Access Manager 4.5 Service Pack 1 Release Notes

October 2019

Access Manager 4.5 Service Pack 1 (4.5.1) includes enhancements, improves usability, and resolves several previous issues.

Many of these improvements are 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 our products meet all your needs. You can post feedback in the Access Manager forum on our community website that also includes product notifications, blogs, and product user groups.

For information about the previous release, see Access Manager 4.5 Hotfix 1 Release Notes (https://www.netiq.com/documentation/access-manager-45/accessmanager45-hf1-release-notes/data/accessmanager45-hf1-release-notes.html).

For more information about this release and for the latest release notes, see the Documentation page. To download this product, see the Product (https://www.netiq.com/products/access-manager/) page.

If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of the specific page in the HTML version of the documentation posted at the Documentation (https://www.netiq.com/documentation/access-manager/) page.

For information about Access Manager support lifecycle, see the Product Support Lifecycle page.

What's New?

This release provides the following enhancements and fixes:

Enhancements

This release includes the following enhancements:

Support for Automatic Hybrid Azure AD Join for Windows Devices

Microsoft Azure Active Directory (Azure AD) provides device management when Windows devices are registered with Azure AD. Azure AD ensures that devices meet organizations' standards for security and compliance.

Access Manager now provides the capability to handle automatic registration for Windows 10 devices to Azure AD.

You can configure hybrid Azure AD join to register your on-premises AD domain-joined Windows resources automatically to Azure AD. Hybrid Azure AD join provides SSO to enterprise applications using Kerberos and OAuth 2.0 tokens.

For more information, see "Automatic Hybrid Azure AD Join for Windows Devices" in the *Access Manager 4.5 Administration Guide*.

Azure AD Conditional Access with Access Manager

Azure AD Conditional Access provides added security by allowing access to your applications across cloud and on-premises only from trusted and compliant devices. It is a policy-based approach. You can configure a Conditional Access policy with the required conditions to apply the access controls. Conditions can be device type, users' attributes, operating systems, client application accessed over web or cloud apps, network login location, sign-in risks, and so forth.

For more information, see "Azure Active Directory Conditional Access with Access Manager" in the *Access Manager 4.5 Administration Guide*.

Integration with Microsoft Intune Mobile Device Management

Using Microsoft Intune Mobile Device Management, you can manage iOS, Android, and Windows devices securely. To enable this feature, you must first set up automatic hybrid Azure AD Join for Windows devices.

For more information, see "Registering Devices to Microsoft Intune Mobile Device Management" in the *Access Manager 4.5 Administration Guide*.

Support for Choosing the Token Format for Each Client Application

JWT is the recommended format for OAuth tokens. However, some browsers such as Internet Explorer can restrict the length of the parameter values used in the token. This limits the use of JWT in these browsers. Access Manager now offers an option to choose binary format per client application for both access and refresh tokens.

For more information, see "Registering OAuth Client Applications" in the *Access Manager 4.5 Administration Guide*.

Support for Logging the SAML 2.0 Request and Response Events

You can now audit the SAML 2.0 request sent to an identity provider and the SAML 2.0 assertion details of the response received.

For more information, refer to the following options under "Defining Options for a SAML 2.0 Identity Provider" in the *Access Manager 4.5 Administration Guide*:

- SAML2 ASSERTION RESPONSE AUDIT EVENT
- SAML2 ASSERTION REQUEST AUDIT EVENT

Support for Monitoring the Health of SaaS Account Management Services

You can now monitor the registered SaaS Account Management Services on Access Manager Administration Console. For more information about monitoring the health, see "Monitoring Health of Services" in the *Access Manager 4.5 Administration Guide*.

Auto-Populating the Username on the Identity Server Login Page

You can now auto-populate the username on the Identity Server login page while accessing an Office 365 application using SAML 2.0. For more information, see "Auto-Populating the Username on the Identity Server Login Page" in the *Access Manager 4.5 Administration Guide*.

Operating System Upgrade

In addition to the existing supported platforms, this release adds support for RHEL 7.7.

NOTE: Upgrading to SLES 12 SP5 from an earlier version is now supported.

NOTE: For more information about system requirements, see "System Requirements" in the *NetIQ Access Manager 4.5 Installation and Upgrade Guide*.

Updates for Dependent Components

This release adds support for the following dependent components:

- ZuluOpenJDK 1.8.0_222
- Apache 2.4.41
- Tomcat 8.5.46
- iManager 3.1.4

Software Fixes

This release includes the following software fixes:

Component	Bug ID	Issue
Security	NA	XSS vulnerability in APIs. (CVE-2019-11659). For more information, see TID 7024155.

Component	Bug ID	Issue
Security	NA	XSS vulnerability in Administration Console (CVE-2019-11673). For more information, see TID 7024157.
Security	NA	A cryptographically weak function is used to generate the secret key (CVE-2019-11671). For more information, see TID 7024166.
Security	NA	Java deserialization vulnerability (CVE-2019-11672). For more information, see TID 7024156.
OAuth 2.0	1113110	When a client application is updated through both Administration Console and REST API, the `nidsOAuthClients` object gets replicated in the eDirectory configuration store.
OAuth 2.0	1141627	The access token fails when using an LDAP load balancer with different read and write LDAP replicas.
Administration Console	1062731	If too many proxy services are configured, Administration Console slows down when you edit a proxy service list.
Policy	1045763	Removing a condition from a policy displays the contents of other policies incorrectly because the `SetOrder` parameter changes.
Identity Server	1129432	The NMAS SAML method makes some attributes unavailable in the user portal because the SHA265 algorithm is enabled by default.
SAML 2.0	1132592	In a SAML 2.0 authentication request, Identity Server sends the response to the default consumer service location instead of the requested location.
SAML 2.0	1133032	In a SAML 2.0 authentication request, the third party identity provider does not send the `AuthnContextRef` parameter to a third party service provider.
SAML 2.0	1131027	When a user accesses an Office 365 application, Access Manager does not auto-populate the username on the Identity Server login page for a SAML 2.0 authentication.
Certificates	1087127	The Identity Server Keystore does not get created if the `ambkup` or `amdiag` file is missing.
Access Gateway	1118142	Configuration change in Access Gateway takes approximately 15 minutes to get updated.
Access Gateway	1131775	Access Gateway fails to clear the mangled cookie in the following scenarios: ◆ When cookie is set without any domain or path ◆ When cookie path is other than "/"
Access Gateway	1116982	When Sharepoint Server 2016 is protected through Access Gateway and HTML rewriting is enabled, then the content on the Sharepoint application are not displayed.

Videos

This release includes the following videos:

- Introduction to Auto Scaling of Access Manager in AWS
- Configuring Auto Scaling of Access Manager in AWS
- Enabling OAuth for Legacy Application

Installing or Upgrading

After purchasing Access Manager 4.5.1, you can access the product in the Customer Center. The activation code is in the Customer Center where you download the software. For more information, see Customer Center Frequently Asked Questions (https://www.netiq.com/cchelp/ncc-faq.html).

To access a full version of Access Manager:

1. Log in to the Customer Center (https://www.netiq.com/customercenter/app/home?execution=e1s1).
2. Click **Software**.
3. On the **Entitled Software** tab, click the appropriate version of Access Manager for your environment to download the product.

The following files are available:

Table 1 *Files Available for Access Manager 4.5.1*

Filename	Description
`AM_451_AccessManagerService_Linux64.tar.gz`	Contains Identity Server and Administration Console .tar file for Linux.
`AM_451_AccessManagerService_Win64.zip`	Contains Identity Server and Administration Console .exe file for Windows Server.
`AM_451_AccessGatewayAppliance_OVF.tar.gz`	Contains Access Gateway Appliance OVF template.
`AM_451_AccessGatewayAppliance.tar.gz`	Contains Access Gateway Appliance .tar file.
`AM_451_AccessGatewayService_Win64.zip`	Contains Access Gateway Service .exe file for Windows Server.
`AM_451_AccessGatewayService_Linux64.tar.gz`	Contains Access Gateway Service .tar file for Linux.

NOTE: This release does not support installation or upgrade of Analytics Server. For a fresh installation of Analytics Server, use `AM_442_AnalyticsServerAppliance.iso` file, then upgrade Analytics Server to 4.4 SP3 version by using `AM_443_AnalyticsServerAppliance.tar.gz` file. If you are already using a previous version of Analytics Server, then upgrade to Analytics Server 4.4 SP3. For more information about installing Analytics Server, see "Installing Analytics Server" in the *NetIQ Access Manager 4.5 Installation and Upgrade Guide*.

For information about the upgrade paths, see "Supported Upgrade Paths" on page 6. For more information about installing and upgrading, see the NetIQ Access Manager 4.5 Installation and Upgrade Guide.

Verifying Version Number after Upgrading to 4.5.1

After upgrading to Access Manager 4.5.1, verify that the version number of the component is indicated as **4.5.1.0-137**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.5.1.0-137**.

Supported Upgrade Paths

To upgrade to Access Manager 4.5.1, you need to be on one of the following versions of Access Manager:

- 4.4 Service Pack 3
- 4.4 Service Pack 4
- 4.4 Service Pack 4 Hotfix 1
- 4.5
- 4.5 Hotfix 1

NOTE: (Windows) Upgrade from 4.4 Service Pack 4 Hotfix 1 and 4.5 Hotfix 1 to Access Manager 4.5.1 is not supported.

For more information about upgrading Access Manager, see "Upgrading Access Manager" in the *NetIQ Access Manager 4.5 Installation and Upgrade Guide*.

Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (http://www.netiq.com/support).

Cannot Download Kibana Service Logs

Issue: When you navigate to **Dashboard** > **Troubleshooting** > **General Logging** > **Analytics Server**, an error is displayed when you download the kibana service log file. This happens because the kibana service is unavailable. The service will be available in the next release of Analytics Server. (Bug 1125405)

Workaround: None.

JCC Hangs after Deleting Appmarks through REST API

Issue: When you delete all appmarks using `deleteAppmark` REST API, JCC hangs. This issue occurs because Access Manager fails to call the `updateIDPCluster()` API. (Bug 1150741)

Workaround: Ensure to call the `updateIDPCluster()` API after deleting every 20 appmarks.

(RHEL) Status of Identity Server Is Red After Upgrading to Access Manager 4.5 SP1

Issue: After upgrading Access Manager from 4.4 SP3 or 4.4 SP4 to 4.5 SP1, status of Identity Server is red. (Bug 1152825)

Workaround: Reboot the virtual machine on which you have installed Identity Server.

(Windows) Cannot Configure Some of the OAuth Features After Upgrading to Access Manager 4.5 SP1

Issue: After upgrading Access Manager on a Windows setup, you cannot perform the following tasks:

- Registering a client application
- Deleting an existing client application
- Creating a Resource Server
- Deleting an existing resource server
- Using any of the configured Access Manager Resource Servers after updating the `nidsOAuthGrant` attribute

These issues occur because the syntax of **nidsOAuth2CFGXML** is set to **string** or **octet** instead of **stream**. (Bug `1151595`)

Workaround: Perform the steps mentioned in "(Windows) Cannot Configure Some of the OAuth Features After an Upgrade" in the *Access Manager 4.5 Administration Guide*.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate website (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

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.netiq.com/company/legal/.