

Novell Access Manager 3.1 SP4 IR1 Readme

May 2012

Novell®

This Readme describes the Novell Access Manager 3.1 SP4 IR1 release.

- ♦ Section 1, "Documentation," on page 1
- ♦ Section 2, "Downloading Access Manager 3.1 SP4 IR1," on page 1
- ♦ Section 3, "Bugs Fixed in Access Manager 3.1 SP4 IR1," on page 5
- ♦ Section 4, "Known Issues in Access Manager 3.1 SP4," on page 6
- ♦ Section 5, "Legal Notices," on page 10

1 Documentation

The following sources provide information about Novell Access Manager:

- ♦ Documentation Web Site (<http://www.netiq.com/documentation/novellaccessmanager31/index.html>).
- ♦ Access Manager Support (<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 (<https://www.netiq.com/products/access-manager/>).

2 Downloading Access Manager 3.1 SP4 IR1

- ♦ Section 2.1, "Downloading the Product," on page 1
- ♦ Section 2.2, "Installing the High-Bandwidth SSL VPN Server," on page 4

2.1 Downloading the Product

Log in to the [Novell Customer Center](http://www.novell.com/center) (<http://www.novell.com/center>) and follow the link that allows you to download the software.

The following files are available:

Filename	Description
AM_31_SP4_IR1_IdentityServer_Linux32.tar.gz	Contains the Linux Identity Server, the Linux Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN.
AM_31_SP4_IR1_IdentityServer_Win32.exe	Contains the Windows Identity Server and Windows Administration Console for Window 2003.

Filename	Description
AM_31_SP4_IR1_IdentityServer_Win64.exe	Contains the Windows Identity Server and Windows Administration Console for Windows 2008.
AM_31_SP4_IR1_AccessGatewayAppliance_Linux_SLES11.tar.gz	Contains the upgrade RPMs for SLES 11 version of the Access Gateway Appliance and the Traditional SSL VPN.
AM_31_SP4_IR1_AccessGatewayAppliance_Linux_SLES9.tar.gz	Contains the upgrade RPMs for SLES 9 version of the Access Gateway Appliance and the Traditional SSL VPN.
AM_31_SP4_IR1_AccessGatewayService_Win64.exe	Contains the Access Gateway Service for Windows Server 2008 R2 with a 64-bit operating system.
AM_31_SP4_IR1_AccessGatewayService_Linux64.bin	Contains the Access Gateway Service for SLES 11 with a 64-bit operating system.
AM_31_SP4_IR1_ApplicationServerAgents_AIX.bin	Contains the Agents service for the AIX platform.
AM_31_SP4_IR1_ApplicationServerAgents_Linux.bin	Contains the Agents service for the Linux platform.
AM_31_SP4_IR1_ApplicationServerAgents_Solaris.bin	Contains the Agents service for the Solaris platform.
AM_31_SP4_IR1_ApplicationServerAgents_Windows.exe	Contains the Agents service for the Windows platform.

For upgrade and installation information:

- ♦ [Section 2.1.1, “Upgrade Instructions,” on page 2](#)
- ♦ [Section 2.1.2, “Installation Instructions,” on page 3](#)
- ♦ [Section 2.1.3, “Verifying That You Are on 3.1 SP3 IR2,” on page 3](#)
- ♦ [Section 2.1.4, “Verifying That You Are on 3.1 SP4,” on page 4](#)
- ♦ [Section 2.1.5, “Verifying the Version Numbers After Upgrading to 3.1 SP4 IR1,” on page 4](#)

2.1.1 Upgrade Instructions

You can upgrade to Access Manager 3.1 SP4 IR1 release either from 3.1 SP3 IR2 or 3.1 SP4.

Table 1 Supported Upgrade Paths for 3.1 SP4 IR1

Source	Target
3.1 SP3 IR 2	3.1 SP4 IR1
3.1 SP4	3.1 SP4 IR1

2.1.1.1 Upgrading When the Source Is 3.1 SP3 IR2

Before you upgrade to 3.1 SP4 IR1, it is important to verify the current version of Access Manager. To verify that your components are running 3.1 SP3 IR2, see [“Verifying That You Are on 3.1 SP3 IR2” on page 3](#)

For instructions on upgrading from 3.1 SP3 IR2, see [Upgrading Access Manager Components \(https://www.netiq.com/documentation/novellaccessmanager313/installation/?page=/documentation/novellaccessmanager313/installation/data/bookinfo.html#bookinfo\)](https://www.netiq.com/documentation/novellaccessmanager313/installation/?page=/documentation/novellaccessmanager313/installation/data/bookinfo.html#bookinfo)

2.1.1.2 Upgrading When the Source Is 3.1 SP4

Before you upgrade to 3.1 SP4 IR1, it is important to verify the current version of Access Manager. To verify that your components are running 3.1 SP4, see [“Verifying That You Are on 3.1 SP4” on page 4](#)

For instructions on upgrading from 3.1 SP4, see [Upgrading Access Manager Components \(https://www.netiq.com/documentation/novellaccessmanager31/installation/data/bg5gcwy.html\)](https://www.netiq.com/documentation/novellaccessmanager31/installation/data/bg5gcwy.html)

2.1.2 Installation Instructions

For the Access Manager Administration Console, the Identity Server, the Linux Access Gateway Appliance, the Access Gateway Service, and the SSL VPN installation instructions, see the [Novell Access Manager 3.1 SP4 Installation Guide](#).

2.1.3 Verifying That You Are on 3.1 SP3 IR2

To confirm that you are on Access Manager version 3.1 SP3 IR2, do the following.

- 1 In the Administration Console, click *Access Manager > Auditing > Troubleshooting > Version*.
- 2 Examine the value in the *Version* field to verify that the component version is 3.1 SP3 IR2.

Component	Version
Administration Console	3.1.3.292
Identity Server	3.1.3.292
Linux Access Gateway	3.1.3.292
Access Gateway Services	3.1.3.292
SSL VPN	3.1.3.292

2.1.4 Verifying That You Are on 3.1 SP4

To confirm that you are on Access Manager version 3.1 SP4, do the following.

- 1 In the Administration Console, click *Access Manager > Auditing > Troubleshooting > Version*.
- 2 Examine the value in the *Version* field to verify that the component version is 3.1 SP4.

Component	Version
Administration Console	3.1.4.27
Identity Server	3.1.4.27
Linux Access Gateway	3.1.4.27
Access Gateway Services	3.1.4.27
SSL VPN	3.1.4.27

2.1.5 Verifying the Version Numbers After Upgrading to 3.1 SP4 IR1

When you have finished upgrading your Access Manager components to 3.1 SP4 IR1, verify that they have all been upgraded.

- 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 3.1 SP4 IR1.

Component	Version
Administration Console	3.1.4.57
Identity Server	3.1.4.57
Linux Access Gateway	3.1.4.57
Access Gateway Services	3.1.4.57
SSL VPN	3.1.4.57

2.2 Installing the High-Bandwidth SSL VPN Server

The key for the high-bandwidth SSL VPN server does not ship with the product because of export laws and restrictions. The high-bandwidth version does not have the connection and performance restrictions that are part of the version that ships with the product. Your regular Novell sales channel can determine if the export law allows you to order the high-bandwidth version at no extra cost.

After you have obtained authorization for the high-bandwidth version, log in to the [Novell Customer Center](http://www.novell.com/center) (<http://www.novell.com/center>) and follow the link that allows you to download the high-bandwidth key.

3 Bugs Fixed in Access Manager 3.1 SP4 IR1

The following bugs are fixed between 3.1 SP4 and 3.1 SP4 IR1 releases:

- ♦ [Section 3.1, “Administration Console,” on page 5](#)
- ♦ [Section 3.2, “Linux Access Gateway Appliance,” on page 5](#)
- ♦ [Section 3.3, “Access Gateway Service,” on page 5](#)
- ♦ [Section 3.4, “Identity Server,” on page 5](#)

3.1 Administration Console

- ♦ Fixed an issue where running the `install.sh` script on a 64-bit platform displays an error. The error message states to install the Audit Server on a separate server.

3.2 Linux Access Gateway Appliance

- ♦ Fixed an issue where carriage returns and line feeds in a URL generated by a custom web application were not supported.
- ♦ Fixed an issue where the Auto-submit functionality stops working with the touch files `/var/novell/.enableInPlaceSilentFill`, and `/var/novell/.enableInPlaceSilentFillNew`.
- ♦ Fixed an issue that caused random process restarts while rewriting extended characters in a web page.
- ♦ Fixed a potential cross-site scripting issue with the Linux Access Gateway redirects from HTTP to HTTPS where an HREF element was included in the returned page.
- ♦ Fixed an issue where downloading files larger than 1.5 GB in size caused the proxy to crash.
- ♦ Fixed an issue where the `ics_dyn` process showed high CPU utilization.
- ♦ Fixed a proxy crash when a protected resource which had the Form-Fill policy enabled, used wild cards in the URL.
- ♦ Fixed an issue with re-writing of the Referer HTTP header after an upgrade from version 3.1 SP2 to version 3.1 SP3.

3.3 Access Gateway Service

- ♦ Fixed an issue with service selection in path based multihoming when multiple slashes (/) were present in the service configuration.
- ♦ Fixed an issue when disabling the *Allow Pages to be Cached by the Browser* option led to problems in accessing the applications.
- ♦ Fixed an issue with session persistence in the backend servers.
- ♦ Fixed the TCP time out issue in tunneling under heavy load.
- ♦ Fixed an issue to display the correct error codes in the browser for authentication failures.

3.4 Identity Server

- ♦ Fixed an issue with the custom LDAP user store plug-in while upgrading from version 3.1 SP1 to version 3.1 SP2.
- ♦ Fixed an issue to display the correct message when the user password expires.

- ♦ Fixed an issue where the non-localized User-Agent did not go back to the default language.
- ♦ Fixed an issue to display the LogoutSuccess page when you access AGLogout with a third-party SAML 2.0 service provider (SAML 2.0 SP). SAML 2.0 SP supports only front channel logout.

4 Known Issues in Access Manager 3.1 SP4

- ♦ Section 4.1, “The Access Gateway Service Does Not Support Unknown HTTP Methods,” on page 6
- ♦ Section 4.2, “On Access Gateway Service Extended Logging Cannot be Configured for Path-Based Proxies,” on page 7
- ♦ Section 4.3, “Role Policies for LDAP Connections Go to One Replica,” on page 7
- ♦ Section 4.4, “SAML 2.0 Response Misses Few Attributes in the Assertion,” on page 7
- ♦ Section 4.5, “Access Gateway List Page Prompts to Update All,” on page 7
- ♦ Section 4.6, “Custom Logout Pages on the Identity Server are not Executed,” on page 7
- ♦ Section 4.7, “LDAP User Attribute Query Uses a Wrong Directory When the passwordFetch Class Is Enabled,” on page 7
- ♦ Section 4.8, “Installing Access Manager 3.1 SP4 or 3.1 SP4 IR1 on a Windows 2008 Server Results in File Not Found Error,” on page 8
- ♦ Section 4.9, “Access Gateway Service on Linux Logs An Error Stating Server Reached Maximum Client Setting,” on page 8
- ♦ Section 4.10, “Stopping the naudit Service Subsequently Stops JCC and Tomcat Services,” on page 8
- ♦ Section 4.11, “Authentication Error If the Overwrite Real User or Overwrite Temporary User Option Is Enabled,” on page 8
- ♦ Section 4.12, “Sometimes SSL VPN Causes a Windows Explorer Crash in Kiosk Mode,” on page 9
- ♦ Section 4.13, “DNS Resolution by Using DNS Servers Pushed from SSL VPN fails on Mac Leopard,” on page 9
- ♦ Section 4.14, “On Windows Server 2008, You Cannot Uninstall the Administration Console,” on page 9
- ♦ Section 4.15, “Error while Uploading Large Files to an IIS 7.x Backend Web Server through the Linux Access Gateway Appliance,” on page 9
- ♦ Section 4.16, “OR Condition Rules Are Not Getting Updated Second Time,” on page 9
- ♦ Section 4.17, “The SP Brokering Functionality Does Not Work with Shibboleth Identity Provider as the Origin Identity Provider,” on page 10
- ♦ Section 4.18, “Service Unavailability Caused by a SLES 11 Issue,” on page 10

4.1 The Access Gateway Service Does Not Support Unknown HTTP Methods

On the Linux Access Gateway Appliance, the support for unknown HTTP methods is provided with help of the `/var/novell/.AllowUnknownHTTPMethods` touch file.

For more information on touch files, see [Using Touch Files \(https://www.netiq.com/documentation/novellaccessmanager31/accessgatewayhelp/data/bbuxw83.html#bn8m606\)](https://www.netiq.com/documentation/novellaccessmanager31/accessgatewayhelp/data/bbuxw83.html#bn8m606)

4.2 On Access Gateway Service Extended Logging Cannot be Configured for Path-Based Proxies

The Linux Access Gateway Appliance supports extended logging. The Access Gateway Service also supports extended logging, but it uses the log profile of the parent and ignores the log profile assigned to the path.

4.3 Role Policies for LDAP Connections Go to One Replica

All the role policies for LDAP connections go to a single replica instead of going to different replicas. This causes an issue in load balancing.

4.4 SAML 2.0 Response Misses Few Attributes in the Assertion

When the *Encrypt name identifiers* and *Encrypt assertions* options are enabled, the SAML 2.0 response misses few attributes in the assertion.

To workaround this issue do the following:

- 1 In the Administration Console, click *Devices > Identity Servers > Edit > SAML 2.0*.
- 2 Under the Security section, deselect the following check boxes:
 - ♦ Encrypt assertions
 - ♦ Encrypt name identifiers
- 3 Click *OK* to confirm the changes.

4.5 Access Gateway List Page Prompts to Update All

When you cancel the changes made to the Access Gateway configuration from the *Web Servers* tab you are prompted to do an *Update All*. This occurs when you navigate to the Access Gateway Servers page by using the Bread Crumbs feature.

To workaround this issue, cancel the configuration changes and navigate to the Access Gateways Servers page by using the *Cancel* button.

4.6 Custom Logout Pages on the Identity Server are not Executed

The query parameters to the logout URL are ignored when the WS-Federation authentication is involved. Customizing the `logoutSuccess.jsp` file to use these query parameters does not work.

To workaround this issue, customize the `logoutSuccess.jsp` file to use query parameters passed into `/nidp/app/logout`.

4.7 LDAP User Attribute Query Uses a Wrong Directory When the passwordFetch Class Is Enabled

When the `passwordFetch` class is executed and you send an LDAP user attribute query, the query goes to the `password_fetch` directory instead of the user store which is used for user authentication.

4.8 Installing Access Manager 3.1 SP4 or 3.1 SP4 IR1 on a Windows 2008 Server Results in File Not Found Error

When you create a user by using the *Roles and Tasks > Create User* option, the following error is displayed:

```
/base/CrtUserAcctAJAXSuccess.jsp File Not Found
```

Ignore this error as the user is created.

4.9 Access Gateway Service on Linux Logs An Error Stating Server Reached Maximum Client Setting

This issue is observed when the audit server is not reachable.

To work around this issue, do the following:

- 1 Add the following lines to `/etc/logevent.conf` file to force the Access Gateway Service to use caching:

```
LogForceCaching=Y
```

```
LogCacheLimitAction=roll cache
```

- 2 Add the following lines to the beginning of the `start` function in the `/etc/init.d/novell-tomcat5` file. These lines ensure that the `lcache` process is started by the `root` user.

```
set n=`ps -aef | grep lcache | grep root | wc -l`  
if [ eval $n != "2" ]; then  
    killall -9 lcache >/dev/null 2>&1
```

```
    LCACHE_USER="root"  
    su - $LCACHE_USER -c "/opt/novell/naudit/lcache -int:600 -c &"  
fi
```

4.10 Stopping the naudit Service Subsequently Stops JCC and Tomcat Services

When the `naudit` service is stopped by using `/etc/init.d/novell-naudit stop` command, occasionally other important services such as Tomcat and JCC also stop. This causes interruption of services.

To work around this issue, manually restart the Tomcat and JCC services. For information, see the TID (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008991&sliceId=1&docTypeID=DT_TID_1_1&dialogID=120228708&stateId=0%20%20247101813).

4.11 Authentication Error If the Overwrite Real User or Overwrite Temporary User Option Is Enabled

If you have two contracts and the *Overwrite Real User* option is enabled for one of them, the first user authentication does not overwrite the second user authentication. It displays the following error message:

```
Unable to authenticate. (409-esp-7271673232708786).
```


This issue is not observed with the Linux Access Gateway. For more information, see the TID (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008992&sliceId=1&docTypeID=DT_TID_1_1&dialogID=120228779&stateId=0%200%20247101935).

4.12 Sometimes SSL VPN Causes a Windows Explorer Crash in Kiosk Mode

The SSL VPN works in Enterprise mode, but it crashes on Windows Explorer browser that uses ActiveX.

If you restore or downgrade the Windows XP client to Windows XP SP3, the SSL VPN works properly in the kiosk mode.

This issue is not observed on Firefox browsers using Java.

4.13 DNS Resolution by Using DNS Servers Pushed from SSL VPN fails on Mac Leopard

If the IP address and DNS servers are configured statically on Mac Leopard and a successful SSL VPN connection is established, the DNS resolution fails to use the DNS server IP address sent from the SSL VPN server.

4.14 On Windows Server 2008, You Cannot Uninstall the Administration Console

When you install the Administration Console and the Identity Server on Windows 2008, you cannot completely uninstall the components. The uninstall program hangs before it cleans all the files and the registry entries. To workaround this issue, see (http://www.netiq.com/documentation/novellaccessmanager31/readme/accessmanager_readme_sp2_ir3.html#br1og3r) in the Novell Access Manager 3.1 SP2 IR3a Readme.

4.15 Error while Uploading Large Files to an IIS 7.x Backend Web Server through the Linux Access Gateway Appliance

You cannot upload large files to an IIS 7.x web server where SSL is enabled between the Linux Access Gateway and IIS 7 server. The maximum upload size depends on the network setup. For information, see the TID (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008505&sliceId=1&docTypeID=DT_TID_1_1&dialogID=120156265&stateId=0%200%20246847206).

4.16 OR Condition Rules Are Not Getting Updated Second Time

When you create rules for the role conditions first time by using the *Brokering* tab, it will be displayed appropriately. When you try to modify this existing role with OR conditions, the role is not updated.

To workaround this issue, delete the existing created role condition and recreate a new role condition.

4.17 The SP Brokering Functionality Does Not Work with Shibboleth Identity Provider as the Origin Identity Provider

If you try to access the Brokering URL after configuring a service provider Brokering group with the Shibboleth identity provider, it fails to access the target application.

4.18 Service Unavailability Caused by a SLES 11 Issue

Because of an issue, the operating system returns the 27.0.0.2 entry when the hostname is resolved. This causes the 127.0.0.2 to be the default address of the listener when the device is added to the cluster.

To workaround this issue:

- 1 Go to the proxy service page. Change the listening IP address to the other cluster member, then select the correct IP address again.
- 2 Click *Update* to save the changes.
- 3 Verify the correct address and add the device to the cluster.

5 Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2012 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

For Novell trademarks, see the Novell Trademark and [Service Mark list \(http://www.novell.com/\)](http://www.novell.com/).

All third-party trademarks are the property of their respective owners.