# Novell Access Manager

3.0 SP2

www.novell.com

SSL VPN USER GUIDE

March 31, 2008

Novell®

## 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., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

## Third-Party Materials

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

# Contents

# About This Guide

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



### 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/novellaccessmanager).

### Additional Documentation

- *Novell Access Manager 3.0 SP2 Administration Guide*
- *Novell Access Manager 3.0 SP2 Installation 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.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

# 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* application is installed on your machine after the successful connection. This application encrypts the traffic passing through the tunnel and sends it to the SSL VPN server.

This section describes the following features of SSL VPN:



## 1.1 Access Modes

You can connect to the SSL VPN by using one of the following modes:



### 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 SSL enabled. Applications that were opened before the SSL VPN connection was established are not enabled for SSL.

The Kiosk mode has the following user restrictions:

- If you do not have administrator rights or `root` privileges to the workstation, you are connected to SSL VPN in Kiosk mode.
- If you have administrator rights or `root` privileges to the workstation, you cannot connect using the Kiosk mode; you must use the Enterprise mode.

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. Also, all the applications including your desktop applications and toolbar applications are SSL enabled.

The Enterprise mode has the following user restrictions:

- If you have administrator or `root` access to a workstation, you can connect to SSL VPN in Enterprise mode.
- If someone with administrator access has pre-installed the SSL VPN thin client components on your machine, you can connect to SSL VPN in Enterprise mode. For more information on pre-installing the thin client components, see "Pre-Installing SSL VPN Client Components" in the *Novell Access Manager 3.0 SP2 Installation Guide*.

For more information on using the 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 be able to access the SSL VPN user portal.



## 1.2.1 Linux Requirements

When you access the SSL VPN user portal in the Linux environment, 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 10.0 and higher |
| | Red Hat* Linux |
| | Novell® Linux Desktop |
| 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 |
| Browser | Mozilla* Firefox 1.5.0_11 or higher |
| | Java and JavaScript enabled |
| Sun* JRE* | 1.5.0_11 or higher |

## 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 Macintosh environment:

***Table 1-2*** *Supported Macintosh Configurations*

| Component | Requirement |
|---|---|
| Operating System | Macintosh Power PC OS 10.4 Tiger* |
| | Macintosh Intel OS 10.5 Leopard* |
| OpenSSL | 0.9.7 |
| Shell | bash |
| Browser | Macintosh Safari* 2.0.4 Build 412 or higher |
| | Java and JavaScript enabled |
| Sun* JRE* | 1.5.0_11 or higher |

## 1.2.3 Windows Requirements

When you access the SSL VPN user portal in the Windows environment, an ActiveX component is downloaded to the client machine. If you want to download the Java applet on your machine instead of the ActiveX control, you need to do some server-side configurations. For more information, refer to *Configuring SSL VPN to Download Applet on Internet Explorer in* the "Novell Access Manager 3.0 SP2 Administration 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* 2000 SP4 |
| | Windows XP* SP2 |
| | Windows Vista* |
| Browser | Internet Explorer 6.0 SP2 or higher |
| | Mozilla Firefox 1.5 or higher |
| | Do not use Windows Explorer to access the SSL VPN client. |
| Sun* JRE* | 1.4.1 or higher |

# Accessing SSL VPN in Kiosk Mode

2

In the Kiosk mode of SSL VPN, only those applications that are opened after connecting to the SSL VPN are enabled for SSL. You must add the applications that were opened before connecting to SSL VPN in order to enable them for SSL.

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



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.

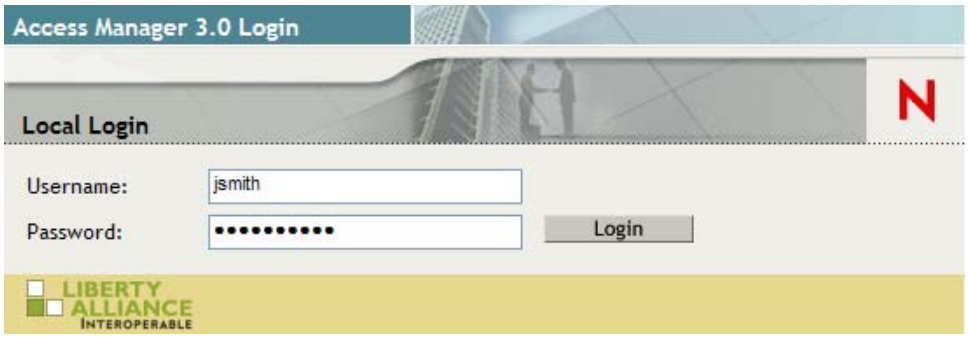
## 2.1 Accessing the SSL VPN User Portal

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.

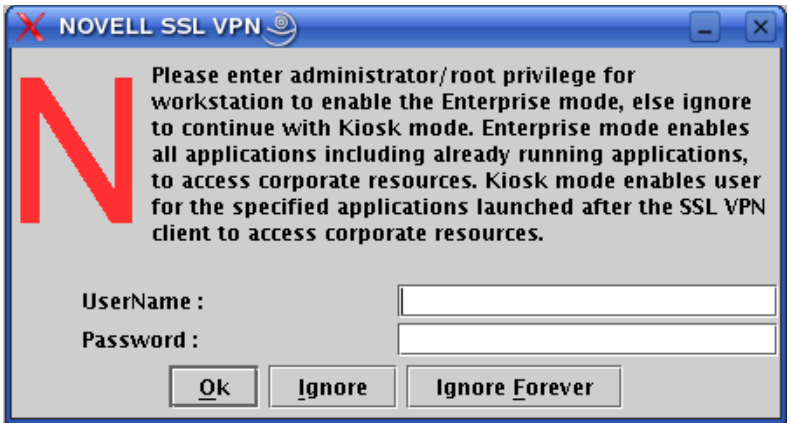
2. On the Access Manager page, specify the username and password, then click *OK*.




   A security alert message appears.

3. Click *Yes* to accept and download the signed ActiveX or Java applet components required for the SSL VPN client.

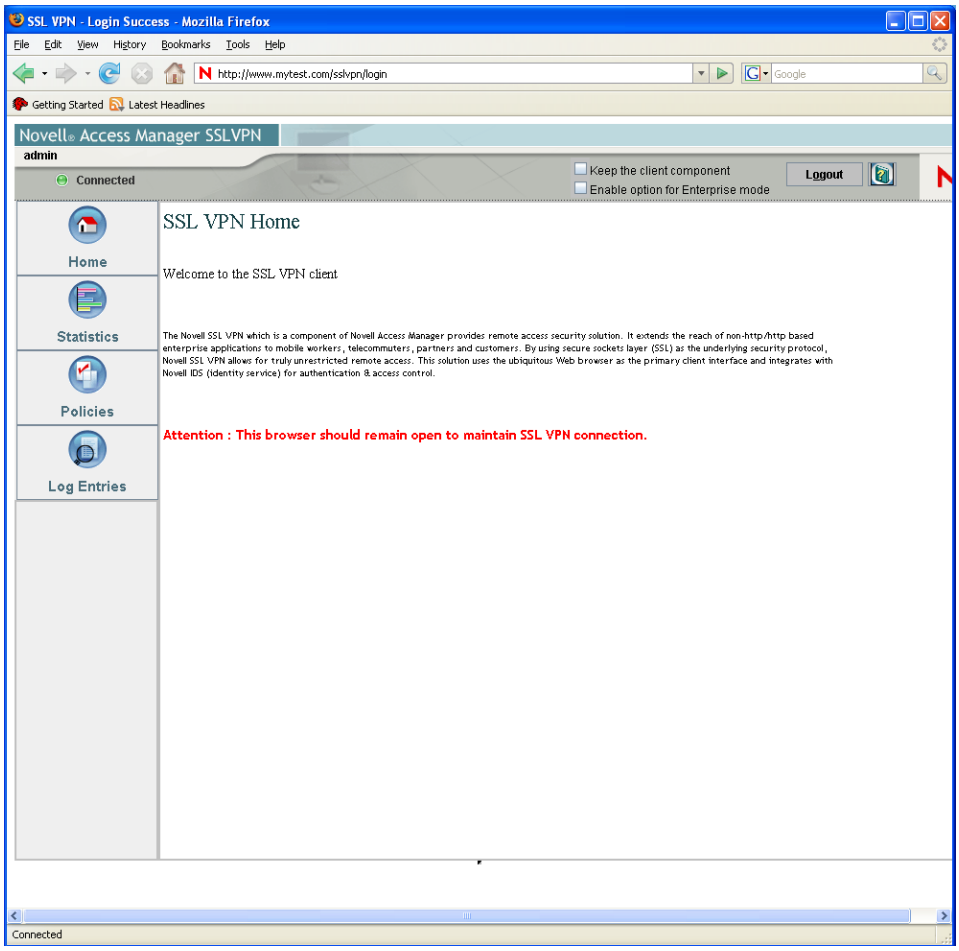
   A dialog box displays, prompting you to specify the administrator username and password.




4 Do one of the following:

- Click *Ignore* to connected to SSL VPN in Kiosk mode for the current session. You are prompted to enter the username and password the next time you log in.
- Click *Ignore Forever* to always connected to SSL VPN in Kiosk mode. If you want to connect to Enterprise mode, after clicking *Ignore Forever*, refer to Section 2.3, “Switching from Kiosk Mode to Enterprise Mode,” on page 16.

The Welcome page of the SSL VPN service is displayed. This allows access to all the resources listed in the *Policy* table.




5 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 2.2.1, “Enabling Linux Applications for SSL,” on page 16.
- **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 2.2.2, “Enabling Macintosh Applications for SSL,” on page 16.
- **Windows:** If you are a Windows user, launch applications to access your protected network.

## 2.2 Enabling Applications for SSL

Adding an application to SSL VPN is known as SSLizing the application.

### 2.2.1 Enabling Linux Applications for SSL

To enable Linux Applications for SSL:

1. Start the SSL VPN services.
2. Create a desktop shortcut for the application that you want to enable for SSL.
3. Click the *Application* tab, then click *SSLize Application*.
4. Launch the application from the desktop shortcut.

To enable terminals that were opened before the SSL VPN session, do one of the following:

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

### 2.2.2 Enabling Macintosh Applications for SSL

To enable applications for SSL:

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

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

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

## 2.3 Switching from Kiosk Mode to Enterprise Mode

If you clicked *Ignore Forever* in the dialog box to enable the Kiosk mode of SSL VPN, you are connected to SSL VPN in Kiosk mode in subsequent connections. If you want to switch to Enterprise mode when you connect to SSL VPN, do the following:

1. Connect in Kiosk mode.
2. On the Welcome page, select the *Enable option for Enterprise mode* check box.


3. Click *Logout* to log out of the current session.
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

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:



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:

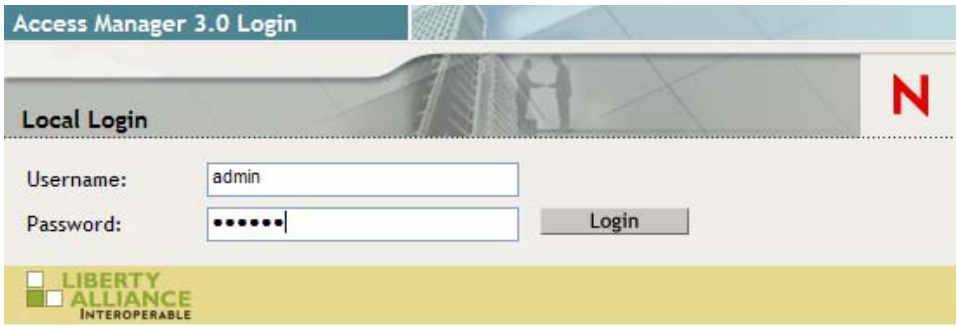
- You should be an admin user in the Windows environment or `root` user in the Linux or Macintosh environment, or a user with the administrative or `root` user access.
- If you are a non-admin or a non-root user and do not have admin or `root` user access, you must pre-install the client components. For more information on pre-installing the client components, see “Pre-Installing SSL VPN Client Components” in the *Novell Access Manager 3.0 SP2 Installation 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 Macintosh user, you must enable `targetpw`. For more information how you can do this, see Section 3.4, “Enabling targetpw in Macintosh,” on page 20.

## 3.2 Accessing SSL VPN When You Are an Admin or root User of the Machine

If you are an admin or a `root` user, the Enterprise mode of SSL VPN is enabled by default. When you are an admin or a `root` user, you can never connect to SSL VPN in the Kiosk mode.

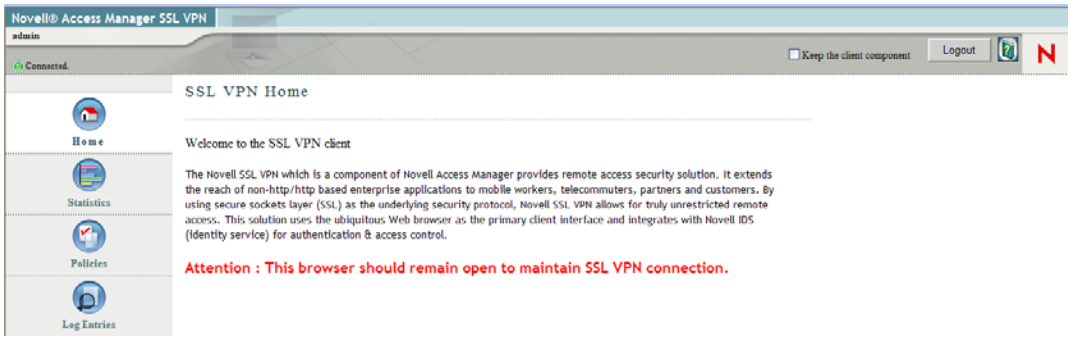
1. Log in to the SSL VPN server by using the following URL:
   `https://<dns_name>/sslvpn/login`

   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.

The Welcome page of the SSL VPN service is displayed, allowing access to all the resources listed on the *Policy* tab.




## 3.3 Accessing SSL VPN When You are a Non-Admin User of the Machine

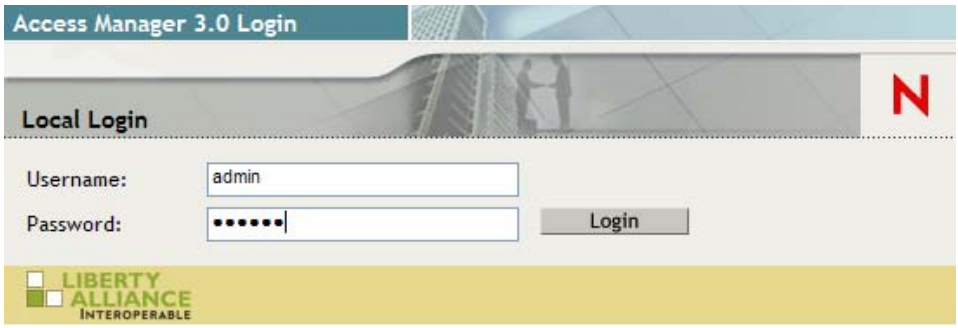
If you are a non-admin or non-`root` user of the machine, but you know the credentials of the administrator or `root` user, you can connect to SSL VPN in Enterprise mode by specifying the credentials of the administrator or root user of tha machine. You are connected to SSL VPN in Enterprise mode by default in the subsequent sessions.

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.

A dialog box displays, prompting you to enter the `root` username and password to enable Enterprise mode of SSL VPN.


4 Specify the username and password of the `root` user as necessary, then click *OK*.

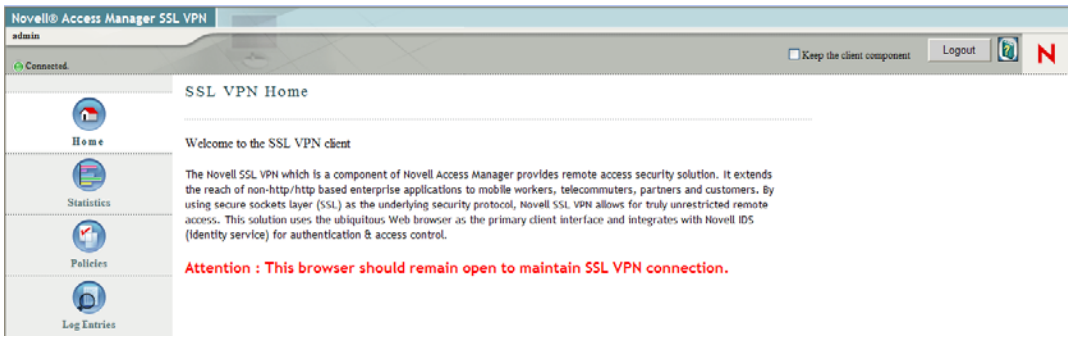
You are connected to SSL VPN in Enterprise mode in the subsequent connections. You are not prompted to for the administrator or `root` username and password the next time you log in.

---

**NOTE:** If you click *OK* in the dialog box to enable Enterprise mode of SSL VPN and you want to switch to the Kiosk mode on the same machine, see Section 3.5, "Switching from Enterprise Mode to Kiosk Mode," on page 20.

---

The Welcome page of the SSL VPN service is displayed, allowing access to all the resources listed on the *Policy* tab.




## 3.4 Enabling targetpw in Macintosh

If you are a Macintosh user, you must enable `targetpw` to connect to SSL VPN in Enterprise mode. In Macintosh, `targetpw` is disabled by default. To manually enable `targetpw`, specify the following lines in the `/etc/sudoers` directory:

```
Defaults targetpw # ask for the password of the target user i.e.
root
ALL ALL=(ALL) ALL # WARNING! Only use this together with 'Defaults
targetpw'!
```

## 3.5 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. If you want to return to Kiosk mode on the same workstation during the next login, uninstall the Enterprise mode thin-client. For more information on uninstalling the thin-client, see Section 3.6, “Uninstalling Enterprise Mode Thin-Client,” on page 20.

## 3.6 Uninstalling Enterprise Mode Thin-Client

To uninstall the Enterprise mode thin-client, do one of the following depending on your operating software:

- **Windows:** If you are a Windows user, log in as admin and run `uninstall.exe` located in the `c:/Program Files/Novell sslvpnservice` directory.
- **Linux:** If you are a Linux user, log in as `root` and enter the following command on the Linux workstation:

  ```
  rpm -e novl-sslvpn-service
  ```

- **Macintosh:** If you are a Macintosh user, log in as root and do the following on the Macintosh workstation:

  1. Enter the following command to stop the SSL VPN services:

     ```
     /System/Library/StartupItems/novell-sslvpn-service/novell-
     sslvpn-service stop
     ```

  2. Enter the following command to remove all the contents of the package:

     ```
     rm -rf /System/Library/StartupItems/novell-sslvpn-service
     ```

```
rm -rf /Library/Receipts/novl-sslvpn-service.pkg
rm -f /usr/sbin/novl-sslvpn-service
rm -f /usr/sbin/novl-sslvpn-service-upgrade
rm -f /etc/novell-sslvpn-serv.conf
```

**NOTE:** If you are an administrator or a `root` user of the machine, you can never switch from Enterprise mode to Kiosk mode.

# Accessing Published Citrix Applications through SSL VPN

4

You can access published Citrix* applications through SSL VPN, if you have configured the Access Gateway for Citrix clients.



For more information, see “Configuring SSL VPN for Citrix Clients” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

## 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 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*.

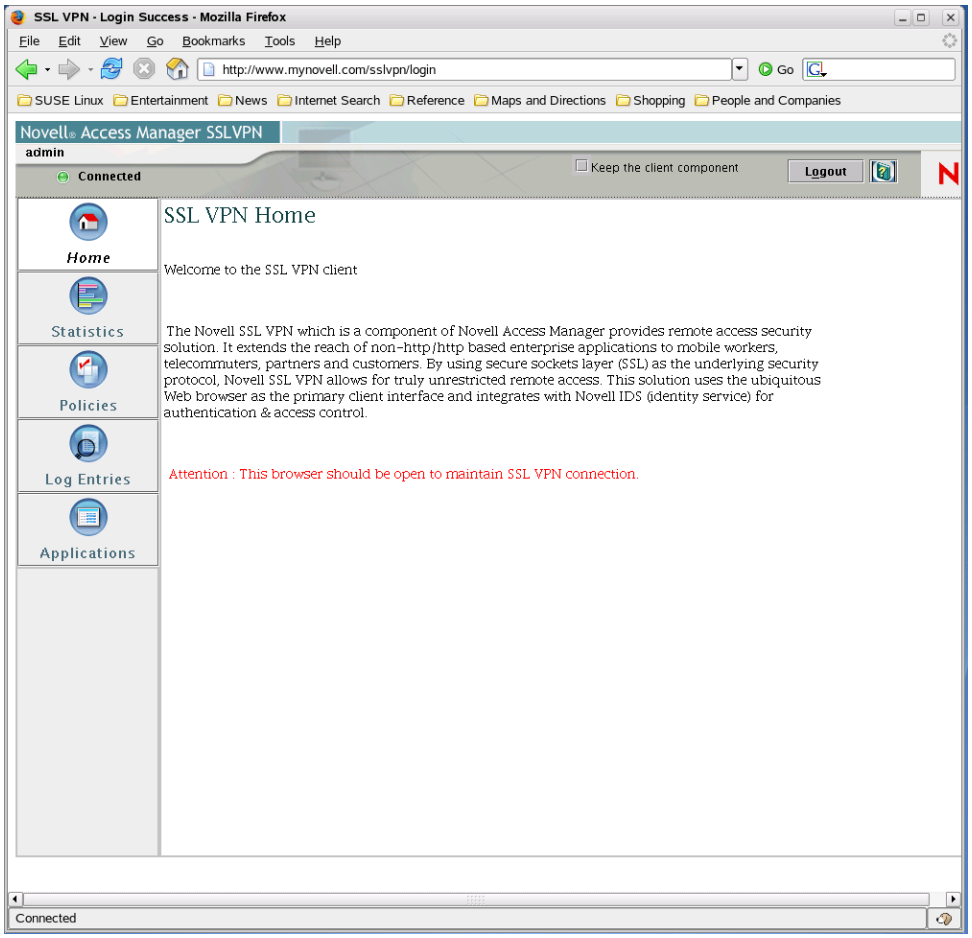
   The SSL VPN connection is automatically established. You can now access the published applications by clicking the corresponding icons on the Citrix Web page.

# Understanding the SSL VPN User Interface

5

When you access SSL VPN through the browser, the SSL VPN Welcome page is displayed after you authenticate to the server.

***Figure 5-1*** *SSL VPN Client User Interface*




This page has the following information:

- **Username:** Specifies the name of the currently logged-in user in the top left corner of the page.
- **Logout:** Click this button to log out of the current session.
- **Keep the Client Component:** Select this check box to reduce the connection time when you log in again. If you select the check box, some of the SSL VPN components are left on the client and the connecting time is reduced because these components are not downloaded again.

  If you do not enable the *Keep the Client Component* check box:

  - All the client components downloaded for the connection are removed in Kiosk mode.

- All client components other than the service RPM or service MSI are removed in Enterprise Mode. This is because the service RPM or service MSI is mandatory for operation in this mode.

- **Enable Option for Enterprise Mode:** This check box is displayed if you clicked *Ignore Forever* in the SSL VPN dialog box, in order to always connect to SSL VPN in the Kiosk mode. If you want to switch to Enterprise mode when you connect to SSL VPN the next time you log in, you must select this check box before clicking the *Logout* button.

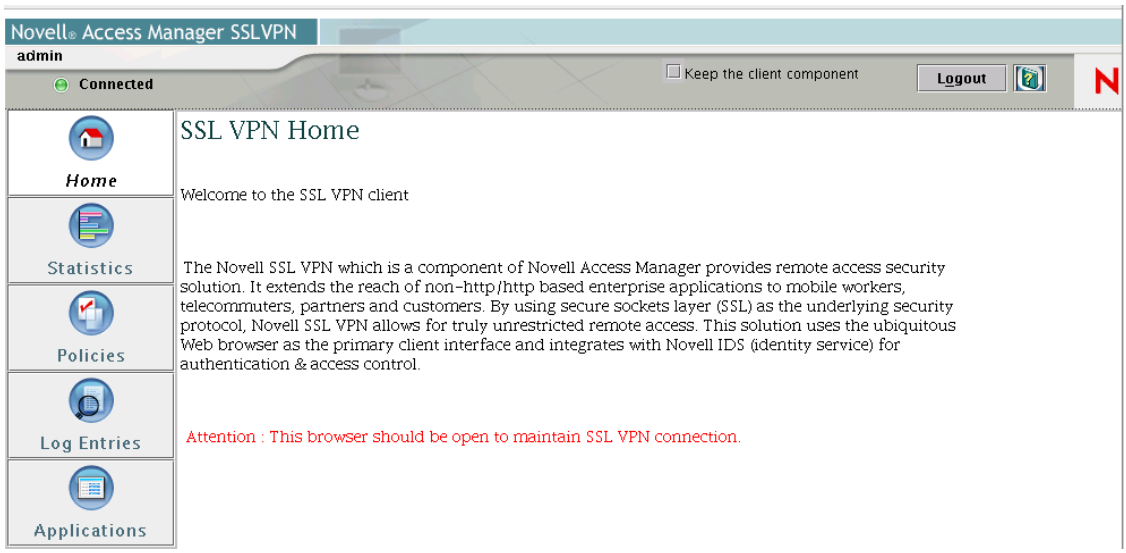
The following tabs are displayed in the SSL VPN user interface:



# 5.1 Home Page

Click the *Home* tab to display the Home page, which shows the customer or the product information. This page can be customized for different organizations.

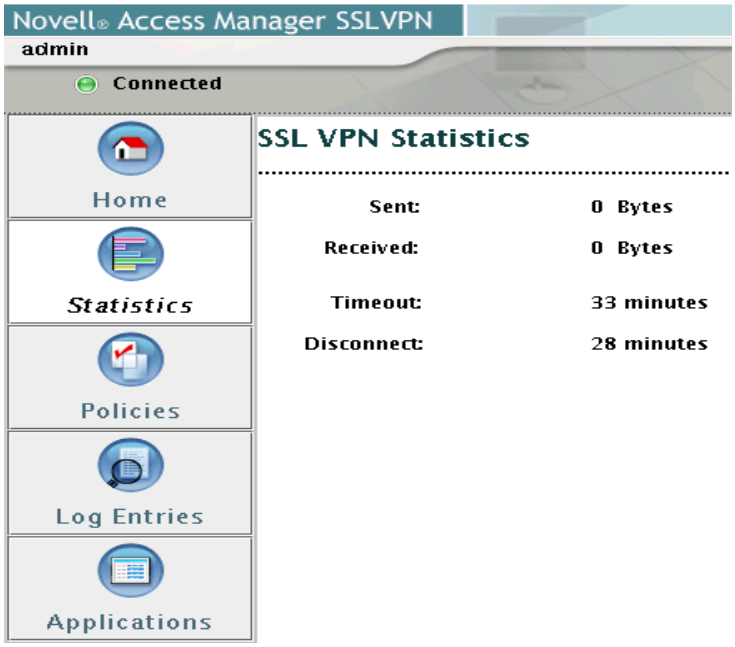
***Figure 5-2*** *SSL VPN Home Page*




# 5.2 Statistics Page

Click the *Statistics* tab to display the client statistics such as the bytes sent and received and the time to disconnect.

***Figure 5-3*** *Statistics Page*




The statistics page has the following information:

**Sent:** Bytes sent through the SSL VPN tunnel.

**Received:** Bytes received through the SSL VPN tunnel.

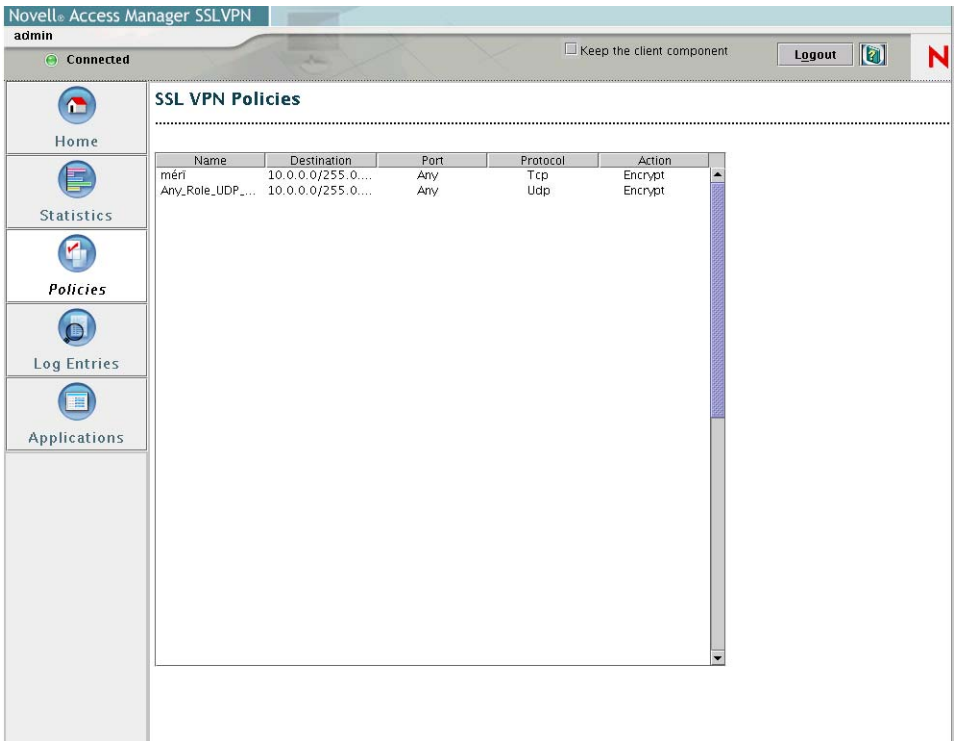
**Timeout:** The time in minutes before an idle connection is disconnected. This time can be configured on the server.

**Time to Disconnect:** The time left before disconnecting during an inactivity period. This counter is decremented only if the client is inactive or if there is no data transfer. The time is reset when there is a data transfer after the inactivity period.

# 5.3 Policies Page

Click the *Policies* tab to display the resources you can access, based on the traffic policies configured for your role. The traffic policies are configured by the administrator on the server.

***Figure 5-4*** *Policies Page*




The Policies page has the following information:

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

**Destination:** The IP address of the destination network.

**Port:** The destination port.

**Protocol:** The protocol can be TCP or UDP or ICMP or any of them.

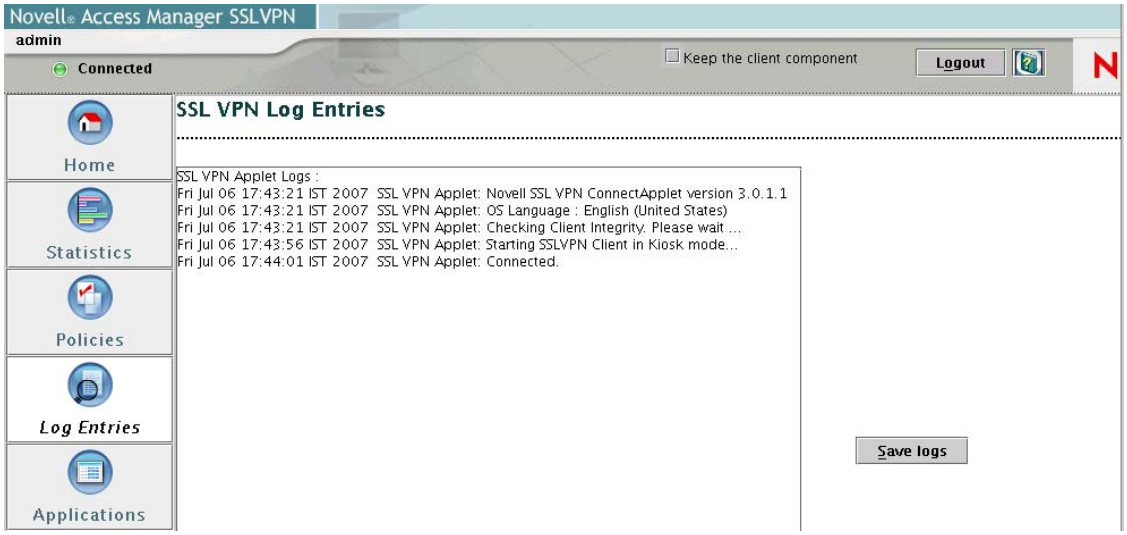
**Action:** The action can be Encrypt or Deny. If the action is Encrypt, you are permitted to access to the protected resources. If the action is Deny, you are denied access to the protected resources.

# 5.4 Log Entries Page

Click the *Log Entries* tab to display ActiveX or Java applet log entries.

If you are a Windows user, log entries are automatically saved. If you are a Linux or Macintosh user, the log entries file is stored temporarily in the `~Userhome/.sslvpn/log` directory. This directory is deleted when you log out of SSL VPN. If you want to save the log entries in order to access them later, click *Save Logs*.

***Figure 5-5*** *Log Entries Page*



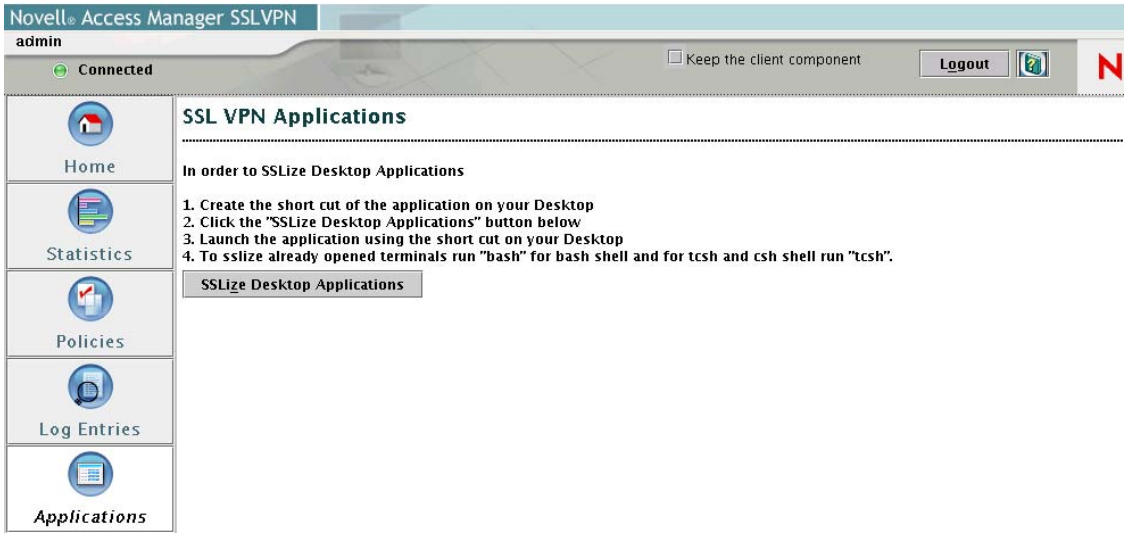

The log files are stored in the following directories:

- **Windows:** *[Your Home directory]*`\Novell\SSLVPN\log\nls\en` if you are a Windows user.
- **Linux or Macintosh:** `~Userhome/sslvpnlogs` if you are a Linux or Macintosh user.

# 5.5 Applications Page

Click the *Applications* tab to display the steps to add desktop applications to SSL VPN. This tab is available only in the Kiosk mode of Linux and Macintosh. For more in formation, see Section 2.2, “Enabling Applications for SSL,” on page 15.

***Figure 5-6*** *Applications Page*




When you add an application to the SSL VPN, it is described as SSLizing the application.

# Monitoring the SSL VPN Connection

6

The status of SSL VPN connection is displayed at the top left side of the SSL VPN User Portal. This section contains the following information:



## 6.1 Understanding the Connection Status

The connection status can be any of the following:

- **Connected:** Indicates that the Java applet or ActiveX has successfully established a connection to the SSL VPN server.
- **Disconnected:** Indicates that you have logged out of the SSL VPN session. This status is displayed when you click the *Logout* button.
- **Connecting:** Indicates that the connection is in progress. To avoid problems, you must wait until a successful connection status is displayed before clicking any other button.
- **Disconnecting:** Indicates that the disconnection is in progress. To avoid problems, you must wait until a successful disconnection status is displayed before clicking any other button.
- **Error: <*Message*>:** Indicates that the ActiveX or Java applet has encountered an error. Check the ActiveX or Applet log for more information.

## 6.2 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.

## 6.3 Logging Out of the Active SSL VPN Session

Do not disconnect the SSL VPN session by closing the browser. To log out of the active SSL VPN session:

- Click the *Logout* button. Close the browser to complete the termination of session.
- If you want to leave some of the SSL VPN components on the client machine, select the *Keep the Client Component* check box. This reduces the connection time when you log in next time, as these components do not need to be downloaded again.

  If you do not enable the *Keep the Client Component* check box:

  - All the client components downloaded for the connection are removed in Kiosk mode.

- All client components other than the service RPM or service MSI are removed in Enterprise Mode. This is because the service RPM or service MSI is mandatory for operation in this mode.

## 6.4 Disconnected NIC Icon in Enterprise Mode

When you disconnect an SSL VPN Enterprise mode connection, a disconnected NIC icon appears on your system tray if you are using the SSL VPN version older than SP3.

This icon is not visible to you if you are accessing Novell SSL VPN 3.0 SP3. But if you move from an older version to the SP3 version, the icon is still visible to you after you disconnect. If you do not want this icon on your desktop, uninstall the Enterprise mode thin-client before accessing the SP3 version of SSL VPN Enterprise mode. For more information on how to uninstall the Enterprise mode thin-client, see Section 3.6, “Uninstalling Enterprise Mode Thin-Client,” on page 20

# Troubleshooting the SSL VPN

# A

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



## A.1 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 implies that SSL VPN is unable to establish a connection with the server through 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 `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.

---

## A.2 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.

## A.3 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 `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.

## A.4 Error: Failed to Receive Keep Alive

If you have upgraded from the Iterative Release version to the Support Pack 1 version, you might get the following error message when you try to establish an SSL VPN connection:

```
Failed to receive keep alive
```

If this happens, go to *Control Panel* > *Java* and click *Delete all Files* to delete all files from the Java cache.

# Error Messages

B

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

### 4352/0x01100: Received Zero Length Data From 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.

### 4353/0x01101: Policy Resolution Request From SOCKS Client Was Not In The Correct Format (Incorrect Message Length).

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

Action: Contact your system administrator.

### 4354/0x01102: Unable to Reply to the Policy Resolution Request by 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.

### 4355/0x01103: Policy Resolution Request From SOCKS Client Was Not In the Correct Format (Incorrect Message Type)

Possible Cause: Possible hack by an intruder.

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

### 4865/0x01301: Unable to Send Statistics Reply to 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.

### 4866/0x01302: Cookie Received From Applet Was Not in the Correct Format (Incorrect Message Length)

Possible Cause: Polresolver to Applet communication is bad.

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

### 4867/0x01303: Unable to Send Acknowledgment to Applet for the Cookie Received

Possible Cause: Polresolver to Applet communication is bad.

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

### 4868/0x01304: Incorrect DNS Information Message Received From 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.

### 4869/0x01305: Unable to Send Acknowledgment to Applet for the DNS Message Received

Possible Cause: Polresolver to Applet communication is bad.

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

### 4870/0x01306: Disconnect Message From Applet Was Incorrect (Incorrect Message Length)

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

Action: Contact your system administrator if the problem persists.

### 4871/0x01307: Unable to Send Acknowledgment to Applet for the Disconnect Message Received

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

Action: Contact your system administrator if the problem persists.

### 4872/0x01308: Polresolver Received An Incomplete Message. Unable to Identify The Sender.

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

Action: Contact your system administrator with appropriate logs.

### 4873/0x01309: Failed to Allocate Memory For Internal Operation.

Possible Cause: Insufficient memory.

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

### 5376/0x01500: 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.

### 5377/0x01501: Statistics Response Message From Stunnel was Incorrect (Incorrect Message Length)

Possible Cause: Polresolver to Stunnel communication is bad.

Action: Contact your system administrator with appropriate logs.

### 5378/0x01502: Unable to Send Disconnect Message From Stunnel.

Possible Cause: Stunnel is down.

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

### 5379/0x01503: Disconnect Acknowledgment Message From Stunnel Was Incorrect (Incorrect Length of Message)

Possible Cause: Polresolver to Stunnel message is bad.

Action: Contact your system administrator with appropriate logs.

### 5380/0x01504: Incorrect Message From Stunnel (Incorrect Length of Message)

Possible Cause: Polresolver to Stunnel communication is bad.

Action: Contact your system administrator with appropriate logs.

### 5381/0x01505: Invalid Message From Stunnel (Message Type Unknown)

Possible Cause: Polresolver to Stunnel communication is bad.

Action: Contact your system administrator with appropriate logs.

### 0x01506: SSL VPN Server Certificate Validation Failed. Please Log out.

Possible Cause: Failed to validate the certificate.

Action: Contact your system administrator with appropriate logs.

### 0x01507: Disconnected due to 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 to connect.

### 0x01701: OpenVPN Authentication Failed. Please Log out.

Possible Cause: Password verification failed.

Action: Contact your system administrator with appropriate logs.

### 0x01702: OpenVPN Connection Error. Please Log out.

Possible Cause: Certificate verification failed.

Action: Contact your system administrator with appropriate logs.

### 0x01703: Received Fatal Error from OpenVPN. Please Log out.

Possible Cause: TUN/TAP allocation failed.

Action: Try disconnecting and connecting again. If the problem persists, contact the system administrator.

### 0x01704: Policy Initialization Failed. Please Log out.

Possible Cause: Temporary file creation failed.

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

### 0x01705:Tun Interface is Down. Please Log out.

Possible Cause: The TUN interface is down.

Action: Contact your system administrator with appropriate logs.

### 0x01801: Service is not Running. Please Log out.

Possible Cause: Failed to find a free port.

Action: Check the system log and contact your system administrator.

### Connections Threshold Exceeded. Please Try Again After Some Time.

Possible Cause: The server has reached the limit for maximum number of connections. The low bandwidth SSL VPN, allows only 249 simultaneous SSL VPN sessions and a transfer rate of 40Mbits per second.

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

If your deployment requires 250 or more concurrent SSL VPN connections, you can install the high bandwidth version of Novell SSL VPN, after getting an export clearnace from the US security board.

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

### 0x01804: Maximum Attempt to Enter Password Reached. Please Close the Browser.

Possible Cause: You have not entered the correct credentials within the maximum tries.

Action: Log in again with the correct credentials.

### 0x01805: Timeout Occurred While Entering Credentials. Please Close the Browser.

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

Action: Log in again with the correct credentials.

### 0x01000: Client Integrity Check Failed. Check Error Logs for More Information.

Possible Cause: The connection requires software that is currently not running in the system.

Action: Check and install the software.

### 0x01001: Server is not Responding.

Possible Cause: Either the VPN server or Access Manager is down or the network is disconnected.

Action: Check the link and reconnect.

### 0x01002: 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 VPN server to the client. 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.

### 0x01003: Problem with One of the Underlying Components/ Connection Error. Please Logout.

Possible Cause: One of the client components encountered a problem.

Action: Check the log entries for more information.

### 0x01004: Problem with One of the Underlying Components. Please Disconnect.

Possible Cause: One of the client components encountered a problem.

Action: Check the log entries for more information.

### 0x01005: Failed to Find Free Ports on Client.

Possible Cause: No free ports are available.

Action: Contact your system administrator.

### 0x01006: Resource Not Found on the Gateway.

Possible Cause: Improper server installation.

Action: Reinstall the SSL VPN server build.

### 0x01007: Failed to Download SSL VPN Files from the Gateway.

Possible Cause: Insufficient space on the client.

Action: Ensure that 2 MB free space is available on the Windows drive on the client.

### 0x01008: Unable to Fetch the Configuration Information from the Gateway.

Possible Cause: Improper server configuration.

Action: Check and change the server configuration.

### 0x01009: Unable to Fetch the Policy Information from the Gateway.

Possible Cause: Improper Access Gateway configuration.

Action: Check and change the Access Gateway configuration.

### 0x0100A: User Denied Access. Please Contact System Administrator.

Possible Cause: The user or the user role does not have a policy.

Action: Contact your system administrator.

### 0x0100B: OpenSSL Needs to be Installed. Please Logout.

Possible Cause: OpenSSL is not installed on the client.

Action: Install OpenSSL 0.9.7 or later.

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

Action: Install OpenSSL 0.9.7 or later in the correct path.

### 0x0100C: Dependent Components not Available in this System. Please Logout.

Possible Cause: OpenSSL is not installed on the client.

Action: Install OpenSSL 0.9.7 or later.

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

Action: Install OpenSSL 0.9.7 or later in the correct path.

### 0x0100D: Another Instance of SSL VPN is Running. Please Close this Browser.

Possible Cause: Another instance of SSL VPN is running in another browser.

Action: Close the browser where another instance of SSL VPN is running.

Possible Cause: The previous connection was not properly cleaned up.

Action: Clean up the previous connection.

### 0x0100E Failed to Receive Keepalive. Please Logout.

Possible Cause: The SSL VPN server is down.

Action: Check the SSL VPN server health status and restart the server.

Possible Cause: The Access Gateway is down.

Action: Check the Access Gateway health status and start the gateway.

### 0x0100F: Gateway Internal Error.

Possible Cause: The server is malfunctioning.

Action: Contact your system administrator.

### 0x01010: Unable to Contact Gateway. Please Close this Browser.

Possible Cause: The SSL VPN server is down.

Action: Check the SSL VPN server health status and restart the server.

Possible Cause: The Access Gateway is down.

Action: Check the Access Gateway health status and start the gateway.

### 0x1011: This Operating System is not Supported. Please Logout.

Possible Cause: Your operating system is not supported.

Action: Contact your system administrator.

### 0x1012: User Does Not Seem to Have Enough Privilege. Please Log out.

Possible Cause: The user does not have enough rights to start the SSL VPN client.

Action: Contact your system administrator.

### 0x1014: Unable to Fetch 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 disconnecting and reconnecting to the SSL VPN gateway. If the problem persists, contact your system administrator.

### 0x1016: Failed to Fetch CIC Policy from the Gateway

Possible Cause: Either the gateway has closed the connection or there is a problem with the connectivity.

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

### 0x1017: No Policies are Configured for this User

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

Action: Contact your system administrator

### 0x1018: Gateway Disconnected

Possible Cause: The gateway might have gone down.

Action: Contact your system administrator.

### 0x1019: Failed to Start the Client. Please Log out.

Possible Cause: The SSL VPN components failed to start.

Action: Try restarting the SSL VPN client. If the problem persists, contact your system administrator.

### 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.*