Product repository (if present) using the following command:

```
zypper mr -e AM-5.0-Product
```

- If you are changing the symbolic link back to SLES.prod, you must disable the AM-5.0-Product repository using the following command:

```
zypper mr -d AM-5.0-Product
```

Now, you can register or deregister the update service, or check for available updates on the Upgrade Assistant page.

NOTE: If the symbolic link of baseproduct -> /etc/products.d/am.prod exists, there will be issues in fetching updates from the SLES updates channel. Hence, it is recommended to keep this configuration only for the duration until the user operations are done on the Upgrade Assistant page. When operations are complete on the Upgrade Assistant page, change the baseproduct symbolic link to SLES.prod.

To change the baseproduct symbolic link to SLES.prod, use the following commands:

```
cd /etc/products.d/
```

Verify the baseproduct symbolic link before changing it using the following command:

```
ll
```

Remove the symbolic link from baseproduct using the following command:

```
rm baseproduct
```

```
ln -s SLES.prod baseproduct
```

Verify the baseproduct symbolic link is now pointing to the SLES.prod file.

```
ll
```

Example output:

```
ll
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 14:36 baseproduct -> SLES.prod
```

NOTE:

- The operating system `prod` file name might vary depending on the operating system. For example, `SLES.prod` file.
- This issue mostly occurs during the upgrade from Access Manager 5.0 to 5.0 Service Pack 1. However, it is recommended to verify the /etc/products.d/baseproduct symbolic link before performing a fresh installation or upgrading from Access Manager 4.5.X to 5.0 Service Pack 1.

Upgrading the Secondary Administration Console from 4.5 Service Pack 4 to 5.0 Service Pack 1 Fails

Workaround: Perform the following steps:

1. Connect to the primary and secondary Administration Console through SSH and verify the SSL EC certificate of secondary Administration Console by using the following command:

   ```
   ndsbackup s | grep "SSL EC"
   ```

2. Run the `ndsconfig upgrade` command first on the primary and then on the secondary Administration Console.

   Specify the admin name with context, password, and confirm if you want to configure Enhanced Background Authentication.

3 Run `ndsbackup s | grep "SSL EC"` again on both primary and secondary Administration Consoles to verify the EC certificate creation.

4 Upgrade from 4.5 Service Pack 4 to 5.0 Service Pack 1.

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 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/.