Novell Access Manager 3.1 SP3 IR2 Readme

July 17, 2011

Novell®

This Readme describes the Novell Access Manager 3.1 SP3 IR2 release.

- Section 1, "Documentation," on page 1
- Section 2, "Upgrading to Access Manager 3.1 SP3 IR2," on page 1
- Section 3, "Bugs Fixed in Access Manager 3.1 SP3 IR2," on page 4
- Section 4, "Known Issues in Access Manager 3.1 SP3 IR2," on page 6
- Section 5, "Legal Notices," on page 9

1 Documentation

The following sources provide information about Novell Access Manager:

- Documentation Web Site (http://www.novell.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 (http://www.novell.com/products/accessmanager/).

2 Upgrading to Access Manager 3.1 SP3 IR2

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

2.1 Upgrading the Purchased Product

After you have obtained Access Manager 3.1 SP3 IR2 or a previous release of Access Manager, log in to the Novell Customer Center (http://www.novell.com/center), then follow the link that allows you to download the software.

The following files are available:

Filename	Description
AM_31_SP3_IR2_IdentityServer_Linux32.tar.gz	Contains the Linux Identity Server, the Linux Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN Server.
AM_31_SP3_IR2_IdentityServer_Win32.exe	

Filename	Description
	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2003.
AM_31_SP3_IR2_IdentityServer_Win64.exe	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2008.
AM_31_SP3_IR2_AccessGatewayAppliance_Linux_SLES9.tar.gz	Contains the upgrade RPMs for the (SUSE Linux Enterprise Server) 9 version of the Access Gateway Appliance and the Traditional SSL VPN server.
AM_31_SP3_IR2_AccessGatewayAppliance_Linux_SLES11.tar.gz	Contains the upgrade RPMs for the (SUSE Linux Enterprise Server) 11 version of the Access Gateway Appliance and the Traditional SSL VPN server.
AM_31_SP3_ConfigurationUpgrade.zip	Contains the script to enable the session stickiness option for existing proxy services and allow target option for the intersite transfer service. This option is disabled on an upgrade from 3.1 SP2 IR3 to 3.1 SP3 IR2.
AM_31_SP3_IR2_AccessGatewayService_Win64.exe	Contains the Access Gateway Service for Windows Server 2008 R2 with a 64-bit operating system.
AM_31_SP3_IR2_AccessGatewayService_Linux64.bin	Contains the Access Gateway Service for (SUSE Linux Enterprise Server) 11 with a 64-bit operating system.
AM_31_SP3_IR2_ApplicationServerAgents_AIX.bin	Contains the Agents service for the AIX platform.
AM_31_SP3_IR2_ApplicationServerAgents_Linux.bin	Contains the Agents service for the Linux platform.
AM_31_SP3_IR2_ApplicationServerAgents_Solaris.bin	Contains the Agents service for the Solaris platform.
AM_31_SP3_IR2_ApplicationServerAgents_Windows.exe	Contains the Agents service for the Windows platform.

For upgrade and installation information:

- "Upgrade Instructions" on page 2
- "Installation Instructions" on page 3
- "Verifying Version Numbers Before Upgrading" on page 3
- "Verifying Version Numbers After Upgrading" on page 3

2.1.1 Upgrade Instructions

For instructions on upgrading from 3.1 SP3, 3.1 SP3 IR1 to 3.1 SP3 IR2, see "Upgrading Access Manager Components" in the *Novell Access Manager 3.1 SP3 Installation Guide*. To verify that your components are running 3.1 SP3, 3.1 SP3 IR1 see "Verifying Version Numbers before Upgrading" on page 3.

Any Access Manager version prior to 3.1 SP2 IR2 should be first upgraded to 3.1 SP3. For more information on upgrading to 3.1 SP3, see the *Novell Access Manager 3.1 SP3 Installation Guide*.

2.1.2 Installation Instructions

For installation instructions for the Access Manager Administration Console, the Identity Server, the Access Gateway Appliance, the Access Gateway Service, and the SSL VPN server, see the *Novell Access Manager 3.1 SP3 Installation Guide*.

2.1.3 Verifying Version Numbers before Upgrading

If you are upgrading from Access Manager 3.0, all components must be first upgraded to Access Manager 3.1 SP3 before upgrading to Access Manager 3.1 SP3 IR2.

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

2 Examine the value in the *Version* field. The following table indicates the versions that can be upgraded to 3.1 SP3 IR2.

Component	3.1 SP3	3.1 SP3 IR1
Administration Console	3.1.3.247	3.1.3.273
Identity Server	3.1.3.247	3.1.3.273
Linux Access Gateway	3.1.3.247	3.1.3.273
Access Gateway Services	3.1.3.247	3.1.3.273
SSL VPN	3.1.3.247	3.1.3.273

2.1.4 Verifying Version Numbers after Upgrading

When you have finished upgrading your Access Manager components, 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 SP3 IR2.

Component	3.1 SP3 IR2
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

Component	3.1 SP3 IR2
SSL VPN	3.1.3.292

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) and follow the link that allows you to download the high-bandwidth key.

3 Bugs Fixed in Access Manager 3.1 SP3 IR2

3.1 Identity Server

Fixed an issue where the password fetch method does not get executed at our SAML2.0 Service Provider while consuming an assertion from the identity provider server through the inter-site transfer URL

Fixed an issue where the user could not set a value for SAML 2.0 RequestedAuthnContext comparison except "Exact."

Fixed an issue where authentication failed for WSFederation with SharePoint 2010 after applying 3.1 SP3 when the times for the identity provider WSFed were not synchronized. For more information, see "Assertion Validity Window."

Fixed an issue where the Kerberos authentication failed when the request was proxied by an identity provider to another identity provider.

Fixed an issue where the cluster cookies did not have any secure and HTTPOnly options. These options are not enabled by default, and the web.xml options are introduced to enable these options. For more information, see "Enabling Secure or HTTPOnly Flags for Cluster Cookies."

Fixed an issue where the service provider generated two SAML SSO requests, resulting in two session indexes that caused incomplete single logout.

Fixed an issue when the identity server in a cluster received a SAML 2.0 logout request where the authentication was performed on a different node.

Fixed an issue where a SAML 2.0 attribute query response did not populate the inResponseTo attribute in SubjectConfirmation.

Fixed an issue where SAML 2.0 ignored the Front Channel Logout option in the logout initiated by the Access Gateway Appliance. For more information, see "Defining Options for Liberty or SAML 2.0"

3.2 Linux Access Gateway Appliance

Fixed an issue with Range requests where the Access Gateway Appliance sends the same request twice to the Web server, resulting in random server crashes.

Fixed an issue where Access Gateway Appliance crashes when the Web server sent content-length response header value smaller than the actual content.

Fixed a login issue in the cluster environment with Access Gateway Appliance when the user name contained double byte characters in it.

Fixed an issue with the Access Gateway Appliance where the user got an error message "403 Forbidden Description: Detected URL tampering."

Fixed a memory leak issue that caused a core dump with Access Gateway Appliance.

Fixed an issue with the OpenHRE login page. If the value for the form number was configured as 0 in the Form Fill policy, the login page was truncated.

Fixed an issue where random process restarts occurred in SP3.

Fixed an issue in the authorization policy with multiple LDAP OU evaluation failures after upgrading from 3.1SP2 to 3.1SP3.

Fixed an issue where the /var/novell/.disableWSHealth touch file was not working. This touch file helps avoid the device health being marked as bad because of some unreachable Web servers. For more information, see "disableWSHealth"

Fixed an issue where the user's private information was getting logged to the soapmessages log file under specific configurations.

Fixed a 403 forbidden issue that resulted when the user posted large data (more than 56 KiloBytes in size) after a session timeout. The Administrator can change the post data parking size limit. For more information, see "ParkingSizeInKiloBytes"

Fixed an issue where the source port of the connection to the Web server was incorrect in the ics_dyn.log file.

Fixed an issue where the Access Gateway Appliance crashed while being redirected from http to https when the host name header exceeds 4k bytes.

Fixed a crash issue with Access Gateway in custom login sequence environment where /nesp/app/plogin request reaches proxy with POST data.

Fixed an issue with downloading large files from a Web server; as the dowload process stopped after downloading a small part of the file through the Access Gateway Appliance.

Fixed an issue where 400 bad requests was observed in the reliability tests for large file scripts.

3.3 Access Gateway Service

Fixed an issue where the Access Gateway Service rewriter removed "%2" incorrectly from the url being rewritten.

Fixed a delay issue with the Access Gateway Service when the audit server was not reachable or not responding.

Fixed a login issue with the Access Gateway Service if users wait for 3+ min at the IDP login page and then submits their credentials.

Fixed an issue where Access Gateway Service session cookie architecture was different from Access Gateway Appliance session cookie architecture.

Fixed an issue where the Access Gateway Service performance drops by 90% when the audit server is not reachable.

4 Known Issues in Access Manager 3.1 SP3 IR2

4.1 Stopping the naudit Service Subsequently Stops JCC and Tomcat Services

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

To work around this issue, manually restart the Tomcat and JCC services. For information, see (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%200%20247101813) in the TID.

4.2 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 (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) in the TID.

4.3 The SSL VPN Causes a Windows Explorer Crash in Kiosk Mode

The SSL VPN client works properly in Enterprise mode, but crashes Windows Explorer using ActiveX.

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

This issue is not observed with Firefox using Java.

4.4 Vulnerability Issues in JRE Security

To work around the JRE security vulnerability issue, see (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008129&sliceId=1&docTypeID=DT_TID_1_1&dialogID=216290409&stateId=0%200%20216288812) in the TID.

4.5 Service Unavailability Caused by a SLES 11 Issue

In SLES 11, 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, then add the device to the cluster.

IMPORTANT: Do not refer to the deployment scenarios in the context sensitive help available with the Access Manager 3.1.3 build. Refer to this information in the Identity Server Guide.

For more information, see (http://www.novell.com/support/php/
search.do?cmd=displayKC&docType=kc&externalId=7008978&sliceId=1&docTypeID=DT_TID_
1_1&dialogID=120230000&stateId=0%200%20247107319) in the TID.

4.6 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 pushed from the SSL VPN server.

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

When you install the Administration Console and the Identity Server on a Windows 2008 machine, 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.novell.com/
documentation/novellaccessmanager31/readme/accessmanager_readme_sp2_ir3.html#br1og3r) in the Novell Access Manager 3.1 SP2 IR3a Readme.

4.8 Error while Uploading Large Files to an IIS 7.x back-end 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 (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) in the TID.

4.9 Error in Secondary IP addresses after Pushing Configuration Updates

With security patches installed on the SLES11 Linux Access Gateway machine, the secondary IP address is missing after pushing configuration updates from the Administration Console to the Linux Access Gateway device. To workaround this issue:

1 Backup the file /etc/sysconfig/network/ifcfg-eth-id-<MAC> then remove it from the directory.

2 Push the configuration from the Administration Console.

4.10 The "include the session timeout attribute in the assertion" Feature Does Not Work

To work around this issue, keep the SP Remote contract timeout the same as the remote identity provider session timeout.

4.11 Issue with SSL VPN While Validating Server Certificates

The SSL VPN client cannot validate server certificate if the trust chain includes one or more intermediate root certificates. For more information, see (http://www.novell.com/support/php/ search.do?cmd=displayKC&docType=kc&externalId=7008465&sliceId=2&docTypeID=DT_TID_ 1_1&dialogID=247083053&stateId=0%200%20247079487) in the TID.

4.12 Linux Access Gateway Appliance Does Not Support RFC 5746

Until a Linux Acess Gateway version including support for RFC 5746 will not be released, the work around is to use the Linux Access Gateway Service, instead of the appliance. For information, see (http://www.novell.com/support/viewContent.do?externalId=7008600&sliceId=1) in the TID.

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2011 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/).

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