

# Access Manager 4.4 Service Pack 4 Release Notes

February 2019



Access Manager 4.4 Service Pack 4 (4.4.4) 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 4.4 Service Pack 3 Release Notes \(https://www.netiq.com/documentation/access-manager-44/accessmanager443-release-notes/data/accessmanager443-release-notes.html\)](https://www.netiq.com/documentation/access-manager-44/accessmanager443-release-notes/data/accessmanager443-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 \(https://www.netiq.com/products/access-manager/\)](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 \(https://www.netiq.com/documentation/access-manager/\)](https://www.netiq.com/documentation/access-manager/) page.

For information about Access Manager support lifecycle, see the [Product Support Lifecycle](#) page.

- ◆ [Section 1, "What's New?," on page 1](#)
- ◆ [Section 2, "Installing or Upgrading," on page 3](#)
- ◆ [Section 3, "Verifying Version Number after Upgrading to 4.4.4," on page 4](#)
- ◆ [Section 4, "Supported Upgrade Paths," on page 4](#)
- ◆ [Section 5, "Known Issues," on page 5](#)
- ◆ [Section 6, "Contact Information," on page 6](#)
- ◆ [Section 7, "Legal Notice," on page 6](#)

## 1 What's New?

This release provides the following enhancements and fixes:

- ◆ [Section 1.1, "Enhancements," on page 1](#)
- ◆ [Section 1.2, "Operating System Upgrade," on page 2](#)
- ◆ [Section 1.3, "Updates for Dependent Components," on page 2](#)
- ◆ [Section 1.4, "Software Fixes," on page 2](#)

### 1.1 Enhancements

This release includes the following enhancement:

### 1.1.1 SharePoint Server 2013 and 2016 Support

This release adds support for configuring Single Sign-On to SharePoint Server 2013 and 2016.

For more information, see “[Configuring SSO to SharePoint Server 2013 and 2016](#)” in the *NetIQ Access Manager 4.4 Administration Guide*.

## 1.2 Operating System Upgrade

In addition to the existing supported platforms, this release adds support for RHEL 7.6.

---

**NOTE:** For more information about system requirements, see “[System Requirements](#)” in the *NetIQ Access Manager 4.4 Installation and Upgrade Guide*.

---

## 1.3 Updates for Dependent Components

This release adds support for the following dependent components:

- ♦ eDirectory 9.1.1.1
- ♦ ZuluOpenJDK 1.8.0\_192
- ♦ OpenSSL 1.0.2q
- ♦ iManager 3.1.2

## 1.4 Software Fixes

This release includes software fixes for the following components:

- ♦ [Section 1.4.1, “Administration Console,” on page 2](#)
- ♦ [Section 1.4.2, “Identity Server,” on page 2](#)

### 1.4.1 Administration Console

The following issue is fixed in Administration Console:

#### 1.4.1.1 Administrator Cannot Decide the Order of Execution of the Authentication Methods

In risk-based authentication, if multiple authentication methods are configured for step up authentication, then Administration Console does not display the methods in any particular order.  
(Bug 1053634)

### 1.4.2 Identity Server

The following issues are fixed in Identity Server:

- ♦ [Section 1.4.2.1, “The Deny Rule of Risk-Based Authentication Does Not Work After Upgrading to Access Manager 4.4,” on page 3](#)
- ♦ [Section 1.4.2.2, “Duo Authentication Fails and Does Not Display the Customized Content of the Login Page,” on page 3](#)
- ♦ [Section 1.4.2.3, “When Risk-Based Authentication After a Login Attempt Triggers an Authentication Method from a Different User Store, It Fails,” on page 3](#)
- ♦ [Section 1.4.2.4, “RADIUS Authentication Does Not Work After Upgrading to Access Manager 4.4.X,” on page 3](#)

- ◆ [Section 1.4.2.5, “X509 Method Fails to Authenticate a User If Used As a Step Up Authentication Method,” on page 3](#)
- ◆ [Section 1.4.2.6, “Access Token Fails to Validate at the UserInfo Endpoint,” on page 3](#)

#### 1.4.2.1 **The Deny Rule of Risk-Based Authentication Does Not Work After Upgrading to Access Manager 4.4**

When the risk score matches the score defined in the deny condition, Access Manager does not display the `Access Denied` message. (Bug 1086823)

#### 1.4.2.2 **Duo Authentication Fails and Does Not Display the Customized Content of the Login Page**

In pre-risk-based authentication, when a user is prompted to execute the duo contract after executing the SNPF contract, authentication fails. When the user retries to execute the duo contract, the customized content of the login page is not displayed and the user cannot specify the credentials. (Bug 1121259)

#### 1.4.2.3 **When Risk-Based Authentication After a Login Attempt Triggers an Authentication Method from a Different User Store, It Fails**

After executing the first post-risk-based authentication method, the user is asked to execute an additional authentication method against another user store. When the user specifies the credentials, Access Manager displays an error message that the user is disabled. (Bug 1121260)

#### 1.4.2.4 **RADIUS Authentication Does Not Work After Upgrading to Access Manager 4.4.X**

When RADIUS is used as a step up authentication method, authentication fails after executing the method. This issue occurs because Access Manager does not send `state` attribute to the client. (Bug 1121366)

#### 1.4.2.5 **X509 Method Fails to Authenticate a User If Used As a Step Up Authentication Method**

While executing a pre-risk-based authentication contract, authentication fails if X509 method is used as the step up authentication method. (Bug 1109549)

#### 1.4.2.6 **Access Token Fails to Validate at the UserInfo Endpoint**

OAuth client receives the access token but when the OAuth client sends the access token to retrieve identity information of a user, the request fails. This is a random issue. (Bug 1121373)

## 2 Installing or Upgrading

After purchasing Access Manager 4.4.4, log in to the [NetIQ Downloads \(http://dl.netiq.com/\)](http://dl.netiq.com/) page and follow the link that allows you to download the software.

The following files are available:

*Table 1 Files Available for Access Manager 4.4.4*

Filename	Description
AM_444_AccessManagerService_Linux64.tar.gz	Contains Identity Server and Administration Console .tar file for Linux.
AM_444_AccessManagerService_Win64.exe	Contains Identity Server and Administration Console .exe file for Windows Server.

Filename	Description
AM_444_AccessGatewayAppliance.iso	Contains Access Gateway Appliance .iso file.
AM_444_AccessGatewayAppliance.tar.gz	Contains Access Gateway Appliance .tar file.
AM_444_AccessGatewayService_Win64.exe	Contains Access Gateway Service .exe file for Windows Server.
AM_444_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 4.4 Installation and Upgrade Guide](#).

For information about the upgrade paths, see [Section 4, “Supported Upgrade Paths,”](#) on page 4. For more information about installing and upgrading, see the [NetIQ Access Manager 4.4 Installation and Upgrade Guide](#).

**NOTE:** Before upgrading Access Manager, ensure to check the [Troubleshooting Section \(https://www.netiq.com/documentation/access-manager-44/install\\_upgrade/data/t48ittstd4c6.html\)](https://www.netiq.com/documentation/access-manager-44/install_upgrade/data/t48ittstd4c6.html) in the [NetIQ Access Manager 4.4 Installation and Upgrade Guide](#).

### 3 Verifying Version Number after Upgrading to 4.4.4

After upgrading to Access Manager 4.4.4, verify that the version number of the component is indicated as **4.4.4.0-22**. To verify the version number, perform the following steps:

- 1 In Administration Console Dashboard, click **Troubleshooting > Version**.
- 2 Verify that the **Version** field lists **4.4.4.0-22**.

### 4 Supported Upgrade Paths

To upgrade to Access Manager 4.4.4, you need to be on one of the following versions of Access Manager:

- ♦ 4.4 Service Pack 1
- ♦ 4.4 Service Pack 1 Hotfix 1
- ♦ 4.4 Service Pack 2
- ♦ 4.4 Service Pack 3

For more information about upgrading Access Manager, see “Upgrading Access Manager” in the [NetIQ Access Manager 4.4 Installation and Upgrade Guide](#).

## 5 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 \(http://www.netiq.com/support\)](http://www.netiq.com/support).

- ♦ [Section 5.1, “\(Windows\) The Attribute of AWS SAML 2.0 Service Provider Does Not Contain the Default Constant Value,” on page 5](#)
- ♦ [Section 5.2, “Identity Server Is Not Able to Connect to User Stores After Upgrading to Access Manager 4.4 SP4,” on page 5](#)
- ♦ [Section 5.3, “Converting a Secondary Administration Console into a Primary Console Fails,” on page 5](#)
- ♦ [Section 5.4, “SharePoint Server 2016 Does Not Render All the Contents of the Web Page When Protected through Access Manager,” on page 6](#)

### 5.1 (Windows) The Attribute of AWS SAML 2.0 Service Provider Does Not Contain the Default Constant Value

**Issue:** When you configure AWS as a SAML 2.0 service provider, the constant value attribute does not contain the expected value. The constant value must contain the role ARN and the trusted SAML provider ARN. For example, `arn:aws:iam::638116851885:role/admin,arn:aws:iam::638116851885:saml-provider/NAMIDP` (Bug 1123154)

**Workaround:** Change the constant value manually.

Perform the following steps:

- 1 Click **Devices > Identity Servers > Shared Settings > Attribute Sets**.
- 2 Select the Amazon Web Service and click **Mapping**.
- 3 Edit and change the constant value.
- 4 Click **Apply**.

### 5.2 Identity Server Is Not Able to Connect to User Stores After Upgrading to Access Manager 4.4 SP4

**Issue:** This issue occurs because there is an incorrect setting in the Tomcat Java options of JNDI. (Bug 1117444)

**Workaround:** Perform the steps mentioned in [TID 7023648 \(https://support.microfocus.com/kb/doc.php?id=7023648\)](https://support.microfocus.com/kb/doc.php?id=7023648).

### 5.3 Converting a Secondary Administration Console into a Primary Console Fails

**Issue:** After converting the Secondary Administration Console to Primary Administration Console, the converted Administration Console does not work because it fails to communicate with other servers. (Bug 1122742)

**Workaround:** None.

## 5.4 SharePoint Server 2016 Does Not Render All the Contents of the Web Page When Protected through Access Manager

**Issue:** This issue occurs when the HTML rewriting is enabled. (Bug 1116982)

**Workaround:** Disable the HTML rewriting.

---

**NOTE:** You cannot use a different published DNS name and port than that of the backend SharePoint server 2016.

---

## 6 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) (<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) (<http://www.netiq.com/support/process.asp#phone>).

For general corporate and product information, see the [NetIQ Corporate website](http://www.netiq.com/) (<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/) (<https://www.netiq.com/communities/>). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

## 7 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/>.

**Copyright © 2019 NetIQ Corporation. All Rights Reserved.**