Access Manager 4.1 Service Pack 1 Release Notes

June 2015

Access Manager 4.1 Service Pack 1 includes updates to dependent components 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 website that also includes product notifications, logs, and product user groups.

For information about the previous release, see Access Manager 4.1 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.

- Section 1, “What’s New?,” on page 1
- Section 2, “Installing or Upgrading Access Manager,” on page 7
- Section 3, “Supported Upgrade Paths,” on page 7
- Section 4, “Verifying Version Numbers After Upgrading to 4.1 Service Pack 1,” on page 8
- Section 5, “Known Issues,” on page 8
- Section 6, “Contact Information,” on page 9
- Section 7, “Legal Notice,” on page 9

1 What’s New?

Access Manager 4.1 Service Pack 1 provides the following updates 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 8.8.8.5
- Java 1.8.0_45
- OpenSSL 1.0.1o
- Platform Agent 2.0.2.77
- Tomcat 8.0.23

NOTE: On Windows, the Administration Console and Identity Server use Tomcat 7.0.56. The Tomcat version is not upgraded to version 8.0.23 due to dependency on iManager. On Linux, only the Administration Console is not upgraded to the latest Tomcat version.

Access Manager 4.1 Service Pack 1 supports Tomcat 8.0.23 and OpenSSL 1.0.1o. Due to this, the Identity Server and the Access Gateway disable requests from clients that are on versions lower than TLS1. However, the Access Gateway can continue communication with web servers that are on versions lower than TLS1.

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 3
- Section 1.2.3, “Access Gateway Service and Access Gateway Appliance,” on page 4

1.2.1 Administration Console

The following issues are fixed in the Administration Console component:

- Section 1.2.1.1, “Administration Console Installation Fails when Installation is Performed from a Shared Network Folder,” on page 2
- Section 1.2.1.2, “Unable to Restore the Administration Console Configuration from a Backup File,” on page 2
- Section 1.2.1.3, “Attempting to Access an Existing Class Configuration Leads to JasperException Error,” on page 2
- Section 1.2.1.4, “Upgrade from 3.2.x to 4.0.x Fails When an NMAS SAML Method is Installed in the eDirectory Server,” on page 3

1.2.1.1 Administration Console Installation Fails when Installation is Performed from a Shared Network Folder

Issue: When you attempt to perform an Administration Console installation from a shared network folder or a read-only NFS mount, the installation fails. [`Bug 925951`]

Fix: This issue is resolved now and the installation succeeds without any errors.

1.2.1.2 Unable to Restore the Administration Console Configuration from a Backup File

Issue: If the Administration Console is configured with a different hostname and the same IP address, restoring it by using the backup file does not work. [`Bug 918778`]

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

1.2.1.3 Attempting to Access an Existing Class Configuration Leads to JasperException Error

Issue: If you attempt to access an existing class configuration by using **Identity Server > Local > Classes** a `JasperException: Unable to compile class for JSP` error is displayed. [`Bug 929422`]

Fix: This issue is resolved now and no error is displayed when existing class configuration is accessed.

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

Issue: If you have selected to install an NMAS SAML method in the eDirectory server, 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 in the eDirectory server.

1.2.2 Identity Server

The following issues are fixed in the Identity Server component:

- Section 1.2.2.1, “Cannot Proxy SAML 2.0 AuthnRequest with an External Contract to a Remote SAML 2.0 Identity Server,” on page 3
- Section 1.2.2.2, “Accessing Logout URL with a Smart Card Causes Auto Login,” on page 3
- Section 1.2.2.3, “Open Redirect in WS-Federation Authentication Causes Redirection Without Validation,” on page 3
- Section 1.2.2.4, “Risk-Based Authentication Cannot Calculate Risk Based on IP Address or Geolocation if Authentication Request is Handled by a Proxy Server,” on page 4
- Section 1.2.2.5, “Secure Flag is Not Set on Cluster Cookies in the Identity Servers and Embedded Service Provider,” on page 4
- Section 1.2.2.6, “Single Sign-On to Office 365 Fails on the Latest Version of iOS Apps,” on page 4
- Section 1.2.2.7, “Identity Server Becomes Non-Responsive Due to SAML Billion Laughs Attack,” on page 4

1.2.2.1 Cannot Proxy SAML 2.0 AuthnRequest with an External Contract to a Remote SAML 2.0 Identity Server

Issue: The AuthnContextClassRef in RequestedAuthnContext statement of the service provider AuthnRequest, does not match the external contract to a remote SAML2 identity provider and leads to failure in processing the assertion request by the identity provider. [Bug 869990]

Fix: This issue is now resolved and the external contract is executed to redirect to a remote Identity Server.

1.2.2.2 Accessing Logout URL with a Smart Card Causes Auto Login

Issue: When a user log in by using a smart card and attempts to log out causes auto login, and the Identity Server displays a login success page instead of a logout page. [Bug 904405]

Fix: This issue is fixed and attempting to logout leads the user to a logout success page.

1.2.2.3 Open Redirect in WS-Federation Authentication Causes Redirection Without Validation

Issue: If you are using WS-Federation for authentication, an open redirect is possible without validation. Failure to validate the redirection can be used for phishing purposes or to redirect to a page containing malicious content. [Bug 903063]

Fix: This issue is now fixed by restricting the target domain in the service providers metadata that includes domain of the single logout URL. This results in an error message being displayed when there is an attempt to access another domain.

1.2.2.4 Risk-Based Authentication Cannot Calculate Risk Based on IP Address or Geolocation if Authentication Request is Handled by a Proxy Server

Issue: In an Identity Server clustered environment if the authentication request is handled by a proxy, the IP address information of the client is not passed to the risk engine. Due to this, if you have created rules based on IP address or Geolocation, risk cannot be assessed. [`Bug 929862`]

Fix: This issue is now fixed and the source IP address details are included in the header.

1.2.2.5 Secure Flag 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.

1.2.2.6 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. For more information about how to fix this issue, see "After upgrading iOS Apps to the Latest Version, Single Sign-On to Office 365 Services Fail" section in the NetIQ Access Manager 4.1 Administration Guide.

1.2.2.7 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 Laughs Attack. [`Bug 914449`]

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

1.2.3 Access Gateway Service and Access Gateway Appliance

The following issues are fixed in the Access Gateway component:

- Section 1.2.3.1, “SAP Application Server Returns 500 Internal Error after a POST Request,” on page 5
- Section 1.2.3.2, “Apache Crashes With a Segmentation Fault Error,” on page 5
- Section 1.2.3.3, “Unable to Authenticate Due to 405 -esp-xxxx Error,” on page 5
- Section 1.2.3.4, “Access Manager Writes Incomplete Shared Secrets to eDirectory,” on page 5
- Section 1.2.3.5, “Issue in Rewriting Location Header with the URL in the Query,” on page 5
- Section 1.2.3.6, “The Form Fill Policy Fails Intermittently,” on page 5
- Section 1.2.3.7, “When Tunneling is Configured the Access Gateway Service Does Not Use Configured Outbound IP Address to Connect to a Webserver,” on page 5
- Section 1.2.3.8, “Adding a Secondary IP Address to the Access Gateway Appliance Removes the Loopback Interface Configuration File,” on page 6
- Section 1.2.3.9, “Memory Leak Causes HTTPd Crash,” on page 6
- Section 1.2.3.10, “Platform Agent Creates Multiple Connections When Set to ForceCache Mode,” on page 6
- Section 1.2.3.11, “Unable to Enable or Disable the Cookie Mangle Advanced Option,” on page 6

- Section 1.2.3.12, “Form Fill Masking Fails to Re-Calculate Valid Content Length,” on page 6
- Section 1.2.3.13, “Authentication Errors in Office 2013 Files,” on page 6
- Section 1.2.3.14, “In a Proxy Setup the Access Gateway Displays an IP Mismatch Error Even Though the IP Address is Not Changed,” on page 6
- Section 1.2.3.15, “Code Promotion Import Fails If the Access Gateway Cluster Name Contains an Underscore Character,” on page 6

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

Issue: When a SAP Application server is protected by the Access Gateway, the SAP Application Server returns a 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).

1.2.3.2 Apache Crashes With a Segmentation Fault Error

Issue: The Apache server crashes with a segmentation fault error if the host header field in the HTTP request is null. [Bug 928727]

Fix: This issue is resolved now by introducing a null check to restrict operations if the host header field contains a null value.

1.2.3.3 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 a 405 -esp xxxx error. [Bug 857620]

Fix: This issue is resolved now and the cookie broker option is populated without errors.

1.2.3.4 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: This issue is now resolved and the shared secrets are written consistently.

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

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

Fix: This issue is now resolved and the Rewriter rewrites the location header with the URL in the query string.

1.2.3.6 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 and the form fill policy does not fail in conditions of heavy load.

1.2.3.7 When Tunneling is Configured the Access Gateway Service Does Not Use Configured Outbound IP Address to Connect to a Webserver

Issue: If multiple IP addresses are configured as part of tunneling in Access Gateway Service, the outbound IP address does not change even if the IP address settings are changed. The older IP address is used as the Outbound IP address. [Bug 916639]

Fix: This issue is resolved and the Outbound IP address is the same as configured in the tunnel settings.

1.2.3.8 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 931631]

Fix: This issue is now resolved.

1.2.3.9 Memory Leak Causes 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 occur during each graceful restart. [Bug 916011]

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

1.2.3.10 Platform Agent Creates Multiple Connections When Set to ForceCache Mode

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

Fix: This issue is resolved now and a newer version of the Platform Agent is bundled with Access Manager 4.0 Service Pack 1.

1.2.3.11 Unable to Enable or Disable the Cookie Mangle Advanced Option

Issue: At the parent and child proxy service level, you cannot enable or disable the **Cookie Mangle** advanced option. [Bug 924285]

Fix: This issue is resolved now and you can enable or disable the **Cookie Mangle** advanced option.

1.2.3.12 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 and the Access Gateway re-calculates content length correctly.

1.2.3.13 Authentication Errors in Office 2013 Files

Issue: Multiple authentication errors are seen while accessing Office 2013 files. [Bug 899905]

Fix: This issue is resolved now and the users can access Office 2013 files.

1.2.3.14 In a Proxy Setup the Access Gateway Displays an IP Mismatch Error Even Though the IP Address is Not Changed

Issue: In a proxy setup, the Access Gateway session cookie contains the IP address of the Access Gateway server instead of the IP address of the remote client. Due to this, the Access Gateway displays an IP mismatch error even though the client IP address is not changed. [Bug 925885]

Fix: This issue is resolved now and the IP mismatch error is not displayed.

1.2.3.15 Code Promotion Import Fails If the Access Gateway Cluster Name Contains an Underscore Character

Issue: If the Access Gateway cluster name contains an underscore character (_), code promotion import fails. [Bug 934661]

Fix: This issue is resolved now and code promotion import does not fail if the Access Gateway cluster name contains an underscore character.

2 Installing or Upgrading Access Manager

After purchasing Access Manager 4.1 Service Pack 1, 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 4.1 Service Pack 1*

Filename	Description
`AM_41_SP1_AccessManagerService_Linux64.tar.gz`	Contains the Identity Server, the Administration Console for Linux.
`AM_41_SP1_AccessManagerService_Win64.exe`	Contains the Identity Server and the Administration Console for Windows Server.
`AM_41_SP1_AccessGatewayAppliance.iso`	Contains the Access Gateway Appliance iso.
`AM_41_SP1_AccessGatewayAppliance.tar.gz`	Contains the Access Gateway Appliance tar file.
`AM_41_SP1_AccessGatewayService_Win64.exe`	Contains the Access Gateway Service for Windows Server.
`AM_41_SP1_AccessGatewayService_Linux64.tar.gz`	Contains the Access Gateway Service tar file.

3 Supported Upgrade Paths

To upgrade to Access Manager 4.1 Service Pack 1, you must be on any one of the Access Manager versions:

From 3.2.x:

- 3.2 Service Pack 2
- 3.2 Service Pack 2 IR1
- 3.2 Service Pack 2 IR2
- 3.2 Service Pack 2 IR3
- 3.2 Service Pack 3
- 3.2 Service Pack 3 HF1

From 4.x:

- 4.0
- 4.0 HF1
- 4.0 HF2
- 4.0 HF3
- 4.0 Service Pack 1
- 4.0 Service Pack 1 HF1

- 4.0 Service Pack 1 HF2
- 4.0 Service Pack 1 HF3
- 4.0 Service Pack 2
- 4.1

For more information on upgrading Access Manager 4.1 Service Pack 1, see *Upgrading Access Manager*.

4 Verifying Version Numbers After Upgrading to 4.1 Service Pack 1

After upgrading to Access Manager 4.1 Service Pack 1, verify that the version number of the component is indicated as **4.1.1.0-32**. To verify the version number, perform the following steps:

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version.**
2. Verify that the **Version** field lists **4.1.1.0-32**.

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.

- Section 5.1, “Risk-Based Cookie is not Created if the Primary Authentication Method is Same for Primary and Secondary Authentication Contract,” on page 8
- Section 5.2, “The amdiagcfg Stylesheet Does Not Include Access Manager 4.1 Feature Configurations,” on page 8

5.1 Risk-Based Cookie is not Created if the Primary Authentication Method is Same for Primary and Secondary Authentication Contract

Issue: If you have successfully authenticated using additional authentication, a cookie is not created if both the primary and secondary contracts have the same primary authentication method. [`Bug 920988`]

Workaround: While configuring the primary and secondary authentication contracts, ensure that the contracts do not use the same primary authentication method.

5.2 The amdiagcfg Stylesheet Does Not Include Access Manager 4.1 Feature Configurations

Issue: The amdiagcfg stylesheet does not include configuration details of features introduced in Access Manager 4.1. [`Bug 922011`]

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 (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

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or inter operates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

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)

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2015 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/ (http://www.netiq.com/company/legal/).