

Access Manager 4.0 Service Pack 1 Hotfix 3 Release Notes

December 2014



Access Manager 4.0 Service Pack 1 Hotfix 3 (4.0.1 HF3) supersedes Access Manager 4.0 Service Pack 1 Hotfix 2.

For the list of software fixes and enhancements in the previous release, see [Access Manager 4.0 SP1 HF2 Release Notes](#)

- ♦ [Section 1, "What's New?," on page 1](#)
- ♦ [Section 2, "Upgrading to 4.0.1 HF3," on page 4](#)
- ♦ [Section 3, "Verifying Version Numbers," on page 5](#)
- ♦ [Section 4, "Known Issues," on page 5](#)
- ♦ [Section 5, "Contact Information," on page 6](#)
- ♦ [Section 6, "Legal Notice," on page 6](#)

IMPORTANT: Installing this patch comprises of the following steps:

1. After you have downloaded and saved the patch file, extract the patch file using the `unzip <patch name>.zip` command, where *<patch filename>* is the name of the patch file, for example, `AM_401_HF3`.
 2. Run the `sh installPatch.sh` command to install the patch and the bundled binaries.
To resolve any errors during installation of the patch, see [TID 7016005](#).
-

1 What's New?

This release includes the following platform updates and fixed issues:

- ♦ [Section 1.1, "Updates for Dependent Components," on page 1](#)
- ♦ [Section 1.2, "Upgrading Dependent Components Manually," on page 2](#)
- ♦ [Section 1.3, "Fixed Issues," on page 3](#)

1.1 Updates for Dependent Components

In this release, the following dependent components are updated to fix the vulnerability issues:

- ♦ eDirectory 8.8 SP8 Patch 4
- ♦ iManager 2.7 SP7 Patch 3
- ♦ Java 1.7.0.72
- ♦ OpenSSL 101j

IMPORTANT: In this release of Access Manager, you must manually upgrade, eDirectory, iManager and Java. For more information about upgrading to the version supported by this Hotfix, see [Section 1.2, “Upgrading Dependent Components Manually,” on page 2](#)

1.2 Upgrading Dependent Components Manually

Perform the following steps to upgrade eDirectory, iManager and Java manually:

- ♦ [Section 1.2.1, “Upgrading eDirectory Manually,” on page 2](#)
- ♦ [Section 1.2.2, “Upgrading iManager Manually,” on page 2](#)
- ♦ [Section 1.2.3, “Upgrading Java Manually,” on page 2](#)

1.2.1 Upgrading eDirectory Manually

Linux:

- 1 Traverse to `/opt/novell/nam/update/HF3/` folder.
- 2 Execute `patchEdir.sh` script.

Windows:

- 1 Traverse to `C:/Program Files (x86)/Novell/update/HF3` folder.
- 2 Open the `edir_update_readme.txt` file and follow the instructions to manually update eDirectory.

1.2.2 Upgrading iManager Manually

Linux:

- 1 Traverse to `/opt/novell/nam/update/HF3/` folder.
- 2 Execute `patchiMan.sh` script.

Windows:

- 1 Traverse to `C:/Program Files (x86)/Novell/update/HF3` folder.
- 2 Open the `iman_update_readme.txt` file and follow the instructions to manually update eDirectory.

1.2.3 Upgrading Java Manually

On Linux, the Java version is 1.7.0.72. No manual steps are required to update the version of Java.

Windows:

- 1 Traverse to `C:/Program Files (x86)/Novell/update/HF3` folder
- 2 Open the `jre_update_readme.txt` file and follow the instructions to manually update Java.

1.3 Fixed Issues

This release includes software fixes in the following components:

- [Section 1.3.1, “Administration Console,” on page 3](#)
- [Section 1.3.2, “Identity Server,” on page 3](#)
- [Section 1.3.3, “Access Gateway,” on page 4](#)

1.3.1 Administration Console

The following issues are fixed in the Administration Console:

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 Cross-Site Scripting Issue Injects Script to the Auditing Page

Issue: The Auditing page is vulnerable to cross-site scripting attacks. The affected URL is:

```
https://<host>:8443/roma/system/cntl?handler=dispatcher&command=auditsave&&secureLoggingServersA=''){};alert('xss');function+x(){if('&port=1289
```

Fix: This the issue is resolved by sanitizing the affected URL. [Bug 904689][CVE-2014-5216]

1.3.1.3 JSP Pages Display Sensitive Information to an Authenticated Administrator

Issue: An administrator can view internal credential details by using specific `.jsp` pages. The affected URLs are:

- `https://<host>:8443/roma/jsp/volsc/monitoring/dev_services.jsp`
- `https://<host>:8443/roma/jsp/debug/debug.jsp`

Fix: This issue is resolved by decrypting the credential information in the affected URLs and the details are not displayed to the administrator. [Bug 904677][CVE-2014-5215]

1.3.2 Identity Server

The following issues are fixed in the Identity Server:

1.3.2.1 Cross-Site Scripting Vulnerability Issue in the JSP Page

Issue: Multiple cross-site scripting vulnerabilities exist in the `x509err.jsp` page of the following URL:

```
https://<host>/nidp/jsp/x509err.jsp?error=%3Cscript%3Ealert%28%27xss%27%29%3C/script%3E
```

Fix: This issue is resolved by sanitizing the `x509err.jsp` page in the affected URL. [Bug 904675][CVE-2014-5216]

1.3.2.2 Cross-Site Scripting Vulnerability Issue With the WS-Federation Authentication Process

Issue: Cross-site scripting vulnerability affects the WS-Federation authentication process in the following URL:

```
cbcxt=&popupui=&vv=&username=fumail01%40basf.com&mkt=&lc=&wfresh=&wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline&wctx=ernw"><script>alert
```

Fix: This issue is resolved by replacing the `.jsp` file in the affected URL. [Bug 903062]

1.3.2.3 JCC Port 1443 Accepts SSLv3 Requests

Issue: In the Identity Server, the JCC port 1443 is affected by POODLE vulnerability as it accepts SSLv3 requests. (CVE-2014-3566)

Fix: This release fixes the POODLE vulnerability by disabling SSLv3 requests on the JCC port 1443. [Bug 903876]

1.3.3 Access Gateway

The following issue is fixed in the Access Gateway:

1.3.3.1 JCC Port 1443 Accepts SSLV3 Requests

Issue: In the Access Gateway, the JCC port 1443 is affected by Poodle vulnerability as it accepts SSLv3 requests. (CVE-2014-3566)

Fix: This release fixes the Poodle vulnerability by disabling SSLv3 requests on the JCC port 1443. [Bug 903876]

2 Upgrading to 4.0.1 HF3

IMPORTANT: Ensure that you are currently on Access Manager 4.0 Service Pack 1, 4.0.1 HF1, or 4.0.1 HF2 before upgrading to Access Manager 4.0.1 HF3.

To upgrade to Access Manager 4.0.1 HF3, perform the below steps:

- 1 Go to [NetIQ Downloads Page \(https://dl.netiq.com/index.jsp\)](https://dl.netiq.com/index.jsp).
- 2 Under **Patches**, click **Search Patches**.
- 3 Specify `AM_401_HF3.zip` in the search box and download the file.
- 4 Save the hotfix file to the server running Access Manager. If you have multiple servers in your set up, ensure that you copy this `.zip` file to all the servers.
- 5 Extract the patch file using the `unzip <patch name>.zip` command, where `<patch filename>` is the name of the patch file, for example, `AM_401_HF3`. For more information about the upgrade process, see [Upgrading Access Manager 4.0 HF* Using the Patch Process for Linux](#) or [Upgrading Access Manager 4.0 HF* Using the Patch Process for Windows](#) in the [NetIQ Access Manager 4.0 SP1 Migration and Upgrade Guide](#).
- 6 Run the `sh installPatch.sh` command. This command installs the patch and the bundled binaries.

3 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrade to Access Manager 4.0.1 HF3, verify the version of existing Access Manager installation.

Before Upgrading:

Perform the below steps:

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

After Upgrading:

Perform the below steps:

- 1 In the Administration Console, click **Access Manager > Auditing > Troubleshooting > Version**.
- 2 After upgrade, the following **Version** field must be displayed:

Components	Upgrading from 4.0.1	Upgrading from 4.0.1 HF1	Upgrading from 4.0.1 HF2
All Access Manager Components	4.0.1.88 + HF3 - 132	4.0.1-88 + HF1-93, HF3-132	4.0.1-88 + HF1-93, HF2-107, HF3-132

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.

- ♦ [Section 4.1, “Cross-Site Request Forgery Script Allows Password of an Authentication Administrator to be Changed,” on page 5](#)
- ♦ [Section 4.2, “Cross-Site Scripting Vulnerability Allows Attacks on URLs,” on page 6](#)

4.1 Cross-Site Request Forgery Script Allows Password of an Authentication Administrator to be Changed

Issue: An attacker can issue a GET request and change the password of an authentication administrator. [CVE-2014-5217]

Workaround: This issue will be fixed in the next release of NetIQ Access Manager. For more information, see [TID 7015997](#)

4.2 Cross-Site Scripting Vulnerability Allows Attacks on URLs

Issue: Cross-Site scripting vulnerability affects the following URLs: [CVE-2014-5216]

- `https://<host>:8443/nps/servlet/webacc?taskId=dev.Empty&merge=dm.GenericTask&location=/roma/jsp/admin/view/main.jss'%2balert+('xss')%2b'`
- `https://<host>:8443/nps/servlet/webacc?taskId=debug.DumpAll&xss=%3Cimg%20src=%22/404%22%20onerror=%22alert+%28%27xss%27%29%22%3E`

Workaround: This issue will be fixed in the next release of NetIQ Access Manager. For more information, see [TID 7015994](#)

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](#).

You can post feedback in the [Access Manager forum on Qmunity \(http://community.netiq.com/forums/30.aspx\)](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 \(http://www.netiq.com/products\)](http://www.netiq.com/products).

6 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 interoperates 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.

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.

© 2014 NetIQ Corporation. All Rights Reserved.

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