opentext

Release Notes

Access Manager Appliance CE 24.2.1 (v5.1.0.1) Release Notes

September 2024

Access Manager Appliance 5.1.0.1 supersedes Access Manager 5.1.

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.

Resolved issues

This release includes the following software fixes:

Component	Bug ID	Issue
SAML2.0	602434	Administration Console SAML 2.0 service provider configuration menu returns the global SAML metadata instead of service provider specific metadata.
NIDS-Authentication	604444	After upgrading to Access Manager 5.1, the service provider displays incorrect signing and encryption certificates.
NIDS-SAML2.0	607120	After upgrading to Access Manager 5.1, Liberty and SAML2.0 identity provider metadata is modified.
NIDS-SAML2.0	608258	After upgrading to Access Manager 5.1, IDP server returns `Request Denied` message on an unsigned SAML2.0 authentication request.
Administration Console	619051	After upgrading to Access Manager 5.1, Administration Console does not allow adding an attribute within a set without defining a remote attribute name.
NIDS-Authentication	636116	Deleting an identity server role that contains a contract, class, or method without disabling it on the identity cluster does not return an error until the identity server is restarted, and this causes server failure.

Component	Bug ID	Issue
Administration Console	639083	Enabling Session Assurance displays error.
Administration Console	646003	After upgrading to Access Manager 5.1, Advanced File Configurator files are empty.
Administration Console	646005	New Attribute Set cannot have _ (underscore) as **Set Name**.
NIDS-WS-Fed	646188	**Office 365 WSFED** application connector fails to save application.
NIDS-User Stores	646205	When the user is not in the first eDirectory context, login fails.
NIDS-OAuth2.0	648005	The **Save** option is disabled even after updating the OAuth2.0 client registration details.

Security vulnerability fixes

Access Manager 5.1.0.1 resolves the following security issue:

Access Manager supports RADIUS authentication class. RADIUS client is updated to consistently send the Message-Authenticator (MA) attribute at the beginning of all RADIUS messages when the `MessageAuthenticatorAttribute` is set to true at `Method` configuration, CVE-2024-3596.

For more information, see Configuring Authentication Methods in the NetIQ Access Manager Appliance CE 24.2 (v5.1) Administration Guide.

Verifying Version Number Before Upgrading to 5.1.0.1

Before upgrading, 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.

Upgrading to Access Manager 5.1.0.1

IMPORTANT: In a cluster setup, ensure that you install the patch on each node of the Access Manager setup.

- "Downloading the Patch" on page 2
- "Upgrading to Access Manager 5.1.0.1" on page 3
- "Managing the Patch" on page 3

Downloading the Patch

The patch helps in upgrading to the latest version of Access Manager with ease.

NOTE: This patch update is not required for Analytics Server.

IMPORTANT: Ensure that you are currently on Access Manager 5.1 before upgrading to Access Manager 5.1.0.1.

You need to procure the license key from the Software License and Download portal to register to 5.1.

Upgrading to Access Manager 5.1.0.1

You can upgrade to Access Manager 5.1.0.1 by using the proceeding steps. This requires few manual interventions to continue the upgrade process.

1 Extract the patch file by using the `unzip AM_5101.zip` command.

After extraction, the following files and folders are created in the `AM_5101` folder:

Table 1 *Files and folders created in the AM_5101 folder after extracting the patch installer ZIP file*

File/Folder Name	Description
`rpm`	Contains rpm files for the patch.
`installPtool.sh`	Script to install the patch and the patch tool.
`installPatch.sh`	Script to install the patch tool and the updated binaries.

2 Log in as the root user.

3 Go to the location where you have extracted the patch files.

4 Run the `installPatch.sh` command.

This command installs the patch and the bundled binaries.

NOTE: To manage the Access Manager patch file, refer to "Managing the Patch" on page 3.

If the patch is already installed, the installer exits with a message.

Managing the Patch

1. After the patch is installed, go to the following folder:

   `/opt/novell/nam/patching/bin`

2. Use the following options to manage the Access Manager patch file:

Option	Description	Command on Linux server
`-qa`	Lists all installed patches.	`./patch -qa`
`-q`	Lists details of an installed patch.	`./patch –q` Example:`./patch –q P1-22`

Option	Description	Command on Linux server
`-i`	Installs a patch. During the installation of a patch, all running services are stopped temporarily. After a patch is installed, all services are restarted and details of the operation are written to log files.	`./patch –i <`*`location and patch name`*`>` Example:`./patch –i /opt/novell/nam/Patches/AM_5101/AM_5101-22.patch`
`-e`	Removes an installed patch. The patch maintains a content relationship among patches. So, if you have installed patch 1 and patch 2, patch 1 cannot be removed without removing patch 2. This is because patch 2 contains details of patch 1 as well. During the patch process, all the running services are stopped temporarily.	`./patch –e <`*`patch name`*`>` Example:`./patch –e P1-22`
`-qpl`	Lists details of a patch that is not installed. If you want to view the changes that are included in the patch file without installing it on your server, use this option	`./patch –qpl <`*`location and patch name`*`>` Example:`./patch –qpl /opt/novell/nam/Patches/AM_5101/ AM_5101-22.patch`
`-v`	Verifies integrity of a patch.	`./patch –v <`*`location and patch name`*`>` Example:`./patch –v /opt/novell/nam/Patches/AM_5101/ AM_5101-22.patch`
`-t`	Verifies if services can be restored by the installer. Use this option to stop/start all services after the installation of patch.	`./patch –t <`*`location and patch name`*`>` Example:`./patch –t /opt/novell/nam/Patches/AM_5101/ AM_5101-22.patch`

Verifying Version Number After Upgrading to 5.1.0.1

After upgrading, verify that the version number of the component is indicated as 5.1.0.1-22. To verify the version number, perform the following steps:

1. On the **Home** page, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists 5.1.0.1-22.

Legal Notice

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see https://www.microfocus.com/en-us/ (https://www.microfocus.com/en-us/).