Novell Access Manager 3.1 SP2 Readme

November 17, 2010

Novell®

This Readme describes the Novell Access Manager 3.1 SP2 release.

- Section 1, “Documentation,” on page 1
- Section 2, “Installing Access Manager 3.1 SP2,” on page 1
- Section 3, “Bugs Fixed in Access Manager 3.1 SP2,” on page 6
- Section 4, “Known Issues in Access Manager 3.1 SP2,” on page 10
- Section 5, “Legal Notices,” on page 31

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 Installing Access Manager 3.1 SP2

- Section 2.1, “Installing or Upgrading the Purchased Product,” on page 1
- Section 2.2, “Downloading the J2EE Agents,” on page 5
- Section 2.3, “Installing the Evaluation Version,” on page 6
- Section 2.4, “Installing the High-Bandwidth SSL VPN Server,” on page 6

2.1 Installing or Upgrading the Purchased Product

After you have purchased Access Manager 3.1 SP2 or a previous release of Access Manager, log in to the Novell Customer 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_SP2_IdentityServer_Linux32.tar.gz	
AM_31_SP2_IdentityServer_Linux32.iso	

Filename	Description
	Contains the Linux Identity Server, the Linux Administration Console, the SSL VPN Server that is installed with an Embedded Service Provider, and the SSL VPN Server that must be protected by an Access Gateway. Can be used for installation and upgrade from 3.0 SP4 to 3.1 SP2, from 3.1 to 3.1 SP2, from 3.1.1 to 3.1 SP2, and from the evaluation version to the product version.
`AM_31_SP2_IdentityServer_Win32.exe`	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2003. Can be used for installation and upgrade from 3.1 to 3.1 SP2, from 3.1.1 to 3.1 SP2, and from the evaluation version to the product version.
`AM_31_SP2_IdentityServer_Win64.exe`	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2008. Can be used only for installation.
`AM_31_SP2_AccessGatewayAppliance_Linux_SLES11.iso`	Contains the CD image for the SUSE Linux Enterprise Server (SLES) 11 version of the Access Gateway Appliance and the SSL VPN Server that must be configured as a protected resource of the Access Gateway. Can be used only for installation.
`AM_31_SP2_AccessGatewayAppliance_Linux_SLES11.tar.gz`	Contains the upgrade RPMs for upgrading the SLES 11 evaluation version of the Access Gateway Appliance to the product version.
`AM_31_SP2_AccessGatewayAppliance_Linux_SLES9.tar.gz`	Contains the upgrade RPMs for the SLES 9 version of the Access Gateway Appliance and the SSL VPN Server that must be configured as a protected resource of the Access Gateway. Can be used for upgrading from 3.0 SP4 to 3.1 SP2, from 3.1 to 3.1 SP2, from 3.1.1 to 3.1 SP2, and from the evaluation version to the product version.
`AM_31_SP2_AccessGatewayService_Win64.exe`	Contains the Access Gateway Service for Windows Server 2008 with a 64-bit operating system. Can be used only for installation.
`AM_31_SP2_AccessGatewayService_Linux64.bin`	Contains the Access Gateway Service for SLES 11 with a 64-bit operating system. Can be used only for installation.

For upgrade and installation information:

- "Upgrade Instructions" on page 3
- "Installation Instructions" on page 3

- "Verifying Version Numbers Before Upgrading" on page 4
- "Verifying Version Numbers After Upgrading" on page 5

2.1.1 Upgrade Instructions

For instructions on upgrading from 3.0 SP4 to 3.1 SP2, see "Upgrading from Access Manager 3.0 SP4 to Access Manager 3.1 SP2" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bgfx9yh.html) in the *Novell Access Manager Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html). To verify that your components have been upgraded to 3.0 SP 4, see "Verifying Version Numbers Before Upgrading" on page 4.

For instructions on upgrading from 3.1 to 3.1 SP2, see "Upgrading Access Manager 3.1 to 3.1 SP2" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bk0lvlm.html) in the *Novell Access Manager Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html). To verify that your Access Manager components are running 3.1, see "Verifying Version Numbers Before Upgrading" on page 4.

For instructions on upgrading from 3.1 SP1 to 3.1 SP2, see "Upgrading Access Manager 3.1 to 3.1 SP2" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bn6ajpt.html) in the *Novell Access Manager Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html). To verify that your Access Manager components are running 3.1, see "Verifying Version Numbers Before Upgrading" on page 4.

IMPORTANT: If you have installed a previous version of the Administration Console or the Identity Server on a machine that does not have at least 1 GB (Linux) or 1.2 GB (Windows) of memory, the upgrade to SP2 fails. The installation script now checks for available memory and exits the upgrade if the machine does not have the minimum required memory.

In addition to the files available through your Novell Customer Center (http://www.novell.com/center) account, the following patch file is available from Novell Downloads (http://download.novell.com/index.jsp).

Filename	Description
`AM_31_SP2_LAG300_keystorePathScript.sh`	Contains a keystore cleanup script that needs to be run before upgrading an Access Gateway Appliance that was first installed with version 3.0 to 3.1 SP2. For more information about this script, see "Upgrading the SP4 Linux Access Gateways" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bgfx9yh.html#bhn7mjv) in the *Novell Access Manager 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 Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html).

2.1.3 Verifying Version Numbers Before Upgrading

If you are upgrading from Access Manager 3.0, all components must be upgraded to at least SP4 before upgrading to Access Manager 3.1 SP2.

1. In the Administration Console, click *Access Manager > Auditing > Troubleshooting > Version.*
2. Examine the value of the *Version* field to see if it displays a 3.0 SP4 version that is eligible for upgrading to 3.1 SP2.

Component	3.0 SP4	3.0 SP4 IR1	3.0 SP4 IR2	3.0 SP4 IR3	3.0 SP4 IR4
Administration Console	3.0.4.38	3.0.4.56	3.0.4.60	3.0.4.70	3.0.4.94
Identity Server	3.0.4.38	3.0.4.56	3.0.4.60	3.04.70	3.0.4.94
Linux Access Gateway	3.0.4.38	3.0.4.56	3.0.4.60	3.0.4.70	3.0.4.94
NetWare Access Gateway	3.0.505	3.0.505a	3.0.505b	3.0.505g	3.0.505h
J2EE Agents (all versions, all platforms)	3.0.4.38	3.0.4.56	3.0.4.60	3.0.4.70	3.0.4.94
SSL VPN	3.0.4	3.0.4	3.0.4	3.0.4	3.0.4

Access Manager 3.1 and all of its interim releases are eligible for upgrading to 3.1 SP2.

1. In the Administration Console, click *Access Manager > Auditing > Troubleshooting > Version.*
2. Examine the value of the *Version* field to see if it displays a 3.1 version that is eligible for upgrading to 3.1 SP2.

Component	3.1	3.1 IR1	3.1 IR2
Administration Console	3.1.0.420	3.1.0.425	3.1.0.431
Identity Server	3.1.0.420	3.1.0.425	3.1.0.431
Linux Access Gateway	3.1.0.420	3.1.0.425	3.1.0.431
J2EE Agents (all versions, all platforms)	3.1.0.420	3.1.0.425	3.1.0.431
SSL VPN	3.1.0	3.1.0	3.1.0

Access Manager 3.1 SP1 and all of its interim releases are eligible for upgrading to 3.1 SP2.

1. In the Administration Console, click *Access Manager > Auditing > Troubleshooting > Version.*
2. Examine the value of the *Version* field to see if it displays a 3.1 SP1 version that is eligible for upgrading to 3.1 SP2.

Component	3.1 SP1	3.1 SP1 IR1	3.1 SP1 IR2	3.1 SP1 IR3
Administration Console	3.1.1.215	3.1.1.235	3.1.1.247	3.1.1.265
Identity Server	3.1.1.215	3.1.1.235	3.1.1.247	3.1.1.265
Linux Access Gateway	3.1.1.215	3.1.1.235	3.1.1.247	3.1.1.265
J2EE Agents (all versions, all platforms	3.1.1.215	3.1.1.235	3.1.1.247	3.1.1.265

Component	3.1 SP1	3.1 SP1 IR1	3.1 SP1 IR2	3.1 SP1 IR3
SSLVPN	3.1.1.215	3.1.1.235	3.1.1.235	3.1.1.265

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 of the *Version* field to verify that the component has been upgraded 3.1 SP2.

Component	3.1 SP2
Administration Console	3.1.2.281
Identity Server	3.1.2.281
Access Gateway (all versions, all platforms)	3.1.2.281
J2EE Agents (all versions, all platforms)	3.1.2.281
SSL VPN	3.1.2.281

2.2 Downloading the J2EE Agents

The J2EE Agents are a free download and are available from Novell Downloads (http://download.novell.com/index.jsp). The following files are available:

Filename	Description
`AM_31_SP2_ApplicationServerAgents_Windows.exe`	Contains the J2EE Agents for Windows (JBoss, WebSphere, and WebLogic) and can only be used for installation.
`AM_31_SP2_ApplicationServerAgents_AIX.bin`	Contains the J2EE Agents for AIX (WebSphere) and can only be used for installation.
`AM_31_SP2_ApplicationServerAgents_Linux.bin`	Contains the J2EE Agents for Linux (JBoss, WebSphere, and WebLogic) and can only be used for installation.
`AM_31_SP2_ApplicationServerAgents_Solaris.bin`	Contains the J2EE Agents for Solaris (WebLogic) and can only be used for installation.

For installation instructions, see *Novell Access Manager J2EE Agent Guide* (http://www.novell.com/documentation/novellaccessmanager31/j2eeagents/data/bookinfo.html).

2.3 Installing the Evaluation Version

To install an evaluation version of Access Manager 3.1 SP2, download the following files from Novell Downloads (http://download.novell.com/index.jsp). When the evaluation version is installed, it displays 3.1.2.280 for the version number.

Filename	Description
AM_31_SP2_IdentityServer_Linux32_Eval-0331.iso	Contains the Linux Identity Server, the Linux Administration Console, the SSL VPN Server that is installed as a standalone version with an Embedded Service Provider, and the SSL VPN Server that must be protected by an Access Gateway.
AM_31_SP2_IdentityServer_Win32_Eval-0331.exe	Contains the Windows Identity Server and Windows Administration Console.
AM_31_SP2_IdentityServer_Win64_Eval-0331.exe	Contains the Windows Identity Server and Windows Administration Console.
AM_31_SP2_AccessGatewayAppliance_Eval-0331.iso	Contains the Linux Access Gateway and the SSL VPN Server that must be configured as a protected resource of the Access Gateway.
AM_31_SP2_AccessGatewayService_Linux64_Eval-0331.bin	Contains the Linux Access Gateway Service.
AM_31_SP2_AccessGatewayAppliance_Win64_Eval-0331.exe	Contains the Windows Access Gateway Service.

For installation instructions, see the *Novell Access Manager Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html).

2.4 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 SP2

- Section 3.1, “Administration Console,” on page 7
- Section 3.2, “Identity Server,” on page 7
- Section 3.3, “Linux Access Gateway Appliance,” on page 9
- Section 3.4, “SSL VPN,” on page 10

3.1 Administration Console

- Fixed an issue that allowed you to copy a policy before saving it, which created two policies with the same ID.
- When you apply changes to the Access Gateway Appliance or the Access Gateway Service, the update command no longer remains in a pending state for 15 minutes.
- Fixed an issue with an error message for the Access Gateway when configuring SSL for the Web servers. The error message disappeared before the administrator could read it and understand the problem.
- Fixed an inconsistency issue with the name conventions for the Gateway Appliance and the Gateway Service.
- Fixed an issue with the uninstall program for the Linux Administration Console that left behind the `/var/novell` directory instead of removing it.
- On a Windows Server 2008 Administration Console, administrators can now back up or restore certificates that have double-byte characters.
- Added an information message to alert administrators that when they import a certificate, they should make sure to add all the CA certificates in the certificate chain.
- Fixed a Tomcat restart issue when upgrading from 3.0 SP4 to 3.1 or later.
- Return the X-Forwarded-For IP condition as a valid condition for an Access Gateway Authorization policy.
- Fixed an issue that caused an upgrade from 3.0 SP4 to 3.1 SP1 or later to fail.

3.2 Identity Server

- Fixed an issue that displayed a blank page when an incorrect password was entered by an NMAS Windows client.
- Root and intermediate revocation checks can now be performed on an X.509 contract.
- Fixed a performance issue with Liberty profiles. The attribute services for Personal Profile, Employee Profile, Customized Profile, and Credential Profile all require that a Liberty User Profile object be created for each authenticated user. This object is created in the configuration data store under a Liberty User Profiles Container object.

  Access Manager was creating these objects even if none of these attribute services were enabled, which caused a substantial LDAP performance degradation. Checks were added to create or read these objects only if an attribute service that required them is enabled.
- Fixed an issue that prevented shared secret attributes from appearing in the list of attributes that could be added to an attribute set.
- Fixed an issue with multiple LDAP replicas that prevented users from being redirected to the change password servlet.
- Fixed an issue that caused the *Force Authentication* option of a request from a service provider to be ignored.
- Fixed an issue with the *Allow multiple browser session logout* option that allowed the user to log in using two browsers, log out of one browser, and still remain logged in on the other browser.
- Fixed an issue that caused an error to display when a user clicked a link in a Word document.

- Fixed an issue that caused a null pointer exception when a user tried to log in again after closing the browser.
- Fixed an issue that allowed the destination port to be incorrectly set to 0 when an Identity Server or Embedded Service Provider forwarded a request to the authoritative cluster member (the one holding the user's session). This issue was exhibited in the log files when the proxy URL contained a port of 0.
- Fixed an issue that caused redirection loops when the user was idle until the soft timeout expired.
- Fixed an issue with the Use Introductions feature for the Liberty protocol.
- Added code to look at the policy to determine if identities should be read during authentication.
- Modified the OCSP validation process so that it isn't required to match the number of OCSP responses with the number of certificates in the request.
- Fixed a cross-site scripting vulnerability in target URLs.
- Fixed an issue that allowed session failover to keep expired X.509 sessions active.
- Fixed an assertion issue that prevented the Identity Server from sending defined LDAP attributes in the assertion at authentication.
- Fixed a federation issue that prevented an Identity Server that was acting as a SAML 2.0 identity provider from prompting the user for authentication credentials. The user no longer needs to select the authentication card before being prompted.
- Fixed an issue that prevented custom login pages from displaying correctly when the contract contained two methods.
- Fixed an issue that caused LDAP sessions to stay with one LDAP server when multiple servers were available.
- Fixed an issue that caused upgrades to fail when an engineering build was installed prior to the official release.
- Fixed an issue that caused Identity Servers to randomly lose their connections to other Identity Servers in the cluster.
- Fixed an issue that corrupted the session failover table when cluster was under heavy load.
- Fixed an issue that prevented users from being redirected to the password expiration service.
- Fixed an authentication issue so that the Identity Server forces a reauthentication when the IP address of the client changes.
- Fixed an issue with Kerberos authentication that prevented the Identity Server from prompting for basic authentication when the users failed the Kerberos authentication check.
- Added health checks for the signing, encryption, and SSL connector certificates.
- Modified the display name for secret store attributes so that they are easier to identify.
- Fixed an issue with non-redirected login, query strings with multiple parameters, and the basic authentication class.
- Fixed an issue with logging that caused an excessive amount of information to be logged to the Access Gateway when the log level was set to Info on the Identity Server logging page.
- Fixed an issue with the Linux Identity Server upgrade that prevented some RPMs from being updated to the latest version.
- Fixed a SAML 2.0 issue that prevented Firefox from handling an encoded target.

- Fixed a SAML 2.0 issue that prevented the *Passive Authentication Only* option from succeeding when the required credentials were available.
- Modified the behavior of the Identity Server so that SAML 2.0 messages with a post profile can be signed.
- Added the ability to select federated, transient, or unspecified as the identifier format for the SAML 2.0 service provider.
- Updated to the latest version of the Microsoft Visual C++ libraries to fix a security issue.

3.3 Linux Access Gateway Appliance

- Fixed an issue with the curl command that caused the Access Gateway Appliance to restart frequently with a Signal 11 error.
- Fixed an issue that caused the Access Gateway Appliance login to loop when the *Set Secure Cookie* option was enabled.
- You can now stop the rewriter from rewriting URLs with an external DNS name with the help of the `/var/novell/.disableExternalDNSRewrite` touch file.
- Fixed an issue with a function that tried to connect to the Web server in the background, which was resulting in an Access Gateway Appliance crash.
- Fixed an issue with log rotation that caused all of the Access Gateway Appliances in a cluster to go down simultaneously.
- Fixed the novell-vmc service crash that occurred every time the service was manually stopped or started or every time the server operating software was restarted.
- Fixed an issue that caused the browser with a POST request to redirect to Identity server for authentication during a soft time out.
- Fixed an issue that caused a delay of 45-60 seconds in Access Gateway Appliance and Embedded Service Provider communication and resulted in the L4 switch marking the appliance as down.
- Fixed an issue that caused a Web application to fail.
- Fixed an issue that caused the Access Gateway Appliance to crash when sending a POSTDATA with form fill.
- Fixed a stale file content problem when WebDAV with Teaming 2.1 was accelerated behind Access Gateway Appliance.
- Fixed an issue that caused the Access Gateway Appliance to crash when an HTTP common log entry was added.
- Fixed an issue that caused the connections to remain in the close_wait state.
- Fixed an issue that caused the Access Gateway Appliance to crash when it was freeing memory.
- Fixed an Access Gateway Appliance crash caused by issues in Form Fill.
- Fixed an issue that caused the idle server connections count to exceed its limit.
- Fixed an issue with the pin list that resulted in the Access Gateway Appliance dumping core.
- Fixed a format error in the `outputtoscreen` function that resulted in an Access Gateway Appliance crash.
- Fixed an issue that caused the Access Gateway Appliance to dump core when a list with an entry was added twice.

- Fixed an issue that caused the Access Gateway Appliance to restart without creating a core dump.
- Starting with Access Manager 3.1 SP1 IR3, the logout process has been slightly modified. When the user makes an `/AGLogout` request, this request no longer creates a 302 redirect request to `/nesp/app/plogout`. An `/AGLogout` request now triggers a `/nesp/app/plogout` request to the Embedded Service Provider.
- Fixed an issue that prevented an Access Gateway Appliance from re-importing when the same DNS name and IP address were used and when the Access Gateway was using certificates imported from an external CA.
- Fixed a domain name issue that prevented the cookie domain from being set to a 2 + 2 domain name such as `portal.zg.ch`.
- Modified the path restrictions for a protected resource so that you can now have the path end with a filename and a wildcard for the extension, such as `/myfile.*`
- Proxy services are now displayed in an alphabetical list.
- Fixed an issue that allowed you to create a proxy service and give it a name with a . (period).

3.4 SSL VPN

- Fixed an issue that caused the client integrity check policy import to fail on the Windows platform.
- Fixed the issue with upgrading from 3.0.SP4 IR4 to SP2 when SSL VPN is installed with the Access Gateway Appliance. You can now use the `lagupgrade.sh` script to upgrade the software.
- The Embedded Service Provider of SSL VPN now includes an updated `jgroups-all.jar` file.
- Fixed a segmentation fault error that occurred when a large number of roles were configured.
- SSL VPN now directly connects to the configured forward proxy.
- Audit logging is now enabled for all SSL VPN components.
- Added a UI option to configure full tunneling.
- Fixed an issue in displaying the contents of a drop-down menu on the Basic Configuration page.
- Fixed an issue that caused the user to be returned to the Dashboard page after modifying the tunnel certificate.
- Fixed issues in regenerating the key for the *Authentication Hardening* option.
- The *Authentication Hardening* option is now enabled by default.
- Fixed a a probable security vulnerability issue in the redirection of the URL query string.
- Added information to the SSL VPN uninstall instructions for the high-bandwidth key RPM. It needs to be uninstalled before uninstalling the SSL VPN server.
- The icon in Confirm Logout dialog box now correctly displays in Internet Explorer 6 and Internet Explorer 7.

4 Known Issues in Access Manager 3.1 SP2

- Section 4.1, “General Issues,” on page 11
- Section 4.2, “Upgrade Issues,” on page 11

- Section 4.3, “Administration Console Known Issues,” on page 12
- Section 4.4, “Identity Server Known Issues,” on page 15
- Section 4.5, “General Access Gateway Issues,” on page 18
- Section 4.6, “Access Gateway Appliance Known Issues,” on page 19
- Section 4.7, “Access Gateway Service Known Issues,” on page 26
- Section 4.8, “SSL VPN Known Issues,” on page 27
- Section 4.9, “J2EE Agent Known Issues,” on page 31

4.1 General Issues

- Ensure that you synchronize the correct date, time, and time zone settings between the Identity Servers and the other Access Manager devices. You must synchronize your servers to within one minute of each other. Otherwise, you encounter federation and session time-out errors. You should use NTP for time synchronization.
- Ensure that DNS names can be resolved.
- Enable (allow) browser pop-ups for the Administration Console (administration server).
- Access Manager 3.1 SP2 does not support installation of the Administration Console, Identity Server, Access Gateway Appliance, and SSL VPN on a single machine.

4.2 Upgrade Issues

- “Upgrading from SLES 9 to SLES 10” on page 11
- “For the Windows 2003 or Windows 2008 Platforms, When You Upgrade from the Evaluation Version of the Administration Console to the Product Version, the Automatic Backup Fails” on page 12
- “For the Windows 2008 Platform, When You Upgrade from the Evaluation Version of the Administration Console to the Product Version, You Cannot Log In to the Administration Console” on page 12
- “After Upgrading from SP1 to SP2, Users Cannot Access Resources that Use Policies” on page 12

4.2.1 Upgrading from SLES 9 to SLES 10

Before upgrading from 3.0 SP4 to 3.1 SP2, you need to upgrade the operating system of your Administration Console and Identity Server machines from SUSE Linux Enterprise Server (SLES) 9 to SLES 10 SP2.

If you do an operating system upgrade rather than a fresh install of the operating system, you need to verify the UID of the D-BUS (messagebus) user on your secondary Administration Consoles. The SLES upgrade creates this user with the same ID as the novlwww user. You need to change this ID before continuing with the upgrade process.

IMPORTANT: If the IDs are the same, Access Manager 3.1 SP2 fails to install.

---

1. Access the control center, then click *User Management*.
2. Set the filter to *System Users*.

3 Select the messagebus (User for D-BUS) user.

4 Click *Edit*.

5 Click the *Details* tab.

6 Change the UID to another ID that is unique.

7 Click *Accept*.

8 Click *Finish*.

4.2.2 For the Windows 2003 or Windows 2008 Platforms, When You Upgrade from the Evaluation Version of the Administration Console to the Product Version, the Automatic Backup Fails

The upgrade program prompts you to perform a backup, but if you answer yes to the prompt, the process fails to create the backup files.

To work around this issue, create a backup before upgrading. Then, when you are prompted to perform a backup, answer no to the prompt.

4.2.3 For the Windows 2008 Platform, When You Upgrade from the Evaluation Version of the Administration Console to the Product Version, You Cannot Log In to the Administration Console

On Windows Server 2008, you cannot upgrade the evaluation version of the Administration Console to the product version. If you try, you receive the following error when you attempt to log in:

```
(Error -634) The target server does not have a copy of what the source server
is requesting. Or, the source server has no objects that match the request and
has no referrals on which to search for the object.
```

To work around this issue, you need to wait for the SP2 IR1 release, which will fix this problem.

4.2.4 After Upgrading from SP1 to SP2, Users Cannot Access Resources that Use Policies

If you have policies that protect Access Gateway resources and then upgrade from Access Manager 3.1 SP1 to 3.1 SP2, sometimes not all of the timeouts are pushed to the Embedded Service Provider of the Access Gateway. When users try to access these resources after the upgrade, they receive 403 errors.

To work around this issue, you need to change the *Authentication Timeout* of the contract (click *Identity Servers* > *Edit* > *Local* > *[Name of Contract]*), then update the Identity Servers and the Access Gateways.

For more information on this issue, see TID 7007113 (http://www.novell.com/support/viewContent.do?externalId=7007113&sliceId=1).

4.3 Administration Console Known Issues

- "Current Date Condition Does Not Work When Letters Are Used to Specify the Month" on page 13
- "Intermittently, Configuration Updates Might Take 10 to 15 Minutes" on page 13
- "After an Upgrade, Certificates Cannot Be Imported" on page 14

- "The Administration Console on Windows Server 2008 Runs Out of Memory" on page 14
- "The Status of the Connection to the LDAP Server Replicas Is Unclear" on page 14
- "You Cannot Select the Install Path for a Windows Administration Console" on page 14
- "Administration Console Fails to Install on VMWare ESX" on page 14
- "A Delegated Administrator Temporarily Inherits All Rights If the Browser Is Not Closed After Creating the Delegated Administrator" on page 15
- "Slow Install" on page 15
- "Liberty Attributes Are Not Visible" on page 15
- "Installation Issue with Ports 389 and 636" on page 15
- "iManager Plug-Ins Fail to Install" on page 15
- "The Access Gateway Service Fails to Cache Events If the Audit Server Is Stopped" on page 15

4.3.1 Current Date Condition Does Not Work When Letters Are Used to Specify the Month

When you create an Access Gateway Authorization policy with the Current Date condition, you need to specify the format of the Value field. If you select a format that allows you to specify the month with letters, the policy creation fails. To workaround this issue, select a format that allows you to use numbers for the month.

4.3.2 Intermittently, Configuration Updates Might Take 10 to 15 Minutes

When you make changes to a cluster of devices (Access Gateways, Identity Servers, or SSL VPNS servers), the status and the command status on the device page can show a pending status for up to 15 minutes. The pending command is usually a service provider refresh.

The problem cannot be reliably duplicated, but it seems to occur intermittently with the following types of updates, which trigger a Tomcat restart without prompting the user:

- Re-importing an Identity Server on a Windows machine.
- Making changes to the Hosts page on the Access Gateway Appliance.
- Making changes to the SSL Connector key store for the ESP-enabled SSL VPN server.

It also occurs intermittently with the following updates, which prompt the user to restart Tomcat:

- Making changes to the SSL Connection, Consumer, or Provider keystores of the Identity Server.
- Creating an Identity Server cluster
- When enabling or disabling an Identity Server protocol.
- When making timeout, encryption algorithm, or policy changes to the SSL VPN configuration.
- When making changes to the redirect option of the ESP-enabled SSL VPN server.
- When distributing JARs for a policy extension.

Until this issue is resolved, you should make changes for the options listed above when the impact of the delay is minimal.

For more information on this issue, see TID 7005580 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7005580&sliceId=2&docTypeID=DT_TID_1_1&dialogID=69826437&stateId=0%200%20133004086).

4.3.3 After an Upgrade, Certificates Cannot Be Imported

You might receive the following error message when trying to import a certificate on a Linux Administration Console:

```
Unable to load NPKIAPI - library could not be found
com.novell.security.japi.pki.NPKIAPI.loadLibrary(NPKIAPI.java:1684)
```

If you see this message, check the Tomcat configuration file located in the `/etc/opt/novell/tomcat5/` directory for the following lines:

```
LD_LIBRARY_PATH=/usr/lib:/opt/novell/lib

LD_LIBRARY_PATH=/var/opt/novell/iManager/nps/WEB-INF/bin/linux:/var/opt/novell/iManager/nps/WEB-INF/bin:/opt/novell/iManager/lib:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH
```

If these lines are missing, add them to the file, then restart Tomcat.

4.3.4 The Administration Console on Windows Server 2008 Runs Out of Memory

When the Administration Console is installed on a Windows Server 2008 R2 server and the server is running as a VMware image, the Administration Console crashes with an out of memory error.

To solve this issue, turn off the SNMP agent on eDirectory.

4.3.5 The Status of the Connection to the LDAP Server Replicas Is Unclear

In the Administration Console, the status of the connection to a user store indicates whether the Administration Console can connect to the server replica. If the Administration Console and the Identity Server are installed on the same machine, the status is quite accurate. If they are installed on different machines, the status does not indicate whether the Identity Server can connect to the server replica.

4.3.6 You Cannot Select the Install Path for a Windows Administration Console

When you install a Windows Administration Console, you are not prompted for a installation location. Because of the dependencies the Administration Console has with other components that require an installation location of `\Program Files\Novell`, this functionality cannot be offered.

4.3.7 Administration Console Fails to Install on VMWare ESX

The VMI kernels have issues with Novell Access Manager that can be worked around by using the information in TID 700224: "Installing Admin Console on VMWare ESX guest using the SLES "VMI" kernel fails" (http://www.novell.com/support/viewContent.do?externalId=7002224&sliceId=1).

4.3.8 A Delegated Administrator Temporarily Inherits All Rights If the Browser Is Not Closed After Creating the Delegated Administrator

If you create delegated administrators and allow them to use your machine and your browser session instead of closing the browser, the delegated administrator inherits all rights until the browser is closed.

After creating delegated administrators, make sure you close the browser if other users are going to be using your machine.

4.3.9 Slow Install

The Administration Console is slow to install on Windows and on Linux with 64-bit hardware. Please be patient. It can take up to an hour to install.

4.3.10 Liberty Attributes Are Not Visible

When you create a Form Fill or Identity Injection Policy and select Liberty attributes that are four levels deep, the attributes are sometimes not visible from an Internet Explorer browser. If this occurs on your machine, you need to use Firefox.

4.3.11 Installation Issue with Ports 389 and 636

Ports 389 and 636 need to be free. If the installation software prompts you to enter different ports because 389 and 636 are in use, the installation fails.

You need to free the ports, then install the Administration Console.

4.3.12 iManager Plug-Ins Fail to Install

There is a potential conflict during the installation of the iManager plug-ins when you have a version of the JRE installed on the machine. To fix this issue, you need to remove the JRE from the machine, install the Administration Console, then reinstall the version of the JRE you removed.

4.3.13 The Access Gateway Service Fails to Cache Events If the Audit Server Is Stopped

If the audit server is stopped in Administration Console, the Access Gateway Service fails to cache events. The audit events are not written to the Access Gateway Service cache or written to the audit log after the audit server is started.

```
(Error -634) The target server does not have a copy of what the source server
is requesting. Or, the source server has no objects that match the request and
has no referrals on which to search for the object.
```

To work around this issue, you need to wait for the SP2 IR1 release, which will fix this problem.

4.4 Identity Server Known Issues

- "You Cannot Select the Install Path for a Windows Identity Server" on page 16
- "After You Make a Change, the Cluster Fails to Return to a Green Status" on page 16
- "When You Attempt to Add a Windows Identity Server to a Cluster, the Action Fails with a Keystore Error" on page 16

- "After Migrating an Identity Server from Windows 2003 to Windows 2008, Personal Cards Cannot Be Used for Authentication" on page 17
- "When You Reinstall the Identity Server on a Windows Machine, Commands Remain in a Pending State" on page 17
- "X.509 Authentication with Other Methods" on page 17
- "HTML Frames Are Lost after a Redirect" on page 17
- "The SAML NMAS Method in Access Manager Is Incompatible with 64-bit eDirectory" on page 17
- "Problems with Session Timeout" on page 18
- "Auto Provision X509" on page 18

4.4.1 You Cannot Select the Install Path for a Windows Identity Server

When you install a Windows Identity Server, you are not prompted for an installation location. Because of the dependencies the Identity Server has with other components that require an installation location of `\Program Files\Novell`, this functionality cannot be offered.

4.4.2 After You Make a Change, the Cluster Fails to Return to a Green Status

After you make a change to a cluster and update the cluster members, if only one member displays a green status and the others remain in a pending state, you might have a corrupted datastore entry.

If you suspect that the cause is a corrupted datastore entry:

1. In the Administration Console, click *Auditing* > *Troubleshooting* > *Configuration*.
2. Scan to the *Devices with Corrupt Data Store Entries* section at the bottom of the page.
3. If you have any devices in this condition, click the *Repair* button to rewrite the invalid entries in the datastore.

For more information on the issue, see TID 7005800 (http://www.novell.com/support/viewContent.do?externalId=7005800&sliceId=2).

4.4.3 When You Attempt to Add a Windows Identity Server to a Cluster, the Action Fails with a Keystore Error

If the configuration datastore is corrupted, you cannot add members to a cluster.

If you suspect that the cause is a corrupted datastore entry:

1. In the Administration Console, click *Auditing* > *Troubleshooting* > *Configuration*.
2. Scan to the *Devices with Corrupt Data Store Entries* section at the bottom of the page.
3. If you have any devices in this condition, click the *Repair* button to rewrite the invalid entries in the datastore.

For more information on the issue, see TID 7005799 (http://www.novell.com/support/viewContent.do?externalId=7005799&sliceId=2)

4.4.4 After Migrating an Identity Server from Windows 2003 to Windows 2008, Personal Cards Cannot Be Used for Authentication

Windows CardSpace Personal Cards cannot be currently be used for authentication when the Identity Server is migrated from Windows Server 2003 to Windows Server 2008.

If you are using CardSpace, do not migrate your Windows Identity Servers to Windows Server 2008 until this issue has been fixed.

4.4.5 When You Reinstall the Identity Server on a Windows Machine, Commands Remain in a Pending State

If you install the Identity Server on a Windows Server 2003 machine that also contains the Administration Console, uninstall the Identity Server, then try to reinstall the Identity Server, some commands remain in a pending state.

To fix this issue, delete the pending commands.

4.4.6 X.509 Authentication with Other Methods

When you configure a method for X.509 authentication, you cannot select multiple methods and also enable the *Force browser restart on logout* option. When you have this type of configuration, users cannot authenticate and the following message is displayed:

```
Error: Your session has been logged out. Please Restart the Browser.
```

Users can successfully authenticate when you have the following configurations:

- You enable the *Force browser restart on logout* option and the only method selected is the X.509 method.
- You deselect the *Force browser restart on logout* option and you select multiple methods, including the X.509 method.

4.4.7 HTML Frames Are Lost after a Redirect

Frames on a protected resource page are lost under the following conditions:

- The Web page includes HMTL multiple frames.
- The user's session times out, the user is redirected to the login page, and the user successfully reauthenticates.
- The logout page has been customized to redirect the user to a Web page that contains multiple HTML frames.

For the workaround to fix this problem, see "HTML frames lost when being redirected to Access Manager login or logout pages" (http://www.novell.com/support/viewContent.do?externalId=7004020&sliceId=1).

4.4.8 The SAML NMAS Method in Access Manager Is Incompatible with 64-bit eDirectory

You cannot use 64-bit eDirectory with SecretStore as a remote SecretStore because a remote SecretStore requires a 64-bit SAML NMAS method, which is currently not available. If you want to use eDirectory 8.8 SP5 as a user store and a remote SecretStore, you need to use the 32-bit version.

4.4.9 Problems with Session Timeout

Some Web applications have security restrictions so that a normal redirect to the Identity Server for session renewal fails. The browser might appear of a hang, and JavaScript errors are often displayed. The frequency of this problem can be reduced by setting the Identity Server session timeout to a higher value.

4.4.10 Auto Provision X509

If there are already values in the LDAP attribute for X509 Subject Name mapping and you enable *Auto Provision X509* for the X509 authentication class, the LDAP attribute values are overwritten with the client certificate subject name.

4.5 General Access Gateway Issues

If you have configured the Access Gateway to protect an application with AJAX or other content that does not allow redirection, the application can fail. The failure occurs when the authentication timeout expires and the next request is redirected by the Access Gateway to the Identity Server for re-authentication. It occurs because AJAX does not allow redirection to a URL with a different scheme, name, or port. The browser can appear to hang or can display an application-generated error.

To reduce the likelihood of this problem, set the application's idle session timeout to a value less than the Access Manager authentication timeout. This allows the user to see the application’s warning for session expiration.

If the application does not have an idle session timeout, you can avoid the issue by configuring protected resources so that the content that is sensitive to redirection uses non-redirected login with basic authentication. Be aware that using basic authentication always comes with its own set of drawbacks, including the following:

- Base64-encoded credentials are placed in all HTTP requests to the authenticated realm.
- As soon as basic authentication is used for to a given realm, session timeout never occurs again because credentials are automatically supplied by the browser.

To set up this type of configuration, you need to configure two protected resources:

- Configure protected resource 1 with the paths of the normal HTML content and with a typical Secure Name/Password-Form authentication contract.
- Configure protected resource 2 with the paths of the redirect-sensitive content and with an authentication procedure with the following options:

  Contract: Set to the same contract as used by protected resource 1.

  Non-Redirected Login: Enabled.

  Realm: Any desired realm name.

  Redirect to Identity Server When No Authentication Header Is Provided: Disabled.

With this configuration, the user sees a form type login on the initial authentication to access the HTML content. If the browser is left idle and the authentication timeout expires, and an action is then performed that sends an AJAX or other non-redirectable request, the user is prompted for basic

authentication. After the user authenticates, the session should continue normally. Remember that after the user has entered the basic credentials for this realm, these credentials are re-used automatically and the user is not prompted for basic login again for this session.

4.6 Access Gateway Appliance Known Issues

This section discusses the known issues that apply to the current release of the Linux Access Gateway.

- "Gzip Has Been Disabled on the SLES 11 Version of the Access Gateway Appliance" on page 20
- "Passing Query Parameters to the Plogout Page Does Not Work As Expected" on page 20
- "NetStorage Only Partially Works with the Access Gateway Appliance" on page 20
- "After a Change, the Cluster Fails to Return to a Green Status" on page 20
- "The Time Zone Selection Page Displays Both Asia/Calcutta and Asia/Kolkata Options" on page 21
- "XML Validation Errors Occur When Applying Changes to the Access Gateway" on page 21
- "When a Browser Session Terminates, All Origin Web Server Session Cookies Are Not Terminated" on page 21
- "Lotus Domino WebAccess Server Cannot be Configured as a Path-Based Multi-Homing Service" on page 21
- "The Secondary Network Gateway Address Is Deleted If the Network Interface Is Restarted" on page 22
- "Reverting to an Earlier Snapshot of the Access Gateway Might Cause Multiple Crashes" on page 22
- "Incorrect Health Status Is Reported and the Listener Creation Fails If the Port Is Used by Another Process" on page 22
- "An Error Occurs When a User Tries to Download Access Manager Logs through Internet Explorer 7 and 8" on page 22
- "The Enforce 128-Bit Encryption between Access Gateway and Web Server Option Is Not Functional in this Release" on page 23
- "Unable to Connect to Access Gateway with Low and Medium Ciphers" on page 23
- "Multiple Sessions Are Created When You Use OpenOffice Tools with a WebDAV Connection" on page 23
- "Cookie and Session Issues with Nautilus File Manager and WebDAV Connections" on page 23
- "On a New Install, the Secure Logging Server Is Not Configured Correctly" on page 23
- "Communication Problems between the Novell Audit Client and the Audit Server Might Crash the Linux Access Gateway" on page 24
- "Installation on VMWare ESX Works in Text Mode Only" on page 24
- "Rewriter On and Off Flags Are Not Effective in a Character Profile" on page 24
- "Issues with the Audit Server While Importing an Access Gateway Configuration" on page 24
- "The Rewriter Does Not Handle the [oa] Option in Search and Replace" on page 24
- "Exclude Alias DNS with Scheme Option Does Not Work" on page 25

- "Form Fill Auto Submit Issue" on page 25
- "Form Fill Does Not Work if the Web Page Contains an Apostrophe" on page 25
- "Form Fill Fails If the Web Server Does Not Send the Content Type" on page 25
- "Form Fill Policy and the Refresh Data Every Option Restrictions" on page 25
- "Manual Deletion of the laghttpheaders and lagsoapmessages Log Files Causes a Linux Access Gateway Crash" on page 25
- "The Access Gateway Does Not Validate the Scheme" on page 25
- "Network Installation of a SLES 11 Access Gateway Results in Signature Error" on page 25
- "Browser Spins on Login in the Access Gateway Cluster Setup" on page 26

4.6.1 Gzip Has Been Disabled on the SLES 11 Version of the Access Gateway Appliance

When Gzip is enabled and the file is chunked encoded, users cannot download the file from a Web server protected by the SLES 11 version of the Access Gateway Appliance.

To work around this issue, Gzip is disabled when you install or migrate to the SLES 11 version of the Access Gateway Appliance. This issue will be fixed in SP2 IR1.

4.6.2 Passing Query Parameters to the Plogout Page Does Not Work As Expected

When you pass query string parameters to the `/nesp/app/plogout` page, they are not being passed to the `logoutSuccess.jsp` file as explained in "Calling Different Logout Pages" (http://www.novell.com/documentation/novellaccessmanager31/accessgatehelp/data/b6but9k.html#bocglgp) in the *Access Gateway Guide* (http://www.novell.com/documentation/novellaccessmanager31/accessgatehelp/data/bookinfo.html). This causes custom logout pages to fail.

To work around this issue, see TID 7006449 (http://www.novell.com/support/viewContent.do?externalId=7006449&sliceId=2).

4.6.3 NetStorage Only Partially Works with the Access Gateway Appliance

Browser connections to NetStorage can be used. WebDAV connections to NetStorage do not work.

4.6.4 After a Change, the Cluster Fails to Return to a Green Status

After you make a change to the cluster and update the cluster members, only one member displays a green status and the others remain in a pending state.

If you suspect that the cause is a corrupted datastore entry:

1. In the Administration Console, click *Auditing* > *Troubleshooting* > *Configuration*.
2. Scan to the *Devices with Corrupt Data Store Entries* section at the bottom of the page.
3. If you have any devices in this condition, click the *Repair* button to rewrite the invalid entries in the datastore.

For more information on the issue, see TID 7005800 (http://www.novell.com/support/viewContent.do?externalId=7005800&sliceId=2)

4.6.5 The Time Zone Selection Page Displays Both Asia/Calcutta and Asia/Kolkata Options

When you install the Access Gateway Appliance, the *Asia/Calcutta* and *Asia/Kolkata* options are both displayed. Select one of the options, depending on your operating software:

- If you are using SLES 9, select *Asia/Calcutta*.
- If you are using SLES 11, select *Asia/Kolkata*.

4.6.6 XML Validation Errors Occur When Applying Changes to the Access Gateway

After upgrading, you might see XML validation errors when you apply configuration changes to the Access Gateway. If you see an XML validation error, check the `/opt/volera/roma/logs/app_sc.0.log` to verify if the following message is present:

```
validateXML(E)org.jdom.input.JDOMParseException: Error on line 6488: cvc-id.1:
There is no ID/IDREF binding for IDREF 'Alert_<string>
```

NOTE: <*string*> can be any alert message. For example, `Alert_icpparentdown`.

If this message is in the file:

1. In the Administration Console, click *Devices* > *Access Gateways* > *Edit*.
2. Cancel all the configuration changes.
3. Select *Alerts*, the delete all the alert profiles.
4. Apply the configuration changes.
5. Select *Alerts*, then create new alert profiles.
6. Apply the configuration changes.

4.6.7 When a Browser Session Terminates, All Origin Web Server Session Cookies Are Not Terminated

If a browser session with an Access Gateway terminates, all origin Web server HTTP session cookies are not terminated.

For example, if two users (User-A and User-B) use the same browser client to access a protected resource, then User-A authenticates to a protected resource, the origin server of the protected resource establishes a session with browser client using HTTP session cookies.

If User-A logs out of the Access Gateway by using the logout URL or because of an idle timeout, the session cookie from the origin Web server remains intact. User-B can then authenticate to Access Gateway, and resume the session to the origin Web server from User-A.

To work around this issue, see *Clearing Novell Access Manager Application Sessions* (http://www.novell.com/communities/node/6731)

4.6.8 Lotus Domino WebAccess Server Cannot be Configured as a Path-Based Multi-Homing Service

You cannot configure Lotus Domino WebAccess Server as a path-based multi-homing service. However, you can configure it as a domain-based multi-homing service.

4.6.9 The Secondary Network Gateway Address Is Deleted If the Network Interface Is Restarted

The secondary gateway IP address for the Access Gateway is deleted when the network interfaces are restarted.

You must add the network gateway address again by using the following command:

```
route add -net <IP address> netmask <netmask> gw <gateway IP>
```

4.6.10 Reverting to an Earlier Snapshot of the Access Gateway Might Cause Multiple Crashes

If you are using a VM environment such as ESXi 4.0, reverting to an earlier snapshot of the Access Gateway might result in multiple crashes.

To work around the issue, clear the cache and restart novell-vmc as follows, after reverting the snapshot:

```
rm /var/novell/.~newInstall
/etc/init.d/novell-vmc restart
```

4.6.11 Incorrect Health Status Is Reported and the Listener Creation Fails If the Port Is Used by Another Process

The Access Gateway Appliance health is reported as green even if the listener creation fails. This occurs because the service creation status of the Access Gateway Appliance reflects the status of the open port. When the port is used by any other process, the Access Gateway cannot distinguish between its own service and the other process.

For example, when the SSL VPN server is installed with the Access Gateway, and port 443 is used by OpenVPN, the service creation fails if you try to create an Access Gateway proxy service that uses port 443,. However, because the health check is looking only for the open port 443, the status is displayed as healthy.

To work around this issue, check netstat after creating the service to confirm if the ics_dyn process of the Access Gateway is running on the corresponding port.

4.6.12 An Error Occurs When a User Tries to Download Access Manager Logs through Internet Explorer 7 and 8

When a user tries to download Access Manager logs by using either Internet Explorer 7 or 8, the `Failed to execute command` error is displayed.

To work around this issue:

1. In the browser, select *Tools* > *Internet Options* > *Security*.
2. Click *Trusted Sites*.
3. Click *Custom Level*.
4. Set the *Downloads* > *Automatic prompting for file downloads* option to Enable.
5. Click *OK*.

4.6.13 The Enforce 128-Bit Encryption between Access Gateway and Web Server Option Is Not Functional in this Release

The *Enforce 128-Bit Encryption between Access Gateway and Web Server* option in the *Devices > Access Gateways > Edit > [Name of Reverse Proxy] > > TCP Listen Options* page is not functional for this release.

4.6.14 Unable to Connect to Access Gateway with Low and Medium Ciphers

The browser is unable to connect to Access Gateway when the *Enforce 128-Bit Encryption between Browser and Access Gateway* option is enabled with low and medium ciphers.

4.6.15 Multiple Sessions Are Created When You Use OpenOffice Tools with a WebDAV Connection

When you use OpenOffice Writer and other tools over WebDAV connections, cookies that are set by the server are not included in requests from the OpenOffice client. As a result, each WebDAV request from the client creates a new session. If you have limited user sessions, the limit can be quickly reached, which results in files left in a locked state or with IO errors.

To solve this problem, do not limit user sessions (*Devices > Identity Servers > Edit*) when users are using OpenOffice tools over a WebDAV connection.

4.6.16 Cookie and Session Issues with Nautilus File Manager and WebDAV Connections

The Nautilus File Manager v2.12.2 in SUSE Linux Enterprise Desktop (SLED) 10 SP1 and SP2 does not include cookies when making WebDAV requests. As a result, when the WebDAV server is accessed through a reverse proxy on the Access Gateway, a new user session is created at the proxy for every WebDAV request sent from Nautilus. A simple file open can result in the creation of multiple sessions.

To solve this problem, do not limit user sessions (*Devices > Identity Servers > Edit*) when users are making WebDAV requests with the Nautilus File Manager.

4.6.17 On a New Install, the Secure Logging Server Is Not Configured Correctly

The `logevent.conf` file, which controls the configuration for the secure logging server, initializes the address of the logging server to 127.0.0.1 instead of the IP address specified in the Administration Console. By default, this address is the IP address of the Administration Console, but it can be configured for an external auditing server such as a Novell Sentinel server.

To fix the problem:

1. Log in to the Access Gateway as `root`.
2. Change to the `/etc` directory
3. Open the `logevent.conf` file and find the following line:

   ```
   LogHost=127.0.0.1
   ```
4. Change the IP address to the address of your secure logging server.
5. Reboot the Access Gateway.

4.6.18 Communication Problems between the Novell Audit Client and the Audit Server Might Crash the Linux Access Gateway

If you have configured your Access Manager system to use a Novell Sentinel or Novell Audit server for auditing, the Novell Audit client sometimes disconnects from the auditing server. This usually happens when communication problems exist on the network. When this happens, the Linux Access Gateway might crash. This issue can also prevent the successful completion of any Linux Access Gateway configuration changes.

To solve this problem, make sure that no communication problems exist between the auditing client on the Linux Access Gateway and the auditing server.

4.6.19 Installation on VMWare ESX Works in Text Mode Only

You must use the text-mode installation for the VMWare ESX platform. The GUI mode for the installation of Linux Access Gateway fails and falls back to the text mode on VMWare ESX.

4.6.20 Rewriter On and Off Flags Are Not Effective in a Character Profile

The NOVELL_REWRITER_ON and NOVELL_REWRITER_OFF tags are not effective in the Access Gateway character profile.

4.6.21 Issues with the Audit Server While Importing an Access Gateway Configuration

When you importing an Access Gateway configuration, the imported configuration might contain an audit server IP address that is different from the audit server IP address that was configured in the Administration Console. Updating the Access Gateway configuration does not correct this address problem. As long as the addresses differ, the Access Gateway can hang during subsequent updates or restarts because the Novell Audit Agent of the Access Gateway cannot connect to its configured audit server.

You must force the Linux Access Gateway to change its Audit server settings.

1. In the Administration Console, click *Access Manager > Auditing*.
2. Specify a different IP address for the Secure Logging Server, then click *OK*.
3. Click *Auditing*, specify the correct IP address for the Secure Logging Server, then click *OK*.
4. Update the Linux Access Gateway.
5. Reboot every Access Manager machine, starting with the Administration Console.

   or

   If you have already configured the other Access Manager machines to use the correct IP address of the Secure Logging Server, rebooting the Access Gateway should be sufficient.

4.6.22 The Rewriter Does Not Handle the [oa] Option in Search and Replace

The character rewriter profile does not support the [oa] option to search and replace plain words and strings.

4.6.23 Exclude Alias DNS with Scheme Option Does Not Work

The *Exclude Alias DNS name with Scheme* option does not work. For example, if you add https://www.mygroup.com, it is not excluded from the list. You must provide only the DNS name, such as www.mygroup.com.

4.6.24 Form Fill Auto Submit Issue

A Form Fill auto-submit fails when an input field in an HTML page contains `name="submit"`.

4.6.25 Form Fill Does Not Work if the Web Page Contains an Apostrophe

The Linux Access Gateway Form Fill does not work if the Web page contains the apostrophe character.

4.6.26 Form Fill Fails If the Web Server Does Not Send the Content Type

Form Fill does not process the page if the Web server does not send the content type. Form Fill processes the following content types:

```
"text/html"
"text/xml"
"text/css"
"text/javascript”
"application/javascript"
"application/x-javascript"
```

4.6.27 Form Fill Policy and the Refresh Data Every Option Restrictions

In a Form Fill policy, you can only set the *Refresh Data Every* option to Request or Session. If you select a time to live, it is the same as selecting Request.

4.6.28 Manual Deletion of the laghttpheaders and lagsoapmessages Log Files Causes a Linux Access Gateway Crash

If you have enabled the debug level of logging for the `laghttpheaders` and `lagsoapmessages` log files, manual deletion of these log files causes the Linux Access Gateway to crash.

To work around this problem, restart the Linux Access Gateway after you manually delete the log files.

4.6.29 The Access Gateway Does Not Validate the Scheme

The Access Gateway does not validate the scheme. You must use the additional DNS List for scheme validation.

4.6.30 Network Installation of a SLES 11 Access Gateway Results in Signature Error

To avoid a signature error for the network mode of installation on SLES11, use the Access Gateway Appliance ISO CD rather than a bootable CD.

4.6.31 Browser Spins on Login in the Access Gateway Cluster Setup

When a browser is closed after accessing a protected resource and the Identity Server login page is displayed, subsequent access to a resource by using the browser creates a loop.

To work around this problem, clear the browser cookies or close the browser instance and try again..

4.7 Access Gateway Service Known Issues

- "The Access Gateway Service Has Not Been Thoroughly Tested Behind an SSL Terminator" on page 26
- "The Log Profile Page Provides Incorrect Information for the Backup Files Option" on page 26
- "The Advanced Log Level Option Displays Incorrectly in Internet Explorer 7 and 8" on page 26
- "Cannot Delete an Access Gateway Service" on page 26
- "When the Audit Server Stops and Starts, the Audit Server Does Not Receive All Cached Events" on page 27
- "If the Form Has an Empty Action Element, the Access Gateway Service Fails to Fill In the Action Element" on page 27
- "Enabling Password Management Support Might Cause Authentication Errors" on page 27

4.7.1 The Access Gateway Service Has Not Been Thoroughly Tested Behind an SSL Terminator

If you place an SSL terminator in front of the Access Gateway Service and enable the *Behind Third Party SSL Terminator* option, some URLs might not be rewritten correctly.

If you try this configuration, report any problems to Novell Support.

4.7.2 The Log Profile Page Provides Incorrect Information for the Backup Files Option

When you configure a log profile (click *Devices* > *Access Gateways* > *Edit* > *Logging* > *[Profile Name]*) and set a value for the *Maximum Backup Files* option, a 0 (zero) value indicates that you do not want any backup files created and a blank value indicates that you want one backup file created. Ignore the message on the page about what these values mean.

4.7.3 The Advanced Log Level Option Displays Incorrectly in Internet Explorer 7 and 8

The *Advanced Log Level* option (click *Access Gateways* > *Edit* > *Logging* > *Log Filters* > *[Filter Name]*) does not appear to be a link, if you are using the Internet Explorer 7 or 8 to access the Administration Console. However, you can still click the option to display the configuration page.

4.7.4 Cannot Delete an Access Gateway Service

If you have an unconfigured Identity Server and you try to delete an Access Gateway Service from the Administration Console, the deletion fails and throws an exception.

To delete the Access Gateway Service, either delete the Identity Server first or configure the Identity Server.

4.7.5 When the Audit Server Stops and Starts, the Audit Server Does Not Receive All Cached Events

When the audit server stops, the events are supposed to be cached until the audit server comes back online. When the audit server is back online, the cached events are supposed to be sent to the audit server. This functionality is not working reliably for the Access Gateway Service.

4.7.6 If the Form Has an Empty Action Element, the Access Gateway Service Fails to Fill In the Action Element

The Access Gateway Service does not correctly process the following type of action element in a form:

```
<FORM name="logonForm" method="post" action="" >
```

To work around this issue, create a custom rewriter profile for the form to fill the action element with a valid value or wait for SP2 IR1.

4.7.7 Enabling Password Management Support Might Cause Authentication Errors

On the Linux Access Gateway Appliance, the `/var/novell/.PasswordMgmt` touch file is required to support the Identity Manager Password Management feature. With this configuration in a cluster deployed behind an L4 switch, users might occasionally report a failure to authenticate with an error indicating that the browser detected infinite redirects. This happens when session stickiness fails at the L4 device for /nesp service URLs.

To work around this issue, you should clear the browser cookies, then restart the browser before accessing the resource again.

4.8 SSL VPN Known Issues

The following sections divide the known issues into general issues that apply to both the Enterprise mode and Kiosk mode and issues that apply only to the Enterprise mode and only to the Kiosk mode:

- "General SSL VPN Issues" on page 27
- "Kiosk Mode Issues" on page 29
- "Enterprise Mode Issues" on page 30

4.8.1 General SSL VPN Issues

- "Full Tunneling Has Limitations with the Mac OS" on page 28
- "The SSL VPN Server Is in a Pending State" on page 28
- "After the Upgrade, the SSL VPN Connection Fails with a Null Pointer Exception Error" on page 28
- "The SSL VPN Statistics Displayed in the Administration Console Are Not in Order" on page 28
- "HTTP Applications Cannot Be Accessed When an SSL VPN Connection Is Made through the Forward Proxy" on page 28

- "An ESP-Enabled SSL VPN Is Imported into the Administration Console as a Traditional SSL VPN" on page 28
- "SSL VPN Connection Goes Into a Non-Responsive Mode If a 64-Bit Internet Explorer Is Used with a 64-Bit Windows 7, Vista, or XP Client" on page 29

4.8.1.1 Full Tunneling Has Limitations with the Mac OS

When full tunneling is enabled in the Mac OS, traffic to resources in a user's local subnet goes outside the tunnel.

4.8.1.2 The SSL VPN Server Is in a Pending State

When the Administration Console, Identity Server, and SSL VPN Server are installed on the same machine, the SSL VPN server sometimes gets into a pending state even when all of its commands have been successful.

To work around this problem:

1. In the Administration Console, click *Devices* > *SSL VPNs*.
2. Click the *Commands* link.
3. Select all the commands, then click *Delete* > *Close*.
4. If the device is still in a pending state, click *Auditing* > *Troubleshooting*.
5. In the *Device Pending with No Commands* section, select the SSL VPN server and remove the pending state.

4.8.1.3 After the Upgrade, the SSL VPN Connection Fails with a Null Pointer Exception Error

After the upgrade, the browser returns a null pointer exception error while trying to establish the SSL VPN connection. This issue occurs because the schema extension failed for the nidsACTimeout and nidsACRefreshRate attributes.

4.8.1.4 The SSL VPN Statistics Displayed in the Administration Console Are Not in Order

The SSL VPN connection statistics that are displayed in the Administration Console are not in any order.

4.8.1.5 HTTP Applications Cannot Be Accessed When an SSL VPN Connection Is Made through the Forward Proxy

If a client uses an HTTP forward proxy to establish the SSL VPN session, no HTTP application can be accessed over this SSL VPN connection because the browser is configured to use the forward proxy server for HTTP requests.

4.8.1.6 An ESP-Enabled SSL VPN Is Imported into the Administration Console as a Traditional SSL VPN

If you uninstall and reinstall the ESP-enabled SSL VPN on the same machine, the server is imported into the Administration Console as a traditional SSL VPN.

To work around this issue, manually delete the Embedded Service Provider entry from the Appliance Container by using the LDAP browser, then try installing the server again.

4.8.1.7 SSL VPN Connection Goes Into a Non-Responsive Mode If a 64-Bit Internet Explorer Is Used with a 64-Bit Windows 7, Vista, or XP Client

When a user tries to connect to SSL VPN in either Kiosk mode or Enterprise mode by using the 64-bit Internet Explorer on a 64-bit Windows 7, Vista, or XP client, the connection hangs and the following error message is displayed:

```
You are seeing this message because ActiveX control is not installed in your
Internet Explorer. To establish the Novell SSL VPN connection, do one of the
following:
```

- `If you see an information bar at the top, click the bar. Click Allow Blocked Content, then click Yes.`
- `If you are a non-administrator or non-root use of your machine, please click the following link: Click here.`
- `Open a new browser window and type the following URL:http(s):<DNS-Name>/sslvpn/login?forcejre=true`

This issue occurs because the 64-bit Internet Explorer does not load the SSL VPN ActiveX component.To work around the issue, do one of the following:

- Use the 32-bit Internet Explorer that is installed by default.
- Download and install the 64-bit JRE, then use the following URL to load the applet component:

  `https:<DNS-Name>/sslvpn/login?forcejre`

4.8.2 Kiosk Mode Issues

- "SSL VPN Data Transfer Fails When Using Internet Explorer 8 on the 32-bit Windows 7 Client" on page 29
- "Firefox Goes into a Non-Responsive Mode in Multiple Windows Kiosk Mode Clients" on page 29
- "HTTP Data transfer fails on a SLED 10 64-bit with 32-Bit Browser" on page 30
- "Unable to Access Protected HTTP Applications on Intel Mac" on page 30
- "No Kiosk Mode Support for 64-Bit Windows Clients" on page 30
- "Domain Name Search Does Not Work in Macintosh" on page 30
- "Active Mode FTP Is Not Supported in Kiosk Mode" on page 30

4.8.2.1 SSL VPN Data Transfer Fails When Using Internet Explorer 8 on the 32-bit Windows 7 Client

On a Windows 7 32-bit client machine, you cannot use the Internet Explorer 8 browser to access HTTP traffic to protected Web servers in Kiosk mode. You can use Internet Explorer 8 to establish the connection to the SSL VPN server, and then use the Mozilla Firefox browser to access HTTP data in the protected Web server.

4.8.2.2 Firefox Goes into a Non-Responsive Mode in Multiple Windows Kiosk Mode Clients

Firefox randomly goes into a non-responsive mode in multiple clients when running in Windows Kiosk mode.

4.8.2.3 HTTP Data transfer fails on a SLED 10 64-bit with 32-Bit Browser

In a SLED 10 64-bit client, a 32-bit instance of Firefox is installed by default, which is not a supported scenario for SSL VPN. So, if a user tries to connect to SSL VPN from a SLED 10 64-bit client machine with a 32-bit browser, the HTTP data transfer fails. To workaround this issue, make sure you install the 64-bit Firefox browser.

4.8.2.4 Unable to Access Protected HTTP Applications on Intel Mac

Using Intel Mac to access protected HTTP applications is not supported.

4.8.2.5 No Kiosk Mode Support for 64-Bit Windows Clients

If you use a 64-bit Windows machine, you can access SSL VPN only in Enterprise mode. Accessing SSL VPN in Kiosk mode is not supported.

4.8.2.6 Domain Name Search Does Not Work in Macintosh

A domain name search does not work in the Kiosk mode in Macintosh.

4.8.2.7 Active Mode FTP Is Not Supported in Kiosk Mode

In SSL VPN Kiosk mode, the active mode of FTP is not supported.

4.8.3 Enterprise Mode Issues

- "Jgroups Does Not Perform a Complete State Transfer If One of the Cluster Nodes Fails to Come Up after Upgrading." on page 30
- "Full Tunneling with a Forward Proxy Enabled Is Not Supported for Web Client Applications" on page 30
- "Tunnel Logs Display Full Tunnel Information in Split Tunnel Mode" on page 30
- "No Error Message Is Displayed for an Invalid Credential Entry on Windows 2000 Machines" on page 31

4.8.3.1 Jgroups Does Not Perform a Complete State Transfer If One of the Cluster Nodes Fails to Come Up after Upgrading.

In an SSL VPN cluster, if one of the cluster nodes fails to come up after you upgrade the SSL VPN servers, stop all the services in all the cluster nodes and restart the services in all the nodes.

4.8.3.2 Full Tunneling with a Forward Proxy Enabled Is Not Supported for Web Client Applications

Full tunneling with a forward proxy on a client network is not supported for Web client applications. This is because, in Enterprise Mode, a route is added in order to enable forward proxy. Any Web clients from that workstation can use this route to bypass the SSL VPN server by using the forward proxy.

4.8.3.3 Tunnel Logs Display Full Tunnel Information in Split Tunnel Mode

If client debug logs are enabled, tunnel logs displayed in the Enterprise mode might contain information for full tunneling, even though only split tunneling is enabled for the user.

4.8.3.4 No Error Message Is Displayed for an Invalid Credential Entry on Windows 2000 Machines

On Windows 2000 machines, if a non-admin user tries to establish an SSL VPN connection in the Enterprise mode and specifies the wrong credentials for the admin user, no error messages are displayed. However, the user is denied access after trying to establish the connection.

4.9 J2EE Agent Known Issues

The following sections discuss the known issues in J2EE agents for JBoss, WebSphere, and WebLogic

- "Authentication Error Is Displayed When a User Tries to Access Resources" on page 31
- "Base URL and SOAP URL Cannot Be Configured with Port 65535" on page 31

4.9.1 Authentication Error Is Displayed When a User Tries to Access Resources

In WebLogic J2EE agents, when users who do not have sufficient rights try to access resources for which they have been denied authorization, the following message is displayed:

```
There was a problem with your authentication
```

The required Web page is displayed if you refresh the page once.

4.9.2 Base URL and SOAP URL Cannot Be Configured with Port 65535

You cannot configure a base or SOAP URL for the Novell Access Manager J2EE Agent with port 65535.

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.