Novell Access Manager 3.1 SP4 Readme

October 2011

Novell

This Readme describes the Novell Access Manager 3.1 SP4 release.

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 SP4

2.1 Installing or Upgrading the Purchased Product

After you have obtained Access Manager 3.1 SP4 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_SP4_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_SP4_IdentityServer_Win32.exe`	

Filename	Description
	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2003.
`AM_31_SP4_IdentityServer_Win64.exe`	
	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2008.
`AM_31_SP4_AccessGatewayAppliance_Linux_SLES11.tar.gz`	
	Contains the upgrade RPMs for SLES 11 version of the Access Gateway Appliance and the Traditional SSL VPN server.
`AM_31_SP4_AccessGatewayAppliance_Linux_SLES9.tar.gz`	
	Contains the upgrade RPMs for SLES 9 version of the Access Gateway Appliance and the Traditional SSL VPN server.
`AM_31_SP4_AccessGatewayService_Win64.exe`	
	Contains the Access Gateway Service for Windows Server 2008 R2 with a 64-bit operating system.
`AM_31_SP4_AccessGatewayService_Linux64.bin`	
	Contains the Access Gateway Service for SLES 11 with a 64-bit operating system.
`AM_31_SP4_ApplicationServerAgents_AIX.bin`	
	Contains the Agents service for AIX platform.
`AM_31_SP4_ApplicationServerAgents_Linux.bin`	
	Contains the Agents service for Linux platform.
`AM_31_SP4_ApplicationServerAgents_Solaris.bin`	
	Contains the Agents service for Solaris platform.
`AM_31_SP4_ApplicationServerAgents_Windows.exe`	
	Contains the Agents service for 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 IR2 to 3.1 SP4, see "Upgrading Access Manager Components" in the *Novell Access Manager 3.1 SP4 Installation Guide*. To verify that your components are running 3.1 SP3, 3.1 SP3 IR2 see "Verifying Version Numbers before Upgrading" on page 3.

Any Access Manager version prior to 3.1 SP3 should be first upgraded to 3.1 SP3. For more information on upgrading to 3.1 SP3, see Novell Access Manager 3.1 SP3 Installation Guide (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html)

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 SP4 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 SP4.

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 SP4.

Component	3.1 SP3	3.1 SP3 IR2
Administration Console	3.1.3.247	3.1.3.292
Identity Server	3.1.3.247	3.1.3.292
Linux Access Gateway	3.1.3.247	3.1.3.292
Access Gateway Services	3.1.3.247	3.1.3.292
SSL VPN	3.1.3.247	3.1.3.292

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 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

2.2 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 SP4

The following bugs are fixed between 3.1 SP3 and 3.1 SP4 releases:

3.1 Administration Console

Fixed an issue where clicking the Share Settings TABs with no configuration changes causes an IDP update to get applied

Fixed an issue in Administration Console where Linux Access Gateway updates sometimes stay in the pending state indefinitely when configuration is applied through the Apply All operation.

Fixed an issue where the Access Gateway Service Management IP address could not be configured.

Fixed a PasswordMush exception issue while accessing the local identity provider in the user store.

3.2 Identity Server

Fixed an issue where the Enhanced Smart Card method did not work.

Fixed an issue where the value of a shared secret could not be changed with a custom authentication class.

Fixed an issue to include the Identity Provider Session Timeout attribute in the assertion.

Fixed an issue to provide the ability to map a federated user with transient name identifier to a local user using the matching attribute.

Fixed an issue associated with SP Brokering where a null pointer exception is generated when logging out from the target service provider.

Fixed an issue where the login page did not pre-populate the username in the user name field after an initial login request failed.

Fixed an issue with the SAML 1.1 post profile to include the assertion consumer URL within the “Recipient” tag.

Fixed an issue where 300101032 error generated processing a SAML assertion when the “Assertion Validity Window” parameter is configured.

Fixed an issue where intruder lockouts occur in a multiple replica environment when a user grace login count is less than the number of LDAP replicas configured.

Fixed an issue where “"There are no login connections available. Please try again later." message is returned to the user after entering incorrect credentials.

Fixed an “Array Index Out of Bounds” exception which occurred while accessing an Access Gateway appliance protected resource after removing an IDP server from a 2- node cluster and applying update.

Fixed an issue when a user is not redirected to the password management servlet after authenticating to the identity provider server in an active directory environment.

Fixed an issue where the users could not access SAML Intersite transfer URL target parameter after upgrading to 3.1 SP3.

Fixed an issue where the debug logs were being printed without enabling logging into the identity provider server.

Fixed an issue where the Tomcat version was displayed on the error pages.

Fixed a potential security vulnerability issue on the identity provider login page with the localized help file frames.

Fixed a 302 redirect issue in the “Relay State” which was URL encoded after consuming a SAML response.

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"

3.3 Linux Access Gateway Appliance

Fixed an issue with Rewriter where HTML page includes apostroph characters.

Fixed an issue where the Access Gateway added a suffix containing the characters "%00" in the URL while using the Safari browser.

Fixed an issue where Access Gateway did not support RFC 5746.

Fixed an issue where Access Gateway was not forwarding the range request to the back-end server in some scenarios.

Fixed an issue where Linux Access Gateway did not complete uncompressing the gzip compressed JavaScript files (`file.js.gz`).

Fixed an issue where secondary IP addresses were disordered or missing after applying configuration updates.

Fixed an issue where users were getting blank pages while accessing resources through Linux Access Gateway.

Fixed an issue where Linux Access Gateway could not work with the Lotus Domino server over https. For more information, see "Linux Access Gateway Does Not Work with the Lotus Domino Server Over HTTPS" in *Novell Access Manager 3.1 SP4 Access Gateway Guide*.

Fixed an issue where rewriting of a path based multi homing accelerator was not working after upgrading to SP3 resulting in a 404 Not Found error.

Fixed an Access Gateway appliance crash after applying the configuration changes immediately after a purge cache when the high availability feature is enabled.

Fixed an issue associated with the Access Gateway Appliance crashing in the rewriter by changing the configuration. The rewriter configuration now works as expected with vmc restarts that are related to the Purge Cache command.

Fixed a cross site scripting issue with the embedded service provider.

Fixed a potential ics_dyn gateway process restart issue, which occurred when the system configuration was applied.

Fixed an issue associated with the Access Gateway appliance that occurred when sending duplicate range requests to the back-end server.

Fixed an issue with the Access Gateway appliance prompting for re-authentication when the password management touch file was enabled, despite the user running a valid session.

Fixed an issue where the Access Gateway appliance did not do a complete TLS handshake during the health check to the back-end server.

Fixed a random Access Gateway appliance crash that caused while updating the configuration with a new protected resource when upgrading from 3.1.2 IR2 to 3.1.2 IR3.

Fixed an issue where the SAML authorization response did not include the authorization request when authentication to the identity server fails.

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

3.4 Access Gateway Service

Fixed an issue where Access Gateway Service was crashing on Windows.

Fixed an issue where Access Gateway Service did not support RFC 5746.

Fixed an issue where Access Gateway Service was crashing regularly with AJAX applications.

Fixed the 100% CPU utilization issue with Access Gateway Service under high load.

Fixed an issue that caused the parent process to crash whenever one of the child processes crashed in the Windows platform.

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.

3.5 SSL VPN

Fixed an issue in SSL VPN where the stunnel client (kiosk mode) could not validate server certificate if the trust chain includes one or more Intermediate Root Certs.

Fixed an issue where users could not connect to the OpenVPN service when 60 static route entries were present on the SSL VPN server.

Fixed a DNS update issue with MAC Leopard, when the IP address configuration along with the DNS server entries are obtained from the DHCP server.

Fixed an issue with the MAC OS java process hitting 100% CPU utilisation immediately after connecting to the SSL VPN.

Fixed an issue where the MAC keychain info was lost after the SSLVPN connection.

3.6 Others

Fixed Access Manager security vulnerability issues in the Java Runtime Environment.

4 Known Issues in Access Manager 3.1 SP4

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 Sometimes 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 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.

4.5 On Windows Server 2008, You Cannot Uninstall 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.

4.6 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.

4.7 Request Containing Encoded CR/LF in URL Fails with Linux Access Gateway Appliance

For more information, see (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008862&sliceId=2&docTypeID=DT_TID_1_1&dialogID=269551712&stateId=0%200%20269553602)

4.8 OR Condition Rules Are Not Getting Updated Second Time

Using Brokering tab when you create rules for the role conditions first time, it will be displayed appropriately and the second time when you want to modify the existing role with OR conditions then the same is not updated and displayed.

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

4.9 The SP Brokering Functionality Does Not Work with Shibboleth IDP as the Origin IDP

If you try to access the Brokering URL after configuring an SP Brokering group with the Shibboleth Identity Provider, it fails to access the target application.

4.10 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.

4.11 DNS Resolution 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 from it, then the DNS resolution fails to use the DNS server IP address pushed from the SSL VPN server.

5 Legal Notices