Access Manager Appliance 4.3 Service Pack 2 Release Notes

June 2017

Access Manager Appliance 4.3 Service Pack 2 (4.3.2) 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 Appliance 4.3 Service Pack 1 Hotfix 1 Release Notes.

For more information about this release and for the latest release notes, see the Documentation page. To download this product, see the Product Upgrade page.

The general support for Access Manager 4.3 ends on 31st May 2018. For more information, see the Product Support Lifecycle page.

- Section 1, “What’s New?,” on page 1
- Section 2, “Installing or Upgrading,” on page 5
- Section 3, “Supported Upgrade Paths,” on page 5
- Section 4, “Verifying Version Number After Upgrading to 4.3.2,” on page 5
- Section 5, “Known Issues,” on page 6
- Section 6, “Contact Information,” on page 6
- Section 7, “Legal Notice,” on page 6

1 What’s New?

Access Manager Appliance 4.3.2 provides the following enhancement and fixes in this release:

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

1.1 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.10
- Java 1.8.0_131
- Tomcat 8.0.44
- iManager 2.7.7.10 (20170428_1848)

NOTE: Access Manager 4.3.2 by default supports Tomcat 8.0.44 and OpenSSL 1.0.2k, but Administration Console uses Tomcat version 7.0.68 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 4

1.2.1 Administration Console

The following issues are fixed in Administration Console:

- When You Edit **Data Entry** Field in **Policies** Using iManager, `HTTP 404` Error Occurs. (TID 7020723)
- The Nessus Scan on NAM 4.3.1 Reports `Plugin 44657 - Linux Daemons with Broken Links to Executable`. (TID 7020149)
- The Nessus Scan Reports `SWEET32` Vulnerability When Running on Oracle Java SE Version (CVE-2016-2183).

  For More Information on this Issue, See TID 7020150.
- Section 1.2.1.1, “The Fourth Node Does Not Add to An Existing Three Node Cluster,” on page 2

1.2.1.1 The Fourth Node Does Not Add to An Existing Three Node Cluster

When you add a fourth node to primary Access Manager appliance, devices are imported but do not add to the existing cluster. `[Bug 1038245]`

1.2.2 Identity Server

The following issues are fixed in Identity Server:

- Java Scripts and HTML Tags Are Allowed In OAuth Scope Description. When Scopes Containing Java Script Are Requested, XSS Attack Can Occur (CVE-2017-7419).

  For More Information about this Issue, See TID 7019893.
- Section 1.2.2.1, “The OAuth GET Requests Return the HTTP 401 Error,” on page 3
- Section 1.2.2.2, “The Fall Back Login Page for Kerberos Contract Displays Question Mark (?) in Username and Password Fields,” on page 3
- Section 1.2.2.3, “The SAML 2.0 Service Provider Login Using Kerberos As Default Contract Does Not Redirect to Service Provider,” on page 3
- Section 1.2.2.4, “Destination URL Validation Fails When URL Includes Default Port,” on page 3
- Section 1.2.2.5, “User Is Not Provisioned Correctly When User Store Contains Multiple Replicas,” on page 3
- Section 1.2.2.6, “The LDAP Query Parameters Cannot Be Changed for Kerberos Method,” on page 3

1.2.2.1 The OAuth GET Requests Return the HTTP 401 Error

In some environments, UserInfo Endpoint returns `HTTP 401 Unauthorized` when using valid tokens. [`Bug 1038997`]

1.2.2.2 The Fall Back Login Page for Kerberos Contract Displays Question Mark (?) in Username and Password Fields

The Kerberos fall back login page is not localized for Asian languages. [`Bug 1039004`]

For More Information on this Issue, See TID 7020724.

1.2.2.3 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 1039006`]

1.2.2.4 Destination URL Validation Fails When URL Includes Default Port

When SAML 2.0 `AuthnRequest` includes the `HTTPS 443` default port in the URL and not in metadata, it causes `Destination URL validation failed` error. [`Bug 1040329`]

1.2.2.5 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 1039001`]

1.2.2.6 The LDAP Query Parameters Cannot Be Changed for Kerberos Method

Issue: The Kerberos class does not allow to change LDAP query parameters. [`Bug 1020879`]

Fix: The LDAP query parameter of Kerberos method can be modified using `SearchQuery` property.

For example if you want to use the `SearchQuery` property for emails, perform the following steps:

1. Navigate to **Identity Servers > Edit > Local > Methods**
2. Click **Kerberos Method**
3. Click **Properties > New**
4. In the Add Property dialog box, specify the following:

   Property Name: `SearchQuery`

   Property Value: `(&(objectclass=person)(mail=%Email%))`

1.2.3 Access Gateway

The following issues are fixed in Access Gateway:

- HTTP Requests with URL Longer than 1531 Characters Returns `HTTP 403 forbidden` Error While Using Access Gateway Service on Windows. (TID 7020720)
- When You Click on Proxy Services and Configuration Pages, Access Gateway Is Marked for Update Even if the Configuration Is Not Changed. (TID 7020721)
- The `Error on DNS mismatch` Does Not Work as Expected When Disabled. (TID 7020722)
- The `SSLProxyCipherSuite` Directive Causes A Configuration Error While Using Domain Based Proxy. (TID 7020725)
- When The Script Is Injected Using Browser Plugin, Referrer Link On NAGError Page Causes XSS Vulnerability (CVE-2017-5191). For More Information on this Issue, See TID 7018793.
- Section 1.2.3.1, “Access to Inject Java Script Policy Enabled Resource Causes Error,” on page 4
- Section 1.2.3.2, “The Global Advanced Option FlushUserCache Causes Looping,” on page 4
- Section 1.2.3.3, “The Syslog Server Communication Failure Reduces the Performance of Access Gateway Server,” on page 4

1.2.3.1 Access to Inject Java Script Policy Enabled Resource Causes Error

When you add an Inject Java script policy and the associated resource is accessed, the browser displays an error. [`Bug 1038996`]

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 1039002`]

1.2.3.3 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 1039829`]

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, refer Specifying the Logging Server and Console Events.

2 Installing or Upgrading

After purchasing Access Manager Appliance 4.3.2, 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 4.3.2*

Filename	Description
`AM_43_SP2_AccessManagerAppliance.iso`	Contains Access Manager Appliance .iso file.
`AM_43_SP2_AccessManagerAppliance.tar.gz`	Contains Access Manager Appliance .tar file.
`AM_43_SP2_AnalyticsServerAppliance.iso`	Contains Analytics Server Appliance .iso file.
`AM_43_SP2_AnalyticsServerAppliance.tar.gz`	Contains Analytics Server Appliance .tar file.

For information about the upgrade paths, see Section 3, “Supported Upgrade Paths,” on page 5. For more information about installing and upgrading, see the *NetIQ Access Manager Appliance 4.3 Installation and Upgrade Guide*.

3 Supported Upgrade Paths

To upgrade to Access Manager 4.3.2, you need to be on one of the following versions of Access Manager:

- 4.2.x
  - 4.2 Service Pack 2
  - 4.2 Service Pack 3
  - 4.2 Service Pack 3 Hotfix 1
  - 4.2 Service Pack 4
- 4.3.x
  - 4.3
  - 4.3 Service Pack 1
  - 4.3 Service Pack 1 Hotfix 1

For more information about upgrading Access Manager Appliance, see “Upgrading Access Manager Appliance” in the *NetIQ Access Manager Appliance 4.3 Installation and Upgrade Guide*.

4 Verifying Version Number After Upgrading to 4.3.2

After upgrading to Access Manager 4.3.2, verify that the version number of the component is indicated as **4.3.2.0-15**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.3.2.0-15**.

5 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. There are no new issues other than the issues mentioned in Access Manager Appliance 4.3 Service Pack 1 Release Notes. If you need further assistance with any issue, please contact Technical Support.

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 Web site (http://www.netiq.com/support/process.asp#phone).

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

For interactive conversations with your peers and NetIQ experts, become an active member of Qmunity (http://community.netiq.com/), our community Web site that offers product forums, product notifications, blogs, and product user groups.

7 Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

© 2017 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.