Access Manager Appliance 4.2 Service Pack 1 Release Notes

March 2016

Access Manager Appliance 4.2 Service Pack 1 (4.2.1) supersedes Access Manager Appliance 4.2.

For the list of software fixes and enhancements in the previous release, see Access Manager Appliance 4.2 Release Notes.

- Section 1, “What’s New?,” on page 1
- Section 2, “Supported Upgrade Paths,” on page 4
- Section 3, “Installing or Upgrading Access Manager,” on page 4
- Section 4, “Verifying Version Numbers After Upgrading to 4.2.1,” on page 4
- Section 5, “Known Issues,” on page 4
- Section 6, “Contact Information,” on page 5
- Section 7, “Legal Notice,” on page 5

1 What’s New?

This release includes the following platform updates and fixed issues:

- Section 1.1, “Operating System Upgrade,” on page 1
- Section 1.2, “Updates for Dependent Components,” on page 1
- Section 1.3, “Fixed Issues,” on page 2

1.1 Operating System Upgrade

In addition to the platforms introduced in Access Manager 4.2 release, this release adds support for the following platforms:

- SLES 12 SP1
- RHEL 7.2

1.2 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.7
- Java 1.8.0_74
- Apache 2.2.27 (This release includes fixes for CVE-2014-0231, CVE-2014-0226, CVE-2013-5704,and CVE-2015-3183)
- OpenSSL 1.0.1s
- Tomcat 8.0.32
- iManager 2.7.7.6

NOTE: This release of Access Manager by default supports Tomcat 8.0.32 and OpenSSL 1.0.1s, but Administration Console uses Tomcat version 7.0.56 due to dependency on iManager.

1.3 Fixed Issues

This release includes software fixes for the following components:

- Section 1.3.1, “Administration Console,” on page 2
- Section 1.3.2, “Identity Server,” on page 2
- Section 1.3.3, “Access Gateway,” on page 3

1.3.1 Administration Console

The following issues are fixed in Administration Console:

- Section 1.3.1.1, “Administration Console Does Not List All the Trusted Roots,” on page 2
- Section 1.3.1.2, “Cross Site Scripting Vulnerability,” on page 2

1.3.1.1 Administration Console Does Not List All the Trusted Roots

Issue: The trusted roots are stored in an alphabetical order in eDirectory. When reading the trusted roots, if Administration Console encounters a corrupt trusted root it throws an exception and terminates the reading. It does not list any of the trusted roots that are stored after the corrupt trusted root. [Bug 940432]

Fix: The issue is resolved. The Administration Console now handles the exception and reads the next trusted root.

1.3.1.2 Cross Site Scripting Vulnerability

Issue: There is a Cross Site Scripting vulnerability issue in Administration Console risk engine. In **Policies > Risk Configuration > NAT Settings**, the **Client IP Header Parser** field displays irrelevant characters. [Bug 954474]

Fix: The issue is resolved. The irrelevant characters are removed from the **Client IP Header Parser** field.

1.3.2 Identity Server

The following issues are fixed in Identity Server:

- Section 1.3.2.1, “SAML Tokens are Line Wrapped,” on page 2
- Section 1.3.2.2, “SAML Attribute Set with Constant Value Cannot be Deleted,” on page 3
- Section 1.3.2.3, “Virtual Attribute Option is Not Listed Under Role Policy Conditions on an Upgraded Access Manager,” on page 3
- Section 1.3.2.4, “OAuth Identity Injection Scope Works Only if Require User Permission Option is Enabled,” on page 3

1.3.2.1 SAML Tokens are Line Wrapped

Issue: The SAML tokens that contain a signature and certificates are line wrapped. This issue happens due to old XML signature library.[Bug 954912]

Fix: The XML signature library has been upgraded. By default the SAML tokens are line wrapped. To disable line wrapping, set the following option in the `/opt/novell/nam/idp/conf/tomcat.conf` file:

```
JAVA_OPTS="${JAVA_OPTS} -Dorg.apache.xml.security.ignoreLineBreaks= true
```

1.3.2.2 SAML Attribute Set with Constant Value Cannot be Deleted

Issue: Define an attribute set with a remote attribute name and set a constant value. Save the attribute set, assign it and update Identity server. If you try to delete the constant value an exception occurs. [Bug 965912]

1.3.2.3 Virtual Attribute Option is Not Listed Under Role Policy Conditions on an Upgraded Access Manager

Issue: On an upgraded Access Manager, the **Virtual Attribute** option is not listed under the role policy conditions. [Bug 958724]

1.3.2.4 OAuth Identity Injection Scope Works Only if Require User Permission Option is Enabled

Issue: While defining scopes and claims for a Resource Server, if the scope is not enabled with the **Require user permission** option, then the OAuth identity injection does not inject this scope even when the request contains this scope. [Bug 965649]

1.3.3 Access Gateway

The following issues are fixed in Access Gateway:

- Section 1.3.3.1, “The Policy Extension Template Does Not Work in a Clustered Environment,” on page 3
- Section 1.3.3.2, “The URL Accessed Audit Event is Triggered Even when this Event Is Disabled,” on page 3
- Section 1.3.3.3, “Apache Crashes on Windows Access Gateway Service when Requested URL has Long Query String,” on page 3

1.3.3.1 The Policy Extension Template Does Not Work in a Clustered Environment

Issue: In a clustered environment, Access Gateway throws an exception for a policy extension template. This happens when the load balancer selects different servers for Identity Server and Access Gateway. However, when the load balancer selects the same servers for Identity Server and Access Gateway, there is no error. [Bug 876869]

Fix: This issue is resolved. The load balancer does not throw an exception and works as expected on different servers.

1.3.3.2 The URL Accessed Audit Event is Triggered Even when this Event Is Disabled

Issue: The **URL Accessed** audit event is triggered even when it is not enabled for auditing. [Bug 968219]

1.3.3.3 Apache Crashes on Windows Access Gateway Service when Requested URL has Long Query String

Issue: On Windows Access Gateway Service, Apache crashes. This is because the requested URL has long query string and the stack size is insufficient. [Bug 847731]

Fix: This issue is resolved. The stack size in Windows Access Gateway Service is increased to prevent Apache from crashing.

2 Supported Upgrade Paths

To upgrade to Access Manager 4.2.1, you must be on any one of the following Access Manager versions:

- 4.2
- 4.1 Service Pack 2
- 4.1 Service Pack 1 HF1
- 4.1 Service Pack 1
- 4.1
- 4.0 Service Pack 2 HF1
- 4.0 Service Pack 2

3 Installing or Upgrading Access Manager

After purchasing Access Manager Appliance 4.2.1, log in to the NetIQ Downloads page and follow the link that allows you to download the software. The following files are available:

Table 1 *Files Available for Access Manager Appliance 4.2.1*

Filename	Description
`AM_42_SP1_AccessManagerAppliance.iso`	Contains the Access Manager Appliance iso.
`AM_42_SP1_AccessManagerAppliance.tar.gz`	Contains the Access Manager Appliance tar file.

For more information about installing and upgrading, see the NetIQ Access Manager Appliance 4.2 Installation and Upgrade Guide.

4 Verifying Version Numbers After Upgrading to 4.2.1

After upgrading to Access Manager 4.2.1, verify that the version number of the component is indicated as **4.2.1.0-29**. To verify the version number, perform the following steps:

1. In the Administration Console, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.2.1.0-29**.

5 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issue is currently being researched. If you need further assistance with any issue, please contact Technical Support.

- Section 5.1, “OAuth Apps Fail After Upgrading Access Manager 4.1 to 4.2,” on page 4

5.1 OAuth Apps Fail After Upgrading Access Manager 4.1 to 4.2

Issue: The OAuth apps fail after you upgrade Access Manager 4.1 to 4.2. This is caused due to the expired authorization code. [`Bug 966216`]

Workaround: To workaround this issue, you need to upgrade both Access Gateway and Identity Provider to Access Manager 4.2 at the same time. For more information, see TID.

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). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. 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/.