

# NetIQ Access Manager 3.2 IR1 Readme

July 2012



This Readme describes the NetIQ Access Manager 3.2 IR1 release.

- ◆ [Section 1, "Upgrading to Access Manager 3.2 IR1,"](#) on page 1
- ◆ [Section 2, "Issues Fixed,"](#) on page 3
- ◆ [Section 3, "Known Issues,"](#) on page 4
- ◆ [Section 4, "Documentation,"](#) on page 6
- ◆ [Section 5, "Legal Notices,"](#) on page 6

For more information about the new features and enhancements added in this release, see ["What's New in Access Manager 3.2"](#) in the *NetIQ Access Manager 3.2 Installation Guide*.

## 1 Upgrading to Access Manager 3.2 IR1

To upgrade to 3.2 IR1, ensure that you are on Access Manager version 3.2. If you are on 3.1 SP4 you must move to version 3.2 before upgrading to 3.2 IR1.

The following files are available for 3.2 IR1:

Filename	Description
<code>AM_32_IR1_AccessManagerService_Linux64.tar.gz</code>	Contains the Linux Identity Server, the Linux Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN Server.
<code>AM_32_IR1_AccessManagerService_Win64.exe</code>	Contains the Windows Identity Server and Windows Administration Console for Windows 2008.
<code>AM_32_IR1_AccessGatewayAppliance_Linux_SLES11_64.tar.gz</code>	Contains the upgrade RPMs for SLES 11SP1 or a higher version of the Access Gateway Appliance and the traditional SSL VPN server.
<code>AM_32_IR1_AccessGatewayService_Win64.exe</code>	Contains the Access Gateway Service for Windows 2008.
<code>AM_32_IR1_AccessGatewayService_Linux_64.tar.gz</code>	Contains the Access Gateway Service for SLES 11 SP1 or a higher version and RHEL 6.2 platforms.

**NOTE:** In this release the J2EE agents were not updated. The J2EE agents in version 3.2 are compatible with 3.2 IR1 version.

For upgrade and installation information:

- ♦ [“Upgrade Instructions” on page 2](#)
- ♦ [“Installation Instructions” on page 2](#)
- ♦ [“Verifying Version Numbers Before Upgrading” on page 2](#)
- ♦ [“Verifying Version Numbers After Upgrading” on page 2](#)

## 1.1 Upgrade Instructions

For instructions on upgrading Access Manager from 3.2 to 3.2 IR1, see [Upgrading from Access Manager 3.2 to 3.2 IR1 or a higher version](#).

## 1.2 Installation Instructions

For installation instructions of Access Manager components, see the [NetIQ Access Manager 3.2 Installation Guide](#).

## 1.3 Verifying Version Numbers Before Upgrading

Before upgrading to Access Manager 3.2 IR1, ensure that you are on version 3.2.

To determine the existing version:

- 1 In the Administration Console, click *Access Manager > Auditing > Troubleshooting > Version*.
- 2 Examine the value in the *Version* field.

Component	Version
Administration Console	3.2.0.327
Identity Server	3.2.0.327
Access Gateway Appliance	3.2.0.327
Access Gateway Services	3.2.0.327
SSL VPN	3.2.0.327

## 1.4 Verifying Version Numbers After Upgrading

After upgrading all the Access Manager components, verify their version as follows:

- 1 In the Administration Console, click *Access Manager > Auditing > Troubleshooting > Version*.
- 2 Examine the value in the *Version* field to verify that the component has been upgraded to 3.2 IR1.

Component	Version
Administration Console	3.2.0.370
Identity Server	3.2.0.370
Access Gateway Appliance	3.2.0.370
Access Gateway Services	3.2.0.370

---

Component	Version
SSL VPN	3.2.0.370

---

**NOTE:** The J2EE agent versions are not updated for 3.2 IR1 release. Hence, the version of these agents in this release is 3.2.0.327.

---

## 2 Issues Fixed

Access Manager 3.2. IR1 release provides fixes for issues in the following components:

- ♦ [Section 2.1, “Administration Console,” on page 3](#)
- ♦ [Section 2.2, “Identity Server,” on page 3](#)
- ♦ [Section 2.3, “Access Gateway Appliance/Service,” on page 3](#)

### 2.1 Administration Console

- ♦ Fixed an issue with the Administration Console performance, which was due to the large number of LDAP connections. Now, the required LDAP connections are optimized. (Bug ID: 761356)
- ♦ Fixed an issue where the Administration Console did not accept a password with special characters. It now accepts special characters in the admin password except colon (:) and double quotes (“). (Bug ID: 759355)
- ♦ Fixed an issue where the access log was enabled by default in the Windows Administration Console and Identity Server. (Bug ID: 754725)
- ♦ Fixed an issue where certificate related errors occurred when protected resources were accessed. (Bug ID: 758307)

### 2.2 Identity Server

- ♦ Fixed an issue where the Identity Server installation does not allow installation to proceed if the password for the Administration Console contains colon (:) and double quotes (“). (Bug ID: 754233)
- ♦ Fixed an issue where the user’s unique identifier (GUID) could not be retrieved from the LDAP user store for sending in the attribute set to the service providers. Now, the GUID can be retrieved and sent. (Bug ID: 740232)
- ♦ Fixed an issue where the SAML 2.0 response was generated without RelayState. (Bug ID: 761181)
- ♦ Fixed an issue where the Identity Server XML log file got created in `/opt/novell/nam/idp/webapps/nidp/WEB-INF/logs/`, resulting in less space in the `/opt` partition than the `/var` partition. (Bug ID: 757552)

### 2.3 Access Gateway Appliance/Service

- ♦ Fixed an intermittent issue where rewriter did not display the correct page. (Bug ID: 756636)
- ♦ Fixed an issue where accessing the protected page was not redirected to the correct page. (Bug ID: 766771)

- ◆ Fixed an issue where logging out did not happen completely in certain cluster scenarios and the Access Manager grants access to secure sites without asking for credentials. (Bug ID: 758755)
- ◆ Fixed an issue where redirecting from HTTP to HTTPS resulted in browser redirection loop. This error occurred when the *Force Secure Cookie* option was enabled. (Bug ID: 758041)
- ◆ Fixed an issue where the Via HTTP header is now sent to the backend server. (Bug ID: 757841)
- ◆ Fixed an issue where the policy configuration requests from the Access Gateway Appliance to the ESP were not cached, thus overloading the ESP. (Bug ID: 762583).
- ◆ Fixed an issue where a protected resource link accessed from a Microsoft Excel sheet resulted in the `Unable to authenticate 404-esp` error. (Bug ID: 768978)
- ◆ Fixed an issue where Apache did not cache a file if the file size exceeded 1 MB. (Bug ID: 758173)
- ◆ Fixed an issue where the 3.1 SP4 Access Gateway and the Access Gateway Appliance had different logging formats for both Common and Extended logs.
- ◆ Fixed an issue when the values were different in `/opt/novell/nam/mag/conf/server.xml` and `/etc/opt/novell/apache2/conf/httpd.conf` files resulted in XML document structures must start and end within the same entity error. (Bug ID: 758767)
- ◆ Fixed an issue with the Identity Injection policies when the resources were protected by the Non-Redirected Login contract in the Access Gateway. (Bug ID: 759509)
- ◆ Fixed an issue where the incorrect logging format caused log analyzers like Webtrend to fail analyzing the extended logs. (Bug ID: 758313)
- ◆ Fixed an issue where the Tomcat version was displayed as part of error pages. (Bug ID: 761589)
- ◆ (Only Access Gateway Service) Fixed an issue with looping when only the `NAGHostOptionsmangleCookies` advanced option was set. This issue was seen in a mixed cluster environment of 3.1 SP4 and 3.2 Access Gateway Services. (Bug ID: 757511)
- ◆ (Only Access Gateway Service) Fixed an issue where migrating from 3.1 SP4 IR1 to 3.2 resulted in the Access Gateway Service failure. (Bug ID: 762365)
- ◆ (Only Access Gateway Service) Fixed an issue where the Access Gateway Service configuration goes into a pending state after installation on the SLES 11 SP2 platform. (Bug ID: 762349)

### 3 Known Issues

The following table lists the known issues and appropriate workaround in Access Manager 3.2 IR1:

Issue	Workaround
The Identity Server delegated administrators do not have view or modify rights after migrating from the 3.1 SP4 Identity Server to the 3.2 Identity Server. (Bug ID: 739475)	<ol style="list-style-type: none"> <li>1. Remove the existing Identity Server delegated administrators before migration.</li> <li>2. Add the delegated administrators back after migration.</li> </ol>
Downloading <code>stdout.logs</code> through the Administration Console on Windows Server 2008 fails. (Bug ID: 746889)	<ol style="list-style-type: none"> <li>1. Log into the Access Gateway on Windows.</li> <li>2. Navigate to <code>C:\Program Files\Novell\Tomcat\logs\stdout.log</code> and access the logs.</li> </ol>
If the data posted to the Access Gateway before authentication exceeds 50 KB, the data will be lost. (Bug ID: 677375)	None.

Issue	Workaround
The Alert feature with Access Gateway Appliance works only for configuration changes and when the service provider is restarted. (Bug ID: 752557)	None.
Changing the IP address of the Access Gateway Management interface fails. (Bug ID: 752788)	<ol style="list-style-type: none"> <li>1. Remove the Access Gateway Appliance from the cluster.</li> <li>2. Change the IP address of the Access Gateway Appliance from YaS.T</li> <li>3. Import the Access Gateway Appliance with the current configuration.</li> </ol>
The SSL VPN client works in Enterprise mode, but shuts down Windows Explorer using ActiveX. If you restore/downgrade the Windows XP client to Windows XP SP3, the SSL VPN client works in Kiosk mode.	Use Firefox with Java.
If the IP address and DNS servers are configured statically on MAC Leopard and the SSL VPN connection is established, the DNS resolution fails to use the DNS server's IP address pushed from the SSL VPN server.	None.
When you install the Administration Console and the Identity Server on a Windows Server 2008, you cannot completely uninstall the components. The uninstall program does not respond before it cleans all the files and the registry entries.	<p>To uninstall all Access Manager files and registry entries:</p> <ol style="list-style-type: none"> <li>1. Run the uninstall program from the <i>Control Panel &gt; Add or Remove Programs</i> &gt; select Access Manager Server.</li> </ol> <p>This program removes most of the files.</p> <ol style="list-style-type: none"> <li>2. If the program hangs, exit the program.</li> <li>3. Delete the following directories: <ul style="list-style-type: none"> <li>◆ C:\Novell</li> <li>◆ C:\Program Files (x86)\Novell</li> <li>◆ C:\Program Files\Novell\Nsure Audit</li> </ul> </li> <li>4. Run <code>regedit</code> and remove the following entries: <ul style="list-style-type: none"> <li>◆ \HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\AccessManager</li> <li>◆ \HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\NDS</li> <li>◆ \HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\nici_x64</li> </ul> </li> <li>5. Restart the machine.</li> </ol>
When the DNS server is not reachable and ESP debug logging is enabled, each authentication request will be delayed by 20 to 30 seconds.	Add an <code>/etc/hosts</code> entry for authentication domain in the Access Gateway Appliance.

Issue	Workaround
When the <i>Remove Path on Fill</i> option is enabled in the Path-Based Multi-Homing page, you may have some issues. For example, issues with the help links and <i>Cancel</i> button. (Bug ID: 700552)	None.
The Administration Console password does not accept special characters colon (:) and double quotes ("). (Bug ID: 763688)	None.
When Kerberos identifies an expired user, it does not redirect to the password management servlet resulting in a HTTP Status 500 error. (Bug ID: 765042)	None.
Error connecting to data store and the response of Access Gateway pages delayed. (Bug ID: 765648)	Copy the <code>jdk1.6.0_26/jre/lib/jsse.jar</code> to <code>jdk1.6.0_30/jre/lib</code> .
Rewrite does not work if the URLs are encoded. For example, if the page contains <code>http%3a%2f%2fYourInternalDnsName%3aYourInternalListeningPort</code> , rewrite does not work. This occurs while accessing the PeopleSoft and the SharePoint servers. (Bug ID: 767585)	None.
If a request to the Access Gateway Appliance from a browser has a query string that matches the data injected by the Identity Injection policy, it corrupts the existing query parameter values. (Bug ID: 764475)	None.

## 4 Documentation

The following sources provide information about Access Manager:

- [Documentation Web Site \(http://www.netiq.com/documentation/novellaccessmanager32/index.html\)](http://www.netiq.com/documentation/novellaccessmanager32/index.html).
- [Access Manager Support \(http://www.novell.com/support/microsites/microsite.do\)](http://www.novell.com/support/microsites/microsite.do). For TIDs and Cool Solutions articles, select *Access Manager* for the *Product* and *Articles / Tips* in the *Advanced Search* options.
- [Novell Access Manager Product Site \(http://www.novell.com/products/accessmanager/\)](http://www.novell.com/products/accessmanager/).

## 5 Legal Notices

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.

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.

**© 2012 NetIQ Corporation and its affiliates. All Rights Reserved.**

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.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

Access Manager, ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Cloud Manager, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PlateSpin, PlateSpin Recon, Privileged User Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its affiliates in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

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.