Access Manager 3.2 Service Pack 3 Readme

August 2014

The Access Manager 3.2 Service Pack 3 release 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 Qmunity, our community Web site that also includes product notifications, logs, and product user groups.

For more information about this release and for the latest documentation, see the Documentation Web site. To download this product, see the Products Web site.

1 What’s New?

The Access Manager 3.2 Service Pack 3 release provides support for new versions of operating system and dependent components in addition to software fixes.

For the list of software fixes in the previous release, see Access Manager 3.2 Service Pack 2 IR3 readme.

1.1 Operating System Support

This version adds support for the following operating systems:

- SLES 11 SP3
- RHEL 6.5

The following operating systems are no longer supported in this release:

RHEL 6.2 and 6.3.

1.2 Updates for Dependent Components

This version provides support for the following dependent components:

- Tomcat 7-7.0.54
- Apache 2.2.24
- JDK 1.7.0_25
- iManager 2.7.7
- eDirectory 8.8.8

1.3 Fixed Issues

The following sections outline the issues resolved in this release:

1.3.1 Vulnerability Issue with OpenSSL

OpenSSL is vulnerable to a man-in-the-middle (MITM) attack. The attack occurs on vulnerable SSL/TLS clients and servers. OpenSSL clients are vulnerable in all versions of OpenSSL. However, OpenSSL servers are known to be vulnerable only in OpenSSL versions before 0.9.8za, from version 1.0.0 until version 1.0.0m, and from version 1.0.1 until version 1.0.1h as mentioned in CVE-2014-0224. For more information about this issue and the resolution, see TID 705158.

1.3.2 Issues with Apache Tomcat 7.0

Apache Tomcat from version 7.0 until version 7.0.50 do not handle large amount of chunked data or unlimited whitespace characters in a HTTP header. For more information about this issue, see CVE-2013-4322.

Apache Tomcat from version 7.0 until version 7.0.47 does not handle certain inconsistent HTTP request headers when HTTP or AJP connectors are used. For more information about this issue, see CVE-2013-4286.

The above vulnerabilities affect the following Access Manager components, that are installed with Tomcat:

- Administration Console
- Identity Server
- Embedded Service Provider running in the Access Gateway server

1.3.3 Software Fixes for the Identity Server

The following issues are fixed in the Identity Server:

1.3.3.1 lcache Fails to Log Audit Events

Issue: The lcache process fails to log audit events as it runs as non-root user after restarting. (Bug 770027)

Fix: The lcache process runs automatically as a root and the Identity Server sends the audit events to the audit server when the server restarts.

1.3.3.2 Properties Not Available in SAML 2.0 Service Provider Options

Issue: It is not possible to configure some of the SAML 2.0 options in the trusted provider UI, which can be set in the `nidpconfig.properties` file. (Bug 841215)

Fix: You can now configure the following options under SAML 2.0. In the Administration Console, click **Devices** > **Identity Servers** > **Edit** > **SAML 2.0**.

- SAML2_AVOID_NAMEIDPOLICY
- SAML2_AVOID_ISPASSIVE
- SAML2_AVOID_CONSENT
- SAML2_AVOID_PROTOCOLBINDING
- SAML2_AVOID_PROXYCOUNT
- SAML2_SIGN_METHODDIGEST_SHA256
- IS_SAML2_POST_SIGN_RESPONSE_TRUSTEDPROVIDERS

1.3.3.3 User Session Does Not Timeout After Defined Default Timeout or Authentication Timeout Values

Issue: The user session does not timeout after the specified authentication timeout value. If more than one contract is configured, the user session timeout is set to the highest value. For example, the user session will timeout after 10 minutes if you set the authentication timeout for two contracts to 5 minutes and 10 minutes. (Bug 852039)

Fix: The user session timeout occurs after the specified authentication timeout value.

1.3.4 Software Fixes for the Access Gateway Service and Access Gateway Appliance

The following issues are fixed in the Access Gateway Serviceand Access Gateway Appliance:

1.3.4.1 HTTP Logging Option Does Not Work

Issue: The Access Gateway does not delete the files that are older than the time you have specified in the **Delete Files Older Than** option under **HTTP Logging**. (Bug 840534)

Fix: When log rotation occurs the existing log files are now tracked and new logs are created. The old logs are deleted based on the time specified in the Delete Files Older Than option.

1.3.4.2 Idle Timeout Value Error Under TCP Connect Options

Issue: If you set the value of **Idle Timeout** under **TCP Connect Options** to a value above 1440, for example 1441, it displays an error even though the value is within the range of 1-1800. (Bug 857505)

Fix: Idle Timeout now accepts values within the range of 1-1800 seconds. If you do not specify a value within this range an error message is displayed.

1.3.4.3 Cannot Inject JavaScript Along With Form Fill Policy

Issue: When you create a Form Fill policy with **Auto Submit** enabled and select the **Inject JavaScript** option, the JavaScript does not get injected in the head and body tags of the HTML page. (Bug 863535)

Fix: The Form Fill policy works without any errors and the JavaScript is injected in head and body tags of the HTML page.

1.3.4.4 Additional DNS Name List Does Not Accept a Web Server Host Name

Issue: When you configure the HTML rewriter, you cannot specify a DNS name that appears on the Web pages of your server in the **Additional DNS Name List** option. (Bug 868388)

Fix: You can now specify the DNS name in the **Additional DNS Name List** option without any error.

1.3.4.5 ESP Cluster Cookies Use the First Cookie Causing Validation Error

Issue: When a browser sends multiple cluster cookies, Access Manager uses the first and not the last cookie. Whereas Apache IPCQZX03 and Tomcat JSESSIONID use the last cookie for session handling. Thus, it proxies the request to the wrong ESP server. (Bug 872953)

Fix: The ESP cluster cookies now consider the last reference to the cluster cookie in the request and you will not be requested to login again.

2 Installing or Upgrading

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 3.2 Service Pack 3.*

Filename	Description
AM_32_SP3_AccessManagerService_Linux64.tar.gz	Contains the Access Manager Service for Linux.
AM_32_SP3_AccessManagerService_Win64.exe	Contains the Access Manager Service for Windows Server 2008.
AM_32_SP3_AccessGatewayAppliance_Linux_SLES11_64.iso	Contains the Access Gateway Appliance.
AM_32_SP3_AccessGatewayAppliance_Linux_SLES11_64.tar.gz	Contains all patches from 3.2 to 3.2 SP3 for the Access Gateway Appliance.
AM_32_SP3_AccessGatewayService_Win64.exe	Contains the Access Gateway Service for Windows Server 2008.
AM_32_SP3_AccessGatewayService_Linux_64.tar.gz	Contains the Access Gateway Service for SLES 11 SP2, SLES 11 SP3, RHEL 6.4, or RHEL 6.5.

IMPORTANT: Before upgrading the Access Gateway Appliance it is important to upgrade the version of the underlying operating system to SLES 11 SP3. For more information about upgrading the base operating system, see "Upgrading the Operating System for Access Gateway Appliance" and for upgrading to 3.2 SP3, see "Upgrading the Access Manager from Version 3.2".

3 Supported Migration and Upgrade Paths

To upgrade to Access Manager 3.2 Service Pack 3 you must be on one of the following Access Manager versions:

- 3.2 SP2
- 3.2 SP2 IR1
- 3.2 SP2 IR2
- 3.2 SP2 IR3

Review the following table to understand the migrate/upgrade paths for Access Manager 3.2 Service Pack 3 from versions prior to Access Manager 3.2 Service Pack 2.

Table 2 *Migration and Upgrade Paths for 3.2 Service Pack 3*

Source	Migrate/Upgrade Paths
3.1.x	Migrate to 3.2 SP2 and then upgrade to 3.2 SP3.
3.2 SP1	Upgrade to 3.2 SP2 and then to 3.2 SP3.

For more information about upgrading or migrating Access Manager 3.2 Service Pack 3, see NetIQ Access Manager 3.2 SP3 Migration and Upgrade Guide.

4 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrade or migrate to Access Manager 3.2 Service Pack 3, verify the existing Access Manager version.

4.1 Verifying Version Number Before and After Upgrading to 3.2 Service Pack 3

Refer the following table to determine if you have the correct version installed.

Access Manager Version	Value in the Version field (Access Manager > Auditing > Troubleshooting> Version)
Access Manager 3.2 Service Pack 2	3.2.2-77
Access Manager 3.2 Service Pack 2 IR1	3.2.2-77 + IR1-108
Access Manager 3.2 Service Pack 2 IR2	3.2.2-77 + IR2-117
Access Manager 3.2 Service Pack 2 IR3	3.2.2-77 + IR3-122

After upgrading toAccess Manager 3.2 Service Pack 3, verify that the version number of the component is indicated as **3.2.3-47** in the **Version** field.

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 Issue with NTLM Authentication

Issue: Authentication fails when you access a protected resource that uses NTLM authentication. (Bug 867593)

Workaround: None

5.2 Issue with the Audit Logging Server

Issue: The Access Gateway health reports the Audit Logging Server service as green with a message indicating it is operational even though the Audit Server is not running. (Bug 878552)

Workaround: None

5.3 Issue with Windows Auditing Configuration Script

Issue: It is possible to run the `windows_script.bat` script file only on the Administration Console and not on any other Access Manager component. Hence, you cannot apply the new PA certificates to any of the Windows based Identity Server or Access Gateway Service. (Bug 883952)

Workaround: None

5.4 Upgrading the Primary or Secondary Administration Console to 3.2 SP3 Throws an LDAP Bind Error

Issue: Upgrading the primary/secondary Administration Console throws an `ldap_bind : Can't contact LDAP server` error. (Bug 887213)

One of the causes of this issue is because the validity of the eDirectory server certificate has expired.

Workaround: SLES and RHEL servers:

From the eDirectory server terminal execute the following commands:

1. `ndsconfig upgrade` [This creates new certificates for the server]
2. `nldap -u` [This unloads and stops LDAP services]
3. `nldap -l` [This command starts and loads the LDAP services]

   After executing these commands, the upgrade proceeds without issues.

Windows servers:

1. Login in to iManager as an administrator.
2. Select **Roles and Tasks > Novell Certificate Server > Repair Default Certificates**
3. Select the server(s) that own the certificates and click **Next**.

4. Select **Yes All Default Certificates will be overwritten** and click **Next**.
5. Review the tasks to be performed and select **Finish**.

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

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

989 Windows XP Enhanced Cryptographic Provider (RSAENH)

990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

997 Microsoft Windows XP

1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)

1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)

1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)

1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)