

Access Manager Appliance 4.0 Service Pack 1 Hotfix 1 Readme

June 2014



The Access Manager Appliance Service Pack 1 Hotfix 1 (4.0.1 HF1) includes fixes for some security vulnerabilities listed in [Section 1.1, "Fixed Issues," on page 1](#).

For the list of software fixes and enhancements in the previous release, see [Access Manager Appliance 4.0 SP1 readme](#).

- ♦ [Section 1, "What's New?," on page 1](#)
- ♦ [Section 2, "Upgrading to 4.0.1 HF1," on page 2](#)
- ♦ [Section 3, "Verifying Version Numbers," on page 2](#)
- ♦ [Section 4, "Known Issue," on page 2](#)
- ♦ [Section 5, "Contact Information," on page 3](#)
- ♦ [Section 6, "Legal Notice," on page 3](#)

1 What's New?

Access Manager 4.0.1 HF1 fixes vulnerability issues with OpenSSL and issues with Apache Tomcat 7.0 in this release.

1.1 Fixed Issues

The following sections outline the issues resolved in this release:

- ♦ [Section 1.1.1, "Vulnerability Issue with OpenSSL," on page 1](#)
- ♦ [Section 1.1.2, "Issues with Apache Tomcat 7.0," on page 1](#)

1.1.1 Vulnerability Issue with OpenSSL

CVE-2014-0224: OpenSSL is vulnerable to a man-in-the-middle (MITM) attack. The attack occurs on vulnerable SSL/TLS clients and servers. OpenSSL clients are vulnerable in all versions of OpenSSL and servers are known to be vulnerable only in OpenSSL versions before 0.9.8za, from version 1.0.0 until version 1.0.0m, and from version 1.0.1 until version 1.0.1h as mentioned in the [CVE-2014-0224](#). For more information about this issue and the resolution, see [TID 705158](#).

1.1.2 Issues with Apache Tomcat 7.0

CVE-2013-4322: Apache Tomcat from version 7.0 until version 7.0.50 do not handle large amount of chunked data or unlimited whitespace characters in a HTTP header. For more information about this issue, see [CVE-2013-4322](#).

CVE-2013-4286: Apache Tomcat from version 7.0 until version 7.0.47 does not handle certain inconsistent HTTP request headers when HTTP or AJP connectors are used. For more information about this issue, see [CVE-2013-4286](#).

The above vulnerabilities affect the following Access Manager components, which are installed with Tomcat:

- ♦ Administration Console
- ♦ Identity Server
- ♦ Embedded Service Provider running in the Access Gateway machine

4.0.1 HF1 updates these components with the latest Tomcat version 7.0.54. For more information about how to upgrade, see [Upgrading to 4.0.1 HF1](#).

2 Upgrading to 4.0.1 HF1

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

To upgrade Access Manager Appliance 4.0.1 HF1, download the `AM_401_HF1.zip` file that contains the Access Manager Appliance Patch Tool and the patch file by using the following steps:

- 1 Go to [NetIQ downloads page](#).
- 2 Under **Patches**, click **Search Patches**.
- 3 Specify `AM_401_HF1.zip` in the search box and download the Hotfix file.
- 4 Upgrade by using the procedure described in [Upgrading Access Manager Appliance 4.0 HF* Using the Patch Process](#) in the [NetIQ Access Manager Appliance 4.0 SP1 Installation Guide](#).

3 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrade to Access Manager 4.0.1 HF1, verify the existing Access Manager version.

Before and after 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.

Before Upgrading: Before upgrading to Access Manager 4.0.1 HF1, go to **Access Manager > Auditing > Troubleshooting > Version** and verify that the version number of the component is indicated as **4.0.1.88** in the **Version** field.

After Upgrading: After upgrading to Access Manager 4.0.1 HF1, go to **Access Manager > Auditing > Troubleshooting > Version** and verify that the version number of the component is indicated as **4.0.1.88 + HF1-93** in the **Version** field.

4 Known Issue

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](#).

4.1 LDAP Group List is not Available

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)

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/>.

[\[Return to Top\]](#)