Access Manager 4.3 Service Pack 3 Release Notes

November 2017

Access Manager 4.3 Service Pack 3 (4.3.3) 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 4.3 Service Pack 2 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.

1 What’s New?

Access Manager 4.3.3 provides the following enhancement and fixes:

1.1 Enhancement

This release introduces the following enhancement:

1.1.1 Identity Server Login Page Includes Cross-Site Request Forgery Token

A new Identity Server global option, `LOGIN CSRF CHECK` is added to enable Cross-Site Request Forgery (CSRF) check. For more information about CSRF token, see LOGIN CSRF CHECK in the NetIQ Access Manager 4.3 Administration Guide.

1.2 Operating System Upgrade

In addition to the existing supported platforms, this release supports installation of Access Manager components on the following platforms:

- RHEL 7.4
- SLES 12 SP3

NOTE: For information about hardware requirements, see Hardware Requirements in the NetIQ Access Manager 4.3 Installation and Upgrade Guide.

1.3 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.11
- Java 1.8.0_152
- Apache 2.2.27 (This release includes fixes for CVE-2016-5387, CVE-2017-7679, CVE-2017-7668, CVE-2017-3169, CVE-2017-3167 and CVE-2017-9788)
- Tomcat 8.0.47
- iManager 2.7.7.11

NOTE: Access Manager 4.3.3 by default supports Tomcat 8.0.47 and OpenSSL 1.0.2m, but Administration Console uses Tomcat version 7.0.81 due to dependency on iManager.

1.4 Fixed Issues

This release includes software fixes for the following components:

1.4.1 Administration Console

The following issues are fixed in Administration Console:

- Reflected Cross Site Scripting Issue in `/roma` URL Parameter (CVE-2017-14800). For More Information about This Issue, See TID 7022356.
- Reflected Cross Site Scripting Issue When Listing Identity Server Cluster (CVE-2017-14801). For More Information about This Issue, See TID 7022357.
- Reflected Cross Site Scripting Issue in `/nps` URL Parameter (CVE-2017-9276). For More Information about This Issue, See TID 7022359.
- Access Manager Uses an Old Prototype JavaScript Library (CVE-2008-7220).

1.4.1.1 Administration Console Deletes Certificate Trust Store Objects

If the cluster object is not found when a trusted root certificate is added, Administration Console might delete certificate trust store objects. (Bug 1034215)

1.4.1.2 Open Redirection Issue with Access Manager Redirect URL

Added a check to prevent redirection if the URL does not belong to /nps (CVE-2017-14802). For more information about this issue, see TID 7022360.

1.4.2 Identity Server

The following issues are fixed in Identity Server:

- Section 1.4.2.1, “Cannot Replace Expired Certificates,” on page 3
- Section 1.4.2.2, “Cannot Assign External Signing Certificate for OAuth,” on page 3
- Section 1.4.2.3, “Kerberos Fall Back Mechanism Does Not Redirect to the Password Reset Page,” on page 3
- Section 1.4.2.4, “Login Page Does Not Render Properly After a Kerberos Authentication Method Failure,” on page 3
- Section 1.4.2.5, “Passive Mode Authentication Fails When Accessing Office 365 with WS-Fed or WS-Trust,” on page 3

1.4.2.1 Cannot Replace Expired Certificates

When you enable signing certificate per SAML service provider, expired certificates cannot be replaced. (Bug 1060784)

1.4.2.2 Cannot Assign External Signing Certificate for OAuth

With this release, you can assign the external signing certificates to OAuth. To assign, add the certificate to the signing keystore of the Identity Server and then use the certificate for OAuth from OAuth certificate section. (Bug 1051651)

1.4.2.3 Kerberos Fall Back Mechanism Does Not Redirect to the Password Reset Page

Kerberos fall back mechanism does not redirect to the password reset page when an expired password or expiring password is detected. (Bug 1053242)

1.4.2.4 Login Page Does Not Render Properly After a Kerberos Authentication Method Failure

Issue: The fallback login page is not rendered properly after a Kerberos method authentication failure. (Bug 1059514)

Fix: The fallback login page now renders properly and retains customization as well. You no longer need to follow the configuration steps mentioned in TID 7015049.

1.4.2.5 Passive Mode Authentication Fails When Accessing Office 365 with WS-Fed or WS-Trust

After upgrading Access Manager, when you access Office 365 using Passive Mode Authentication method, the authentication fails. (Bug 1048641)

1.4.3 Access Gateway

The following issues are fixed in Access Gateway:

- 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.

- Requests Sent from ESP can Cause XSS Vulnerability (CVE-2017-14799). For More Information about This Issue, See TID 7022358.
- Mangled Cookie Becomes Invalid When a User Accesses a Protected Resource. For More Information about This Issue, See TID 7022368. (Bug 1051390)
- Section 1.4.3.1, "Clustered Access Gateway Does Not Restore Postparked Data for Web Server After Authentication," on page 4

1.4.3.1 Clustered Access Gateway Does Not Restore Postparked Data for Web Server After Authentication

In an Access Gateway cluster, if the data is parked in one of the Access Gateways and ESP requests are sent on another Access Gateway, then after authentication data is not restored. (Bug 1058334)

2 Installing or Upgrading

After purchasing Access Manager 4.3.3, log in to the Customer Centre page to download the software. The following files are available:

Table 1 *Files Available for Access Manager 4.3.3*

Filename	Description
AM_43_SP3_AccessManagerService_Linux64.tar.gz	Contains Identity Server and Administration Console .tar file for Linux.
AM_43_SP3_AccessManagerService_Win64.exe	Contains Identity Server and Administration Console .exe file for Windows Server.
AM_43_SP3_AccessGatewayAppliance.iso	Contains Access Gateway Appliance .iso file.
AM_43_SP3_AccessGatewayAppliance.tar.gz	Contains Access Gateway Appliance .tar file.
AM_43_SP3_AccessGatewayService_Win64.exe	Contains Access Gateway Service .exe file for Windows Server.
AM_43_SP3_AccessGatewayService_Linux64.tar.gz	Contains Access Gateway Service .tar file for Linux.
AM_43_SP3_AnalyticsServerAppliance.iso	Contains Analytics Server Appliance .iso file.
AM_43_SP3_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 4.3 Installation and Upgrade Guide*.

3 Supported Upgrade Paths

To upgrade to Access Manager 4.3.3, you need to be on one of the following versions of Access Manager:

- 4.2 Service Pack 5
- 4.3 Service Pack 1
- 4.3 Service Pack 1 Hotfix 1
- 4.3 Service Pack 2

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

4 Verifying Version Number After Upgrading to 4.3.3

After upgrading to Access Manager 4.3.3, verify that the version number of the component is indicated as **4.3.3.0-24**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.3.3.0-24**.

See TID 7004764 to view the list of Access Manager release versions.

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.

5.1 Log Files Are Not Created After Moving to Windows 64-Bit

Issue: Log files are not created in the correct folder after moving to Windows 64-bit. (`Bug 1048139`)

Workaround: Run the following command in command prompt:

```
C:\Windows\System32\icacls.exe "C:\Program Files (x86)\Novell\log" /Q /C /T /
grant:r novlwww:(OI)(CI)F
```

5.2 The Audit Logs Are Not Sent to the Log File When Administration Console Is Configured As a Remote Audit Server for Syslog

Issue: When you enable auditing for Syslog server (click **Auditing** and then select **Syslog** > **Send to Third party**), the audit logs are not sent to `/var/log/NAM_Audits.log`. This issue occurs when Identity Server or Access Gateway is running on a Windows platform. (`Bug 1068602`)

Workaround: Perform the following steps in:

Identity Server: To view the audit logs of Identity Server audit events, create a user `novlwww` with full permission in the Syslog directory at `C:\Program Files (x86)\Novell`.

Access Gateway: To view the audit logs of Access Gateway audit events, add the following in the `log4j.base.xml` file at `C:\Program File\Novell\amlogging\config`:

```
<appender name="async" class="org.apache.log4j.AsyncAppender">
      <param name="BufferSize" value="3000"/>
     <param name="blocking" value="false"/>
     <appender-ref ref="AMAuditSyslogAuditAppender"/>
 </appender>


 <logger name="AUDIT-SYSLOG-ASYNC" additivity="false">
      <level value="all"/>
     <appender-ref ref="async"/>
  </logger>
```

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/.

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