Access Manager 4.0 Service Pack 1 Hotfix 2 Readme

October 2014

Access Manager 4.0 Service Pack 1 Hotfix 2 (4.0.1 HF2) supercedes Access Manager 4.0 Service Pack 1 Hotfix 1.

For the list of software fixes and enhancements in the previous release, see Access Manager 4.0 SP1 HF1 readme

1 What's New?

Access Manager 4.0.1 HF2 provides the following fixes:

1.1 Software Fixes for the Administration Console

The following issues are fixed in the Administration Console:

1.1.1 Issue with Including Semicolon in a Protected Resource Path

Issue: The Administration Console displays an invalid path error when a semicolon (;) is included in the protected resource path. [`Bug 884452`]

Fix: You can now include a semicolon in the protected resource path.

1.1.2 Timestamps Are Not Written to the Audit Log File

Issue: After upgrading Access Manager version from 3.2 to 4.0, timestamps are not written to the audit log file. [`Bug 889844`]

Fix: To ensure timestamps are written to the audit log file, perform the following steps:

1. Upgrade to the 4.0.1 HF 2 patch. For more information about how to upgrade, see Section 2, "Upgrading to 4.0.1 HF2," on page 5.
2. Traverse to the `/opt/novell/nam/adminconsole` folder.
3. Extract the tar file by using the `tar -xzvf nauditfix.tar` command.
4. Traverse to the nauditfix folder by using the `cd nauditfix` command.

5 Run the script by using `./fix_audit_server.sh` command.

5a Validate the IP address of the Administration Console.

5b Specify the Administration Console credentials to continue installation of the script.

After installation of the script, verify logs placed in `/opt/novell/nam/adminconsole/nauditfix` folder.

1.1.3 Incorrect Web Server Status Displayed

Issue: Status on the dashboard incorrectly displays connected and active status (Green color) even though the Access Gateway server is down. [`Bug 881619`]

Fix: The status of the Web servers are now displayed correctly.

1.1.4 Backup Fails When the Backup File Is Not Stored in the Root Partition

Issue: If the backup location is on another partition than the root partition, `ambkup.sh` does not create the LDIF file and back up fails. [`Bug 897311`]

Fix: The backup process works without errors even if backup location is on another partition.

1.2 Software Fixes for the Identity Server

The following issues are fixed in the Identity Server:

1.2.1 Parameters Passed to Logout URL Are Not Available in logoutSuccess.jsp Page

Issue: The query string parameters (used for special redirect after logout success) passed with logout URL `/nidp/app/logout` are missing. [`Bug 878070`]

Fix: Parameters sent with logout URL are persistent and are available in the `logoutSuccess.jsp` file.

1.2.2 The LDAP Group List Is Not Available in the Administration Console

Issue: While creating an Identity Server role policy with **LDAP Group** as a condition, the LDAP Group list is not available in the **Value** field. [`Bug 876776`]

Fix: You can see the LDAP Group list in the **Value** field.

1.2.3 Cannot Run Post Authentication Methods in Federated Setup that Requires Multiple Prompts for User Input

Issue: In a federated setup, you cannot run post authentication methods that has multiple prompts for user input. [`Bug 856573`]

Fix: You can now have multiple prompts for user input.

1.2.4 Federation Fails if SAML 2.0 Post Response Is Signed

Issue: Federation fails if the SAML 2.0 POST response contains signature whereas the assertion does not contain signature. [`Bug 886777`]

Fix: To fix this issue, nidp config property SAML2_AVOID_SIGN_AND_VALIDATE_ASSERTION_TRUSTEDPROVIDERS is added to the service provider and the identity provider. If response is signed and assertion is not, federation is successful. For more information, see *Avoiding Assertion Signing Validation by Service Provider* in Configuring SAML 2.0 to Sign Messages.

1.3 Software Fixes for the Access Gateway

The following issues are fixed in the Access Gateway:

1.3.1 Issue With NTLM-Enabled Web Server

Issue: NTLM authentication enabled Web server prompts the user to login each time the user accesses its resources. [`Bug 867593`]

Fix: The NTLM authentication enabled Web server does not ask credentials each time a resource is accessed.

1.3.2 Issue With Protected Resources Not Matching When URL Includes Query String

Issue: If you create a protected resource with a wildcard for a specific type of file (/formfill/*.do) and if it does not include query strings, a matching resource accessing that URL is found. If it includes query strings, it resolves to another protected resource. [`Bug 876278`]

Fix: The correct protected resource is now selected even if the requested URL contains query string parameters.

1.3.3 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, the request is sent to the wrong ESP server. The ESP cluster cookie, it contains reference to the first session and due to this the request is sent to the wrong ESP server. This causes a session invalidation error on the browser and you are prompted to login again.[`Bug 879621`]

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

1.3.4 After Upgrading to Access Manager to 4.0.1 HotFix AGLogout Fails with xerces Exception

Issue: After upgrading Access Manager to 4.0.1 HotFix 1, logging out through AGLogout results in a 500 internal error with the following message: [`Bug 891906`]

```
HTTP Status 500 - javax.xml.parsers.FactoryConfigurationError: Provider
org.apache.xerces.jaxp.DocumentBuilderFactoryImpl not found
```

Fix: AGLogout suceeds without any exception.

1.3.5 Issue with OpenSSL TLS Protocol Downgrade Attack (CVE-2014-3511)

Issue: A flaw in the OpenSSL SSL/TLS server code causes the server to negotiate TLS 1.0 instead of higher protocol versions when the ClientHello message is badly fragmented. By modifying the client's TLS records, a man-in-the-middle attack forces you to downgrade to TLS 1.0 even if both the server and the client support a higher protocol version. [`Bug 893336`]

Fix: This vulnerability has been fixed by moving to OpenSSL version 1.0.1i.

1.3.6 Issue in the Administration Console Communication with JCC

Issue: Adding a new secondary IP in the Access Gateway Service results in cancelation of communication with the Administration Console and an error occurs when you select this IP as a **Management IP**. [`Bug 878294`]

Fix: The issue is resolved and no error occurs.

1.3.7 Incomplete Comment Tag Causes the Access Gateway to Terminate

Issue: A protected resource that has a Form Fill login policy with Auto Submit enabled, causes Access Gateway to terminate because of malformed HTML code or an incomplete comment tag in the form. [`Bug 865990`]

Fix: The issue with the malformed HTML code is now fixed.

1.3.8 Web Server Load Balancing Does Not Work

Issue: When multiple back end Web servers exist, the traffic is not evenly balanced among the back end Web servers causing load balancing issues. [`Bug 842496`]

Fix: The load balancing issue is resolved.

1.3.9 Redirect Message to LAGBroker Is Corrupt

Issue: When SSL terminator is enabled, you cannot authenticate as the Access Gateway sends garbled or corrupt redirect message to the LAGBroker. [`Bug 876715`]

Fix: The Access Gateway now sends a valid redirection message to the LAGBroker.

1.3.10 The Access Gateway Does Not Forward Mangled Cookie

Issue: If you enable cookie mangling and then access a public resource, the cookie set by the application is mangled. If the user then tries to access another protected resource on the same application, the redirects cause the mangled cookie to be removed from the Access Gateway. Due to this the Access Gateway does not send the unmangled cookie to the application even though the incoming request from browser includes it. As the Web server sets a new cookie, the Access Gateway expires the old cookie leading to session failure. [`Bug 891291`]

Fix: The Access Gateway does not clear mangled cookies and session continues without errors.

1.3.11 Identity Injection Fails to Inject Authentication Header

Issue: When the Access Gateway sends an authorization header configured in the Identity Injection policy and receives a 401 error, it is because Identity Injection injects invalid credentials. Hence, the Access Gateway does not send authorization header in the next request and impacts the basic authentication header. It does not affect any other custom headers that are injected. [`Bug 892554`]

Fix: The following global advanced option is introduced to ensure that when a browser sends an authentication header, the Access Gateway overwrites it with the authentication header configured in the Identity Injection policy.

`NAGGlobalOptions OverWriteAuthHeaderWithIIData=`*off* [Setting it to off ensures that when the browser sends an authentication header, it is not overwritten with the authentication header configured in the Identity Injection policy]

`NAGGlobalOptions OverWriteAuthHeaderWithIIData=`*on* [Setting it to on ensures that when a browser sends an authentication header, it is overwritten with the authentication header configured in the Identity Injection policy.]

1.3.12 URL Matching Criteria with Query Strings Results in Broken Applications after Upgrading Access Manager to 4.0

Issue: After upgrading Access Manager to 4.0, URL matching criteria with query strings results in breaking the applications that work with Access Gateway Service. [`Bug 891548`]

Fix: The protected resource matching works properly even when query string is present in the URL.

2 Upgrading to 4.0.1 HF2

IMPORTANT: Ensure that you are currently on Access Manager 4.0 Service Pack 1 or 4.0.1 HF1 before upgrading to Access Manager 4.0.1 HF2.

To upgrade to Access Manager 4.0.1 HF2, use the following steps to download the `AM_401_HF2.zip` file that 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_401_HF2.zip` in the search box and download the file.
4. Upgrade by using the procedure described in Upgrading Access Manager 4.0 HF* Using the Patch Process for Linux and Upgrading Access Manager 4.0 HF* Using the Patch Process for Windows in the NetIQ Access Manager 4.0 SP1 Migration and Upgrade Guide.

3 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrade to Access Manager 4.0.1 HF2, verify the version of existing Access Manager installation.

Before Upgrading:

To verify the version numbers before upgrading to 4.0.1 HF2:

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**
2. Verify that the **Version** field displays the following version.

Components	4.0.1	4.0.1 HF1
All Access Manager Components	4.0.1.88	4.0.1.88 + HF1-93

After Upgrading:

To verify the version number after upgrading to 4.0.1 HF2:

1 In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**

2 Verify that the **Version** field displays the following version:

Components	Upgrading from 4.0.1	Upgrading from 4.0.1 HF1
All Access Manager Components	4.0.1.88 + HF2 -107	4.0.1-88 + HF1-93, HF2-107

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.

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.

To download this product, go to Access Manager on the All Products Page (http://www.netiq.com/products).

5 Legal Notice

[Return to Top]