Access Manager 4.0 Service Pack 2 Release Notes

June 2015

Access Manager 4.0 Service Pack 2 (4.0 SP2) 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 Qmunity, our community Web site that also includes product notifications, logs, and product user groups.

For information about the previous release, see Access Manager 4.0 SP1 Hotfix 3 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.

1 What’s New?

Access Manager 4.0 SP2 provides the following platform updates and fixed issues:

1.1 Operating System Support

In addition to the platforms introduced in the previous Access Manager release, this release adds support for the following platform:

- RHEL 6.6

1.2 Updates for Dependent Components

This release adds support for the following dependent components:

- Apache 2.2.27 (This release includes fixes for CVE-2014-0231, CVE-2014-0226, and CVE-2013-5704)
- eDirectory 8.8.8.4
- iManager 2.7.7.4

- Java 1.8.0_45-1
- Platform Agent 2.0.2.77
- Tomcat 7.0.56

1.3 Fixed Issues

This release includes software fixes for the following components:

- Section 1.3.1, “Administration Console,” on page 2
- Section 1.3.2, “Access Gateway,” on page 3
- Section 1.3.3, “Identity Server,” on page 4

1.3.1 Administration Console

The following issues are fixed in the Administration Console component:

- Section 1.3.1.1, “Cross-Site Scripting Vulnerability Issue in JSP Pages,” on page 2
- Section 1.3.1.2, “Upgrade from 3.2.x to 4.0.x Fails When NMAS Method is Installed in the eDirectory Server,” on page 2
- Section 1.3.1.3, “Unable to Restore the Administration Console Configuration From Backup,” on page 2

1.3.1.1 Cross-Site Scripting Vulnerability Issue in JSP Pages

Issue: Multiple cross-site vulnerabilities exist in `debug.jsp` page. The affected URLs are:

- `https://<host>:8443/roma/jsp/debug/debug.jsp?xss=%3Cscript%3Ealert%28%27xss%27%29%3C/script%3E`
- `https://<host>/sslvpn/applet_agent.jsp?lang=%22%3E%3Cscript%3Ealert%28%27xss%27%29%3C/script%3E`

Fix: This issue is resolved by sanitizing `.jsp` pages in the affected URLs. [`Bug 906241`][`CVE-2014-5214`]

1.3.1.2 Upgrade from 3.2.x to 4.0.x Fails When NMAS Method is Installed in the eDirectory Server

Issue: If you have selected to install the NMAS SAML method in the eDirectory tree, upgrading from Access Manager 3.2.x to 4.0.x fails with an error. This happens because the eDirectory schema is not successfully extended with NMAS objects. [`Bug 888263`]

Fix: This issue is now fixed and upgrading to Access Manager 4.0.x does not fail even when NMAS SAML method is installed.

1.3.1.3 Unable to Restore the Administration Console Configuration From Backup

Issue: When you restore the Administration Console from backup, the previous configuration is lost. This is because the restored Administration Console is configured on a different hostname under the same IP address. [`Bug 905684`]

Fix: This issue is resolved now as you can restore the Administration Console with a different hostname under the same IP address.

1.3.2 Access Gateway

The following issues are fixed in the Access Gateway component:

1.3.2.1 SAP Application Server Returns 500 Internal Error after a POST Request

Issue: When a SAP Application server is protected by the Access Gateway, SAP Application Server returns 500 internal error after POST request. This happens because the Access Gateway corrupts the ZNPCQ. [Bug 872117]

Fix: The Access Gateway no longer corrupts the ZNPCQ (session stickiness cookie).

1.3.2.2 Unable to Authenticate Due to 405 -esp-xxxx Error

Issue: When both **Enable SSL with Embedded Service Provider (ESP)** and **Behind Third Party SSL Terminator** are enabled and both **Enable SSL between browser** and **Access Gateway** are disabled, the cookie broker option is not properly populated. This results in 405 error. [Bug 915987]

Fix: This issue is resolved now as the cookie broker option is properly populated.

1.3.2.3 Access Manager Writes Incomplete Shared Secrets to eDirectory

Issue: When LDAP server replicas are used, Access Manager does not write shared secrets consistently to the eDirectory. [Bug 917508]

Fix: Now, the shared secrets are written consistently.

1.3.2.4 Issue in Rewriting Location Header with the URL in the Query

Issue: Rewriter does not rewrite the location header with the URL in the query string. [Bug 915839]

Fix: Now, the rewriter rewrites the location header with the URL in the query string.

1.3.2.5 The Form Fill Policy Fails Intermittently

Issue: The Form Fill policy fails intermittently due to heavy load. [Bug 880083]

Fix: This issue is now resolved by adding conditions to re-evaluate the Form Fill policy during null response under load conditions.

1.3.2.6 Cross-Domain Authentication Sends Access Gateway Session Cookie as a URL Query String Parameter

Issue: The Access Gateway session cookie is sent as a query parameter during the cross-domain authentication without encryption. That in turn causes security concerns. [`Bug 928875`]

Fix: Now, the Access Gateway session cookie sent as a query parameter during the cross-domain authentication is encrypted to prevent security issues. For additional security, you can change the default key used for this encryption by using the `NAGSessionKey` advanced option.

1.3.2.7 Memory Leak Leads to HTTPd Crash

Issue: The HTTPd crashes due to frequent graceful restarts. This is due to the increase in the size of the memory leaks that occurs during each graceful restart. [`Bug 896935`]

Fix: This issue is resolved now as the HTTPd does not crash due to frequent graceful restarts.

1.3.2.8 Platform Agent Creates Multiple Connections When Set to ForceCache Mode

Issue: Platform Agent creates multiple connections when it is set to ForceCache mode. [`Bug 905373`]

Fix: A newer version of Platform Agent is bundled with Access Manager 4.0 SP2 that resolves this issue.

1.3.2.9 Unable to Turn On/Off the Cookie Mangle Advanced Option

Issue: At the parent and child proxy service level, you cannot turn on/off the **Cookie Mangle** advanced option. [`Bug 924285`]

Fix: This issue is resolved now as you can turn on/off the **Cookie Mangle** advanced option.

1.3.2.10 Adding a Secondary IP Address to the Access Gateway Appliance Removes the Loopback Interface Configuration File

Issue: When you add a secondary IP address to the Access Gateway Appliance, it removes the Loopback Interface Configuration file. [`Bug 883503`]

Fix: This issue is now resolved.

1.3.2.11 Form Fill Masking Fails to Re-Calculate Valid Content Length

Issue: When Form Fill masking is enabled, the Access Gateway fails to re-calculate content length after the data is unmasked. This leads to single sign-on failure. [`Bug 915988`]

Fix: This issue is resolved now as the Access Gateway re-calculates content length correctly.

1.3.3 Identity Server

The following issues are fixed in the Identity Server component:

- Section 1.3.3.1, “Secure Flags is Not Set on Cluster Cookies in the Identity Servers and Embedded Service Provider,” on page 5
- Section 1.3.3.2, “Single Sign-On to Office 365 Fails on the Latest Version of iOS Apps,” on page 5
- Section 1.3.3.3, “Identity Server Becomes Non-Responsive Due to SAML Billion Laughs Attack,” on page 5

1.3.3.1 Secure Flags is Not Set on Cluster Cookies in the Identity Servers and Embedded Service Provider

Issue: In a clustered environment, secure flag is not set on the server cluster cookie `UrnNovellNidpClusterMemberId`. [`Bug 919960`]

Fix: This issue is fixed and by default, the secure flag is set on the `UrnNovellNidpClusterMemberId` cookie.

1.3.3.2 Single Sign-On to Office 365 Fails on the Latest Version of iOS Apps

Issue: Single sign-on to Office 365 fails when you upgrade to the latest version of the Office 365 iOS apps. [`Bug 916003`]

Fix: This issue is resolved now. You can single sign-on from latest version of the Office 365 iOS apps. To establish single sign-on from iOS apps to Office 365 services, perform the following steps:

1. In the Administration Console, click **Devices > Identity Servers > Edit > Local > Contract**.
2. Specify a name to identity the contract.
3. Specify the URI as `http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password`.
4. Select **Name/Password - Form - WebService** method.

1.3.3.3 Identity Server Becomes Non-Responsive Due to SAML Billion Laughs Attack

Issue: When you modify the SAML authentication request and append the XML with specific strings of data and encode it, the Identity Server becomes non-responsive. This is due to the Billion Laugh Attack. [`Bug 914449`]

Fix: This issue is fixed now as the Identity Server can handle the modified XML and discard the request. Also, you can log the reason in the server logs now.

2 Upgrading to Access Manager 4.0 SP2

After purchasing Access Manager 4.0 SP2, log in to the NetIQ Downloads page and follow the link that allows you to download the software. Ensure that you are currently on any one of the following Access Manager versions, before upgrading to Access Manager 4.0 SP2:

- 3.2 SP2: All versions
- 3.2 SP3: All versions
- 4.0: All versions
- 4.0 SP1: All versions

3 Verifying Version Number Before and After Upgrading to 4.0 SP2

Before upgrading, verify the version number of the existing Access Manager components and ensure that you have the correct version of files on your system.

After upgrading to Access Manager 4.0 SP2, verify that the version number of the component is indicated as **4.0.2-34** in the **Version** field.

4 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.

4.1 Upgrading Access Manager from 4.0 SP2 to 4.1 Terminates Abruptly

Issue: If you attempt to upgrade from 4.0 SP2 to 4.1, the upgrade process terminates abruptly. [`Bug 928302`]

Workaround: If you are planning an upgrade from 4.0 SP2 to 4.1, perform the following steps:

1. Extract the 4.1 installer files and locate `upgrade_utility_functions.sh` file.
2. Locate the section that includes the following line:
   `supportedVersions="3.2.2\|3.2.3\|4.0.0\|4.0.1\|4.1.0.0"`
3. Modify the **supportedVersion** section by adding 4.0.2 as the supported upgrade platform in the following manner: `supportedVersions="3.2.2\|3.2.3\|4.0.0\|4.0.1\|4.0.2\|4.1.0.0"`
4. Upgrade the components using the information in Upgrading Access Manager.

4.2 Accessing an Accelerated SSL Web Server on RHEL 6.6 Server Results in an SSL Handshake Error

Issue: When you attempt to access a proxy service on the RHEL Access Gateway Service and the Accelerated web server has a self-signed certificate, it results in an SSL handshake error. [`Bug 929662`]

Workaround: None

5 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 Web site.

For general corporate and product information, see the NetIQ Corporate Web site.

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

6 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)