AUTHORIZED DOCUMENTATION

SSL VPN User Guide

Novell
Access Manager

3.1 SP2

November 16, 2010

www.novell.com

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.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

Third-Party Materials

Contents

About This Guide

This document is intended to help you understand and use the SSL VPN user portal. It contains the following information:

- Chapter 1, “Overview of SSL VPN,” on page 9
- Chapter 2, “Accessing SSL VPN in Kiosk Mode,” on page 13
- Chapter 3, “Accessing SSL VPN in Enterprise Mode,” on page 17
- Chapter 4, “Accessing Published Citrix Applications through SSL VPN,” on page 23
- Chapter 5, “Using SSL VPN,” on page 25
- Appendix B, “Troubleshooting SSL VPN,” on page 51
- Appendix A, “Error Messages,” on page 33

Audience

This guide is intended for Novell Access Manager SSL VPN end users.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *SSL VPN User Guide*, visit the Novell Access Manager Documentation Web site (http://www.novell.com/documentation/novellaccessmanager31).

Additional Documentation

- *Novell Access Manager 3.1 SP2 SSL VPN Server Guide*
- *Novell Access Manager 3.1 SP2 Installation Guide*
- *Novell Access Manager 3.1 SP2 Setup Guide*
- *Novell Access Manager 3.1 SP2 Administration Console Guide*
- *Novell Access Manager 3.1 SP2 Identity Server Guide*
- *Novell Access Manager 3.1 SP2 Access Gateway Guide*

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

Overview of SSL VPN

1

The Novell Access Manager SSL VPN allows you to use a Web browser to access corporate resources securely from a remote site. It uses a Secure Socket Layer (SSL) with a virtual private connection (VPN). It is a clientless solution, and it eliminates the need to install or configure a VPN client on your desktop or laptop. This gives you the flexibility to access the corporate resources from a laptop, a home computer, or a Web browsing kiosk.

When you access the SSL VPN server through a Web browser, a Java applet or an ActiveX control is installed on your machine after the successful connection. This encrypts the traffic passing through the tunnel and sends it to the SSL VPN server.

This section describes the following features of SSL VPN:

- Section 1.1, "Access Modes," on page 9
- Section 1.2, "Client Machine Requirements," on page 10

1.1 Access Modes

The Novell SSL VPN uses both clientless and thin-client access methods. The clientless method is called the Kiosk mode SSL VPN and the thin-client method is called the Enterprise mode SSL VPN.

- Section 1.1.1, "Kiosk Mode," on page 9
- Section 1.1.2, "Enterprise Mode," on page 10

1.1.1 Kiosk Mode

Kiosk mode is the usual choice for computers not controlled by the organization, such as home computers and computers in Web-browsing kiosks. When you connect to SSL VPN in Kiosk mode, only a limited set of applications are enabled for SSL.

Applications that were opened before the SSL VPN connection was established are not enabled for SSL. You must manually enable the applications that were opened before the SSL VPN connection. For more information, see Section 5.5, "Enabling Applications for SSL," on page 29.

You are connected to SSL VPN in Kiosk mode if:

- You do not have administrator rights or `root` privileges to the workstation, and you do not know the credentials of the administrator or `root` user of the machine.
- You have administrator rights or `root` privileges to the workstation, but you are required by the system administrator to connect in Kiosk mode only.

For more information on using the Kiosk mode, see Chapter 2, "Accessing SSL VPN in Kiosk Mode," on page 13.

1.1.2 Enterprise Mode

The Enterprise mode is the usual choice for computers that are controlled by the organization, such as notebooks provided by the organization for employees.When you connect to SSL VPN in Enterprise mode, all applications are enabled for SSL, regardless of whether they were opened before or after connecting to the SSL VPN. This includes your desktop applications and toolbar applications.

You are connected to SSL VPN in Enterprise mode if:

- You are the administrator or `root` user of a workstation, if the system administrator has not required you to connect in Kiosk mode only.
- You are not the administrator or `root` user of a workstation, but you know the credentials of the administrator or `root` user.
- If someone with administrator access has preinstalled the SSL VPN thin-client components on your machine, you can connect to SSL VPN in Enterprise mode. For more information on preinstalling the thin-client components, see "Preinstalling the SSL VPN Client Components" in the *Novell Access Manager 3.1 SP2 SSL VPN Server GuideNovell Access Manager 3.1 SP2 SSL VPN Server Guide*.

For more information on using Enterprise mode, see Chapter 3, "Accessing SSL VPN in Enterprise Mode," on page 17.

1.2 Client Machine Requirements

This section explains the operating software and browser requirements for the client machine, in order to access the SSL VPN user portal.

- Section 1.2.1, "Linux Requirements," on page 10
- Section 1.2.2, "Macintosh Requirements," on page 11
- Section 1.2.3, "Windows Requirements," on page 11

1.2.1 Linux Requirements

When you access the SSL VPN user portal in the Linux a Java applet is downloaded to the client machine. The following table lists the supported versions of operating software and browsers for the Linux environment:

Table 1-1 *Supported Linux Configurations*

Component	Requirement
Operating Systems	SUSE Linux Enterprise Desktop (SLED) 10.0 and SLED 11 are supported for 32-bit and 64-bit platforms.
OpenSSL	0.9.7 or higher. If your OpenSSL version is higher than 0.9.7, you must install an OpenSSL 0.9.7 compatible library.
Shells	bash
	xterm

Component	Requirement
Browser	Mozilla Firefox 2.x, 3.0.X and 3.x
	Java and JavaScript enabled
Sun JRE	1.5.0_11 or higher

NOTE: If you are using SLED 11.0 64-bit client, make sure that you have the latest JRE installed on your machine.

1.2.2 Macintosh Requirements

When you access the SSL VPN user portal in the Macintosh environment, a Java applet is downloaded to the client machine. The following table lists the supported versions of operating software and browsers in the Mac environment:

Table 1-2 *Supported Macintosh Configurations*

Component	Requirement
Operating System	Mac PPC 10.4 Tiger
	Mac Intel 10.5 Leopard
	Mac OSX 10.6 Snow Leopard
OpenSSL	0.9.7
Shell	bash
Browser	Mac Safari 2.0.4 Build 412 or higher
	Firefox 2.x, 3.0.X or 3.5
	Java and JavaScript enabled
Sun JRE	1.5.0_11 or higher

NOTE: GroupWise 7.0 and 8.0 does not work when SSL VPN Kiosk mode is running on Macintosh Tiger OS.

1.2.3 Windows Requirements

When you access the SSL VPN user portal in the Windows environment, an ActiveX control is downloaded to the client machine. If you want to download the Java applet on your machine instead of the ActiveX control, the administrator needs to perform some server-side configurations. For more information, refer to "Configuring SSL VPN to Download the Java Applet on Internet Explorer" in the *Novell Access Manager 3.1 SP2 SSL VPN Server Guide*.

The following table lists the supported versions of operating software and browsers in the Windows environment:

Table 1-3 *Supported Windows Configurations*

Component	Requirement
Operating System	Windows XP SP2/SP3 - 32-bit and 64-bit Windows Vista - 32-bit and 64-bit Windows 7 32-bit and 64-bit **NOTE:** Windows 64-bit is supported only in Enterprise Mode
Browser	Internet Explorer 7.0 and 8.0 Mozilla Firefox 2.x, 3.0.x, 3.5, 3.6 x **NOTE:** Do not use Windows Explorer to run SSL VPN.
Sun JRE	1.4.1 or higher **NOTE:** If you are using Firefox 3.6, you must have Java SE 6 update 10 or higher.

Accessing SSL VPN in Kiosk Mode

2

Kiosk mode is the usual choice for computers not controlled by the organization, such as home computers and computers in Web-browsing kiosks.

In the Kiosk mode of SSL VPN, only those applications that are opened after connecting to the SSL VPN server are enabled for SSL. You must manually add the applications that were opened before connecting to SSL VPN in order to enable them for SSL. For more information on manually adding the applications, see Section 5.5, “Enabling Applications for SSL,” on page 29.

This section has the following information on accessing SSL VPN in Kiosk mode:

- Section 2.1, “Accessing the SSL VPN User Portal,” on page 13
- Section 2.2, “Switching from Kiosk Mode to Enterprise Mode,” on page 15

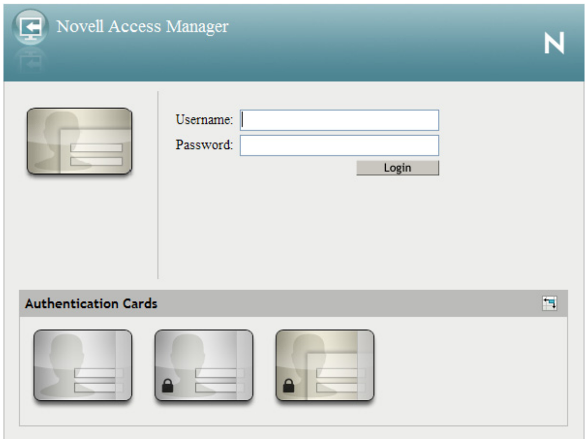
For information on connecting to the SSL VPN user portal in Enterprise mode, see Chapter 3, “Accessing SSL VPN in Enterprise Mode,” on page 17.

2.1 Accessing the SSL VPN User Portal

1 Log in to the SSL VPN server by using the following URL:

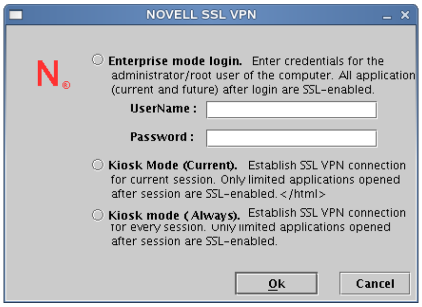
```
https://<dns_name>/sslvpn/login
```

Replace <*dns_name*> with the DNS name of your SSL VPN server.



2 On the Access Manager page, specify the username and password, then click *OK*.

3 Click *Yes* in the warning message to accept and download the signed ActiveX control or Java applet required for the SSL VPN client. The SSL VPN mode selection dialog box is displayed.



NOVELL SSL VPN

○ **Enterprise mode login.** Enter credentials for the administrator/root user of the computer. All application (current and future) after login are SSL-enabled.

UserName :

Password :

○ **Kiosk Mode (Current).** Establish SSL VPN connection for current session. Only limited applications opened after session are SSL-enabled. </html>

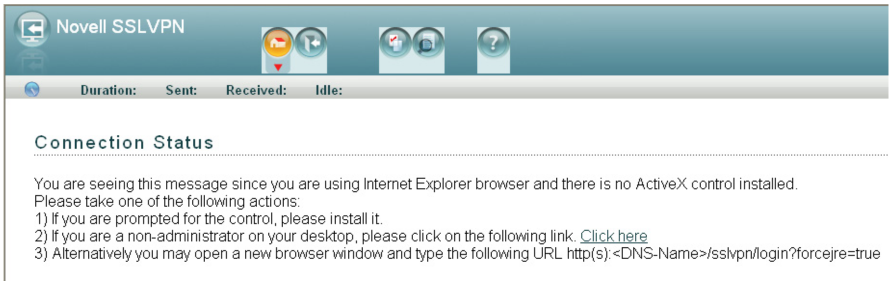
○ **Kiosk mode (Always).** Establish SSL VPN connection for every session. Only limited applications opened after session are SSL-enabled.

4 Do one of the following:

- Select *Kiosk Mode (Current)* to connect to SSL VPN in Kiosk mode for the current session. When you select this option, you are prompted to enter the username and password for the administrator user the next time you log in.
- Click *Kiosk Mode (Always)* to always connect to SSL VPN in Kiosk mode. When you select this option, you are connected to SSL VPN in Kiosk mode in the subsequent logins without being prompted to select the mode. If you want to connect to SSL VPN in Enterprise mode in one of the subsequent connections, you can do so. For more information, see Section 2.2, "Switching from Kiosk Mode to Enterprise Mode," on page 15.

5 Click *OK*. If you click *Cancel* you are connected to SSL VPN in Kiosk mode for the current session.

6 (Conditional) If you are a non-admin user and if you are using Internet Explorer to connect to SSL VPN, click the link displayed in option 2 of the following screen to proceed with the SSL VPN connection.



Connection Status

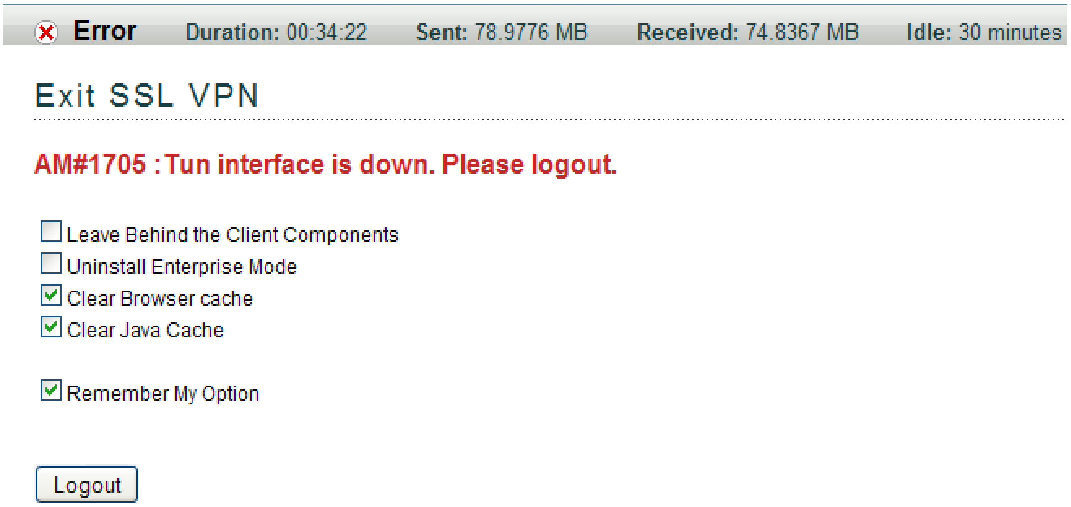
You are seeing this message since you are using Internet Explorer browser and there is no ActiveX control installed.
Please take one of the following actions:
1) If you are prompted for the control, please install it.
2) If you are a non-administrator on your desktop, please click on the following link. Click here
3) Alternatively you may open a new browser window and type the following URL http(s):<DNS-Name>/sslvpn/login?forcejre=true

This page is displayed because a non-admin user of the machine cannot download the ActiveX control, which is essential to establish the SSL VPN connection. Clicking the link downloads the applet on your machine and establishes the connection.

7 If the SSL VPN connection is successful, the SSL VPN Home page is displayed. Make sure that you keep the browser open throughout the SSL VPN session, and continue with Step 8.

or

If the SSL VPN connection fails, an error message is displayed. Skip to Step 9.



Error Duration: 00:34:22 Sent: 78.9776 MB Received: 74.8367 MB Idle: 30 minutes

Exit SSL VPN

AM#1705 : Tun interface is down. Please logout.

☐ Leave Behind the Client Components
☐ Uninstall Enterprise Mode
☑ Clear Browser cache
☑ Clear Java Cache

☑ Remember My Option

8 Do one of the following, depending on whether you are a Linux, Macintosh, or Windows user:

- **Linux:** If you are a Linux user, open a new terminal to launch applications that need to be enabled for SSL. For more information, see Section 5.5.1, "Enabling Linux Applications for SSL," on page 29.
- **Macintosh:** If you are a Macintosh user, open a new terminal to launch applications that need to be enabled for SSL. For more information, see Section 5.5.2, "Enabling Macintosh Applications for SSL," on page 30.
- **Windows:** If you are a Windows user, open applications that you want to access from your protected network.

9 If the SSL VPN connection fails, click *Logout* to close the session and retry. For more information on these error messages, see Appendix A, "Error Messages," on page 33

2.2 Switching from Kiosk Mode to Enterprise Mode

If you selected *Kiosk Mode (Always)* when you first connected to SSL VPN, you are connected to SSL VPN in Kiosk mode in subsequent connections. However, you can switch to Enterprise mode after you connect.

1 Connect in Kiosk mode.

2 Click *Exit* to log out of the current session.

3 Select the *Enable Enterprise mode* check box in the Exit SSL VPN page.

4 Log in again in Enterprise mode.

For more information on connecting to SSL VPN in Enterprise mode, see Chapter 3, "Accessing SSL VPN in Enterprise Mode," on page 17.

Accessing SSL VPN in Enterprise Mode 3

The Enterprise mode is the usual choice for computers that are controlled by the organization, such as notebooks provided by the organization for employees.

When you access the SSL VPN user portal in Enterprise mode, all applications are enabled for SSL, whether they were opened before or after the SSL VPN connection was made.

This section contains the following information on using the SSL VPN user portal in Enterprise mode:

- Section 3.1, "Prerequisites," on page 17
- Section 3.2, "Accessing SSL VPN When You Are an Admin or root User," on page 17
- Section 3.3, "Accessing SSL VPN as a Non-Admin User," on page 19
- Section 3.4, "Switching from Enterprise Mode to Kiosk Mode," on page 21
- Section 3.5, "Enabling the Sudo Command for Standard Users in the Mac OS," on page 21

For information on connecting to the SSL VPN user portal in Kiosk mode, see Chapter 2, "Accessing SSL VPN in Kiosk Mode," on page 13.

3.1 Prerequisites

To connect to SSL VPN in Enterprise mode:

- You should be an admin user in the Windows environment or `root` user in the Linux or Macintosh environment, or a user with the administrative or `root` user access.
- If you are a non-admin or a non-`root` user and do not have admin or `root` user access, you must pre-install the client components. For more information on pre-installing the client components, see "Preinstalling the SSL VPN Client Components" in the *Novell Access Manager 3.1 SP2 SSL VPN Server Guide*.
- You must have the recommended browser or operating software installed in your system. For more information, see Section 1.2, "Client Machine Requirements," on page 10.
- If you are a standard user, make sure that the sudo command is enabled. For more information, see Section 3.5, "Enabling the Sudo Command for Standard Users in the Mac OS," on page 21.

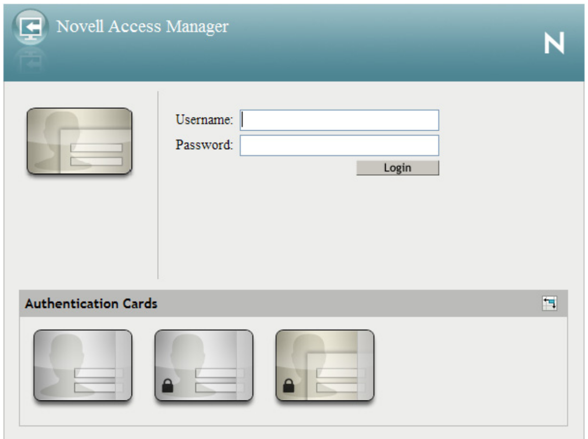
3.2 Accessing SSL VPN When You Are an Admin or root User

If you are an admin or `root` user, the Enterprise mode of SSL VPN is enabled by default unless the SSL VPN administrator has configured you to connect in Kiosk mode only.

1 Log in to the SSL VPN server by using the following URL:

```
https://<dns_name>/sslvpn/login
```

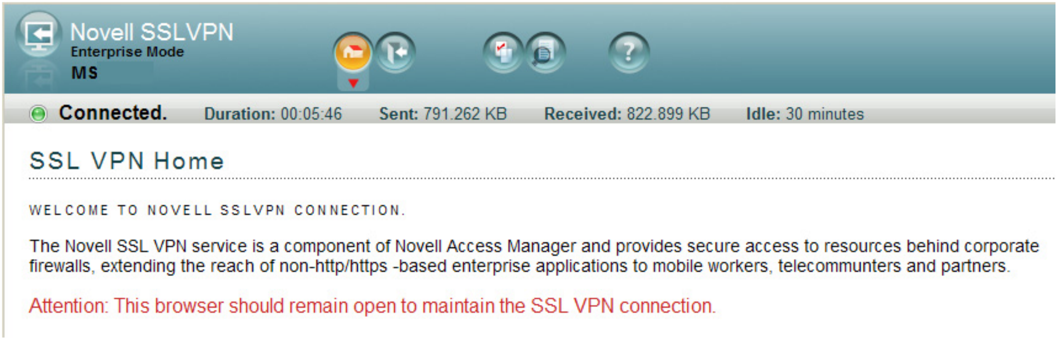
Replace <*dns_name*> with the DNS name of your SSL VPN server.



2 On the Access Manager page, specify the username and password, then click *OK*.

3 Click *Yes* in the warning message to accept and download the signed applet components required for SSL VPN.

4 (Conditional) If the connection is successful, the SSL VPN Home page is displayed, allowing access to all the resources listed on the *Policy* tab. Make sure that you do not close this browser during the SSL VPN session.



Connected. Duration: 00:05:46 Sent: 791.262 KB Received: 822.899 KB Idle: 30 minutes

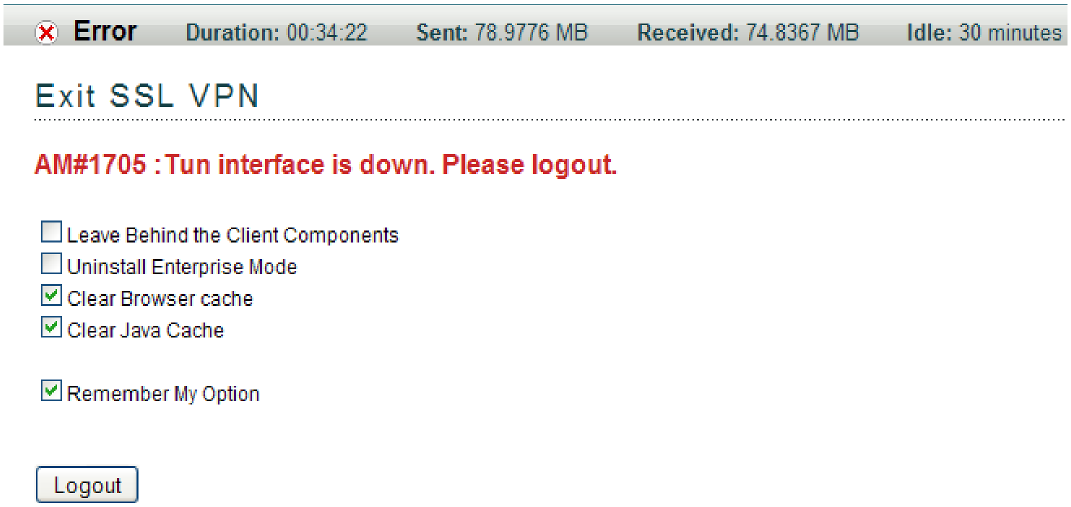
SSL VPN Home

WELCOME TO NOVELL SSLVPN CONNECTION.

The Novell SSL VPN service is a component of Novell Access Manager and provides secure access to resources behind corporate firewalls, extending the reach of non-http/https -based enterprise applications to mobile workers, telecommunters and partners.

Attention: This browser should remain open to maintain the SSL VPN connection.

If the SSL VPN connection fails, an error message is displayed.



Error Duration: 00:34:22 Sent: 78.9776 MB Received: 74.8367 MB Idle: 30 minutes

Exit SSL VPN

AM#1705 : Tun interface is down. Please logout.

☐ Leave Behind the Client Components
☐ Uninstall Enterprise Mode
☑ Clear Browser cache
☑ Clear Java Cache

☑ Remember My Option

5 (Conditional) If you see this error message, click *Logout* to log out of the session. For more information on these error messages, see Appendix A, "Error Messages," on page 33.

3.3 Accessing SSL VPN as a Non-Admin User

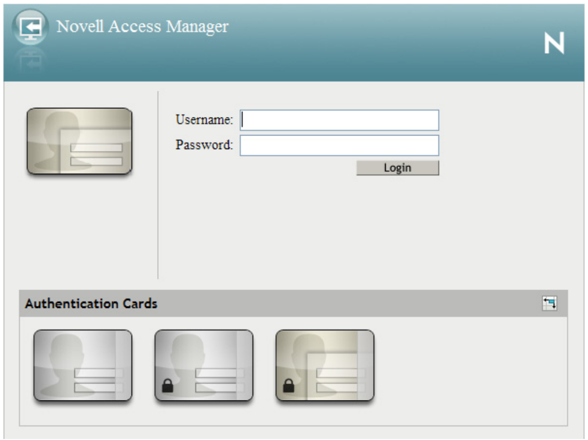
If you are a non-admin or a non-`root` user, but you know the credentials of the administrator or `root` user, you can connect to SSL VPN in Enterprise mode as follows:

1 Log in to the SSL VPN server by using the following URL:

`https://<dns_name>/sslvpn/login`

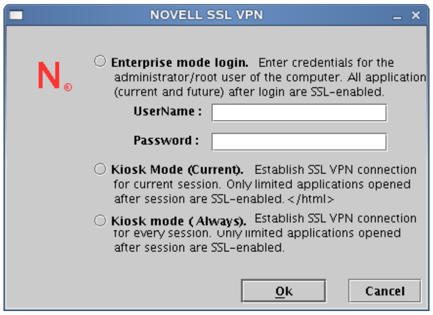
Replace <*dns_name*> with the DNS name of your SSL VPN server.

2 On the Access Manager page, specify the username and password of the administrator or the `root` user of the machine, then click *OK*.



3 Click *Yes* to download the signed applet components required for SSL VPN.

4 Select *Enterprise mode login* in the dialog box prompting you to select a mode of SSL VPN.



○ **Enterprise mode login.** Enter credentials for the administrator/root user of the computer. All application (current and future) after login are SSL-enabled.

UserName :

Password :

○ **Kiosk Mode (Current).** Establish SSL VPN connection for current session. Only limited applications opened after session are SSL-enabled. </html>

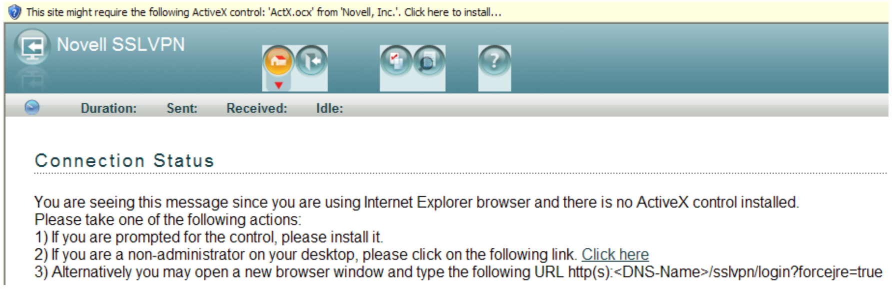
○ **Kiosk mode (Always).** Establish SSL VPN connection for every session. Only limited applications opened after session are SSL-enabled.

5 Specify the username and password of the administrator or `root` user, then click *OK*.

You are connected to SSL VPN in Enterprise mode in subsequent connections. You are not prompted for the administrator or `root` username and password the next time you log in.

If you click *OK* in the dialog box to enable Enterprise mode of SSL VPN and you later want to switch to the Kiosk mode on the same machine, see Section 3.4, "Switching from Enterprise Mode to Kiosk Mode," on page 21

6 (Conditional) If you are using the Internet Explorer browser and the ActiveX control is not installed, click the toolbar of the following screen to download the ActiveX control:


This site might require the following ActiveX control: 'ActX.ocx' from 'Novell, Inc.'. Click here to install...

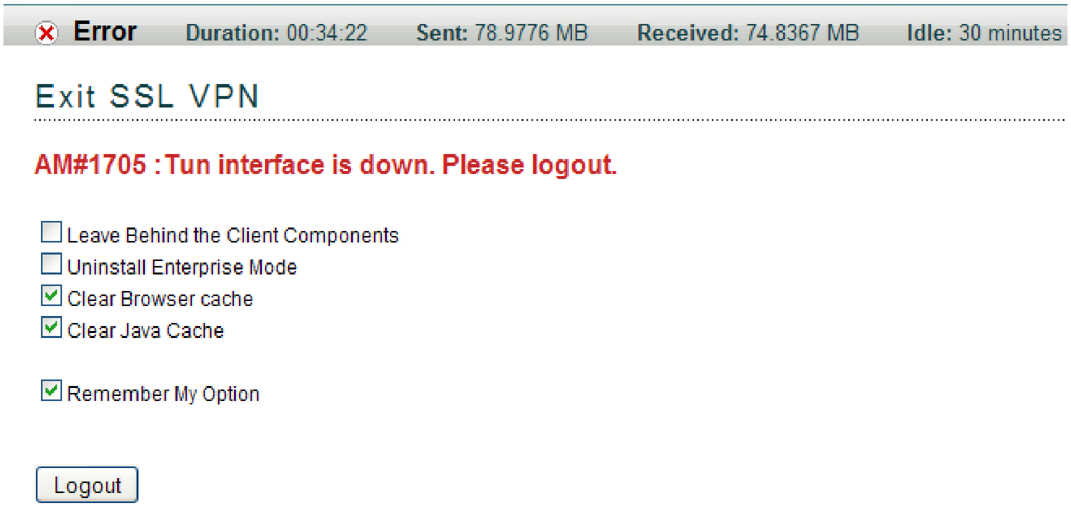
Connection Status

You are seeing this message since you are using Internet Explorer browser and there is no ActiveX control installed.
Please take one of the following actions:
1) If you are prompted for the control, please install it.
2) If you are a non-administrator on your desktop, please click on the following link. Click here
3) Alternatively you may open a new browser window and type the following URL http(s):<DNS-Name>/sslvpn/login?forcejre=true

7 (Conditional) If the connection is successful, the SSL VPN Home page is displayed, allowing access to all the resources listed on the *Policy* page. Make sure that you do not close this browser during the SSL VPN session.

or

If the SSL VPN connection fails, an error message is displayed. For more information on these error messages, see Appendix A, "Error Messages," on page 15



☒ Error Duration: 00:34:22 Sent: 78.9776 MB Received: 74.8367 MB Idle: 30 minutes

Exit SSL VPN

AM#1705 : Tun interface is down. Please logout.

☐ Leave Behind the Client Components
☐ Uninstall Enterprise Mode
☑ Clear Browser cache
☑ Clear Java Cache

☑ Remember My Option

3.4 Switching from Enterprise Mode to Kiosk Mode

If you are a non-admin or non-`root` user and you enabled the Enterprise mode of SSL VPN, you are connected to SSL VPN in the Enterprise mode in subsequent logins. You can return to Kiosk mode on the same workstation during the next login.

1. Connect in Enterprise mode.
2. Click *Exit* to log out of the current session.
3. Select the *Uninstall Enterprise mode* check box on the Exit SSL VPN page.
4. Log in again in Kiosk mode.

   For more information on connecting to SSL VPN in Kiosk mode, see Chapter 2, "Accessing SSL VPN in Kiosk Mode," on page 13.

3.5 Enabling the Sudo Command for Standard Users in the Mac OS

Novell SSL VPN uses the `sudo` command to gain root privileges for non-root users in the Mac OS. This command is not enabled by default for standard users in the Mac OS.

To manually enable the command:

1. Open `/etc/sudoers`
2. Add the following lines:

   ```
   Defaults targetpw
   ALL ALL=(ALL) ALL
   ```
3. Save and close the file.

Accessing Published Citrix Applications through SSL VPN

4

You can access published Citrix applications through SSL VPN.

- Section 4.1, "Accessing Published Citrix Applications in Kiosk Mode," on page 23
- Section 4.2, "Accessing Published Citrix Applications in Enterprise Mode," on page 23

4.1 Accessing Published Citrix Applications in Kiosk Mode

1 Connect to a Citrix server by using the following URL:

```
http://<DNS name of Citrix Server>/Citrix/MetaFrame
```

Replace *<DNS name of Citrix Server>* with the DNS name of your Citrix server. The Access Manager login page is displayed.

2 Specify your login credentials.

3 Click *Allow* to accept and download signed certificates and change the browser setting.

4 Click *OK* in the dialog box when you are prompted.

The SSL VPN connection is automatically established. You can now access the published applications by clicking the corresponding icons on the Citrix Web page.

4.2 Accessing Published Citrix Applications in Enterprise Mode

1 Connect to a Citrix server by using the following URL:

```
http://<DNS name of Citrix Server>/Citrix/MetaFrame
```

Replace *<DNS name of Citrix Server>* with the DNS name of your Citrix server. The Access Manager login page is displayed.

2 Specify your login credentials. You are authenticated to both the Citrix and SSL VPN servers.

3 Depending on your server-side configuration, you might need to accept and download signed certificates. When you are prompted, click *Allow*.

The SSL VPN connection is automatically established. You can now access the published applications by clicking the corresponding icons on the Citrix Web page.

Using SSL VPN

5

When you connect successfully to SSL VPN, the SSL VPN Home page is displayed to you by default. Use this page as the central point for your SSL VPN activities.

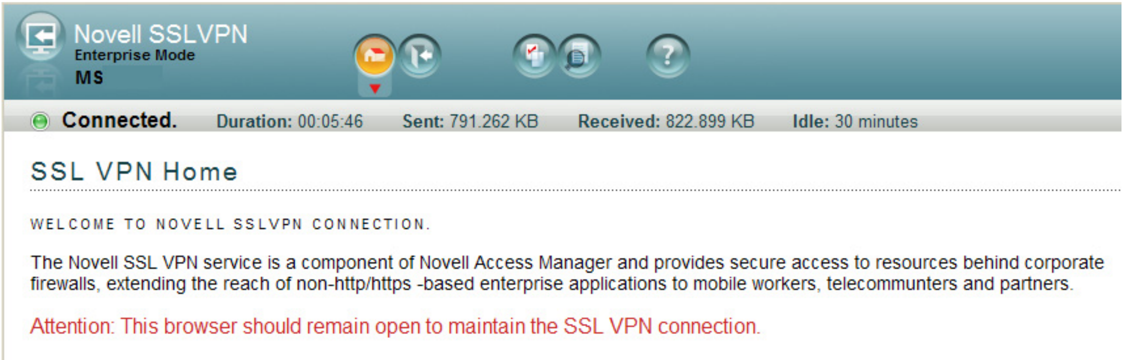
Make sure that you do not close the browser during a session. To access Web pages from the protected network, use another browser instance.

5.1 Using the SSL VPN Home Page

Click the *Home* icon to display the Home page. How this page is displayed to you depends on how your organization has customized this page.

The following figure displays the default Novell SSL VPN home page.

Figure 5-1 *SSL VPN Home Page*



Connected. Duration: 00:05:46 Sent: 791.262 KB Received: 822.899 KB Idle: 30 minutes

SSL VPN Home

WELCOME TO NOVELL SSLVPN CONNECTION.

The Novell SSL VPN service is a component of Novell Access Manager and provides secure access to resources behind corporate firewalls, extending the reach of non-http/https -based enterprise applications to mobile workers, telecommunters and partners.

Attention: This browser should remain open to maintain the SSL VPN connection.

This page displays the following:

- **Home:** Displays the customer or the product information. This page can be customized for different organizations.
- **Logout:** Click the *Logout* icon to log out of the current session.

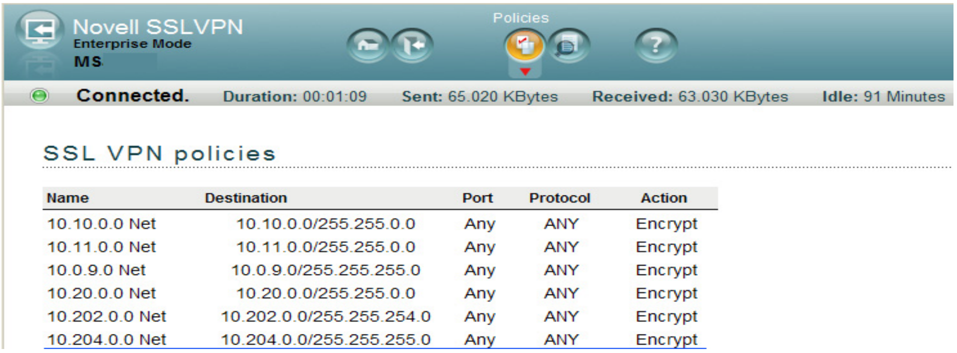
- **Policies:** Displays the resources accessible by the user, based on the traffic policies configured for your role. The traffic policies are configured by the administrator on the server. For more information on the Policies page, see Section 5.2, “Using the Policies Page,” on page 26.
- **Cleanup Options:** This page lists some of the desktop cleanup options that can be selected before logging out of an active SSL VPN connection.

  For more information on the Cleanup options page, see Section 5.6, “Logging Out of the Active SSL VPN Session,” on page 30.
- **Log Entries:** Displays ActiveX or Java applet logs. For more information on the Log Entries page, see Section 5.4, “Viewing SSL VPN Logs,” on page 28.
- **Applications:** Specifies steps to add desktop applications to SSL VPN. This tab is available only in the Kiosk mode of Linux and Macintosh, because in these two platforms, applications that were opened before establishing the SSL VPN connection are not enabled for SSL. For more information on the Applications page, see Section 5.5, “Enabling Applications for SSL,” on page 29.
- **Username:** Specifies the name of the currently logged-in user in the top left corner of the page.
- **Duration:** Specifies the duration that the SSL VPN connection has been on.
- **Sent:** Displays bytes sent through the tunnel.
- **Received:** Displays bytes received through the tunnel.
- **Idle:** Displays the time left in minutes before disconnecting, if there is no data transfer happening in the tunnel.
- **Status of Connection:** Indicates the state of connection. The following table describes the different connection statuses:

Status	Description
🟢 *<Mode>*	Indicates that the Java applet or ActiveX has successfully established a connection to the SSL VPN server. It also displays the connection mode.
⛔ Disconnected	Indicates that the user has logged out of the SSL VPN server. This status is displayed when the user clicks the *Exit* button.
🔵 Connecting	Indicates that the connection is in progress. To avoid problems, the user must wait until a successful connection status is displayed before clicking any other button.
🔵 Disconnecting	Indicates that disconnection is in progress. To avoid problems, the user must wait until a successful disconnection status is displayed before clicking any other button.
❌ Error: Message	Indicates that ActiveX or the Java applet has an error. Check ActiveX or the Java applet log for more information on the error. For more information on error messages, see Appendix A, “Error Messages,” on page 33.

5.2 Using the Policies Page

1 On the SSL VPN Home page, click the *Policies* icon.



Connected. **Duration:** 00:01:09 **Sent:** 65.020 KBytes **Received:** 63.030 KBytes **Idle:** 91 Minutes

SSL VPN policies

Name	Destination	Port	Protocol	Action
10.10.0.0 Net	10.10.0.0/255.255.0.0	Any	ANY	Encrypt
10.11.0.0 Net	10.11.0.0/255.255.0.0	Any	ANY	Encrypt
10.0.9.0 Net	10.0.9.0/255.255.255.0	Any	ANY	Encrypt
10.20.0.0 Net	10.20.0.0/255.255.0.0	Any	ANY	Encrypt
10.202.0.0 Net	10.202.0.0/255.255.254.0	Any	ANY	Encrypt
10.204.0.0 Net	10.204.0.0/255.255.255.0	Any	ANY	Encrypt

2 Review the information on the page.

This page displays the resources you can access, based on the traffic policies configured by your system administrator for your role. The information is displayed as follows:

Name: The name of the traffic policy applicable for your role.

Destination: The IP address of the destination network.

Port: The destination port.

Protocol: TCP, UDP, or ICMP.

Action: The action can be Encrypt or Deny. If the action is Encrypt, you are permitted to access the protected resources. If the action is Deny, you are denied access to the protected resources.

5.3 Configuring the Cleanup Options

1 On the SSL VPN Home page, click the *Cleanup Options* icon.

2 Select one or more of the following options before you log out of the SSL VPN session:

NOTE: In Firefox and Safari browsers, all the components downloaded on the system to establish the SSL VPN connection, and the cookies, Internet Explorer add-on, and cache are deleted from the system when all instances of the browser are closed after disconnecting.

- **Leave Behind the Client Components:** Select this option to reduce the connection time when you log in again. When you select this option, some of the SSL VPN components are left behind in the client. This reduces the time to connect in subsequent logins because these components need not do not need to be downloaded again.
- **Uninstall Enterprise Mode:** This option is displayed only if you are the administrator or `root` user of the machine and have connected in Enterprise mode, or if you selected the *Enterprise mode* option in the SSL VPN dialog box. If you want to switch to Enterprise mode when you connect to SSL VPN the next time you log in, you must select this option before clicking the *Exit* button.
- **Enable Option for Enterprise Mode:** This option is displayed only if you have selected the *Kiosk Mode (Always)* option. You must select this option before clicking the *Exit* button if you want to connect to SSL VPN in the Enterprise Mode the next time you log in.
- **Clear Browser Private Data:** If you use Internet Explorer to establish the SSL VPN connection, this option appears as a check box. If you use Firefox to establish the SSL VPN connection, this option appears as a button. Select the appropriate option in order to clear the browser history and cache when you log out.

- **Unregister ActiveX Control:** This option is displayed only if you use the Internet Explorer to connect to SSL VPN.
- **Clear Java Cache:** This option is available only if you use Firefox to connect to SSL VPN. Select this check box to clear the Java cache when you log out. This clears not only the files and the applet used by SSL VPN, but clears all files and applets in the cache.

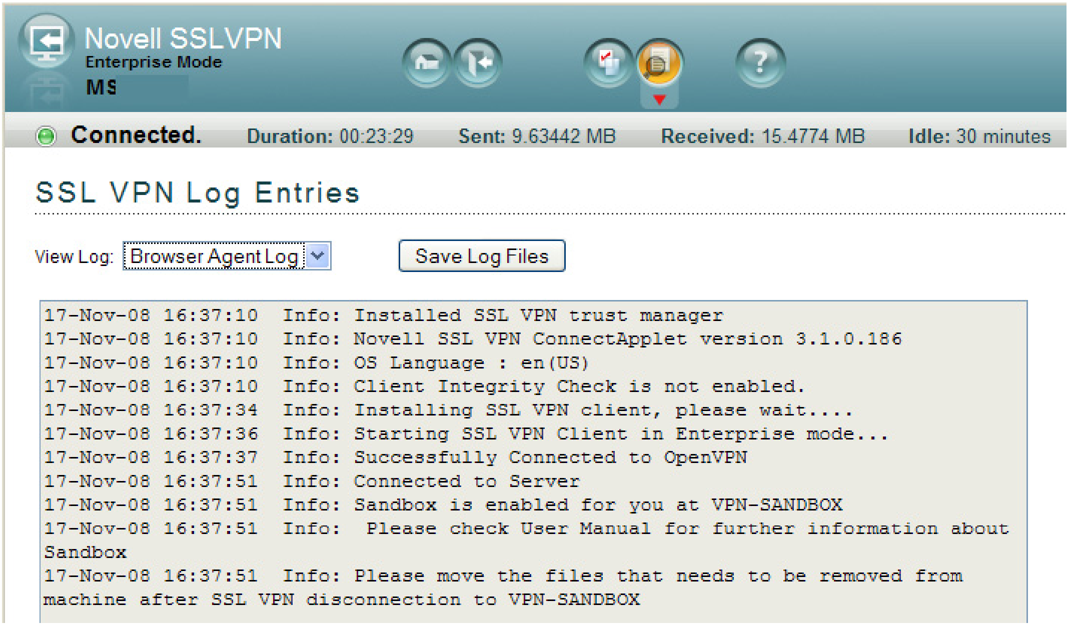
NOTE: If you are using Firefox or the Force JRE option in Internet Explorer, the logout options selected during the previous login are not displayed if you use the same instance of the browser to connect to SSL VPN again.

3 Click *Remember My Option* to remember the logout options that you have selected. If you select this option, the option selection dialog box is not displayed the next time you log out of SSL VPN.

5.4 Viewing SSL VPN Logs

The Log Entries page displays the log files. These log files are useful to you or your system administrator for troubleshooting any issues that come up during the connection.

1 On the SSL VPN Home page, click the *Log Entries* icon. The Log Entries page is displayed.



Connected. Duration: 00:23:29 Sent: 9.63442 MB Received: 15.4774 MB Idle: 30 minutes

SSL VPN Log Entries

View Log: Browser Agent Log

```
17-Nov-08 16:37:10  Info: Installed SSL VPN trust manager
17-Nov-08 16:37:10  Info: Novell SSL VPN ConnectApplet version 3.1.0.186
17-Nov-08 16:37:10  Info: OS Language : en(US)
17-Nov-08 16:37:10  Info: Client Integrity Check is not enabled.
17-Nov-08 16:37:34  Info: Installing SSL VPN client, please wait....
17-Nov-08 16:37:36  Info: Starting SSL VPN Client in Enterprise mode...
17-Nov-08 16:37:37  Info: Successfully Connected to OpenVPN
17-Nov-08 16:37:51  Info: Connected to Server
17-Nov-08 16:37:51  Info: Sandbox is enabled for you at VPN-SANDBOX
17-Nov-08 16:37:51  Info:  Please check User Manual for further information about
Sandbox
17-Nov-08 16:37:51  Info: Please move the files that needs to be removed from
machine after SSL VPN disconnection to VPN-SANDBOX
```

2 To view logs for a particular component or action, click one of the following links in the *View Log* list:

Browser Agent Logs: Displays the ActiveX or applet logs.

Install Logs: Displays the installation logs.

NOTE: When you click the installation logs, you might notice the log message `Sandbox is enabled for you at VPN-SANDBOX`. This message indicates that a folder named VPN-SANDBOX was automatically created for you on your desktop during the SSL VPN connection. Copy or download all the files into this folder. This folder, along with its contents, is deleted automatically, when you disconnect the SSL VPN connection. Section 5.7, "Using the Sandbox Feature," on page 30

Tunnel Logs: Displays the tunnel logs. This contains STunnel logs if the SSL VPN connection is in Kiosk mode and OpenVPN logs if the SSL VPN connection is in Enterprise mode.

Service Logs: Displays logs about the SSL VPN service.

CIC Logs: Displays the Client Integrity Check logs.

Cleanup Logs: Displays the cleanup logs. However, no desktop cleanup logs are displayed if you are using ActiveX.

NOTE: Occasionally, the cleanup logs might display messages such as `Error copying file` or `File not found exception`. These messages indicate that there was an error in making a backup of some of the files. These messages do not affect the desktop cleanup or indicate that the desktop cleanup process is incomplete.

3 Click *Save Logs*, then select a location to save the log files. You can alternatively use one of the following shortcut keys to save logs, depending on your browser.

NOTE: If you are using Mac OS, manually specify a name for the folder where you want to save logs.

- If you are using Firefox, press Alt+Shift+s.
- If you are using Safari, press Alt+Shift+Ctrl+s.
- If you are using Internet Explorer, press Alt+s.

5.5 Enabling Applications for SSL

If you are a Kiosk mode user in Linux or Macintosh, you must enable applications for SSL if they were opened before the SSL VPN connection was established.

This section has the following information:

- Section 5.5.1, "Enabling Linux Applications for SSL," on page 29
- Section 5.5.2, "Enabling Macintosh Applications for SSL," on page 30
- Section 5.5.3, "Enabling Terminals for SSL," on page 30

5.5.1 Enabling Linux Applications for SSL

1 Start the SSL VPN services.

2 Create desktop shortcuts for application that you want to enable for SSL.

3 On the SSL VPN page, click the *Application* tab, then click *SSLize Application*.

4 Launch the application from the desktop shortcut.

NOTE: Applications in the program menu are not enabled for SSL in Linux.

5.5.2 Enabling Macintosh Applications for SSL

1. Create an alias for the application you want to enable for SSL by selecting the application and pressing Command+L.
2. Drag and drop the newly created alias into the SSL VPN folder on desktop.
3. On the SSL VPN Home page, click the *Application* tab, then click *SSLize Application*.
4. Launch the application by using the alias in the SSL VPN folder on desktop.

5.5.3 Enabling Terminals for SSL

To enable terminals that were opened either before or after the start of SSL VPN for SSL in Linux or Macintosh, do one of the following:

- Run `bash` on bash shell.
- Run `tcsh` on tcsh or csh shell.

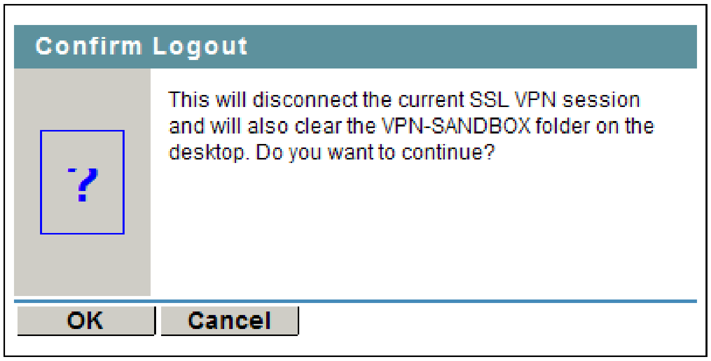
5.6 Logging Out of the Active SSL VPN Session

Use the following procedure to log out of the active SSL VPN session. Do not disconnect the session by closing the browser. If you close the browser without exiting the session, the client components that were downloaded to establish the SSL VPN connection might not be deleted from your machine.

NOTE: If you have logged into SSLVPN from multiple machines by using the same credentials, you are logged out of all the machines when you log out of one of them.

To log out of the active SSL VPN session:

1. On the SSL VPN Home page, click the *Logout* icon. The Confirm Logout dialog box is displayed.


Confirm Logout

This will disconnect the current SSL VPN session and will also clear the VPN-SANDBOX folder on the desktop. Do you want to continue?

2. Click *OK* to confirm logout.

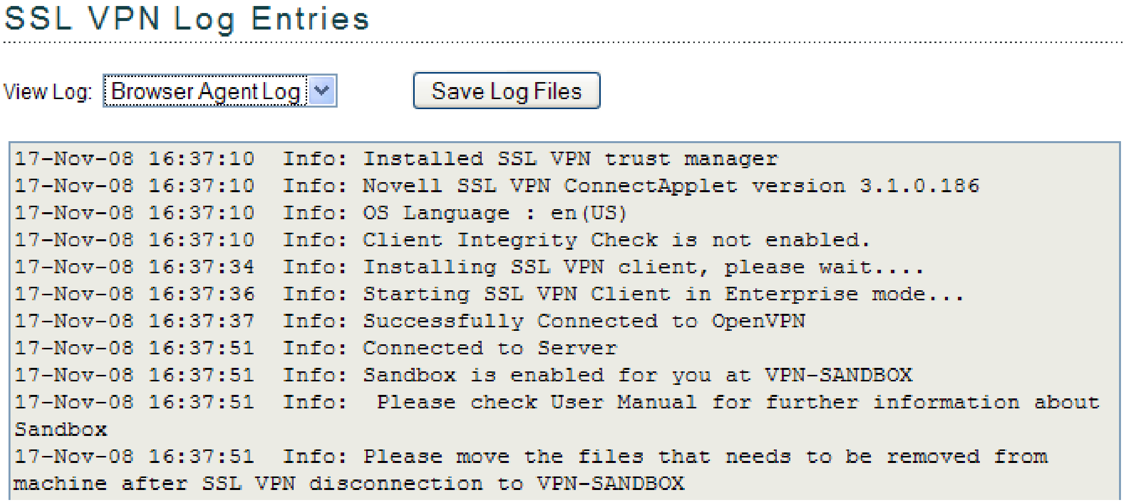
5.7 Using the Sandbox Feature

The SSL VPN client comes with the sandbox feature. When you connect to SSL VPN in either Kiosk mode or Enterprise mode, a folder named VPN-SANDBOX is created on your desktop. You can copy all the files and folders that you have downloaded from your corporate network, or that you have created into this folder. This folder is automatically deleted when the SSL VPN connection is terminated. This is a very useful feature if you are browsing from an Internet Kiosk and you do not want any sensitive information to reach other persons.

Figure 5-2 *Sandbox Folder on Your Desktop*

The *Browser Agent* logs indicate that the Sandbox folder has been created on your desktop. For more information on how to view SSL VPN logs, see Section 5.4, “Viewing SSL VPN Logs,” on page 28.

Figure 5-3 *Log Message in the Sandbox Folder*

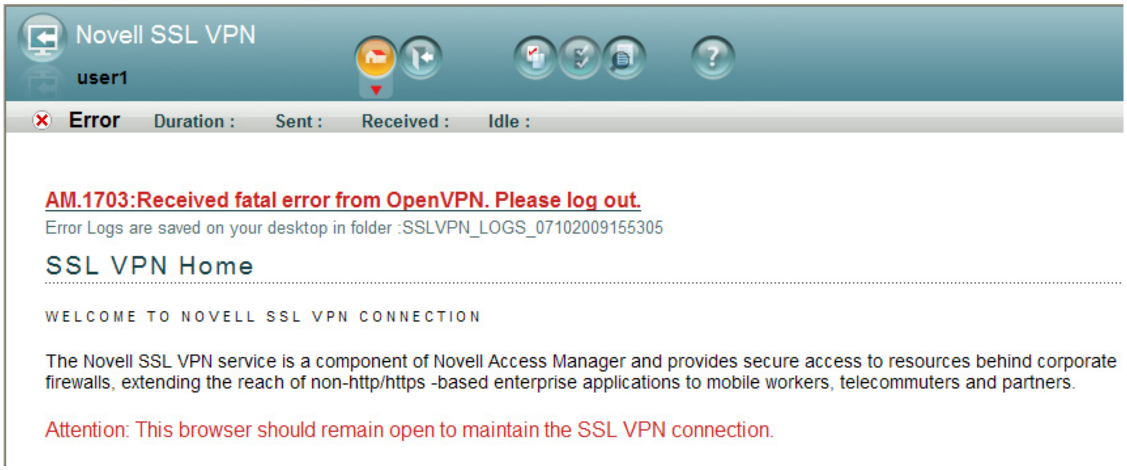


SSL VPN Log Entries

View Log: Browser Agent Log

```
17-Nov-08 16:37:10  Info: Installed SSL VPN trust manager
17-Nov-08 16:37:10  Info: Novell SSL VPN ConnectApplet version 3.1.0.186
17-Nov-08 16:37:10  Info: OS Language : en(US)
17-Nov-08 16:37:10  Info: Client Integrity Check is not enabled.
17-Nov-08 16:37:34  Info: Installing SSL VPN client, please wait....
17-Nov-08 16:37:36  Info: Starting SSL VPN Client in Enterprise mode...
17-Nov-08 16:37:37  Info: Successfully Connected to OpenVPN
17-Nov-08 16:37:51  Info: Connected to Server
17-Nov-08 16:37:51  Info: Sandbox is enabled for you at VPN-SANDBOX
17-Nov-08 16:37:51  Info:  Please check User Manual for further information about
Sandbox
17-Nov-08 16:37:51  Info: Please move the files that needs to be removed from
machine after SSL VPN disconnection to VPN-SANDBOX
```

5.8 Error



Error Duration : Sent : Received : Idle :

AM.1703:Received fatal error from OpenVPN. Please log out.

Error Logs are saved on your desktop in folder :SSLVPN_LOGS_07102009155305

SSL VPN Home

WELCOME TO NOVELL SSL VPN CONNECTION

The Novell SSL VPN service is a component of Novell Access Manager and provides secure access to resources behind corporate firewalls, extending the reach of non-http/https -based enterprise applications to mobile workers, telecommuters and partners.

Attention: This browser should remain open to maintain the SSL VPN connection.

This page is displayed to you if you click the *Cleanup Options* icon or if the SSL VPN connection fails and disconnects. If the SSL VPN connection fails, an error message is displayed. For more information on error messages, see Error Messages.

5.9 Connecting after the Session Timeout Period

If there is no data communication over the SSL VPN channel for more than the specified timeout period, the connection becomes inactive. You must log in again to establish the SSL VPN session. Do not use the *Refresh*, *Back*, or *Forward* options in the browser.

5.10 Downloading the Applet on Internet Explorer

The SSL VPN client components are downloaded to the client desktop through a Java applet or through ActiveX, along with the policies and the required client components.

Some Windows clients do not allow ActiveX controls to run in Internet Explorer. In such scenarios, the user can force the Windows client to load a Java-based applet instead of the ActiveX controls. In order to force load the applet, enter the following URL to launch the SSL VPN user interface:

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

Error Messages

A

Some frequently encountered error messages and their explanations are given below:

- "AM.1811: For More Information on the Error, Please Check the Logs or the Error Codes Page in the Online Help" on page 49
- "AM.1812: You have not accepted the security certificate. Please log out." on page 49
- "Object Does Not Support This Property or Method" on page 49
- "Connections Threshold Exceeded. Please Try Again Later." on page 49

AM.1000: Client Integrity Check Failed. Check Error Logs for More Information.

Possible Cause: The SSL VPN connection requires software or a package that is currently not running in your system.

Action: Click *Log Entries*, then select *CIC Logs* from *View Logs* to check details on the software or package that is missing in your system. Install the software or package, then try to reconnect.

Possible Cause: The administrator has not configured any Client Integrity Check levels for your role.

Action: Click *Log Entries*, select *Browser Agent Logs* from *View Logs* to check details, then contact your system administrator.

AM.1001: Server Is not Responding.

Possible Cause: Either the SSL VPN server or Access Manager is down or the network connection has failed.

Action: Check the network connectivity and reconnect.

AM.1002: Client Is Inactive for More Than <x> Minutes. Please Log Out.

Possible Cause: The client is not active or there was no data transfer from the VPN client to the server. However, this does not log the client out of Access Manager.

Action: Log out of the SSL VPN connection, then log in again to connect.

AM.1003: Problem with One of the Underlying Components/ Connection Error. Please Log Out.

Possible Cause: There was an error starting the Kiosk mode binaries. The binaries could have been exited with errors.

Action: Click *Log Entries*, select *Polresolver Logs, Tunnel Logs*, and *Service Logs*, from *View Logs* to check details, then contact your system administrator.

AM.1004: Problem with One of the Underlying Components/Connection. Please Log Out.

Possible Cause: A forward proxy is configured in the browser and UDP is configured in the SSL VPN server.

Action: Click *Log Entries*, select *Polresolver Logs, Tunnel Logs* and *Service Logs* from *View Logs* to check details, then contact your system administrator.

Possible Cause: The SSL VPN tunnel is down.

Action: Click *Log Entries*, then select *Tunnel Logs* from *View Logs* to check details. Try reconnecting again. If the problem persists, contact your system administrator.

AM.1005: Failed to Find Free Ports on the Client.

Possible Cause: No free ports are available.

Action: Contact your system administrator.

AM.1006: Resource Not Found on the Gateway.

Possible Cause: The client binaries failed to download properly.

Action: Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1007: Failed to Download SSL VPN Files from the Gateway.

Possible Cause: The client binaries failed to download properly.

Action: Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1008: Unable to Fetch Configuration Information from the Gateway.

Possible Cause: There was an error while reading your configuration from the server.

Action: Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1009: Unable to Fetch Policy Information from the Gateway.

Possible Cause: There was an error while reading your access control policy from the server.

Action: Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.100A: User Denied Access. Please Contact the System Administrator.

Possible Cause: There are no policies configured for your role.

Action: Contact your system administrator.

AM.100B: OpenSSL Needs to Be Installed. Please Log Out.

Possible Cause: OpenSSL is not installed on your machine.

Action: Click *Log Entries*, then select *Install Logs* from *View Logs* to check details. Try reconnecting. Save the logs and contact your system administrator.

Possible Cause: OpenSSL is not installed in the correct path.

Action: Click *Log Entries*, then select *Install Logs* from *View Logs* to check details. Try reconnecting. Save the logs and contact your system administrator.

AM.100C: Dependent Components Are not Available in this System. Please Log Out.

Possible Cause: OpenSSL is not installed on the client.

Action: Click *Log Entries*, then select *Install Logs* from *View Logs* to check details. Try reconnecting. Save the logs and contact your system administrator.

Possible Cause: OpenSSL is not installed in the correct path.

Action: Click *Log Entries*, then select *Install Logs* from *View Logs* to check details. Try reconnecting. Save the logs and contact your system administrator.

AM.100D: Another Instance of SSL VPN Is Running. Please Close this Browser.

Possible Cause: Check if SSL VPN is running in another browser.

Action: Log out of the SSL VPN connection and close the browser.

Possible Cause: Check if openvpn, polresolver, or stunnel are running in your system.

Action: If any of these processes are running, terminate the processes, close all instances of browser, and reconnect.

Possible Cause: The previous connection terminated without a proper logout.

Action: Click *Logout* to log out of the active SSL VPN connection.

AM.100E: SSL VPN Session Disconnected as Because the Server Is Not Responding. Please Log Out.

Possible Cause: Your network connectivity is lost.

Action: Check your network connection and try reconnecting.

Possible Cause: The load on the SSL VPN server is high, so it is taking some time to respond.

Action: Try reconnecting from a fresh instance of the browser.

AM.100F: Gateway Internal Error. Please contact the System Administrator.

Possible Cause: The SSL VPN server is down and must be restarted by the system administrator.

Action: Contact your system administrator.

AM.100G: The Enterprise Server Is Down. Please Contact the System Administrator.

Possible Cause: The SSL VPN server is down and must be restarted by the system administrator.

Action: Contact your system administrator.

AM.100H: The Kiosk Server Is Down. Please Contact the System Administrator.

Possible Cause: The SSL VPN server is down and must be restarted by the system administrator.

Action: Contact your system administrator.

AM.100I: Your SSL VPN connection was terminated by the System Administrator. Please Log Out.

Possible Cause: The system administrator has disconnected your connection.

Action: Try reconnecting. If the problem persists, contact your system administrator.

AM.100J: Your SSL VPN connection was terminated because of configuration changes in the server or because the server was restarted. Please log out.

Possible Cause: The SSL VPN restarted to apply the configuration changes.

Action: Log out of SSL VPN connection. Try reconnecting after a few minutes.

Possible Cause: One of the SSL VPN server components might have gone down.

Action: Log out of SSL VPN connection. Try reconnecting after a few minutes.

AM.101A: Failed to find free ports for CIC on the client

Possible Cause: All the system ports are in use.

Action: Log out of the current session. Close all instances of the browser and try reconnecting from a fresh browser instance.

If the problem persists, try reconnecting after a while.

AM.101B: Failed to install the CIC package

Possible Cause: The CIC MSI package failed to install.

Action: Click *Log Entries*, then select *CIC Logs* for more details. If the problem persists, contact your system administrator.

AM.101C: Failed to accept CIC call

Possible Cause:

Action:

AM.101D: Invalid message type received from CIC

Possible Cause: CIC sent a message in an invalid message type.

Action: Click *Log Entries*, then select *CIC Logs* for more details. Try reconnecting again from a fresh instance of the browser.

AM.101E: Connection closed by CIC

Possible Cause: The CIC process might not be running.

Action: Click *Log Entries*, then select *CIC Logs* for more details. Check if the following processes are running:

- `lincic.rpm` in Linux
- `wincic.exe` in Windows
- `maccic.rpm` in Mac

Try reconnecting again from a fresh instance of the browser.

AM.101F: Failed to Uninstall the CIC Package

Possible Cause: The CIC MSI package failed to uninstall.

Action: Check `uninstall_log.txt` in the *<userhome>* directory for more details. If the problem persists, contact your system administrator.

AM.101G: Error in CIC Policy Processing

Possible Cause: The CIC policies are in the wrong format.

Action: Close all instances of the browser and try reconnecting. If the problem persists, contact the system administrator.

AM.101H: Failed to Run CIC

Possible Cause: Failed to execute the Windows CIC process.

Action: Click *Log Entries*, then select *Browser Agent Logs* from *View Logs* for more details. Make sure that `wincic.exe` is installed at `<userhome>\Novell\SSLVPN\Wincic\`. If the problem persists, contact the system administrator.

AM.101I: Failed to send policy to CIC.

Possible Cause: The CIC policies were not sent to CIC.

Action: Click *Log Entries*, then select *CIC Logs* for more details. Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.101J: Failed to download the SSL VPN CIC client

Possible Cause: The CIC client failed to download from the server.

Action: Click *Log Entries*, then select *Browser Agent Logs* from *View Logs* for more details. Make sure that there is sufficient free disk space on your workstation. Clear the browser cache, close all instances of browser, and try connecting again. If the problem persists, contact the system administrator.

AM.101K: CIC might not be running. Please log out.

Possible Cause: The CIC process might not be running.

Action: Click *Log Entries*, then select *CIC Logs* for more details. Check if the following processes are running:

- `lincic.rpm` in Linux
- `wincic.exe` in Windows
- `maccic.rpm` in Mac

Try reconnecting again from a fresh instance of the browser.

AM.1010: Unable to Contact the Gateway. Please Close this Browser.

Possible Cause: You are already successfully logged out of the session.

Action: Close the browser. If you want to reconnect, initiate the connection from a fresh instance of the browser.

AM.1011: This Operating System Is not Supported. Please Log Out.

Possible Cause: Your operating system is not supported.

Action: Click *Log Entries*, then select *Browser Agent Logs* from *View Logs* for more information. Check the *Novell Access Manager 3.1 SSL VPN User Guide* (http://www.novell.com/documentation/novellaccessmanager31/sslvpn_userguide/index.html?page=/documentation/novellaccessmanager31/sslvpn_userguide/data/bookinfo.html) for supported platforms.

AM.1012: The User Does Not Seem to Have Enough Privileges. Please Log Out.

Possible Cause: There was a problem in installing the SSL VPN client component.

Action: Click *Log Entries*, then select *Install Logs* from *View Logs* to check details. Save the logs and contact your system administrator.

AM.1013: Unable to Fetch the Certificate Subject Name from the Gateway

Possible Cause: The browser agent is unable to fetch the subject name from the gateway because of authentication or network problems.

Action: Make sure that you have entered proper log in credentials. Close all instances of the browser and try connecting from a fresh instance of the browser.

If the problem persists, contact the system administrator.

AM.1014: Unable to Fetch the CA Certificate from the Gateway

Possible Cause: Either the certificate file is not present in the gateway or there is a problem with the connectivity.

Action: Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1015: Failed to Install the SSL VPN Client.

Possible Cause: There was a problem in installing the SSL VPN client.

Action: Click *Log Entries*, select *Install Logs* and *Browser Agent Logs* from *View Logs* and Save Logs, then contact your system administrator.

AM.1016: Failed to Fetch the CIC Policy from the Server

Possible Cause: Some of the server components are down.

Action: Try disconnecting and reconnecting to the SSL VPN server. If the problem persists, contact your system administrator.

AM.1017: There Are No Policies Configured for This User

Possible Cause: The administrator has not configured a policy for the user’s role.

Action: Contact your system administrator

AM.1018: Server Disconnected

Possible Cause: The SSL VPN server might be down or the network connectivity was lost.

Action: Try reconnecting after some time. If the problem persists, contact your system administrator.

AM.1019: Failed to Start the Client Using Thin Client. Please Log Out.

Possible Cause: The thin client or the client service might not be installed properly.

Action: Click *Log Entries*, select *Service Logs* and *Tunnel Logs* from *View Logs* and Save Logs, then contact your system administrator.

AM.1020: Failed to Fetch the Cookie from the Server

Possible Cause: Failed to fetch session information from the server.

Action: Check your network connectivity. Clear the browser cache, close all instances of browser, and try connecting again. If the problem persists, contact the system administrator.

AM.1020A: Failed to Fetch the Cookie from the Browser

Possible Cause: Failed to fetch session information from the browser.

Action: Make sure that the browser or the version of the browser that you are using is supported by Novell SSL VPN. For more information, see Novell Access Manager 3.1 SSL VPN User Guide (http://www.novell.com/documentation/novellaccessmanager31/sslvpn_userguide/index.html?page=/documentation/novellaccessmanager31/sslvpn_userguide/data/ba9j4uq.html).

If your browser is supported by Novell SSL VPN, close all instances of the browser and try connecting from a fresh instance of the browser.

AM.1021: Failed to Send a Keepalive Message to Server

Possible Cause: Failed to send the session persistence packets to the server.

Action: Click *Log Entries*, then select *Browser Agent Logs* from *View Logs* for more details. Check your network connectivity. Clear the browser cache, close all instances of browser, and try connecting again. If the problem persists, contact the system administrator.

AM.1022: Failed to Send Cookie Message to Polresolver

Possible Cause: The polresolver process might not be responding.

Action: Click *Log Entries*, select *Browser Agent Logs* from *View Logs,* and check if the polresolver binary is running. If it is not running, log out of the current session and reconnect after some time.

AM.1023: Failed to Send a DNS Message to Polresolver

Possible Cause: The polresolver process might not be responding.

Action: Click *Log Entries*, select *Browser Agent Logs* from *View Logs,* and check if the polresolver binary is running. If it is not running, log out of the current session and reconnect after some time.

AM.1023A: Failed to Send a Policy Message to Polresolver

Possible Cause: The policy information was not sent to the policy resolver.

Action: Click *Log Entries*, select *Browser Agent Logs* from *View Logs,* and check if the polresolver binary is running. If it is not running, log out of the current session and reconnect after some time.

AM.1024: Failed to Uninstall the SSL VPN Package

Possible Cause: Uninstalling the SSL VPN client MSI package has failed.

Action: Check the MSI `uninstall_log.txt` in <*userhome*> for more details. If the problem persists, contact the system administrator.

AM.1025: Unable to fetch a HASH from server

Possible Cause: The browser agent is unable to get the HASH values from the gateway.

Action: Check the network connectivity. Log out of the current session. Close all browser instances and try connecting from a fresh instance of the browser.

AM.1026: Error occurred during service communication

Possible Cause: Problem in connection with the Enterprise client service.

Action: Click *Log Entries*, then select *Browser Agent Logs* and *Service Logs* from *View Logs* for more information. Check if the enterprise thin client service binary novell-sslvpn-serv is running.

AM.1100: Received Zero Length Data from the SOCKS Client.

Possible Cause: The SSL-enabled application crashed while performing a policy resolution.

Action: Run the application again. If the problem persists, contact your system administrator.

AM.1101: Policy Resolution Request from the SOCKS Client Was Not in The Correct Format (Incorrect Message Length).

Possible Cause: A message from the SOCKS client is corrupted.

Action: Contact your system administrator.

AM.1102: Unable to Reply to the Policy Resolution Request by the SOCKS Client.

Possible Cause: The SSL-enabled application that requested policy resolution crashed.

Action: Run the application again. If the problem persists, contact your system administrator.

AM.1103: Policy Resolution Request from the SOCKS Client Was Not in the Correct Format (Incorrect Message Type)

Possible Cause: Possible hack by an intruder.

Action: Restart your session. Check the list of currently running processes in the system for viruses.

AM.1201: Failed to Open the File. Please Check Logs for More Information.

Possible Cause: Unable to open the file.

Action: Click *Log Entries*, then select *Browser Agent Logs* from *View Logs* for more details. If the problem persists, contact the system administrator.

AM.1203: Error Parsing the Home URL. Please Check Logs For More Information.

Possible Cause: Wrong format of the server URL.

Action: Click *Log Entries*, then select *Browser Agent Logs* from *View Logs* for more details. Check your network connectivity. Clear the browser cache, close all instances of browser, and try connecting again. If the problem persists, contact the system administrator.

AM.1301: Unable to Send Statistics Reply to the Applet

Possible Cause: The user closed the browser or the applet closed without sending a disconnect.

Action: Contact your system administrator if the problem persists.

AM.1302: Cookie Received from the Applet Was Not in the Correct Format (Incorrect Message Length)

Possible Cause: Polresolver – Applet communication is bad.

Action: Disconnect the session and reconnect. Contact your system administrator if the problem persists.

AM.1303: Unable to Send Acknowledgment to the Applet for the Cookie Received

Possible Cause: Polresolver – Applet communication is bad.

Action: If the problem persists, the session is disconnected automatically.

AM.1304: Incorrect DNS Information Message Received from the Applet (Incorrect Length of Message)

Possible Cause: Incorrect DNS message from the applet.

Action: Disconnect the session and connect again to be able to use DNS across the protected network.

AM.1305: Unable to Send Acknowledgment to the Applet for the DNS Message Received

Possible Cause: Polresolver – Applet communication is bad.

Action: If the problem persists, the session is automatically disconnected.

AM.1306: Disconnect Message from the Applet Was Incorrect (Incorrect Message Length)

Possible Cause: Polresolver – Applet communication is bad or the session cleanup is incomplete.

Action: Contact your system administrator if the problem persists.

AM.1307: Unable to Send Acknowledgment to the Applet for the Disconnect Message Received

Possible Cause: Polresolver – Applet communication is bad or the session cleanup is incomplete.

Action: Contact your system administrator if the problem persists.

AM.1308: Polresolver Received an Incomplete Message.

Possible Cause: An intruder might be probing Polresolver with an incorrect message.

Action: Contact your system administrator with appropriate logs.

AM.1309: Failed to Allocate Memory for Internal Operation.

Possible Cause: Insufficient memory.

Action: This message is usually accompanied by another error code, indicating which operation failed. Restart the session.

AM.1500: Failed to Send Statistics Request to Stunnel.

Possible Cause: Stunnel is down. This message is sent only after trying for a specified number of times.

Action: Restart the session. If the problem persists, contact your system administrator.

AM.1501: Statistics Response Message from Stunnel was Incorrect (Incorrect Message Length)

Possible Cause: Polresolver – Stunnel communication is bad.

Action: Contact your system administrator with appropriate logs.

AM.1502: Unable to Send Disconnect Message from Stunnel

Possible Cause: Stunnel is down.

Action: Restart the session. Contact your system administrator if the problem persists.

AM.1503: Disconnect Acknowledgment Message from Stunnel Was Incorrect (Incorrect Length of Message)

Possible Cause: Polresolver – Stunnel message is bad.

Action: Contact your system administrator with appropriate logs.

AM.1504: Incorrect Message from Stunnel (Incorrect Length of Message)

Possible Cause: Polresolver – Stunnel communication is bad.

Action: Contact your system administrator with appropriate logs.

AM.1505: Invalid Message from Stunnel (Message Type Unknown)

Possible Cause: Polresolver – Stunnel communication is bad.

Action: Contact your system administrator with appropriate logs.

AM.1506: SSL VPN Server Certificate Validation Failed. Please Log Out.

Possible Cause: Failed to validate the certificate.

Action: Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1507: Disconnected Because of Hibernation/Standby. Please Log Out.

Possible Cause: The machine went into the hibernation or standby mode.

Action: Log out of the SSL VPN connection, then log in again from a fresh instance of the browser.

AM.1701: OpenVPN Authentication Failed. Please Log Out.

Possible Cause: There was a gateway internal error.

Action: Check the network connectivity. Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1702: OpenVPN Connection Error. Please Log Out.

Possible Cause: Your network connectivity is down or is interrupted.

Action: Check your network connectivity. Try reconnecting from a fresh instance of the browser if the network connection is up again.

Possible Cause: Your IP address might have changed because of renewal or a network restart.

Action: Click *Log Entries*, then select *Tunnel Logs* from *View Logs* to check logs. Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

Possible Cause: The Access Gateway might have been restarted.

Action: Click *Log Entries*, then select *Tunnel Logs* from *View Logs* to check logs. Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1703: Received a Fatal Error from OpenVPN. Please Log Out.

Possible Cause: Your network connectivity is down or is interrupted.

Action: Check your network connectivity. Try reconnecting from a fresh instance of the browser if the network connection is up again.

Possible Cause: Your IP address might have changed because of renewal or a network restart.

Action: Click *Log Entries*, then select *Tunnel Logs* from *View Logs* to check logs. Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

Possible Cause: The Access Gateway might have been restarted.

Action: Click *Log Entries*, then select *Tunnel Logs* from *View Logs* to check logs. Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1704: Policy Initialization Failed. Please Log Out.

Possible Cause: The tunnel component had a problem in initializing the policies configured for you.

Action: Close all the browser instances and try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1705: Tunnel Adapter Interface Is Down. Please Log Out.

Possible Cause: The tunnel adapter interface is down.

Action: Select *Start* > *Control Panel* > *Network Connections* and check if the installed device is named TAP-Win 32 Adapter. Then, check if the installed device is in the Enabled state. If it is not, right-click the device and select *Enabled*.

If the problem persists, contact your system administrator with appropriate logs.

AM.1706: System Routing table has been modified in Full Tunneling mode. Disconnecting.

Possible Cause: The system routing table was modified to cofeature SSL VPN for the full tunneling mode.

Action: Close all the browser instances and try reconnecting from a fresh instance of the browser.

AM.1801: Service Is not Running. Please Log Out.

Possible Cause: The installation of the thin client might have failed.

Action: Click *Log Entries*, then select *Service Logs* from *View Logs* to check logs. Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1801A: Connection to Service Failed

Possible Cause: Failed to establish the connection with the thin-client service or the connection established with the thin-client service has been terminated.

Action: Click *Log Entries*, then select *Browser Agent Logs* from *View Logs* for more details. Go to the Task Manager and check if the process `novell-sslvpn-serv.exe` is running. If it is not running, go to *Control Panel* > *Administrative Tools* > *Services Panel* and look for a service named novell-sslvpn-serv. If it is found, restart it. If it is not found, then the thin-client service is not installed properly. Close all instances of browser and try connecting again.

Action: Check if SSL VPN is running in another instance of the browser. If it is, click *Logout*, then close the browser. Try connecting again. If the problem persists, contact your system administrator.

AM.1801B: Failed to Run SSL VPN Services

Possible Cause: Failed to run the client installer.

Action: Click *Log Entries*, then select *Browser Agent Logs* and *Install Logs* from *View Logs* for more details.

AM.1804: Maximum Attempts to Enter Password Reached. Please Close the Browser.

Possible Cause: You have not entered the correct credentials for the administrator or the `root` user of the machine.

Action: You must enter the correct credentials of the administrator and the `root` user of the machine. Check if the Caps Lock is on for your keyboard. Try reconnecting from a fresh instance of the browser. If the problem persists, contact your system administrator.

AM.1805: Timeout Occurred While Entering Credentials. Please Close the Browser.

Possible Cause: You have not entered the correct credentials within the timeout period.

Action: Make sure you specify the correct credentials within three minutes. Close all instances of the browser and try reconnecting from a fresh instance of the browser.

AM.1805A: You Have Been Forced to Use the Enterprise Mode. Please Close the Browser

Possible Cause: You must use the Enterprise mode of SSL VPN. You cannot connect to SSL VPN in Kiosk mode.

Action: Specify the credentials of the administrator or `root` user of the machine in the mode selection dialog box.

Action: Try connecting from a machine on which you have the administrator or `root` user rights.

Action: Close all instances of the browser. Try reconnecting from a fresh instance of the browser.

AM.1806: Unable to Initialize Browser Cache Cleaner

Possible Cause: There was a problem in clearing your browser cache.

Action: Click *Log Entries*, then select *Cleanup Logs* from *View Logs* for more information. Close all instances of the browser and try reconnecting from a fresh instance of the browser.

AM.1807: Failed to Update the Thin Client with Policies

Possible Cause: The Kiosk mode client was not updated with policies.

Action: Click *Log Entries*, then select *Service Logs* from *View Logs* for more information. Close all instances of the browser and try reconnecting from a fresh instance of the browser. Contact your system administrator if the problem persists.

AM.1808: Pop-up Window Inactivity Time Is Up

Possible Cause: You have not selected any client mode in the SSL VPN mode selection dialog box.

Action: Log out from the current session and connect again. When the Mode selection dialog box appears, select a client mode.

For more information on SSL VPN modes, see *the Novell Access Manager SSL VPN User Guide* (http://www.novell.com/documentation/novellaccessmanager31/sslvpn_userguide/index.html?page=/documentation/novellaccessmanager31/sslvpn_userguide/data/bac4n0o.html)

AM.1809: Error: Failed to Start SSL VPN Desktop Cleanup

Possible Cause: There was an error in initiating the desktop cleanup action.

Action: Click *Log Entries*, then select *Cleanup Logs* from *View Logs* for more information. Close all instances of the browser and try reconnecting from a fresh instance of the browser.

AM.1810: Please Log Out of the Current Session or Close the Browser before Connecting Again

Possible Cause: You clicked the *Exit* button.

Action: You must select the Logout options and click *Logout*. Close the browser to complete the browser session.

AM.1811: For More Information on the Error, Please Check the Logs or the Error Codes Page in the Online Help

Possible Cause: Your SSL VPN connection has encountered an error.

Action: Click *Log Entries* to find more information in the logs or click the Error Codes page in the online help.

AM.1812: You have not accepted the security certificate. Please log out.

Possible Cause: You might have clicked *No* or *Deny* when prompted to accept the security certificate.

Action: Click *Logout* to log out of the current session, then close the browser. Try reconnecting from a fresh instance of the browser. Click *OK* when prompted to accept the security certificate. If the problem persists, clear the browser cache and then try reconnecting.

Object Does Not Support This Property or Method

Possible Cause: ActiveX controls are not loaded into the Internet Explorer browser.

Action: Add the Access Gateway URL to the trusted sites list in *Internet Explorer* > *Tools* > *Internet Options* > *Security.*

Connections Threshold Exceeded. Please Try Again Later.

Possible Cause: The server has reached the limit for the maximum number of connections. The low bandwidth SSL VPN allows only 249 simultaneous SSL VPN sessions and a transfer rate of 40 Mbps because of some export restrictions.

Action: Try to connect again after some time. If any user has disconnected, you will be connected to the server.

If you cannot download the high bandwidth version of SSL VPN because of export restrictions, you can set up more than one SSL VPN server in a cluster.

If your deployment requires 250 or more concurrent SSL VPN connections, your regular Novell® sales channel can determine if the export law allows you to order the high bandwidth version at no extra cost.

Troubleshooting SSL VPN

B

This section provides various troubleshooting scenarios that you might encounter while configuring SSL VPN.

B.1 SSL VPN Fails to Load If Firefox 3.0 Is Used on Vista 64-bit

When a user tries to connect to SSL VPN by using Firefox 3.0 (32-bit) on Vista 64-bit, the SSL VPN applet fails to load. This is because Sun JRE 1.6 Update 12 additionally bundles a newer Java plug-in for Firefox, so some applets fail to load.

To work around this problem, disable the newer Java plug-in and roll back to the older plug-in as follows:

1. Open the Java Control Panel in one of the following ways:
   - Browse to `<Install_Folder>\Java\jre6\bin`, then run `Javacpl.exe`.
   - Go to *Start* > *Control Panel* > *Java*.
2. Select *Advanced* > *Java Plug-in* and deselect *Enable the next generation Java plug-in*.
3. Select *Advanced* > *Default Java For Browsers* and make sure that *Mozilla Family* option is enabled.
4. Restart the browser.

B.2 Error: Failed to Fetch CIC Policy from the Server

The SSL VPN Kiosk mode connection fails in the HTTPS access mode on a Windows XP machine, with the following log message:

```
Error: Failed to Fetch CIC Policy from the Server
```

This error is caused because of a problem with the certificate. To work around this issue, remove old certificates from the server and create new ones.

B.3 Stability Issues when You Use a Firefox Browser on a Vista 64-Bit Machine

If you are using a Windows Vista 64-bit machine and the Firefox browser to connect to SSL VPN, the connection might fail after running for a few hours, because of a Firefox browser stability issue. To work around this problem, make sure you upgrade to Firefox 3.0.10 or later.

B.4 Unable to Connect to SSL VPN Because of the OpenVPN Error

Occasionally, the SSL VPN connection in Enterprise mode fails and the following OpenVPN error message is displayed in the log files:

```
Failed to Renew DHCP IP Address Lease on TAP-Win 32 Adapter: The system cannot
find the file specified.
```

To work around this issue, do the following before attempting to connect to SSL VPN again:

1. Select *Start* > *Control Panel* > *Network Connections*.

2 Right-click the Local Area Connection with the device name TAP-Win 32 Adapter, then select *Properties*.

3 Click *Configure*, then select the *Advanced* tab.

4 Select *Media Status* and set the value to *Always Connected*.

5 Click *OK*.

B.5 The SSL VPN Applet Fails to Download on a SLED 11 64-bit Machine

If you are using a SUSE Linux Enterprise Desktop (SLED) 11 64-bit machine, the SSL VPN applet might fail to download after logging in, and a blank page is displayed to you. This is because SSL VPN fails to load the page as if the browser fails to find the appropriate JRE plug-in installed on the client machine.

To work around the problem

1 Specify the following command to check if JRE plug-in is installed:

```
rpm -aq | grep jre-plugin
```

2 If JRE plug-in is not installed, select *YaST* > *Software Management*.

3 Search and install the Sun JRE plug-in.

4 Reconnect to SSL VPN.

B.6 Unable to Connect to SSL VPN

If you are unable to connect to SSL VPN, check the SSL VPN logs to see if there is any reference to proxy configuration. If there is a reference, it indicates that SSL VPN is unable to establish a connection with the server through a forward proxy. To enable SSL VPN to connect through forward proxy, modify the `proxy.conf` file as follows:

1 Browse to the user home directory and open the `proxy.conf`. If the file does not already exist, create a text file in the user home directory and save it as `proxy.conf`.

2 Enter the proxy configuration information in the following format:

```
proxyHost=<IP address>:<port>
```

Replace <*IP address*> with the IP address of the forward proxy and <*port*> with the port number.

3 Save and close the file.

NOTE: If you are using Firefox to connect to the SSL VPN server, restart the browser before reconnecting.

B.7 Unable to Connect to SSL VPN from the Same Internet Explorer Browser Session

If you are trying to connect to SSL VPN from the same Internet Explorer browser session from which you logged out, the following error message might be thrown:

```
AM.100D: Another Instance of SSL VPN Is Running. Please Close this Browser
```

This issue occurs if the *Clear Browser Private Data* option is selected when logging out of the session. To workaround the issue, close all browser sessions and connect to SSL VPN from a new browser session.

B.8 The SSL VPN Connection Fails with an OpenVPN Connection Error

- If your previous connection failed with an error, you might get this error when you try to reconnect. Select the *Logout* button in the Exit page to log out of the session and reconnect again.
- Check to see if the *Log Entries* > *Tunnel* logs displays the following message:

  ```
  No Buffer Space Available
  ```

  This indicates that there is not enough buffer space. You must free memory space by closing some of the applications that are running, or by restarting the machine, then reconnecting to SSL VPN.

B.9 The Browser Cache Is Not Cleared When Multiple Tabs Are Used in Vista

In Windows Vista 32-bit and 64-bit machines, if you use multiple tabs in the same browser to access protected resources, the browser cache is not cleared from the registry entry, even if you selected *Clear Browser Cache* in the Exit page. This issue occurs if Internet Explorer versions earlier than 7.0 are used with the Add Tab plug-in or if Internet Explorer 7.0 is used to connect to SSL VPN, and the protected resources are accessed in the other tabs of the same resource. To clear the cache, browse to the following location and manually delete the files:

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs
```

B.10 Failed to Connect to SSL VPN

Sometimes the SSL VPN connection might fail with the error message `Failed to Connect to SSL VPN`. If this error occurs, you need to clear the Java cache and then try to connect to SSL VPN again.

On a Linux machine, enter the following command in the command prompt:

```
/usr/lib/jvm/jre/bin/controlpanel
```

On a Windows machine, do the following:

1. *Control Panel* > *Java*.
2. Click *Delete Files* in the *General* tab.
3. Select the *Downloaded Applets* check box in the Delete Temporary Files dialog box.
4. Click *OK*.

B.11 Mozilla Firefox Browser Displays an “X” Mark

If you see an “X” on the top left corner of Mozilla Firefox while trying to access the SSL VPN end user portal, it indicates that the Java Runtime Environment* (JRE) is not installed on the client machine.

Install Sun JRE 1.5.0_11 or above from http://www.java.com/en/download/index.jsp.

B.12 Applications Are Not Enabled from the Terminal after Running the su Command

If you are a Linux or a Macintosh user, do the following to access the private network after running the `su` command in a terminal:

- If you are using the `Bash` shell, run the source `sslize_bashrc` file located in the home directory of the logged-in user.
- If you are using the `tcsh` or `csh` shell, run the source `sslize_tcshrc` file located in the home directory of the logged-in user.

If you have changed directories after running the `su` command, you must give the complete path to the above files.

B.13 SSL VPN Session Disconnects after Approximately 10 Hours

If the SSL VPN client session disconnects after being in use for approximately 10 hours, check the version of the JRE. If the version of JRE is 1.4, download and install JRE 1.5 or later.

B.14 Error: Failed to Download the SSLVPN Files from Gateway

If you see the `Failed to download the SSLVPN Files from Gateway` error while trying to connect to SSL VPN through the Internet Explorer, add the `forcejre=true` command at the end of the URL as follows:

```
http://<DNS-Name>/sslvpn/login?forcejre=true


For example, http://www.digitalairlines.com/sslvpn/login?forcejre=true
```

B.15 Unable to Connect After the Previous Connection Ended Abruptly

If you needed to close the SSL VPN connection in the previous session by closing the browser because the browser stopped responding, you might not be able log in to SSL VPN again. This is because some of the SSL VPN processes are running on your system.

To work around the problem:

1. Close all the instances of the browser.
2. Delete the `polresolver, stunnel, openvpn, java client-clear.jar and java_vm` processes as follows:
   - If you are a Linux user, kill the processes by using the following command:

     ```
     pkill <processname>
     ```
   - If you are a Windows user, press Ctrl+Alt+Delete to invoke the Windows Task Manager, select the *Processes* tab, select the processes, and click *End Process.*
3. Check for the following file in your home directory and delete it:

   ```
   .cleanupLock
   ```

B.16 SSL VPN Client Displays the Nonsecure Items Dialog Box

In Internet Explorer, the SSL VPN client randomly displays the *Do you want to display the nonsecure items* dialog box after the connection is established. Click *Yes* to close the dialog box. If you do not click *Yes*, SSL VPN disconnects. You can also follow the steps given below to resolve the problem if you are planning to use SSL VPN for a long session.

1. Open the Internet Explorer browser.
2. Select *Tools* > *Internet Options*.
3. Select the *Security* tab.
4. Select *Internet Zone*, then click the *Custom Level* button.
5. Select *Enable* for the *Display mixed content* option.
6. Click *OK*.

B.17 Clear Cache Option Retains Some Image Files in the Temporary Internet Folder

When you log out of the SSL VPN connection from Internet Explorer, some of the image files might be retained in the temporary Internet folder even if you selected the *Clear Browser Cache* and the *Clear Java Cache* options. This is an Internet Explorer issue. However, the images do not contain any user information.

B.18 SSL VPN Fails to Retrieve Help Pages When There Is an Error

When the SSL VPN client is in an error state because of a Tomcat failure at the server, the error message link or the help link fails to retrieve the relevant help information for the error code. This is because the help pages are served to the SSL VPN client by the Tomcat.

B.19 The Browser Becomes Non-Responsive If Clear Browser Private Data Is Repeatedly Clicked

The browser might become non-responsive if the button in the SSL VPN applet is repeatedly clicked. This issue occurs with the JRE Update 06 version. To work around this issue, upgrade the JRE to the latest update.

B.20 SSL VPN Issues with the Latest Versions of JRE 1.6

Occasionally, when newer versions of JRE 1.6 are used, the following files are left behind in the SSL VPN install directory:

- **Windows:** `OpenVPN` and `client MSI`
- **Linux:** `sslpackage`, `installsc`, `openvpnclientinstall`, and `openvpn`

These files do not affect the consequent SSL VPN connections. You can manually delete these files after logging out of the SSL VPN connections. This issue does not appear in JRE 1.6 update 7.

B.21 Unable to Access Protected HTTP Applications through a Safari Browser

On a Mac Power PC, you cannot use the Safari browser to access protected HTTP applications. However, you can use Safari to connect to SSL VPN and use another browser such as Firefox to access the protected HTTP applications.

B.22 Linux Browser Issues in Kiosk Mode

In Linux, you cannot access protected HTTP traffic on the Firefox browser during the first SSL VPN connection, but subsequent connections work without problems.

To work around this problem, you can use another browser to access the protected resource as follows:

1. Establish an SSL VPN connection in the Kiosk mode.
2. Create a shortcut or launcher for Firefox on the desktop.
3. Click *SSLize Desktop Applications*.
4. Log out of the SSL VPN.
5. Launch Firefox by using the SSL VPN-enabled shortcut.

   The Firefox browser launches even though there is no SSL VPN connection.
6. Establish an SSL VPN connection in the Kiosk mode.

   New tabs and new instances of the Firefox browser now tunnel HTTP traffic.

B.23 Issues with the Intlclock Toolbar Application

The Intlclock toolbar application running on the SUSE Linux Enterprise Desktop (SLED) 10 SP1 crashes when an SSL VPN connection is established or disconnected.

B.24 Socks Client Logs Are Displayed under Service Logs

When the SSL VPN applet is installed in Kiosk mode, the Socks Client logs are displayed under Service Logs.

B.25 Connection Fails in SSL VPN If the Root User Password Is Not Set in Macintosh

In Macintosh, the SSL VPN connection fails if you log in as a `root` user and there is no password set for the `root` user. When there is no password set for the `root` user, you can log in by using the credentials of the admin user.