Access Manager Appliance 4.2 Service Pack 5 Release Notes

October 2017

Access Manager Appliance 4.2 Service Pack 5 (4.2.5) supersedes Access Manager Appliance 4.2 Service Pack 4.

For the list of software fixes and enhancements in the previous release, see Access Manager Appliance 4.2 Service Pack 3 Hotfix 1 Release Notes (https://www.netiq.com/documentation/access-manager-42-appliance/accessmanager424-releasenotes/data/accessmanager424-releasenotes.html).

The general support for Access Manager 4.2 ends on 30th Nov 2017. For more information, see the Product Support Lifecycle page.

1 What’s New?

This release includes the following:

1.1 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.11
- Java 1.8.0_144-b01
- Tomcat 8.0.47
- iManager 2.7.7.11

NOTE: This release of Access Manager by default supports Tomcat 8.0.47 and OpenSSL 1.0.2k, but Administration Console uses Tomcat version 7.0.81 due to dependency on iManager.

1.2 Fixed Issues

This release includes software fixes for the following components:

- Section 1.2.1, “Administration Console,” on page 2
- Section 1.2.2, “Identity Server,” on page 2
- Section 1.2.3, “Access Gateway,” on page 2

1.2.1 Administration Console

The following issue is fixed in Administration Console:

- Section 1.2.1.1, “Administration Console Randomly Deletes Certificate Trust Store Objects,” on page 2

1.2.1.1 Administration Console Randomly Deletes Certificate Trust Store Objects

The Identity Server cluster is not displayed in Administration Console because the certificates get deleted from the trust store. Hence, you must re-configure the Identity Server cluster. `(Bug 1061807)`

1.2.2 Identity Server

The following issues are fixed in Identity Server:

- Office 365 SSO With SAML Triggers nidsIdentity Object to Be Removed and Re-Added With Every Login (TID 7018539). `(Bug 1058411)`
- Section 1.2.2.1, “User Is Not Provisioned Correctly When User Store Contains Multiple Replicas,” on page 2
- Section 1.2.2.2, “The SAML 2.0 Service Provider Login Using Kerberos As Default Contract Does Not Redirect to Service Provider,” on page 2

1.2.2.1 User Is Not Provisioned Correctly When User Store Contains Multiple Replicas

LDAP replica stickiness is not configured to provision profiles. The create user requests reach different replicas during provisioning, attribute modification and authenticated principal search. `(Bug 1061801)`

1.2.2.2 The SAML 2.0 Service Provider Login Using Kerberos As Default Contract Does Not Redirect to Service Provider

When Kerberos is used as default contract and the user accesses SAML 2.0 service provider using Identity server initiated login, the user is not redirected to the service provider. The user remains on the Identity portal page. `(Bug 1050964)`

1.2.3 Access Gateway

The following issues are fixed in Access Gateway:

- Section 1.2.3.1, “The Syslog Server Communication Failure Reduces the Performance of Access Gateway Server,” on page 3
- Section 1.2.3.2, “The Global Advanced Option FlushUserCache Causes Looping,” on page 3
- Section 1.2.3.3, “Injecting a Script Using Browser Plugin Causes XSS Vulnerability,” on page 3

1.2.3.1 The Syslog Server Communication Failure Reduces the Performance of Access Gateway Server

Issue: When Syslog is enabled and Access Gateway Server cannot access Syslog Server, the audit events are not sent to Access Gateway. It reduces the Access Gateway performance. `(Bug 1060781)`

Fix: This issue is fixed in this release.

NOTE: If you are upgrading from a previous version of Access Manager, you must update the IP address and port number of the Syslog server to receive the system and server alerts in Administration Console.

When you upgrade Access Manager to this release, you can update the IP address and port number of the Syslog server by using any of the following methods:

- Modify the `SERVERIP` and `SERVERPORT` values of Syslog server at `/etc/Auditlogging.cfg`. Perform this step for all the devices, then restart the devices.
- In Administration Console, navigate to the **Auditing** Administrative task and update the IP address and port number of the Syslog server. For more information, see Specifying the Logging Server and Console Events.

1.2.3.2 The Global Advanced Option FlushUserCache Causes Looping

When `FlushUserCache` advanced option is enabled and multiple resources with different contracts are accessed in the same browser session, looping occurs. `(Bug 993619)`

1.2.3.3 Injecting a Script Using Browser Plugin Causes XSS Vulnerability

When the script is injected using browser plugin, referrer link on NAGError page causes XSS vulnerability (CVE-2017-5191). For more information about this Issue, see TID 7018793. `(Bug 1036222)`

2 Supported Upgrade Paths

To upgrade to Access Manager 4.2.5, you must be on any one of the following Access Manager versions:

- 4.2 Service Pack 4
- 4.2 Service Pack 3 Hotfix 1
- 4.2 Service Pack 3
- 4.2 Service Pack 2

3 Installing or Upgrading Access Manager

After purchasing Access Manager Appliance 4.2.5, 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 4.2.45*

Filename	Description
`AM_42_SP5_AccessManagerAppliance.iso`	Contains Access Manager Appliance iso.

Filename	Description
`AM_42_SP5_AccessManagerAppliance.tar.gz`	Contains 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 4.2.5

After upgrading to Access Manager 4.2.5, verify that the version number of the component is indicated as **4.2.5.0-10**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field displays **4.2.5.0-10**.

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.

- Upgrade From Access Manager 4.2.5 to 4.4 is Not Supported.
- Section 5.1, "Kerberos Constrained Delegation Does Not Work on Windows Server 2012 R2," on page 4

5.1 Kerberos Constrained Delegation Does Not Work on Windows Server 2012 R2

Issue: Access Manager does not support protecting kerberized resources with Kerberos Constrained Delegation when Access Gateway is installed on Windows Server 2012 R2. For more information, see TID 7022060. `(Bug 982954)`

Workaround: None.

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/.