

Novell BorderManager®

3.9

April 05, 2007

VIRTUAL PRIVATE NETWORK CLIENT
INSTALLATION GUIDE

www.novell.com



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 \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 1997-2007 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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 \(http://www.novell.com/company/legal/patents/\)](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 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	7
1 Overview	9
1.1 Novell BorderManager VPN Client on Windows	9
1.1.1 Features	9
1.1.2 System Requirements	9
1.2 Novell BorderManager VPN Client on Linux	10
1.2.1 Features	10
1.2.2 System Requirements	10
2 Installing Novell BorderManager VPN Client	13
2.1 Installing the Novell BorderManager 3.9 VPN Client on Windows	13
2.2 Installing Novell BorderManager 3.9 VPN Client on Linux	14
2.2.1 Before you Begin	14
2.2.2 Installing the Client	14
3 Uninstalling the Novell BorderManager 3.9 VPN Client	15
3.1 Uninstalling Novell BorderManager 3.9 VPN Client From Windows	15
3.2 Uninstalling Novell BorderManager 3.9 VPN Client From Linux	15
4 Using the VPN client for Linux	17
4.1 Accessing VPN Client	17
4.1.1 Root Access	17
4.1.2 Non-Root Access	17
4.2 Creating A VPN Client Profile To Connect To Novell BorderManager 3.9	18
4.3 Connection Profiles	19
4.3.1 Creating a Profile for Connecting to the Standard IPsec Gateway	19
4.3.2 Creating a Profile for Connecting to the Nortel Contivity Server	21
4.3.3 Editing a Profile	23
4.3.4 Deleting a Profile	23
4.4 Establishing a VPN Connection	24
4.4.1 Using the Graphical User Interface	24
4.4.2 Using the Command Line Utility	26
A Troubleshooting Novell VPN client for Linux	29
A.1 Guidelines for the User	29
A.1.1 General Guidelines	29
A.1.2 IKE Status	29
A.1.3 IKE Log	30
A.2 Application Errors	30
A.3 Scenarios	30
A.3.1 IKE Phase 1 Deleted	30
A.3.2 Failed to Connect to IKE	30
A.3.3 Non-Root User: Failed to Connect to IKE	31
A.3.4 Fragmentation of TCP Packets	31

A.3.5	Profile Creation Failed	31
A.3.6	Firewall Issues	32
A.4	FAQs	32
A.4.1	Where can I get information on the error codes that I encounter while using the VPN Client?	32
A.4.2	explaining temporary unavailability of resources. What does this mean?	33
A.4.3	What should I do to get IKE debug logs?	33
A.4.4	How can I find out if the VPN Client is installed on my system?	33
A.4.5	I cannot see all of the VPN Client GUI on my monitor. What should I do?	33

B Error Codes 35

B.1	GUI Messages	35
B.2	CLI Messages	38

About This Guide

Novell® BorderManager® 3.9 includes premier firewall and Virtual Private Network (VPN) technologies that safeguard your network and help you build a secure identity management solution. These technologies protect networks and resources, while ensuring end-user productivity.

With the powerful directory-integrated features in Novell BorderManager, you can monitor users' Internet activities and control their remote access to corporate resources.

In addition, Novell BorderManager provides Internet access control and supports numerous content-filtering solutions. These features protect your network from undesirable Internet content, including programs that destroy or steal data, games that waste users' time, and Web pages that expose your company to legal liability.

This documentation presents an introduction to VPN Client, which is part of Novell BorderManager 3.9.

Audience

This audience for this documentation are experienced network administrators.

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 most recent version of the *Virtual Private Network Installation Guide*, visit the [Novell Documentation Web site](http://www.novell.com/documentation/nbm39/index.html). (<http://www.novell.com/documentation/nbm39/index.html>)

Additional Documentation

This *Virtual Private Network Client Installation Guide* is a part of documentation set for Novell BorderManager 3.9.

- ◆ *Novell BorderManager 3.9 Administration Guide*
- ◆ *Novell BorderManager 3.9 Installation Guide*
- ◆ *Novell BorderManager 3.9 Proxy and Firewall Overview and Planning Guide*
- ◆ *Novell BorderManager 3.9 Troubleshooting Guide*
- ◆ *Novell BorderManager 3.9 Virtual Private Network Deployment Frequently Asked Questions*

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

1

The VPN client software is installed on a remote workstation. It communicates with a VPN server on an enterprise network or, with a service provider and creates a secure connection over the Internet. Through this connection, you can access the private network as if you were an on-site user.

With this release of Novell BorderManager, you can install the VPN client on Linux* as well as Windows.

This section contains information on the following:

1.1 Novell BorderManager VPN Client on Windows

The following sections explain the features and system requirements of VPN client on Windows:

- ◆ [Section 1.1.1, “Features,” on page 9](#)
- ◆ [Section 1.1.2, “System Requirements,” on page 9](#)

1.1.1 Features

- ◆ Novell BorderManager VPN client on Windows operates in IKE mode to communicate with Novell BorderManager 3.9 and Novell BorderManager 3.8 SP5 VPN servers.
- ◆ In IKE mode, it supports X509 certificate and pre-shared key (NMAP and LDAP).
- ◆ NMAP supported methods include:
 - ◆ NDS eDirectory™
 - ◆ Simple Password
 - ◆ Enhanced Password
 - ◆ Universal SmartCard
 - ◆ LDAP

1.1.2 System Requirements

Novell BorderManager 3.9 VPN client has the following system requirements:

Hardware Requirements

- ◆ Pentium* IV
- ◆ Minimum of 128 MB of free disk space
- ◆ Minimum of 64 MB of RAM

Software Requirements

- ◆ Windows 2000, Windows XP

NOTE: Novell Client™ 4.91 is recommended for Windows 2000, XP, and XP Home edition.

The following software is installed along with the Novell BorderManager VPN client:

- ◆ NCI 1.7.0

This is a kernel version of NCI and can co-exist with a user space NCI. If an earlier version of NCI exists on your workstation, this version overwrites the earlier version.

- ◆ NCI 2.6

This is a user space version of NCI and can co-exist with a kernel version of NCI. If an earlier version of NCI exists on your workstation, this version overwrites the earlier version.

- ◆ PKI client 2.4.0
- ◆ SAL 2.0
- ◆ LDAP SDK 2.1.0 and DClient 8.7
- ◆ NMAE EE 2.2.4

This is an optional installation. It is packaged with Novell BorderManager VPN client to enable users to install it if required.

1.2 Novell BorderManager VPN Client on Linux

The following sections explain the features and system requirements of VPN client on Linux:

- ◆ [Section 1.2.1, “Features,” on page 10](#)
- ◆ [Section 1.2.2, “System Requirements,” on page 10](#)

1.2.1 Features

- ◆ The Novell BorderManager VPN client on Linux operates in SKIP mode to communicate with earlier versions of the VPN server and Novell BorderManager 3.9 VPN server.
- ◆ In SKIP mode, it uses the eDirectory mode of authentication.
- ◆ NMAE supported methods include NDS (eDirectory)

1.2.2 System Requirements

Novell BorderManager 3.9 VPN client has the following system requirements:

Hardware Requirements

- ◆ Pentium IV
- ◆ Minimum of 128 MB of free disk space
- ◆ Minimum of 64 MB of RAM

Software Requirements

- ◆ NCI 2.6.4 or later
- ◆ NMAE 3.2.0 or later

- ◆ SUSE® Linux Enterprise Desktop (SLED) 10

Installing Novell BorderManager VPN Client

2

This section contains the following information:

- ♦ [Section 2.1, “Installing the Novell BorderManager 3.9 VPN Client on Windows,” on page 13](#)
- ♦ [Section 2.2, “Installing Novell BorderManager 3.9 VPN Client on Linux,” on page 14](#)

2.1 Installing the Novell BorderManager 3.9 VPN Client on Windows

To install Novell BorderManager 3.9 VPN client on your Windows workstation:

- 1 Do one of the following:
 - ♦ At the root of the Novell BorderManager 3.9 CD, go to `cl_inst\vpn\exes`, and copy `setupex.exe` to the local drive where you want to install the VPN client, then click `setupex.exe`.
 - ♦ From the Novell BorderManager CD, go to `cl_inst\vpn`, and copy the `Disk 1` directory to the local drive where you want to install the VPN client, then go to `Disk 1` and run `setupex.exe`.
- 2 Follow the on-screen instructions to install the VPN client on your workstation.
The setup configures the parameters associated with a secure connection.
- 3 During the process, the install prompts you to configure or install the following:
 - ♦ Dial-up VPN client
 - ♦ NMAS client

WARNING: If you have installed the latest version of the Novell Client, do not select the NMAS™ install option during the install.

It also installs the following two versions of NICI on your system:

- ♦ NICI 1.7.0 (128-bit)
 - ♦ NICI 2.6.0 (128-bit)
- 4 After the VPN client is installed, it prompts you to re-start your workstation. During the re-start, if your workstation has the Novell Client, the VPN client registers with NetWare® client. If your workstation does not have NetWare, the VPN client resides on the desktop. If the operating system on your system is Windows XP, go to *My Computer > Hardware > Driver Signing*. If the option is `Block`, change the option to `Warn`. To enable NMAS and Token Password, the workstation should have NMAS EE 2.2.4 or later.

For detailed on information on VPN client on Windows, refer the *Novell BorderManager 3.9 Administration Guide* “[Virtual Private Network Client](#)”.

2.2 Installing Novell BorderManager 3.9 VPN Client on Linux

This section contains the following information on installing the Novell BorderManager 3.9 VPN client on Linux:

- [Section 2.2.1, “Before you Begin,” on page 14](#)
- [Section 2.2.2, “Installing the Client,” on page 14](#)

2.2.1 Before you Begin

Before you begin with the actual installation, uninstall the following RPMs if they are already installed in the system. Uninstall them in the following order:

1. NetworkManager-novellvpn
2. nortel-plugins
3. turnpike
4. novell-ipsec-tools-devel
5. novell-ipsec-tools

2.2.2 Installing the Client

To install the Novell BorderManager 3.9 VPN client on your Linux workstation:

- 1 At the root of the Novell BorderManager 3.9 CD, go to `Border Manager Folder/CL_INST/VPN/Linux`, and copy `tar.gz` to the local drive where you want to install the VPN client.

- 2 Log in as `root`.

IMPORTANT: The VPN client can be installed only with `root` privileges.

- 3 Install NICE 2.6.4 or later and NMAP 3.2.0 or later.

IMPORTANT: If these are not installed, you cannot continue with the installation.

- 4 Untar the `tar.gz`.

- 5 Install using the `NVPN-INST` script.

- 6 Restart `racoon` with the following command: `/etc/init.d/racoon restart`

- 7 Create the profiles using Network Manager VPN connections and connect to Novell BorderManager.

Uninstalling the Novell BorderManager 3.9 VPN Client

3

This section contains information on the following:

- [Section 3.1, “Uninstalling Novell BorderManager 3.9 VPN Client From Windows,”](#) on page 15
- [Section 3.2, “Uninstalling Novell BorderManager 3.9 VPN Client From Linux,”](#) on page 15

3.1 Uninstalling Novell BorderManager 3.9 VPN Client From Windows

- 1 Click *Start > Settings > Control Panel > Add/Remove Programs*.
- 2 Select *Novell BorderManager 3.9 VPN Client > Remove*.

This removes all the bindings imposed during the VPN client installation. It provides you with an option to remove the components installed with VPN client.

3.2 Uninstalling Novell BorderManager 3.9 VPN Client From Linux

- 1 Log in as `root`.
- 2 Enter the following command to uninstall the RPMs:

```
rpm -e rpm name
```

Replace *rpm name* with the name of the RPM.

Uninstall the RPMs in the following order:

1. `NetworkManager-novellvpn`
2. `novell-nortelplugins`
3. `novell-nbplugins`
4. `turnpike`
5. `novell-ipsec-tools-devel`
6. `novell-ipsec-tools`

Using the VPN client for Linux

4

This chapter provides the following information to help you effectively set up and use Novell VPN client for Linux.

- ♦ [Section 4.1, “Accessing VPN Client,” on page 17](#)
- ♦ [Section 4.2, “Creating A VPN Client Profile To Connect To Novell BorderManager 3.9,” on page 18](#)
- ♦ [Section 4.3, “Connection Profiles,” on page 19](#)
- ♦ [Section 4.4, “Establishing a VPN Connection,” on page 24](#)

4.1 Accessing VPN Client

This section contains information on the following:

- ♦ [Section 4.1.1, “Root Access,” on page 17](#)
- ♦ [Section 4.1.2, “Non-Root Access,” on page 17](#)

4.1.1 Root Access

A super user can directly access VPN.

4.1.2 Non-Root Access

All users belonging to the primary group *users* created by *root* can use VPN client.


If *users* is not the primary group of those users who require VPN access, *non-root* access can be allowed by doing the following:

By default, all users belong to this group.

- 1 Log in as *root*.
- 2 Open the `/etc/racoon/racoon.conf` file.
- 3 Replace *users* with the name of the group that requires VPN access.

```
#isakmp :::1 [7000];
#isakmp 202.249.11.124 [500];
#admin [7002];          # administrative's port by kmpstat.
#strict_address;      # required all addresses must be bound.
adminsock "/var/racoon/racoon.sock" "root" "users" 660;
}

# Specification of default various timer.
timer
```



- 4 Restart IKE by entering the following command:

```
/etc/init.d/racoon restart
```

IMPORTANT: The `root` does not allow multiple groups to use VPN client. So, if you modify `racoon.conf` to permit a new group, only users belonging to that group can access the VPN.

4.2 Creating A VPN Client Profile To Connect To Novell BorderManager 3.9

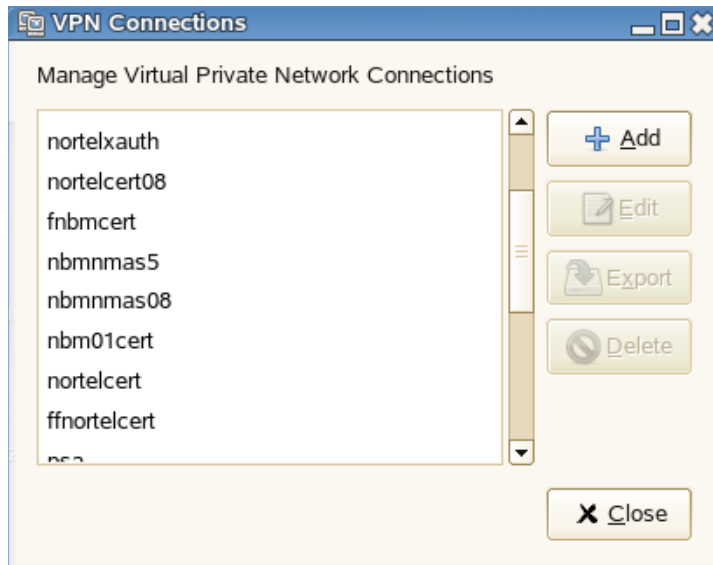
This section explains the procedures to create a VPN client profile to connect to Novell BorderManager 3.9.

To create a VPN client profile, do the following:

- 1 After you have installed the VPN Linux client, open a system terminal. Install the VPN Linux client; change to root and using `su`, run the following command:

```
cat /var/log/vpnClientInstall.log
```

After this, you get a message that the installation is terminated successfully.
- 2 Using KDE, click *KnetworkManager* > *VPN Connections*.
- 3 Next, click *+Add*.



- 4 Click *Forward*.
- 5 In the *Connect To* options, select *NovellvpnClient*.

TIP: You had installed VPN client with no errors and still do not see any options here, reboot your computer.

- 6 Provide a connection name, provide a name to identify this connection.
- 7 Select the gateway type as Novell BorderManager.
- 8 Select the authentication type as NMAS.
- 9 For the gateway, provide the IP address of the Novell BorderManager server.
- 10 Select *NMAS*.
- 11 Select the sequence as NDS.

- 12 Provide the *Context* of the user and the *UserName*.
- 13 Under the *Optional Information*, click *DH Group > DH2*.
- 14 Next, click *PFS Group > 1*.
- 15 Click *Apply*. Your profile is now created.

Verify that racoon service is ready. As root on a system console type: `rcracoon restart`.

To use this profile to connect to your Novell BorderManager server, do the following:

- 1 Click *KnetworkManager*.
- 2 Select *Connect to NBM 3.9*
- 3 Provide the username and password. Your connection is now made.

To verify whether the connection is made, on the terminal server console, type *ifconfig*. You will see an *ethx:x* interface with the IP address of the VPN client pool you configured in the iManager.

You will now be able to access your internal networks through the VPN Linux client.

4.3 Connection Profiles

Connection profiles contain a unique configuration of the parameters used for making a successful VPN connection. Each profile in XML format is saved as a `.prf` file. VPN client provides a Profile Manager to help you with the connection profiles.

The Profile Manager helps you create, edit, or delete profiles. While editing profiles, you cannot change the profile names.

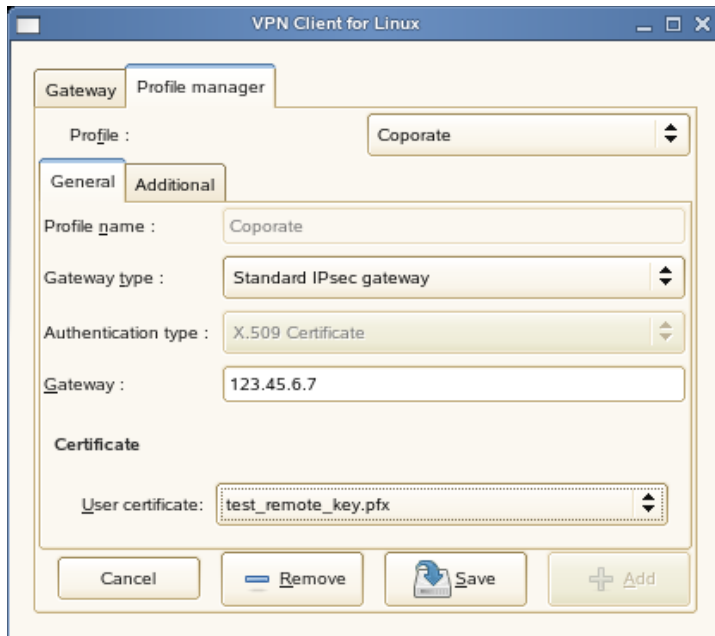
NOTE: You cannot create profiles using CLI. You must use the Profile Manager to create and modify profiles.

- ♦ [Section 4.3.1, “Creating a Profile for Connecting to the Standard IPsec Gateway,” on page 19](#)
- ♦ [Section 4.3.2, “Creating a Profile for Connecting to the Nortel Contivity Server,” on page 21](#)
- ♦ [Section 4.3.3, “Editing a Profile,” on page 23](#)
- ♦ [Section 4.3.4, “Deleting a Profile,” on page 23](#)

4.3.1 Creating a Profile for Connecting to the Standard IPsec Gateway

- 1 Open the VPN client for Linux dialog.
GNOME: Click *Computer > More Applications > System > VPN Login*.
KDE: Click the main menu *> System > VPN Login*.
- 2 In the *Profile name* drop-down list, select *Profile manager*.
- 3 Click *Add* to create a profile.
- 4 In the *Profile name* field, specify a name for the profile.

- 5 Select *Standard IPsec gateway* from the *Gateway type*.drop-down list.



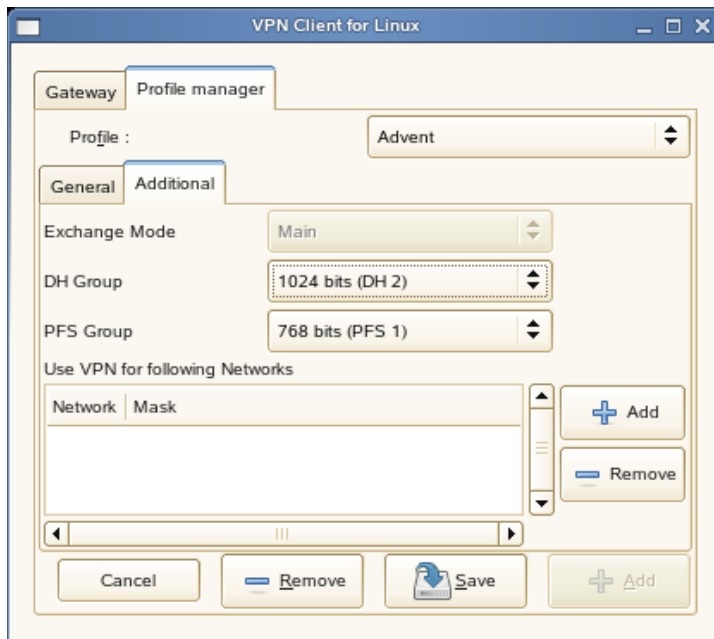
TIP: If you have not copied the user certificate in .pfx format, the error No .pfx files appears. For details, refer to [“Copying the User Certificate” on page 24](#).

- 6 Specify the following details:
- ♦ **Gateway:** Specify the gateway IP address or gateway name.

NOTE: “Gateway” refers to your Novell BorderManager 3.9 VPN server.

- ♦ **User certificate:** Select the user certificate.

- 7 Click the *Additional* tab to configure the exchange mode, DH group, PFS group, network, and mask.



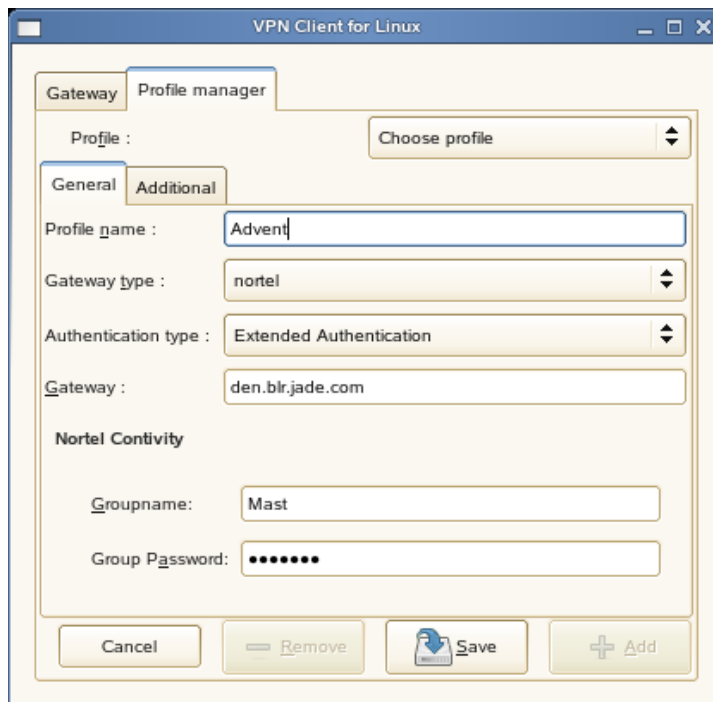
IMPORTANT: Ensure that the VPN client configuration matches the configuration on the gateway to which you are connecting. If you are connecting to a standard Novell BorderManager 3.9 server, the preceding image shows the correct values.

- 8 Click *Save* to save the profile.
- 9 Click *Done* to return to the VPN client dialog.

4.3.2 Creating a Profile for Connecting to the Nortel Contivity Server

- 1 Open the VPN client for Linux dialog.
GNOME: Click *Computer > More Applications > System > VPN Login*.
KDE: Click the main menu > *System > VPN Login*.
- 2 In the *Profile name* drop-down list, select *Profile manager*.
- 3 Click *Add* to create a profile.
- 4 In the *Profile name* field, specify a name for the profile.

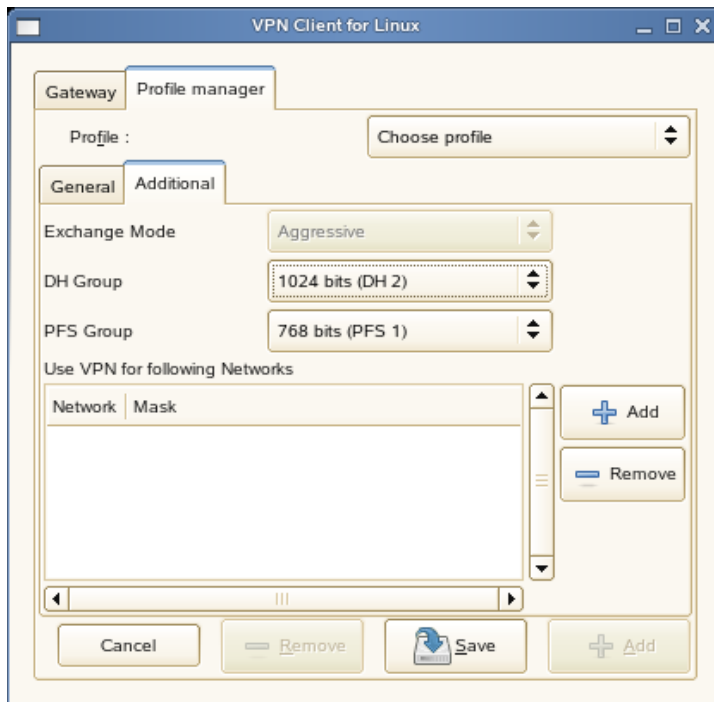
5 Select *Nortel* from the *Gateway type*.drop-down list.



6 Specify the following details:

- ♦ **Gateway:** Specify the gateway IP address or gateway name.
- ♦ **Groupname:** Specify the user group name.
- ♦ **Group Password:** Specify the group password.

- 7 Click the *Additional* tab to configure the exchange mode, DH group, PFS group, network, and mask.



IMPORTANT: Ensure that the VPN client configuration matches the configuration on the gateway you are connecting to.

- 8 Click *Save* to save the profile.
- 9 Click *Done* to return to the VPN client dialog.

4.3.3 Editing a Profile

- 1 Open the VPN client for Linux dialog.
GNOME: Click *Computer > More Applications > System > VPN Login*.
KDE: Click the main menu > *System > VPN Login*.
- 2 In the *Profile name* drop-down list, select *Profile manager*.
- 3 Click *Choose profile*, then select the name of the profile you want to edit.
You can edit all the parameters except the profile name.

4.3.4 Deleting a Profile

- 1 Open the VPN client for Linux dialog.
GNOME: Click *Computer > More Applications > System > VPN Login*.
KDE: Click the main menu > *System > VPN Login*.
- 2 In the *Profile name* drop-down list, select *Profile manager*.

- 3 Click *Choose profile*, then select the name of the profile you want to delete.
- 4 Click *Remove*.

4.4 Establishing a VPN Connection

The VPN client for Linux lets you establish a connection with a Nortel* Contivity* server or Standard IPsec gateway. You can do this using either the Graphical User Interface (GUI) or the Command Line Interface (CLI).

IMPORTANT: The CLI and GUI options might not interact properly. We do not recommend using them at the same time.

- ♦ [Section 4.4.1, “Using the Graphical User Interface,” on page 24](#)
- ♦ [Section 4.4.2, “Using the Command Line Utility,” on page 26](#)

4.4.1 Using the Graphical User Interface

The following section describe how to use the graphical user interface

Connecting to a Standard IPsec Gateway

- ♦ [“Copying the User Certificate” on page 24](#)
- ♦ [“Connecting to the Gateway” on page 24](#)

Copying the User Certificate

Copy your user certificate in `.pfx` format to the following path:

```
/user's home directory/.turnpike/usercerts
```

Connecting to the Gateway

- 1 Open the VPN client for Linux dialog.

GNOME: Click *Computer > More Applications > System > VPN Login*.

KDE: Click the main menu *> System > VPN Login*.

- 2 Select a *Standard IPsec Gateway* profile from the *Profile name* drop-down list.



All the fields in the upper section of the dialog are automatically displayed.

- 3 In the *Password* field, specify the certificate password.
- 4 Click *Connect*.

The *Connection Details* tabbed page displays the progress of the connection.

- 5 Click *Disconnect* if you want to end the connection.

NOTE: For the VPN connection to a Standard IPsec gateway, after Phase 1 is established, any data going to the network is encrypted.

Connecting to a Nortel Contivity Server

- 1 Open the VPN client for Linux dialog.

GNOME: Click *Computer > More Applications > System > VPN Login*.

KDE: Click the main menu *> System > VPN Login*.

- 2 Select a Nortel Contivity Server profile from the *Profile name* drop-down list.



The Gateway information is automatically displayed.

- 3 In the *Nortel Contivity* section, specify the following details:
 - ♦ **Username:** The name of the user who requires the connection.
 - ♦ **User Password:** The user password.
 - 4 Click *Connect*.
- The *Connection Details* tabbed page displays the progress of the connection.
- 5 Click *Disconnect* if you want to end the connection.

4.4.2 Using the Command Line Utility

The VPN client for Linux provides a command line utility to carry out the major VPN functions. After installing VPN client for Linux, you can access the help by entering the following in a terminal.

```
nvpn -h
```

NOTE: You must have root privileges to run this command.

This lists all the CLI commands and the available options, described in the following table:

Option	Description
<code>nvpn -c</code>	Connects to the VPN gateway in the PROFILENAME.
<code>nvpn -d</code>	Disconnects from the VPN gateway.
<code>nvpn -h</code>	Displays the VPN client help.
<code>nvpn -l</code>	Lists the available profiles along with their gateway types.

Option	Description
<code>nvpn -v</code>	Displays a detailed log when used with the connect option as follows: <code>nvpn -v -c</code>

Creating Profiles Using a CLI

You cannot create connection profiles using the CLI feature. Profiles must be created and edited using the GUI. See [Section 4.3, “Connection Profiles,” on page 19](#) for more information.

Connecting to the Gateway

IMPORTANT: The VPN client for Linux allows only one connection at a time.

To connect to the gateway, enter any of the following commands:

```
nvpn -c profile
```

```
nvpn --connect profile
```

```
nvpn -v -c profile
```

```
nvpn --verbose --connect profile
```

TIP: Use the command `nvpn -l` command for a list of all available profiles along with their gateway types.

Disconnecting from the Server

To disconnect from the server, enter the following command:

```
nvpn -d
```


Troubleshooting Novell VPN client for Linux

A

This appendix provides troubleshooting scenarios that you might encounter while working with the Novell BorderManager 3.9 VPN client for Linux.

- ◆ [Section A.1, “Guidelines for the User,” on page 29](#)
- ◆ [Section A.2, “Application Errors,” on page 30](#)
- ◆ [Section A.3, “Scenarios,” on page 30](#)
- ◆ [Section A.4, “FAQs,” on page 32](#)

A.1 Guidelines for the User

- ◆ [Section A.1.1, “General Guidelines,” on page 29](#)
- ◆ [Section A.1.2, “IKE Status,” on page 29](#)
- ◆ [Section A.1.3, “IKE Log,” on page 30](#)

A.1.1 General Guidelines

- ◆ Do not modify the IKE configuration file (`/etc/racoon/racoon.conf`).
- ◆ Do not modify the XML files in `/user's home directory/.turnpike/profiles`.
- ◆ Do not use the `setkey` command to alter the IPsec policies or IPsec security association (SA).
- ◆ If you are exiting, a session (for instance GNOME* or KDE), disconnect from the VPN *before* logout. Otherwise, the VPN connection continues.
- ◆ Use the CLI and the GUI options separately, because these features might not interact properly.

A.1.2 IKE Status

NOTE: You must log in as `root` to check the IKE status.

To check the IKE status, use the following command:

```
/etc/init.d/racoon status
```

Either of the following statuses is displayed

- ◆ **Running:** IKE is up and running.
- ◆ **Unused/Dead:** To start the IKE, use the following command:

```
/etc/init.d/racoon start
```

To stop the IKE daemon, use the following command:

```
/etc/init.d/racoon stop
```

A.1.3 IKE Log

If IKE is running at the default log level, all information including the error messages is logged.

The IKE log can be accessed at `/var/log/messages`.

A.2 Application Errors

Application errors are unidentified errors with the VPN client application.

If you encounter any of the application errors referred to in [Appendix B, “Error Codes,” on page 35](#), try reinstalling the VPN client. If the error repeats, try installing the latest version of VPN client.

A.3 Scenarios

- ◆ [Section A.3.1, “IKE Phase 1 Deleted,” on page 30](#)
- ◆ [Section A.3.2, “Failed to Connect to IKE,” on page 30](#)
- ◆ [Section A.3.3, “Non-Root User: Failed to Connect to IKE,” on page 31](#)
- ◆ [Section A.3.4, “Fragmentation of TCP Packets,” on page 31](#)
- ◆ [Section A.3.5, “Profile Creation Failed,” on page 31](#)
- ◆ [Section A.3.6, “Firewall Issues,” on page 32](#)

A.3.1 IKE Phase 1 Deleted

You might see the message `IKE Phase 1 Deleted` at different times.

If you get the message at the beginning of a VPN connection, ignore it.

If your connection is in progress, and the status shows *Connecting* for a while before you see the status message, it means an error has occurred in the connection procedure.

Possible Cause: Connectivity issues with your machine.

Action: Fix the connectivity issues and proceed.

Possible Cause: The gateway is down or VPN service is not running on the gateway.

Action: Ensure that the gateway is prepared for a VPN connection.

Possible Cause: Issues with the login credentials.

Action: In the case of a Standard IPsec gateway, ensure that the certificate password is valid. If you are connecting to a Nortel Contivity server, ensure that the group credentials are valid.

A.3.2 Failed to Connect to IKE

If you cannot connect to the IKE, check the status of the IKE by using the following command:
`/etc/init.d/racoon status`

NOTE: You must log in as `root` to check the IKE status.

A.3.3 Non-Root User: Failed to Connect to IKE

If you are a non-root user and you receive the message `Failed to connect to the Racoon Daemon` while attempting a VPN connection, do the following:

- 1 Ensure that IKE is running by using the following command:

```
/etc/init.d/racoon status
```

NOTE: You must log in as `root` to check the IKE status.

- 2 If IKE is not running, use the following command to start it:

```
/etc/init.d/racoon start
```

- 3 If IKE is running, check the IKE log at `/var/log/messages`.

For details, refer to [Section A.1.3, “IKE Log,” on page 30](#).

- 4 If you see the message `ERROR: File does not have correct permissions. Expected : 432 Has : 384` in the IKE log, verify that you have the required user privileges to use VPN client.

For details, refer to [Section 4.1.2, “Non-Root Access,” on page 17](#).

A.3.4 Fragmentation of TCP Packets

When you are connected to a Nortel server, encryption and decryption of IP fragmentation is not handled effectively. Therefore, applications sending IP fragments might not work.

For TCP applications, you can use the workaround of setting the route MTU (to the gateway server) to less than 1400 for Ethernet. The recommended MTU is 1350.

To do this, after a successful VPN connection:

- 1 At the command prompt, enter `ip route`.

The routing information to the VPN server is displayed in the following format:

```
VPNSERVERIPADDR via GATEWAYIPADDR dev NETWORKDEVICE
```

- 2 Delete the route by using the following command:

```
route delete VPNSERVERIPADDR
```

- 3 Add the route with your mss value by using the following command:

```
route add VPNSERVERIPADDR gw GATEWAYIPADDR NETWORKDEVICE mss  
1350
```

TIP: For variable details, refer to the routing information (discussed in [Step 1](#)).

A.3.5 Profile Creation Failed

Causes

- ♦ The system runs out of memory
- ♦ `Libxml2.so` is missing

Actions

- ◆ Ensure that you have a minimum 128 RAM of memory.
- ◆ `Libxml2.so` is provided along with the SLED 10 installation. If it is missing, reinstall the library.

A.3.6 Firewall Issues

If you have an iptables firewall running on your machine with policies configured to deny outgoing and incoming packets, configure the following rules to allow the packets:

Table A-1 Outgoing Packets

Port	Configuration Command
UDP-500	<code>iptables -A OUTPUT -p UDP -s 0/0 -d 0/0 --dport 500 -j ACCEPT</code>
UDP-4500	<code>iptables -A OUTPUT -p UDP -s 0/0 -d 0/0 --dport 4500 -j ACCEPT</code>

Table A-2 Incoming Packets

Port	Configuration Command
UDP-500	<code>iptables -A INPUT -p UDP -s 0/0 -d 0/0 --dport 500 -j ACCEPT</code>
UDP-4500	<code>iptables -A INPUT -p UDP -s 0/0 -d 0/0 --dport 4500 -j ACCEPT</code>

A.4 FAQs

This section lists some frequently asked questions and suggests appropriate actions.

- ◆ [Section A.4.1, “Where can I get information on the error codes that I encounter while using the VPN Client?”](#) on page 32
- ◆ [Section A.4.2, “explaining temporary unavailability of resources. What does this mean?”](#) on page 33
- ◆ [Section A.4.3, “What should I do to get IKE debug logs?”](#) on page 33
- ◆ [Section A.4.4, “How can I find out if the VPN Client is installed on my system?”](#) on page 33
- ◆ [Section A.4.5, “I cannot see all of the VPN Client GUI on my monitor. What should I do?”](#) on page 33

A.4.1 Where can I get information on the error codes that I encounter while using the VPN Client?

Refer to [Appendix B, “Error Codes,”](#) on page 35.

A.4.2 explaining temporary unavailability of resources. What does this mean?

You get these messages when you send data to a protected network (for example when you use FTP, Telnet, or ping). This is because a new security association is in the process of negotiation.

Retry the application to resolve this issue.

A.4.3 What should I do to get IKE debug logs?

In `/var/log/messages`, go to `/etc/racoon/racoon.conf` and comment out the `log debug2` line.

A.4.4 How can I find out if the VPN Client is installed on my system?

Run the following command:

```
rpm -qi turnpike
```

A.4.5 I cannot see all of the VPN Client GUI on my monitor. What should I do?

Change your monitor resolution to 1024 x 768 pixels.

Error Codes

B

This section contains the error codes for the Novell VPN client. For each error code, the possible cause and action that you can take are provided.

Also refer to [Appendix A, “Troubleshooting Novell VPN client for Linux,” on page 29](#) for various troubleshooting scenarios that you might encounter while working with Novell VPN Client for Linux.

B.1 GUI Messages

This section explains some of the common GUI error messages that you come across while working with Novell BorderManager 3.9 VPN client.

- ◆ “Certificate not found. Ensure that the certificate is available.” on page 35
- ◆ “Enter gateway name/IP address.” on page 36
- ◆ “The certificate name is too lengthy. Rename the certificate name to proceed.” on page 36
- ◆ “Enter the password.” on page 36
- ◆ “Certificate not found. Ensure that the certificate is available.” on page 36
- ◆ “Failed to read certificate.” on page 36
- ◆ “Gateway name or IP address is not valid.” on page 36
- ◆ “Server address error: Failed to resolve the DNS name. Retry after some time.” on page 36
- ◆ “Cannot read profile. Re-create the profile.” on page 36
- ◆ “Profile is not valid.” on page 36
- ◆ “Failed to connect to IKE. Restart IKE.” on page 37
- ◆ “IKE failed to respond. The client is exiting.” on page 37
- ◆ “Gateway name or IP address is not valid.” on page 37
- ◆ “Failed to meet system requirements.” on page 37
- ◆ “Unable to locate the help file. Reinstall the client.” on page 37
- ◆ “Profile directory does not exist. Client installation might be incomplete.” on page 38
- ◆ “Invalid Network. Re-enter.” on page 38
- ◆ “Invalid Mask. Re-enter.” on page 38
- ◆ “Time-out occurred while waiting for a connection response from gateway. The client is exiting.” on page 38
- ◆ “Authentication Failed. Verify your credentials.” on page 38
- ◆ “Gateway is not responding. The client is exiting.” on page 38

Certificate not found. Ensure that the certificate is available.

Possible Cause: The profile you chose for the VPN connection has an invalid certificate. Possibly, the profile was removed, renamed, or tampered with.

Action: Re-create the profile with another certificate. For details, refer to [Section 4.3, "Connection Profiles,"](#) on page 19.

Enter gateway name/IP address.

Possible Cause: You have not specified the IP address or gateway name.

Action: Specify the IP address or gateway name.

The certificate name is too lengthy. Rename the certificate name to proceed.

Possible Cause: The number of characters in the certificate name has exceeded the limit. Only 80 characters are permitted (including the pathname). For example, /home/user1/.turnpike/usercerts/mycert.pfx is treated as having 42 characters.

Action: Rename the certificate so that it adheres to the character limit.

Enter the password.

Possible Cause: You have not specified the password.

Action: Specify the password.

Certificate not found. Ensure that the certificate is available.

Possible Cause: /user's home directory/.turnpike/usercerts/ does not contain the certificate file.

Action: Copy the certificate file in .pfx format to the path given above.

Failed to read certificate.

Possible Cause: Either the certificate is not valid or the password is incorrect.

Action: Verify the validity of the certificate and password.

Gateway name or IP address is not valid.

Possible Cause: The gateway name or IP address that you have specified is not valid.

Action: Specify a valid gateway name or IP address.

Server address error: Failed to resolve the DNS name. Retry after some time.

Possible Cause: Either the network or DNS server is down.

Action: Ensure that your network and DNS server are up and running.

Cannot read profile. Re-create the profile.

Possible Cause: The profile file in XML format is corrupt.

Action: Use the Profile Manager to delete the profile and create a new one. For details, refer to [Section 4.3, "Connection Profiles,"](#) on page 19.

Profile is not valid.

Possible Cause: You have not specified the certificate password.

Action: Specify the certificate password.

Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is down.

Action: As `root`, restart IKE.

Action: Verify the IKE log for details. The log file can be accessed at `/var/log/messages`.

Possible Cause: IKE might be running, but you do not have sufficient user rights.

Action: Get access rights to use VPN Client. For details, refer to [Section 4.1.2, “Non-Root Access,” on page 17](#).

Possible Cause: Application error. For details, refer to [Section A.2, “Application Errors,” on page 30](#).

Action: Use the following command to restart the IKE:
`/etc/init.d/racoon restart`

Possible Cause: The server failed to respond.

Action: Check the IKE log for details. The log file can be accessed at `/var/log/messages`.

IKE failed to respond. The client is exiting.

Possible Cause: IKE is down.

Action: Check the IKE log for details. The log file can be accessed at `/var/log/messages`.

Action: As `root`, restart IKE.

Gateway name or IP address is not valid.

Possible Cause: The gateway name or IP address you have specified is not valid.

Action: Specify the correct gateway name or IP address.

Failed to meet system requirements.

Possible Cause: `gmodule` support is not available on your machine.

Action: Provide `gmodule` support for your machine. For details, refer to the [GNOME developer Web site \(http://developer.gnome.org/doc/API/2.0/glib/glib-Dynamic-Loading-of-Modules.html\)](http://developer.gnome.org/doc/API/2.0/glib/glib-Dynamic-Loading-of-Modules.html).

Unable to locate the help file. Reinstall the client.

Possible Cause: Issues with VPN Client installation.

Possible Cause: The help file was removed.

Action: Reinstall the VPN Client.

Profile directory does not exist. Client installation might be incomplete.

Possible Cause: Application error. For details, refer to [Section A.2, “Application Errors,” on page 30](#).

Action: Reinstall the VPN Client.

Invalid Network. Re-enter.

Possible Cause: The format in which you specified the network details is not valid.

Action: Specify the details in the dotted IP address format (for example, 10.0.0.0).

Invalid Mask. Re-enter.

Possible Cause: A possible cause of the problem.

Action: What can be done to resolve the problem.

Time-out occurred while waiting for a connection response from gateway. The client is exiting.

Possible Cause: The connection failed. There is no response after connection attempts for a period of time (more than five minutes).

Action: Check the IKE logs to find out the reason. For details, refer to [Section A.1.3, “IKE Log,” on page 30](#).

Authentication Failed. Verify your credentials.

Possible Cause: You have specified an incorrect username, password, or both.

Action: Specify the correct username and password.

Gateway is not responding. The client is exiting.

Possible Cause: The connection failed. There is no response from the VPN gateway.

Action: Ensure that the gateway is up and running.

B.2 CLI Messages

The following are some of the CLI message that you might encounter:

Cannot open the file filename for editing.

Possible Cause: You do not have the required user rights to open and edit the file.

Action: Ensure that you have sufficient user rights. For details, refer to [Section 4.1.2, “Non-Root Access,” on page 17](#).

Gateway name or IP address is not valid.

Possible Cause: The gateway name or IP address is not valid.

Action: Specify a valid gateway name or IP address in the profile.

Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is down.

Action: Check the IKE log for details. The log file can be accessed at `/var/log/messages`.

Action: As `root`, restart IKE using the following command:
`/etc/init.d/racoon start`

Possible Cause: The server failed to respond. Either the server is not up or the network is down.

Possible Cause: Application error. For details, refer to [Section A.2, “Application Errors,” on page 30](#).

Action: Use the following command to restart IKE:
`/etc/init.d/racoon restart`

Possible Cause: IKE is not running, the server is not responding, or the network is down.

Action: Ensure that IKE, the server, and the network are up and running.

Cannot read the profile.

Possible Cause: The profile file (in XML format) is corrupt.

Action: Use the Profile Manager to delete the profile and create a new one. For details, refer to [Section 4.3, “Connection Profiles,” on page 19](#).

Profile name is not valid.

Possible Cause: The profile file uses an incorrect file format.

Action: Using the Profile Manager, re-create the profile. For details, refer to [Section 4.3, “Connection Profiles,” on page 19](#).

Profile directory name does not exist.

Possible Cause: The `profile` directory was not created or it has been removed.

Action: Use the Profile Manager provided with the GUI to re-create the profile. For details, refer to [Section 4.3, “Connection Profiles,” on page 19](#). By default, the profile is created in the proper directory.

Profile name not found.

Possible Cause: The profile is missing.

Action: Use the Profile Manager provided with the GUI to re-create the profile. For details, refer to [Section 4.3, “Connection Profiles,” on page 19](#).

Too many arguments.

Possible Cause: You have provided multiple parameters. Only one parameter is allowed.

Action: Provide one option at a time (for example `vpnc -d`). Only the `vpnc -v -c profile` command is allowed to have multiple parameters.

Possible Cause: You have provided more parameters than required.

Action: The CLI does not allow more parameters than required for the function. Refer to [“Connecting to the Gateway” on page 27](#) or use `vpnc -h` before proceeding.

Verbose mode has no meaning when specified alone.

Possible Cause: You have used the verbose mode without specifying any other parameter.

Action: Verbose mode makes sense only when used along with other parameters. For options, refer to [Section 4.4.2, “Using the Command Line Utility,” on page 26](#). Specify the parameters as in the example `vpnc -v -c profile`.

Profile name does not exist.

Possible Cause: The specified profile does not exist.

Action: Specify a valid profile. If no valid profile exists, use the Profile Manager provided with the GUI to re-create the profile. For details, refer to [Section 4.3, “Connection Profiles,” on page 19](#).

Certificate path does not exist.

Possible Cause: The specified profile is corrupt.

Action: Re-create the profile using the Profile Manager provided with the GUI. For details, refer to [Section 4.3, “Connection Profiles,” on page 19](#).

Possible Cause: The certificate path is not created or it was deleted.

Action: Re-create the certificate path `/user's home directory/.turnpike/usercerts/` and copy the certificate to this path.

Failed to read certificate.

Possible Cause: Either the certificate is not valid or the password is incorrect.

Action: Verify the validity of the certificate and password. Relaunch the CLI and specify the correct certificate password.

Profile is not valid.

Possible Cause: The specified profile is corrupt.

Action: Use the Profile Manager provided with the GUI to re-create the profile. For details, refer to [Section 4.3, “Connection Profiles,” on page 19](#).

Possible Cause: The specified profile is not in the correct format.

Action: Use the Profile Manager provided with the GUI to re-create the profile. For details, refer to [Section 4.3, “Connection Profiles,” on page 19](#).

Possible Cause: The gateway IP address you specified in the profile is not valid.

Action: Use the Profile Manager provided with the GUI to edit the profile. Specify the correct IP address or gateway name.

DNS resolution failed for gateway address specified in the profile.

Possible Cause: You have specified an incorrect DNS name.

Action: Ensure that the DNS name you specified is valid.

Possible Cause: The network or the DNS server is down.

Action: Ensure that the network and the DNS server are up and running.

Time-out occurred while waiting for a connection response from gateway. The client is exiting.

Possible Cause: The connection attempt failed.

Action: Check the IKE logs to find out the reason. For details, refer to [Section A.1.3, “IKE Log,”](#) on page 30.

Profile does not exist. Create the profile using the GUI.

Possible Cause: There is no profile directory.

Action: Use the GUI to create a profile. For details, refer to [Section 4.3, “Connection Profiles,”](#) on page 19.

Authentication Failed. Verify your credentials.

Possible Cause: You have specified an incorrect username, password, or both.

Action: Specify the correct username and password.