Access Manager Appliance 4.2 Service Pack 2 Release Notes

July 2016

Access Manager Appliance 4.2 Service Pack 2 (4.2.2) supersedes Access Manager Appliance 4.2 Service Pack1 (4.2.1).

For the list of software fixes and enhancements in the previous release, see Access Manager Appliance 4.2.1 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 5
- Section 4, “Verifying Version Numbers After Upgrading to 4.2.2,” on page 5
- Section 5, “Known Issues,” on page 5
- Section 6, “Contact Information,” on page 5
- Section 7, “Legal Notice,” on page 6

1 What’s New?

This release includes the following:

- Section 1.1, “Security Guide,” on page 1
- Section 1.2, “Updates for Dependent Components,” on page 1
- Section 1.3, “Fixed Issues,” on page 2

1.1 Security Guide

In addition to the existing deliverables, this release introduces the Security Guide in the documentation library.

1.2 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.8
- Java 1.8.0_92
- OpenSSL 1.0.1t
- Tomcat 8.0.35
- iManager 2.7.7.7 (20160708_1400)

NOTE: This release of Access Manager by default supports Tomcat 8.0.35 and OpenSSL 1.0.1t, but Administration Console uses Tomcat version 7.0.68 due to dependency on iManager.

1.3 Fixed Issues

This release includes software fixes for the following:

- 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 4

1.3.1 Administration Console

The following issues are fixed in Administration Console:

- The Webshell files uploaded through JSP Pages with Cert server Snapins, can trigger system calls. (TID 7017807)
- The .htaccess file from iManager configuration is susceptible to attacks. (TID 7017811)
- The Nessus scan reports in a web application are susceptible to the Clickjacking in iManager. (TID 7017812)
- iManager application URLs are susceptible to the Cross-Site Scripting (XSS) attack. (TID 7017813)
- Access Manager is prone to phishing attack through iFrame manipulation on the Administration Console login page. (TID 7017818)
- Cross-Site Request Forgery prevention is not working under heavy load. (TID 7017817)

1.3.2 Identity Server

The following issues are fixed in Identity Server:

- The risk servlet points to remotely accessible DTD and executes an XML External Entity (XXE) attack. (TID 7017797)
- Identity Server can execute an XXE that can in turn read the any readable file on the system. (TID 7017806)
- Manipulating the Assertion Consumer Service URL in SAML request leads to the XSS vulnerability. (TID 7017808)
- The unsigned request does not validate incoming AuthnRequest Assertion Consumer Service (ACS) URL tag. (TID 7017809)
- Access Manager 4.2 default login pages are susceptible to the Reflected Cross-Site Scripting vulnerability. (TID 7017810)

- Section 1.3.2.1, “Access Manager uses SHA1 Instead of SHA2 During HTTP Redirect Binding Request,” on page 3
- Section 1.3.2.2, “The Step-up Authentication is bypassed Manually,” on page 3
- Section 1.3.2.3, “Identity Server is not Compatible with Regional SAML Identity Server,” on page 3
- Section 1.3.2.4, “Identity Server does not Send Configured ForceAuthn Parameter,” on page 3
- Section 1.3.2.5, “The Unsigned Request does not Validate Incoming AuthnRequest Assertion Consumer Service (ACS) URL Tag,” on page 3
- Section 1.3.2.6, “The Modified Attribute Entries are Not Returned at UserInfo EndPoint Response,” on page 4

- Section 1.3.2.7, “The OAuth Token Request does Not Check Only the Default User Store for Authentication,” on page 4
- Section 1.3.2.8, “Multi-valued LDAP Attribute does not Inject Any Value,” on page 4

1.3.2.1 Access Manager uses SHA1 Instead of SHA2 During HTTP Redirect Binding Request

Issue: When Access Manager acts as an Identity provider, during an HTTP Redirect binding request, the requests are signed with SHA1 instead to SHA2. [Bug 963483]

Fix: The issue is resolved as all requests are signed and validated with SHA2 now.

1.3.2.2 The Step-up Authentication is bypassed Manually

Issue: When you assign a step-up authentication to a contract in a service provider, you can manually bypass the assertion by authenticating it with a lower authentication level. [Bug 971938]

Fix: The issue is resolved now as the authentication does not bypass the step-up authentication.

1.3.2.3 Identity Server is not Compatible with Regional SAML Identity Server

Issue: When Access Manager acts as a service provider, it is not compatible with the regional SAML Identity servers. This leads to unauthorized SAML AuthnRequest requests, [Bug 974948]

Fix: This issue is resolved. Add the following SAML options in the remote Identity server options: `SAML2_ISSUER_FORMAT`, `SAML2_ISSUER_NAMEQUALIFIER`, and `SAML2_NAMEIDPOLICY_ALLOWCREATE`. For more information, see TID.

1.3.2.4 Identity Server does not Send Configured ForceAuthn Parameter

Issue: When Access Manager acts as a service provider, it does not send the configured ForceAuthn parameter. [Bug 977859]

Fix: This issue is resolved. For more information, see TID.

1.3.2.5 The Unsigned Request does not Validate Incoming AuthnRequest Assertion Consumer Service (ACS) URL Tag

Issue: When an authentication request from a service provider is not signed, Identity Provider cannot validate the authenticity and integrity of the request. So any malicious user who can intercept the request can change the ACS URL in the request and make the Identity Provider to send the assertion to malicious sites. [Bug 986799]

Fix: This issue is resolved. Two SAML options `SAML2_ACS_DOMAIN_WHITELIST` and `SAML2_ACS_URL_RESTRICT` are introduced.

SAML2_ACS_URL_RESTRICT: This option ensures that Identity Provider validates the Assertion Consumer Service URL in the request against the trusted metadata URL before sending the assertion.

To define this option, go to **Devices > Identity Servers > IdP Cluster > SAML2 >** *[Service Providers]* **> Options > New > OTHERS**. Specify **Property Value** as **True**

SAML2_ACS_DOMAIN_WHITELIST: This option ensures that Identity Provider validates the Assertion Consumer Service URL in the request against a white list of domains.

To define this option, go to **Devices > Identity Servers > IdP Cluster > SAML2 >** *[Service Providers]* **> Options > New > OTHERS**. Specify **Property Value** as domain names separated with semi-colon(;) and no space. For example, *www.airlines.com*;*www.example.com*.

1.3.2.6 The Modified Attribute Entries are Not Returned at UserInfo EndPoint Response

Issue: On an existing scope that is already assigned or issued with attribute entries, when you modify an existing attribute entry in an attribute set, the modified values are not returned at the UserInfo EndPoint response. [Bug 955509]

Fix: This issue is resolved. The modified attribute entries reflect in the **UserInfo EndPoint** response.

1.3.2.7 The OAuth Token Request does Not Check Only the Default User Store for Authentication

Issue: In the resource owner OAuth flow, the authentication occurs at all user stores. Due to this, even when the user has enabled intruder lockout detection, the OAuth token is still issued if the user is found on other user stores. [Bug 970459]

Fix: This issue is resolved now as only the default user store is used for authentication.

1.3.2.8 Multi-valued LDAP Attribute does not Inject Any Value

Issue: If an LDAP attribute contains multiple values, none of the attributes gets injected into the backend web application. [Bug 978808]

Fix: This issue is resolved now as the LDAP attribute gets injected into the backend web application.

1.3.3 Access Gateway

The following issues are fixed in Access Gateway:

- Section 1.3.3.1, “Issue in the Exclude DNS Name List Option,” on page 4
- Section 1.3.3.2, “Access Manager 4.1, or 4.2 Upgrade Fails Causing SSL Issues,” on page 4

1.3.3.1 Issue in the Exclude DNS Name List Option

Issue: In a clustered environment, the **Exclude DNS Name List** option does not work as expected. The HTML Rewriting happens even when the backend DNS name is included in the Exclude DNS Name list. This happens when backend DNS is mapped to multiple proxy services. [Bug 927855]

Fix: This issue is resolved. To exclude the DNS name from being rewritten by that domain, an advanced option `NAGGlobalOptions ExcludeDNSFull on` is introduced. To enable this option, go to **Administration Console Dashboard > Devices > Access Gateways > Edit > Advanced Options**.

1.3.3.2 Access Manager 4.1, or 4.2 Upgrade Fails Causing SSL Issues

Issue: If you upgrade Access Manager 4.1, or 4.2 to a higher version, the upgrade fails causing SSL issues. [Bug 975291]

Fix: This issue is resolved now as there is no SSL issue during an upgrade.

2 Supported Upgrade Paths

To upgrade to Access Manager 4.2.2, you must be on any one of the following Access Manager versions:

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

3 Installing or Upgrading Access Manager

After purchasing Access Manager Appliance 4.2.2, 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 4.2.2*

Filename	Description
`AM_42_SP2_AccessManagerAppliance.iso`	Contains Access Manager Appliance iso.
`AM_42_SP2_AccessManagerAppliance.tar.gz`	Contains Access Manager Appliance tar file.

NOTE: If you do not upgrade the base operating system to SLES 11 SP4 before upgrading, upgrade will display an error message and terminate.

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 4.2.2

After upgrading to Access Manager 4.2.2, verify that the version number of the component is indicated as **4.2.2.0-40**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field displays **4.2.2.0-40**.

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, “The OAuth Authorization Code Grant Fails on Custom Login Pages,” on page 5

5.1 The OAuth Authorization Code Grant Fails on Custom Login Pages

Issue: The OAuth Authorization code grant fails on custom login pages. This occurs when the authentication happens at the Identity provider. [`Bug 976081`]

Workaround: There is no workaround available currently.

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. 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/.

Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.