Access Manager 4.0 Hotfix 1 Readme

March 2014

Access Manager 4.0 Hotfix 1 includes an enhancement and resolves several previous issues.

Many of these improvements were 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 (http://community.netiq.com/forums/30.aspx), our community Web site that also includes product notifications, blogs, and product user groups.

For the list of software fixes and enhancements in the previous release, see Access Manager 4.0 Readme.

For more information about this release and for the latest release notes, see the Documentation Web site. To download this product, go to Access Manager on the All Products Page (http://www.netiq.com/products).

NOTE: From this release onwards, NetIQ Corporation replaces the word IR with Hotfix.

---

1 What’s New?

Access Manager 4.0 Hotfix 1 supports OpenSSL 1.0.1 and the following issues are resolved in this release:

1.1 Support for TLS 1.1 and 1.2

For advanced security, Access Manager now supports TLS 1.1 and TLS 1.2. For more information, see Enabling TLS 1.1 and 1.2 for Access Manager 4.0.

1.2 Software Fixes for the Identity Server

NetIQ Access Manager 4.0 Hotfix 1 resolves the following Identity Server issues.

1.2.1 Errors Occur During SAML Logout

Issue: During SAML logout, session id resolves to random class E IP address. (Bug 849442)

Fix: The dot (.) is now removed while calculating the random number in the session index and it will not appear like an IP address format.

1.2.2 Radius Authentication with Token Fails

Issue: On a Radius server, authentication fails and the login page is displayed the second time. (Bug 859390)

Fix: Changes are made to the JSP where the submitted parameter value now accepts the value entered by the users.

1.2.3 NetIdentity Users are Prompted Twice for Credentials

Issue: When you enable the NetIdentity client and configure the Kerberos authentication, you are prompted for credentials twice even though correct credentials are used the first time. (Bug 859395)

Fix: If the NetIdentity flag is enabled and the NetIdentity header exists with the request, the Identity Server will not execute Kerberos. Hence, the Identity Server will not ask you for credentials the second time.

1.3 Software Fixes for the Access Gateway

NetIQ Access Manager 4.0 Hotfix 1 resolves the following Access Gateway issues.

1.3.1 Cannot Restart the Access Gateway Appliance if more than 99 IP Addresses are Added

Issue: Restarting the Access Gateway fails with an error that the Access Gateway could not bind the address when you have added more than 99 IP addresses to the Access Gateway Appliance. (Bug 798501)

Fix: The limit to the number of IP addresses is removed and the script can now handle more than 1000 IP addresses.

1.3.2 Looping Issues in the Access Gateway on Microsoft Windows

Issue: There are looping issues on Windows Access Gateway when you re-authenticate after the original session times out. (Bug 859379)

Fix: Access Gateway sends a correct response to the other cluster members if the session has expired.

1.3.3 GZip Compression Issues with Small Payloads Accelerating Sentinel or Liferay

Issue: When GZip is enabled and you access Sentinel/Liferay portal through Access Manager, a blank page is displayed. (Bug 859380)

Fix: The Access Gateway now decompresses the GZip data even if data is less than 10 bytes.

1.3.4 Multiple Authentication Requests While Opening Microsoft Excel Files

Issue: Access Manager prompts for multiple authentications when you open Microsoft Excel files through the Access Gateway. (Bug 859392)

Fix: Access Manager now handles WebDAV options request, and you can now open the Microsoft Excel files without entering the credentials multiple times.

1.3.5 Cannot Log Cached Status Extended Log Field

Issue: The **Cached Status** field is not logged in the logging configuration though you have enabled the extended HTTP logging for a proxy service. (Bug 859394)

Fix: The Access Gateway now adds **Cached Status** field in the logging configuration.

1.3.6 HTTP Logging Does Not Work on Windows Access Gateway Service

Issue: In Microsoft Windows, the Access Gateway does not create extended logs for reverse proxy requests configured for extended logging. (Bug 859398)

Fix: Updates are made to handle "/" and "\" for Microsoft Windows paths.

1.3.7 Rewriter Fails to Rewrite Meta HTML Headers

Issue: The Access Gateway does not rewrite the name from the backend server to a published name if you configure the Web server IP address as DNS name instead of the IP address. (Bug 859442)

Fix: If the Web server host name is configured as DNS name, the Access Gateway rewrites the URL if the back end DNS name exists as part of the URL.

1.3.8 Upgrading Access Manager Fails

Issue: When you upgrade Access Manager from 3.0 to 3.1 and then to 3.2, adding the Access Gateway appliance into an existing 3.1 cluster fails to populate the correct configuration file. This is because the Access Gateway appliance is expecting an `Order` attribute on the re-writer profiles. (Bug 859443)

Fix: HTTPD starts without any issues if you remove `Order` attribute from the configuration file and you restart the Access Gateway appliance.

1.3.9 Form Fill Policy Does Not work

Issue: There is an issue with the closing script tag in the login page under the header section. Hence, the Form Fill policy does not work. (Bug 859445)

Fix: The begin and end script tag in the login page will now consider '\x3c' and '/\' and Form Fill works as expected.

1.3.10 Access Gateway Does Not Work When the <form> Tag Includes an Empty Method Element

Issue: The Access Gateway does not work when the <form> tag includes an empty method element while processing a Form Fill policy. (Bug 859446)

Fix: With the introduction of a null check the Access Gateway works without any issue.

1.3.11 IP Mismatch Errors Display an Incorrect Message

Issue: When you access a protected resource from the Access Gateway and change the IP address of the client, the Access Gateway displays an Access Forbidden or NULL message. (Bug 859449)

Fix: The Access Gateway now displays a valid error message.

1.3.12 403 Error Occurs When URLs Contain %0A

Issue: The 403 permission denied error occurs when URLs query string contains the %0A character. (Bug 859580)

Fix: The Access Gateway now accepts URLs that contain the %0A and %20.

1.3.13 Identity Injection Policy Continuously Appends the Injected Query Line

Issue: The Identity Injection policy enabled on a protected resource duplicates the credential information sent to the Web server. For more information, see TID 7013274. (Bug 859581)

Fix: When the tag name in the request sent from the browser and the query string injected by the Identity Injection policy are same, only one tag is retained. Duplicates of same tag are now not injected.

2 Upgrading Access Manager

To upgrade Access Manager 4.0 Hotfix 1, download the `AM_400_HF1.zip`, which contains the Access Manager Patch Tool and the patch file.

1. Go to NetIQ downloads page.
2. Under **Patches**, click **Search Patches**.
3. Specify `AM_400_HF1.zip` in the search box to download the Hotfix file.

NOTE: To upgrade to this version, you must be using Access Manager 4.0.

You can upgrade to Access Manager 4.0 Hotfix 1 from Access Manager 4.0. For more information about upgrading, see Upgrading Access Manager Using the Patch Process for Linux and Upgrading Access Manager 4.0 Using the Patch Process for Windows.

2.1 Verifying Version Numbers

It is important to verify the version number of existing Access Manager components before you upgrade to 4.0 Hotfix 1. This ensures that you have the correct version of files on your system.

2.1.1 Verifying Version Number Before Upgrading to 4.0 Hotfix 1

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**
2. Examine the value of the Version field to see if it displays a version that is eligible for upgrading to 4.0 Hotfix 1. The Version field should list 4.0.0-110.

2.1.2 Verifying Version Number After Upgrading to 4.0 Hotfix 1

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**
2. Verify that the **Version** field lists 4.0.0-110 + HF1-139 when you upgrade from version 4.0.

3 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.

3.1 Issue During SSL Renegotiation When X.509 Authentication is Configured

Issue: An error occurs during SSL renegotiation after you select a client certificate while accessing a resource. (Bug 842019)

Workaround: Copy the CA certificates manually to the `/etc/opt/novell/apache2/conf/cacerts/custom` folder and restart Apache.

3.2 Web Server Load Balancing Does Not Work

Issue: Load balancing does not occur equally among the Web servers in a proxy service setup. (Bug 842496)

Workaround: Restart the Access Gateway when you update the server instead of a graceful restart. Edit the `agm.properties` file, search for `linux.apache.command.gracefulrestart` and replace it with `linux.apache.command.restart`. Restart the Access Gateway by using the `/etc/init.d/novell-mag restart` command. For more information and to fix this issue, see TID 7014203.

3.3 The Access Gateway Does Not Work When Syslog Level Logging to error_log Is Not Enabled

Issue: The Access Gateway has performance and stability issues when the proxy is enabled in the verbose mode and errors are reported regularly in the error_log file. (Bug 842805)

Workaround: Enable syslog level logging on the Access Gateway Proxy server if the Access Gateway service is running on SLES or RedHat. For more information, see TID 7011611.

3.4 Authentication Assertion Fails When Encrypt Assertions is Selected

Issue: If you have imported metadata initially by using a URL or text and edited manually, then no authentication assertions are returned in response when **Encrypt assertions** and **Want assertion to be signed** options are selected. (Bug 846558)

Workaround: Reimport the metadata through URL or text and follow the documentation steps available at Configuring SAML 2.0 to Sign Messages to enable message signing and use `nidpconfig.properties` for configuring it.

3.5 Certificate Verification Fails

Issue: An error occurs after importing the SAML2 metadata when Certificate Revocation List (CRL) check is enabled. (Bug 856049)

Workaround: To workaround this issue, perform the following procedure:

1. Go to **Security** > **Trusted Roots** > **Import** and import the encryption and signing trusted roots into the Administration Console.
2. From the Identity Server, go to **Edit** > **Security** > **Trusted Stores** > **NIDP Trust Store** and select the certificate you added in the previous step.

4 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 (http://community.netiq.com/), our community Web site that offers product forums, product notifications, blogs, and product user groups.

5 Legal Notice

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.

[Return to Top]