Access Manager Appliance 4.1 Release Notes

March 2015

![(Product Name and Version)] Access Manager Appliance 4.1 includes new features, 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 Appliance 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?

![The sections listed here are just samples. Use those that are applicable to your release. If not for any features, there will definitely be software fixes and enhancements that can be added to this section.] Access Manager Appliance 4.1 provides the following key features, enhancements, and fixes in this release:

NOTE:

The SSL VPN component is removed from Access Manager 4.1 onwards. After upgrading to Access Manager Appliance 4.1, manually remove the proxy services and protected resources that refer to SSL VPN. Access Manager indicates the Access Gateway cluster health in yellow if you do not remove the referenced proxy services and protected resources. For more information, see Remove The Referenced Proxy Services and Protected Resources section.

After upgrading Access Manager Appliance from 3.2.2 or higher to 4.1, the Access Manager Appliance portal is no longer available. After you upgrade to Access Manager Appliance 4.1, manually remove the proxy services and protected resources that refer to the portal. Access Manager indicates the Access Gateway cluster health in yellow if you do not remove the referenced proxy services and protected resources. For more information, see Remove The Referenced Proxy Services and Protected Resources section.

1.1 New Features

This release introduces the following new features:

- Section 1.1.1, “Risk-Based Authentication,” on page 2
- Section 1.1.2, “OAuth And OpenID Connect,” on page 2
- Section 1.1.3, “Code Promotion,” on page 2
- Section 1.1.4, “Reporting,” on page 3
- Section 1.1.5, “Support to Launch Login Pages on a Handheld Device,” on page 3
- Section 1.1.6, “Simplified Mobile Access Integration,” on page 3

1.1.1 Risk-Based Authentication

This release introduces an authentication technique called Risk-based authentication.

Risk-based authentication provides context-aware access control that acts to balance the level of trust against risk. It enables organizations to address access-related risks while improving the user experience. Risk-based authentication allows runtime validation of an access request, and then take an appropriate actions such as asking for advanced authentication or denying access. For more information about configuring Risk-based authentication, see “Risk-Based Authentication”.

1.1.2 OAuth And OpenID Connect

This release introduces support for OAuth and OpenID Connect. OAuth 2.0 is an open protocol to allow secure authorization. It enables users to allow third-party clients to access users’ private resources. Users do not need to share their credentials. The third-party clients can be web applications, mobile phones, handheld devices, and desktop applications. OAuth provides a method to issue Access tokens to third-party clients with the user's approval. The third-party client can then use the Access token to access protected resources hosted by the resource server.

OAuth allows users to control the access to web resources by scope, action, and time. Access Manager uses OpenID Connect along with OAuth. OpenID Connect implements a single sign-on protocol on top of the OAuth authorization process. It allows clients to verify the identity of a user based on the authentication performed by the Identity Server (authorization server). It also allows client applications to obtain a user’s basic profile information. For more information about configuring OAuth and OpenID Connect, see “Configuring OAuth and OpenID Connect”.

1.1.3 Code Promotion

Code Promotion helps you replicate the configuration data of Access Manager from one setup to another. You can export the configuration data as a password-protected encrypted file, then import this file into another Access Manager system and seamlessly replicate the configuration into the target system.

The exported configuration data includes generic Identity Server cluster configuration, customization files, proxy services, protected resources, and policy configuration. This exported data is independent of the device specific data and network specific data. Therefore, you can use Code Promotion to replicate configuration between two Access Manager systems that are in different networks, with a different number of devices, and with different user stores. For more information about Code Promotion, see Code Promotion.

1.1.4 Reporting

Access Manager uses Sentinel Solution Pack to generate reports. This solution pack consists of predefined report definitions. Access Manager requires NetIQ Sentinel or Sentinel Log Manager to use this feature. You can use these reports to analyze users' accesses to applications protected by Access Manager, in auditing, and for compliance purposes. For more information about Reporting, see Reporting.

1.1.5 Support to Launch Login Pages on a Handheld Device

With this feature, the mobile login pages become more responsive. You can customize the logo and the header size for better readability on a hand-held device. For more information about how to customize the mobile login page, see Customizing the Identity Server Login Page.

1.1.6 Simplified Mobile Access Integration

With this feature, integration with the Mobile Access is simplified. You do not need to log in to the Administration Console to configure any settings. For more information about using Mobile Access with Access Manager, see Using NetIQ® CloudAccess as a Trusted Identity Provider for NetIQ® Access Manager.

1.2 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.4
- iManager 2.7.7.4 (This release includes fixes for CVE-2014-5216)
- Java 1.8.0_31
- OpenSSL 1.0.1m
- Apache 2.2.27 (This release includes fixes for CVE-2014-0231, CVE-2014-0226, and CVE-2013-5704)
- Tomcat 8.0.18

NOTE: Administration Console is not upgraded to the latest Tomcat version.

Access Manager 4.1 by default supports Tomcat 8.0.18 and OpenSSL 1.0.1m. Due to this, the Identity Server and 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.

1.3 Browser Support

This release adds support for latest versions of the following browsers:

- Internet Explorer 11 (Non Metro UI)
- Chrome

1.4 Enhancements

This release introduces the following enhancements:

- Section 1.4.1, “Capability to Bookmark a Protected Resource,” on page 4
- Section 1.4.2, “Office 365 Support for Multi-Domains,” on page 4
- Section 1.4.3, “Encryption of Access Gateway Session Cookie,” on page 4
- Section 1.4.4, “Updating Session ID After Authentication,” on page 5
- Section 1.4.5, “Single Sign-On to Office 365 By Using the Latest Version of iOS Apps,” on page 5
- Section 1.4.6, “Facility to Encode the Attribute Value,” on page 5
- Section 1.4.7, “HTML Rewriter Supports IPP Protocol For Print,” on page 5

1.4.1 Capability to Bookmark a Protected Resource

In this release, you can bookmark a protected resource. The Identity Server login page now includes a target in the URL. When you try to log in to the resource that is bookmarked, Access Manager authenticates you and redirects you to the resource.

If you have bookmarked a resource earlier, ensure that you update the existing bookmark with the new one.

NOTE: You cannot bookmark a login page that is used in a federation setup.

1.4.2 Office 365 Support for Multi-Domains

In this release, you can configure Office 365 to support multiple domains. This is achieved by using `STS_OFFICE365_MULTI_DOMAIN_SUPPORT_AUTO` parameter in the `nidpconfig.properties` file. This ensures that if you have users included in different domains, these users can access Office 365 services using the Issuer URI specific their domain. For more information about configuring Office 365 service, see Configuring Federation with Office 365 Services for Multiple Domains.

1.4.3 Encryption of Access Gateway Session Cookie

The Access Gateway session cookie sent as a query parameter during 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. For more information about this advanced option, see Advanced Access Gateway Options.

1.4.4 Updating Session ID After Authentication

The session fixation issue is fixed by updating the session ID after authentication. Post authentication, the session ID is regenerated each time. For more information about the Advanced Access Gateway option, see Advanced Access Gateway Options. For more information about the Identity Server Advanced option, see Enabling Secure Cookies.

1.4.5 Single Sign-On to Office 365 By Using the Latest Version of iOS Apps

This release introduces an enhancement that allows you to single sign-on from latest iOS apps version to Office 365. For more information see, Configuring Single Sign-On for Office 365 Services.

1.4.6 Facility to Encode the Attribute Value

This release provides different options to encode the values of attributes in an attribute set. The available encoding options are: **Special Characters Encoded**, **Not Encoded** and **Entire Value Encoded**.

1.4.7 HTML Rewriter Supports IPP Protocol For Print

The HTML Rewriter now supports Internet Printing Protocol (IPP) protocol. This enables printing through NetIQ Access Manager.

1.5 Fixed Issues

This release includes software fixes for the following components:

- Section 1.5.1, “Administration Console,” on page 5
- Section 1.5.2, “Identity Server,” on page 6
- Section 1.5.3, “Access Gateway,” on page 6

1.5.1 Administration Console

The following issues are fixed in the Administration Console component:

- Section 1.5.1.1, “Existing Access Privileges of Delegated Administrators are Revoked If a New Node is Added to the Cluster,” on page 5
- Section 1.5.1.2, “Curly Bracket in the URL Leads to Policy Evaluation Failure and User is Logged Out,” on page 5

1.5.1.1 Existing Access Privileges of Delegated Administrators are Revoked If a New Node is Added to the Cluster

Issue: If you add a new node in a cluster, Access Manager revokes the existing access rights of delegated administrators. [`Bug 891068`]

Fix: This issue is resolved now and the existing privileges of delegated administrators are not revoked even if a new node is added to the cluster.

1.5.1.2 Curly Bracket in the URL Leads to Policy Evaluation Failure and User is Logged Out

Issue: If the protected resource URL contains an unescaped curly bracket ({}) it leads to a policy evaluation failure and the user is denied access. [`Bug 885682`]

Fix: This issue is fixed and now unescaped curly brackets are allowed in authorization policy URLs.

1.5.2 Identity Server

The following issue is fixed in the Identity Server component:

1.5.2.1 Certificate Validation is Unsuccessful During SAML Assertions

Issue: The validation of expired certificate is unsuccessful in SAML assertions. [`Bug 899649`]

Fix: This issue is now resolved as the SAML assertions with expired certificates are rejected.

1.5.3 Access Gateway

The following issues are fixed in the Access Gateway component:

- Section 1.5.3.1, "Authentication Error in Office 2013 Files," on page 6
- Section 1.5.3.2, "Login Form Does Not Support the .doc Extension," on page 6
- Section 1.5.3.3, "Frequent Crashes Due to ActiveMQ API," on page 6
- Section 1.5.3.4, "Form Fill Policy Fails Intermittently," on page 6
- Section 1.5.3.5, "HttpOnly Flag is Not Set On Non-ESP Proxy," on page 6
- Section 1.5.3.6, "Form Fill Masking Fails to Re-Calculate Valid Content Length," on page 7
- Section 1.5.3.7, "Installation Continues Even if Both Public and Private IP Addresses Are in Same Subnet," on page 7
- Section 1.5.3.8, "Custom Policy Injects Incorrect Values," on page 7
- Section 1.5.3.9, "Host HTTP Header Attack," on page 7

1.5.3.1 Authentication Error 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 seamlessly in Access Manager.

1.5.3.2 Login Form Does Not Support the .doc Extension

Issue: The Form Fill policy is not processed when the Login Form has the `.doc` file extension. [`Bug 889599`]

Fix: This issue is now resolved and the Login Form supports the `.doc` extension.

1.5.3.3 Frequent Crashes Due to ActiveMQ API

Issue: The Apache HTTPd crashes frequently due to the ActiveMQ API. [`Bug 865204`]

Fix: This issue is resolved and the ActiveMQ API no longer crashes.

1.5.3.4 Form Fill Policy Fails Intermittently

Issue: The Form Fill policy fails intermittently due to heavy load. [`Bug 916540`]

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

1.5.3.5 HttpOnly Flag is Not Set On Non-ESP Proxy

Issue: The HttpOnly flag is not set on non-ESP proxy even after you enable it globally and on the proxy service. [`Bug 899885`]

Fix: This issue is resolved now as the HttpOnly flag is set correctly on non-ESP.

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

Issue: When Form Fill masking is enabled, Access Gateway fails to re-calculate content length after the data is unmasked. This leads to SSO failure. [`Bug 899135`]

Fix: This issue is resolved now as the content length is getting re-calculated correctly.

1.5.3.7 Installation Continues Even if Both Public and Private IP Addresses Are in Same Subnet

Issue: While configuring secondary interface, installation continues without showing any error even when both the public and private IP addresses are in the same subnet. [`Bug 887116`]

Fix: This issue is resolved now. The installation does not continue when both public and private IP are in the same subnet.

1.5.3.8 Custom Policy Injects Incorrect Values

Issue: The Custom policy injects incorrect values even after the attribute is updated. [`Bug 865775`]

Fix: This issue is resolved now and the Custom policy injects updated attribute values.

1.5.3.9 Host HTTP Header Attack

Issue: In the Access Gateway, a Host HTTP Header attack exists. An additional HTTP header is added with the original header. This header redirects you to a malicious URL. [`Bug 905262`]

Fix: This issue is resolved now as the Access Gateway in no longer susceptible to host HTTP Header attack.

2 Installing or Upgrading

After purchasing Access Manager Appliance 4.1, 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 Appliance 4.1*

Filename	Description
`AM_41_AccessManagerAppliance.iso`	Contains the Access Manager Appliance iso.
`AM_41_AccessManagerAppliance.tar.gz`	Contains the Access Manager Appliance tar file.

3 Supported Upgrade Paths

To upgrade to Access Manager 4.1, you need to be either on Access Manager 3.2 Service Pack 2 or higher or on Access Manager 4.0 or higher

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 4.0.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

For more information about upgrading Access Manager Appliance 4.1, see “NetIQ Access Manager Appliance 4.1 Installation and Upgrade Guide” in the *Upgrading Access Manager Appliance*.

4 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrading to Access Manager 4.1, verify the existing Access Manager version.

4.1 Verifying Version Number Before and After Upgrading to 4.1

Before upgrading, it is important to verify the version number of the existing Access Manager components. This ensures that you have the correct version of files on your system.

After upgrading to Access Manager 4.1, verify that the version number of the component is indicated as **4.1.0.0-201** 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.

- Section 5.1, “Access Gateway Indicates The Cluster Health In Yellow After Upgrading to Access Manager Appliance 4.1,” on page 9
- Section 5.2, “Risk-Based Cookie is not Created if the Primary Authentication Method is Same for Primary and Secondary Authentication Contract,” on page 9
- Section 5.3, “Rule Execution Fails if an IP Address Rule is Configured Using IP Subnet Condition,” on page 9
- Section 5.4, “The HTTP Rewriter Rewrites the SRC URL Incorrectly,” on page 9
- Section 5.5, “Memory Leak Leads to HTTPd Crash,” on page 9
- Section 5.6, “An Error Message Is Not Displayed When the Backend Server Is Unavailable,” on page 9
- Section 5.7, “The amdiagcfg Stylesheet Does Not Include Access Manager 4.1 Feature Configurations,” on page 10

5.1 Access Gateway Indicates The Cluster Health In Yellow After Upgrading to Access Manager Appliance 4.1

Issue: After upgrading the Access Manager Appliance to 4.1, the Access Gateway indicates the cluster health in yellow. [`Bug 919416`]

Workaround: After upgrading to Access Manager Appliance 4.1, manually remove the SSLVPN and portal referenced proxy services and protected resources from Access Gateway. For more information, see Removing Proxy Services And Protected Resources.

5.2 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.

5.3 Rule Execution Fails if an IP Address Rule is Configured Using IP Subnet Condition

Issue: When you configure an IP Address Rule using IP Subnet Condition the rule execution fails even though the IP subnet is valid. [`Bug 897927`]

Workaround: It is not possible to configure a rule using the IP subnet condition. Instead, use the IP range condition if you want to configure an IP address rule with an IP subnet condition.

5.4 The HTTP Rewriter Rewrites the SRC URL Incorrectly

Issue: The HTTP Rewriter rewrites SRC URL incorrectly when the links are from different HTTP chunks. This is a random issue. [`Bug 884593`]

Workaround: None.

5.5 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 916011`]

Workaround: Disable graceful restart by applying the following configuration change.

Locate `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` and change the command to `linux.apache.command.gracefulrestart command=restart`. You have to reconnect to regain the existing connections while applying changes.

5.6 An Error Message Is Not Displayed When the Backend Server Is Unavailable

Issue: Access Manager does not display any error message when the backend server is unavailable. [`Bug 869274`]

Workaround: In the error document `/opt/novell/apache2/share/apache2/error/HTTP_SERVICE_UNAVAILABLE.html.var`, change the `$REDIRECT_URL` value to ***/\/$*** instead of ***/\/$/***.

5.7 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.

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