Novell VPN Client for Linux

1.0

www.novell.com

USER AND ADMINISTRATOR GUIDE

September 14, 2005

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.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2005 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 at 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

Novell VPN Client for Linux User and Administrator Guide
September 14, 2005

Online Documentation: To access the online documentation for other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Novell is a registered trademark of Novell, Inc., in the United States and other countries.
SUSE is a registered trademark of SUSE Linux AG, a Novell business.

Third-Party Materials

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

Contents

About This Guide 9

1 Understanding Novell VPN Client for Linux 11

Introduction . . . 11
Features . . . 11
General Features . . . 11
Standard IPsec Gateway-Related Features . . . 12
Nortel Contivity-Related Features . . . 12
Requirements . . . 12

2 Installing Novell VPN Client for Linux 13

Installing Novell VPN Client for Linux . . . 13
Prerequisites 13
Accessing the Files . . . 13
Installation . . . 14
Checking the Installation . . . 14
Uninstalling Novell VPN Client for Linux . . . 14
Package Description . . . 14

3 Using VPN Client for Linux 15

Access Information: Who Can Use VPN Client . . . 15
Root Access . . . 15
Non-Root Access . . . 15
Connection Profiles . . . 16
Using the Profile Manager . . . 16
Creating a Profile for Connecting to the Standard IPsec Gateway . . . 16
Creating a Profile for Connecting to the Nortel Contivity Server . . . 17
Editing a Profile . . . 18
Deleting a Profile . . . 19
Establishing a VPN Connection . . . 19
Using the Client with a GUI . . . 19
Using the Client with a CLI . . . 24

A Troubleshooting Novell VPN Client for Linux 27

Guidelines for the User . . . 27
General Guidelines . . . 27
IKE Status . . . 27
IKE Log . . . 28
Application Errors . . . 28
Scenarios . . . 28
IKE Phase 1 Deleted . . . 28
Failed to Connect to IKE . . . 28
Non-Root User: Failed to Connect to IKE . . . 29
Fragmentation of TCP Packets . . . 29
Profile Creation Failed . . . 29
Firewall Issues . . . 30

FAQs . . . 30
Where can I get information on the error codes that I encounter while using VPN Client? . . . 30
I get a message explaining temporary unavailability of resources. What does this mean? . . . 30
What should I do to get IKE debug logs? . . . 30
How can I ensure that VPN Client is installed on my system? . . . 30
The VPN Client GUI does not fit in the monitor, causing reading difficulties. What should I do? . . . 31

B Error Codes 33

GUI Messages . . . 33
VPNCLIENT-GUI-0000 Certificate not found. Ensure that the certificate is available. . . . 33
VPNCLIENT-GUI-0002 Enter gateway name/IP address. . . . 33
VPNCLIENT-GUI-0003 The certificate name is too lengthy. Rename the Certificate name to proceed. . . . 33
VPNCLIENT-GUI-0004 Enter the password. . . . 33
VPNCLIENT-GUI-0006 Certificate not found. Ensure that the certificate is available. . . . 33
VPNCLIENT-GUI-0008 Failed to read certificate. . . . 34
VPNCLIENT-GUI-0009 Gateway name/IP address is not valid. . . . 34
VPNCLIENT-GUI-0011 Server address error: Failed to resolve the DNS name. Retry after some time. . . . 34
VPNCLIENT-GUI-0012 Cannot read profile. Re-create the profile. . . . 34
VPNCLIENT-GUI-0013 Profile is not valid. . . . 34
VPNCLIENT-GUI-0014 Failed to connect to IKE. Restart IKE. . . . 34
VPNCLIENT-GUI-0015 Failed to connect to IKE. Restart IKE. . . . 34
VPNCLIENT-GUI-0016 Failed to connect to IKE. Restart IKE. . . . 34
VPNCLIENT-GUI-0017 Failed to connect to IKE. Restart IKE. . . . 35
VPNCLIENT-GUI-0018 IKE failed to respond. The client is exiting. . . . 35
VPNCLIENT-GUI-0019 Gateway name/IP address is not valid. . . . 35
VPNCLIENT-GUI-0020 Failed to meet system requirements. . . . 35
VPNCLIENT-GUI-0021 Unable to locate the help file. Reinstall the client. . . . 35
VPNCLIENT-GUI-0022 Profile directory does not exist. Client installation might be incomplete. . . . 35
VPNCLIENT-GUI-0023 Invalid Network. Re-enter. . . . 35
VPNCLIENT-GUI-0024 Invalid Mask. Re-enter. . . . 36
VPNCLIENT-GUI-0025 Time-out occurred while waiting for a connection response from gateway. The client is exiting. 36
VPNCLIENT-GUI-0026 Authentication Failed. Verify your Credentials . . . 36
VPNCLIENT-GUI-0026 Gateway is not responding. The client is exiting. . . . 36
CLI Messages . . . 36
VPNCLIENT-CLI-256 Cannot open the file *filename* for editing. . . . 36
VPNCLIENT-CLI-258 Gateway name/IP address *gateway name/IP address* is not valid. . . . 36
VPNCLIENT-CLI-259 Failed to connect to IKE. Restart IKE. . . . 36
VPNCLIENT-CLI-260 Failed to connect to IKE. Restart IKE. . . . 37
VPNCLIENT-CLI-261 Failed to connect to IKE. Restart IKE. . . . 37
VPNCLIENT-GUI-262 Failed to connect to IKE. Restart IKE. . . . 37
VPNCLIENT-CLI-263 Failed to connect to IKE. Restart IKE. . . . 37
VPNCLIENT-CLI-264 Failed to connect to IKE. Restart IKE. . . . 37
VPNCLIENT-CLI-265 Failed to connect to IKE. Restart IKE. . . . 37
VPNCLIENT-CLI-266 Cannot read the profile. . . . 38
VPNCLIENT-CLI-267 Profile *profile name* is not valid. . . . 38
VPNCLIENT-CLI-268 Profile directory *directory name* does not exist. . . . 38
VPNCLIENT-CLI-269 Profile *profile name* not found. . . . 38
VPNCLIENT-CLI-272 Too many arguments . . . 38
VPNCLIENT-CLI-273 Too many arguments . . . 38
VPNCLIENT-CLI-274 Verbose mode has no meaning when specified alone. . . . 38
VPNCLIENT-CLI-275 Profile *profile name* does not exist. . . . 39
VPNCLIENT-CLI-278 Certificate path *path* does not exist. . . . 39
VPNCLIENT-CLI-279 Failed to read certificate. . . . 39
VPNCLIENT-CLI-280 Profile is not valid. . . . 39
VPNCLIENT-CLI-281 Failed to connect to IKE. Restart IKE. . . . 39

VPNCLIENT-CLI-282 Profile is not valid. 39
VPNCLIENT-CLI-284 Profile is not valid. 39
VPNCLIENT-CLI-285 DNS resolution failed for gateway address specified in the profile. 40
VPNCLIENT-CLI-286 Time-out occurred while waiting for a connection response from gateway. The client is exiting. . 40
VPNCLIENT-CLI-287 Profile does not exist. Create the profile using the GUI. 40
VPNCLIENT-CLI-287 Authentication Failed. Verify your Credentials 40

About This Guide

This guide provides the information that you need to install and use Novell® VPN Client for Linux software.

The guide is divided into the following sections:

- Chapter 1, “Understanding Novell VPN Client for Linux,” on page 11
- Chapter 2, “Installing Novell VPN Client for Linux,” on page 13
- Chapter 3, “Using VPN Client for Linux,” on page 15
- Appendix A, “Troubleshooting Novell VPN Client for Linux,” on page 27
- Appendix B, “Error Codes,” on page 33

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.

Documentation Updates

For the most recent version of the *Novell VPN Client for Linux User and Administrator Guide*, visit the Novell documentation Web site (http://www.novell.com/documentation).

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment 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.

1 Understanding Novell VPN Client for Linux

This chapter provides an introduction to Novell® VPN Client for Linux by explaining the following:

- "Introduction" on page 11
- "Features" on page 11
- "Standard IPsec Gateway-Related Features" on page 12
- "Nortel Contivity-Related Features" on page 12
- "Requirements" on page 12

Introduction

Novell VPN Client for Linux allows you to remotely access of the corporate network. The virtual private network created between the client and the gateway helps you to communicate securely over the Internet using standard protocols. From your Linux workstation, you can connect to a network protected by

- Standard IPsec Gateway (supporting X.509)
- Nortel* Contivity Server
- Novell Security Manager powered by Astaro*

Features

General Features

Following are the general features of VPN Client for Linux:

- **Interface Options:** Provides both Graphical user interface (GUI) and command line interface (CLI) options for connection.
- **Support for Network Address Translation (NAT) Traversal:** Allows the VPN client to work from behind a NAT device.
- **Profile Manager:** An interactive feature that helps in creating, modifying, and deleting user-based profiles specific to the gateways.
- **Non-root access:** Users without root privileges can also use VPN Client. For details, refer to "Non-Root Access" on page 15.

Standard IPsec Gateway-Related Features

- **Certificate Mode of Authentication:** Lets you authenticate using x.509 certificates (.pfx format).

Nortel Contivity-Related Features

- **Radius Authentication:** Lets you authenticate based on the credentials stored in the Radius server.
- **IP Address Assignment:** Assigns an IP address to the VPN client connecting to the gateway.
- **Dead Peer Detection:** Detects and informs if the Nortel gateway is not responding.

Requirements

Following are the minimum system requirements needed for VPN Client for Linux to operate:

- PC with Pentium* III or higher processor
- Novell Linux Desktop® (NLD) 9, SP2
- 10 MB in /opt and 10 MB in /usr
- 128 MB RAM
- Monitor resolution of 1024 x 768 pixels

2 Installing Novell VPN Client for Linux

This chapter provides the following information on how to download and install Novell® VPN Client for Linux:

- "Installing Novell VPN Client for Linux" on page 13
- "Uninstalling Novell VPN Client for Linux" on page 14
- "Package Description" on page 14

Installing Novell VPN Client for Linux

Prerequisites

- ❑ All IPsec packages (for example FreeS/WAN or IPsec-tools) on your system are uninstalled.

  IPsec-tools on your system cannot coexist with the IPsec-tools RPM that gets installed during the VPN Client installation.

  - To check for any previously installed IPsec tools, enter

    ```
    rpm -qa ipsec-tools
    ```

  - To uninstall IPsec tools, enter

    ```
    rpm -e ipsec-tools
    ```

- ❑ You have root privileges.

  VPN Client RPM can be installed only with root privileges.

- ❑ If firewall rules are already configured on the VPN Client machine, ensure that the you have the following ports open:

  UDP-500
  UDP-4500

  This is necessary because the VPN connection goes through these ports. For details on configuration, refer to "Firewall Issues" on page 30.

Accessing the Files

VPN Client for Linux can be installed through the *Extras* channel in the Red Carpet updater. Get the following RPMs:

- turnpike-0.1.0-15.i586.rpm
- ipsec-tools-0.5-1_suse92-7.i586.rpm
- nortelplugins-0.1-13.i586.rpm

Installation

1. Log in as root.

   IMPORTANT: VPN Client RPM can be installed only with root privileges.

2. Enter the following to install VPN Client:

   ```
   rpm -ivh *.rpm
   ```

Checking the Installation

When VPN Client for Linux is installed on your system, the IKE starts running and the VPN login icon appears in the NLD main menu.

If you are a CLI user, enter the following command to check if VPN Client for Linux is installed on your system:

```
rpm -qi turnpike
```

NOTE: Currently GNOME and KDE are the supported desktops.

Uninstalling Novell VPN Client for Linux

1. Enter the following to uninstall the Nortel plug-ins:

   ```
   rpm -e nortelplugins
   ```

2. Enter the following to uninstall the IPsec-tools:

   ```
   rpm -e ipsec-tools
   ```

3. Enter the following to uninstall VPN Client:

   ```
   rpm -e turnpike
   ```

Package Description

The package description provides the detailed information about the files that are installed as part of VPN Client installation. Run the following command to view the package description:

```
rpm -qlp rpm
```

3 Using VPN Client for Linux

This chapter provides the following information to help you effectively set up and use Novell® VPN Client for Linux:

- "Access Information: Who Can Use VPN Client" on page 15
- "Connection Profiles" on page 16
- "Using the Client with a GUI" on page 19
- "Using the Client with a CLI" on page 24

Access Information: Who Can Use VPN Client

Root Access

Super user can directly access VPN.

Non-Root Access

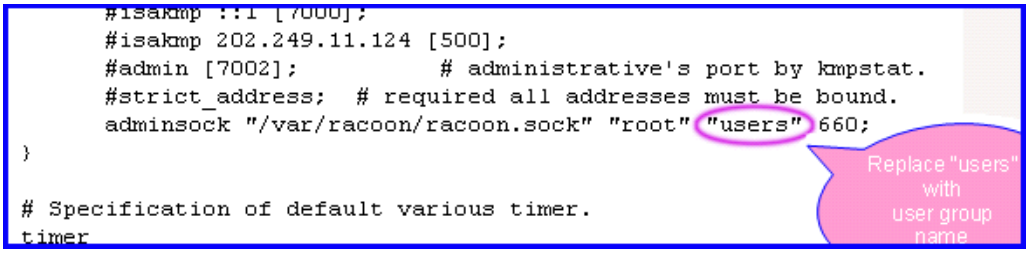
users Group Users

All users belonging to the primary group *users* created by root can use VPN client. By default, all users belong to this group.

Non-users group Users

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

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



4. Restart IKE by entering the following:

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

The root cannot allow multiple groups to use VPN client. So, if a new group is permitted by modifying the racoon.conf, only users belonging to that group can access VPN.

Connection Profiles

Connection profiles comprise 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.

Using the Profile Manager

The Profile Manager helps you create, edit, or delete profiles. While editing profiles, you are not allowed to change the profile names.

NOTE: You cannot create profiles using CLI. Therefore, use Profile Manager to create and modify profiles.

Creating a Profile for Connecting to the Standard IPsec Gateway

1. In the Profile Name field of the VPN Client for Linux dialog, select Profile Manager.

   The Profile Manager tabbed page is displayed.

2. Click Add to create a profile.

   The General screen is displayed.

3 Specify the following details:

- **Profile Name:** Specify the profile name.
- **Gateway Type:** Select Standard IPsec gateway as the gateway type.

  TIP: If you have not copied the user certificate in the .pfx format, the error `No .pfx files` appears. For details, refer to "Copying the User Certificate" on page 20.
- **Gateway:** Specify the gateway IP address or gateway name.
- **User Certificate:** Select the user certificate.

4 Click the IKE Phase1 tab to configure the encryption algorithm, hash algorithm, DH group, mode, and authentication method.

IMPORTANT: While configuring IKE phase 1 and IKE phase 2, ensure that the VPN Client configuration matches the configuration on the gateway you are connecting to.

5 Click the IKE Phase 2 tab to configure the common parameters (encryption algorithm, hash algorithm, and PFS group), network, and mask.

6 Click Save to save the profile.

7 Click Done to return to the VPN Client dialog.

Creating a Profile for Connecting to the Nortel Contivity Server

1 In the Profile Name field of the VPN Client for Linux dialog, select Profile Manager.

The Profile Manager tabbed page is displayed.

2 Click Add to create a profile.

The General screen is displayed.

3 Specify the following details:

- **Profile Name:** Specify the profile name.
- **Gateway Type:** Select Nortel as the gateway type.
- **Gateway:** Specify the gateway IP address or gateway name.
- **Groupname:** Specify the user group name.
- **Group Password**: Specify the group password.

4 Click the IKE Phase1 tab to configure the encryption algorithm, hash algorithm, and DH group.

You cannot change the default configuration for Mode and Authentication Method.

IMPORTANT: While configuring IKE phase 1 and IKE phase 2, ensure that the VPN client configuration matches the configuration on the gateway you are connecting to.

5 Click the IKE Phase 2 tab to configure the common parameters (encryption algorithm, hash algorithm, and PFS group).

WARNING: Configuring Network and Mask settings can result in undesirable consequences.

6 Click Save to save the profile.

7 Click Done to return to the VPN Client dialog.

Editing a Profile

In the Profile Manager, select the profile you want to edit using the Choose Profile option. You can edit all the parameters except the profile name.

Deleting a Profile

To delete a profile,

1. Select the profile you want to delete (Profile Manager > Choose Profile).
2. Click Remove button.

Establishing a VPN Connection

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

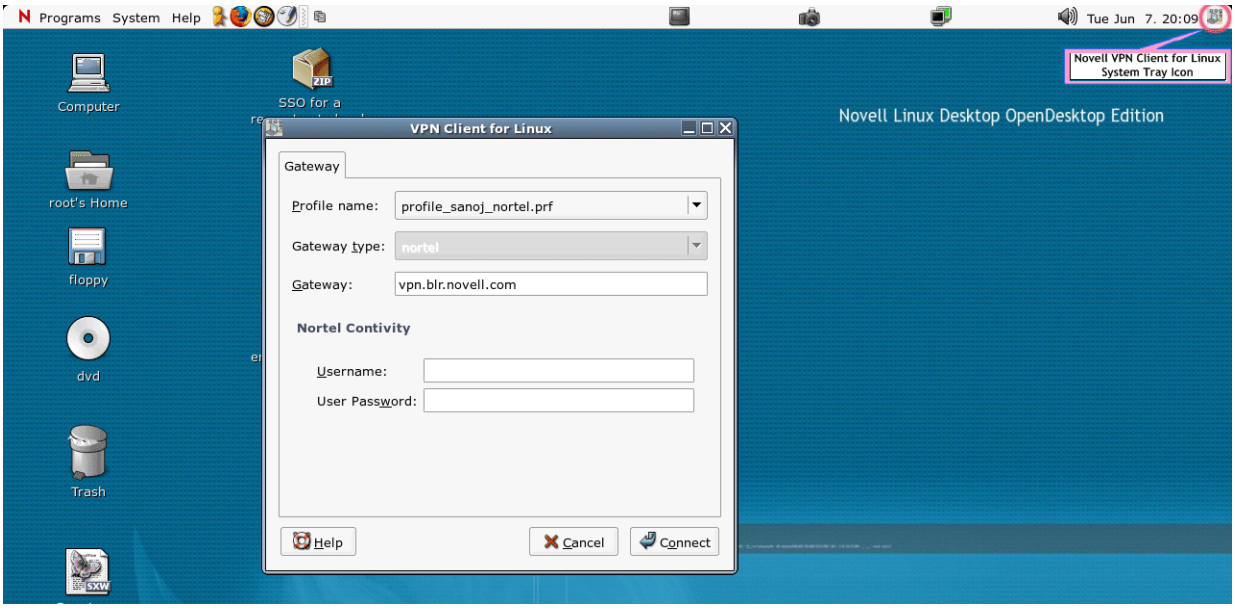
IMPORTANT: The CLI and GUI options might not interact properly. We recommend using either of the options at a time.

Using the Client with a GUI

To launch VPN client GUI,

1. From the NLD main menu, select Programs > VPN Login.

The Novell VPN Client dialog is displayed and the VPN icon appears in the system tray.



TIP: KDE users might not be able to launch VPN Client as mentioned above. If you are a KDE user, launch VPN Client using the command **`vpnlogin`** at the command prompt.

Use the VPN Client dialog to set up VPN connection to a Nortel Contivity server or a Standard IPsec Gateway by selecting a profile from the Profile Name field.

NOTE: If you do not have a profile already or want to create a new profile, select Profile Manager instead. For details, refer to “Connection Profiles” on page 16.

Connecting to a Standard IPsec Gateway

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

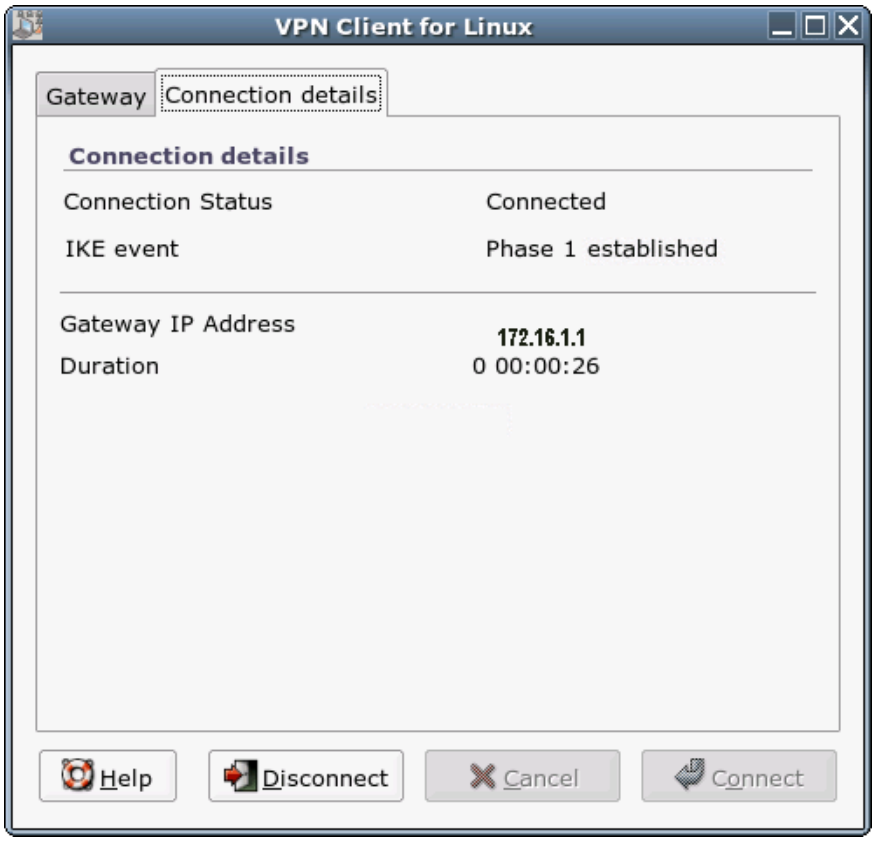
1 In the Profile Name field, select the profile created for a Standard IPsec Gateway connection.

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

2 In the Password field, specify the certificate password.

3 Click Connect.

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



4 Click Disconnect if you want to end the connection.

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

Connecting to Nortel Contivity Server

1 In the Profile Name field, select the profile created for connecting to a Nortel Contivity server.

The Gateway information is automatically displayed.

2 In the Nortel Contivity section, specify the following details:

- **Username:** The name of the user who requires the connection.
- **User Password:** The user password.

3 Click Connect.

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

4 Click Disconnect if you want to end the connection.

Using the Client with a CLI

VPN Client provides a CLI (Command Line Interface) to carry out the major VPN functions.

After installing VPN Client for Linux, run vpnc help by entering the following:

```
vpnc -h
```

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

Option	Description
`vpnc -c`	Connects to the VPN gateway in the PROFILENAME.
`vpnc -d`	Disconnects from the VPN gateway.
`vpnc -h`	Displays the VPN Client help.
`vpnc -l`	Lists the available profiles along with their gateway types.
`vpnc -v`	Displays a detailed log when used with the connect option as follows: `vpnc -v -c`

Creating Profiles Using a CLI

You cannot create connection profiles using the CLI feature. Profiles must be created and edited using the GUI. For details, refer to “Connection Profiles” on page 16.

Connecting to the Gateway Using a CLI

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

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

```
vpnc -c profile
```

```
vpnc --connect profile
```

```
vpnc -v -c profile
```

```
vpnc --verbose --connect profile
```

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

Disconnecting from the Server

To disconnect from the server, enter the following command:

```
vpnc -d
```

A Troubleshooting Novell VPN Client for Linux

This appendix provides various troubleshooting scenarios that you might encounter while working with Novell® VPN Client for Linux:

- "Guidelines for the User" on page 27
- "Application Errors" on page 28
- "Scenarios" on page 28
- "FAQs" on page 30

Guidelines for the User

General Guidelines

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

IKE Status

NOTE: You have to 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 make the IKE run, use the following command:

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

  To stop the IKE daemon, use the following command:

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

IKE Log

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

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

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 33, try reinstalling the VPN Client. If the error repeats, try installing the latest version of VPN Client.

Scenarios

IKE Phase 1 Deleted

You might encounter the message `IKE Phase 1 Deleted` in the following scenarios.

At the Beginning of a Connection

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

While the Connection Is in Process

If your connection status shows *Connecting* for a relatively longer duration, and then you encounter the status message, it means an error has occurred in the connection procedure.

Possible Cause: Connectivity issues with your machine.

Action: Rectify 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.

Failed to Connect to IKE

Possible Cause

The IKE is not running.

Action

Check the status of the IKE using the following command:

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

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

If the status is Dead or Unused, use the following command to start IKE:

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

Non-Root User: Failed to Connect to IKE

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

1. Ensure that IKE is running.

   For details, refer to "IKE Status" on page 27.

2. If IKE is not running, start it.

   For details, refer to "Failed to Connect to IKE" on page 28.

3. If IKE is running, check the IKE log.

   For details, refer to "IKE Log" on page 28.

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 "Non-Root Access" on page 15.

Fragmentation of TCP Packets

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

But in the case of TCP applications, you might 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, do the following:

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 using the following command:

   `route delete VPNSERVERIPADDR`

3. Add the route with your mss value 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).

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 NLD installation. If for some reason it is missing, install the library.

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 1 Outgoing Packets

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

Table 2 Incoming Packets

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

FAQs

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

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

Refer to the Appendix B, “Error Codes,” on page 33.

I get a message explaining temporary unavailability of resources. What does this mean?

You get such 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.

What should I do to get IKE debug logs?

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

How can I ensure that VPN Client is installed on my system?

Run the following command:

```
rpm -qi turnpike
```

The VPN Client GUI does not fit in the monitor, causing reading difficulties. What should I do?

Change your monitor resolution to 1024 x 768 pixels.

B Error Codes

This appendix contains the error codes for Novell® VPN Client for Linux. 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 27 for various troubleshooting scenarios that you might encounter while working with Novell VPN Client for Linux.

GUI Messages

VPNCLIENT-GUI-0000 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 is removed, renamed, or tampered with.

Action: Re-create the profile with another certificate. For details, refer to "Connection Profiles" on page 16.

VPNCLIENT-GUI-0002 Enter gateway name/IP address.

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

Action: Specify the IP address/gateway name to proceed.

VPNCLIENT-GUI-0003 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.

VPNCLIENT-GUI-0004 Enter the password.

Possible Cause: You have not specified the password.

Action: Specify the password.

VPNCLIENT-GUI-0006 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 mentioned above.

VPNCLIENT-GUI-0008 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.

VPNCLIENT-GUI-0009 Gateway name/IP address is not valid.

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

Action: Specify a valid gateway name/IP address.

VPNCLIENT-GUI-0011 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.

VPNCLIENT-GUI-0012 Cannot read profile. Re-create the profile.

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

Action: Using the Profile Manager, delete the profile and create a new one. For details, refer to "Connection Profiles" on page 16.

VPNCLIENT-GUI-0013 Profile is not valid.

Possible Cause: You have not specified the certificate password.

Action: Specify the certificate password.

VPNCLIENT-GUI-0014 Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is down.

Action: As root, restart IKE.

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 "Non-Root Access" on page 15.

VPNCLIENT-GUI-0015 Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is down.

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

VPNCLIENT-GUI-0016 Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is down.

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

VPNCLIENT-GUI-0017 Failed to connect to IKE. Restart IKE.

Possible Cause: Application error. For details, refer to "Application Errors" on page 28.

Action: Restart IKE using the following command:

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

Possible Cause: Server failed to respond.

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

VPNCLIENT-GUI-0018 IKE failed to respond. The client is exiting.

Possible Cause: IKE is down.

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

Possible Cause: IKE is down.

Action: As root, restart IKE.

VPNCLIENT-GUI-0019 Gateway name/IP address is not valid.

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

Action: Specify the correct gateway name/IP address.

VPNCLIENT-GUI-0020 Failed to meet system requirements.

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

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

VPNCLIENT-GUI-0021 Unable to locate the help file. Reinstall the client.

Possible Cause: Issues with VPN Client installation.

Possible Cause: The help file is removed.

Action: Reinstall VPN Client.

VPNCLIENT-GUI-0022 Profile directory does not exist. Client installation might be incomplete.

Possible Cause: Application error. For details, refer to "Application Errors" on page 28.

Action: Reinstall VPN Client.

VPNCLIENT-GUI-0023 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).

VPNCLIENT-GUI-0024 Invalid Mask. Re-enter.

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

Action: Specify the details in the dotted IP address format (for example, 255.0.0.0).

VPNCLIENT-GUI-0025 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 "IKE Log" on page 28.

VPNCLIENT-GUI-0026 Authentication Failed. Verify your Credentials

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

Action: Specify the correct username and password.

VPNCLIENT-GUI-0026 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.

CLI Messages

VPNCLIENT-CLI-256 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 "Non-Root Access" on page 15.

VPNCLIENT-CLI-258 Gateway name/IP address *gateway name/IP address* is not valid.

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

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

VPNCLIENT-CLI-259 Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is down.

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

Possible Cause: Application error. For details, refer to "Application Errors" on page 28.

Action: Restart IKE using the following command:

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

VPNCLIENT-CLI-260 Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is not running.

Action: Start IKE using the following command:

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

Possible Cause: Application error. For details, refer to “Application Errors” on page 28.

Action: Restart IKE using the following command:

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

VPNCLIENT-CLI-261 Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is down.

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

Possible Cause: Application error. For details, refer to “Application Errors” on page 28.

Action: Restart IKE using the following command:

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

VPNCLIENT-GUI-262 Failed to connect to IKE. Restart IKE.

Possible Cause: Application error. For details, refer to “Application Errors” on page 28.

Action: Restart IKE using the following command:

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

VPNCLIENT-CLI-263 Failed to connect to IKE. Restart IKE.

Possible Cause: Application error. Refer to “Application Errors” on page 28.

Action: Restart IKE using the following command:

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

VPNCLIENT-CLI-264 Failed to connect to IKE. Restart IKE.

Possible Cause: Application error. Refer to “Application Errors” on page 28.

Action: Restart IKE using the following command:

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

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

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

VPNCLIENT-CLI-265 Failed to connect to IKE. Restart IKE.

Possible Cause: IKE is down.

Action: As root, restart IKE using the following command:

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

VPNCLIENT-CLI-266 Cannot read the profile.

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

Action: Using the Profile Manager, delete the profile and create a new one. For details, refer to "Connection Profiles" on page 16.

VPNCLIENT-CLI-267 Profile *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 "Connection Profiles" on page 16.

VPNCLIENT-CLI-268 Profile directory *directory name* does not exist.

Possible Cause: The profile directory is not created or it is removed.

Action: Re-create the profile using the Profile Manager provided with the GUI. For details, refer to "Connection Profiles" on page 16. By default, the profile gets created in the proper directory.

VPNCLIENT-CLI-269 Profile *profile name* not found.

Possible Cause: The profile is missing.

Action: Re-create the profile using the Profile Manager provided with the GUI. For details, refer to "Connection Profiles" on page 16.

VPNCLIENT-CLI-272 Too many arguments

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

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

VPNCLIENT-CLI-273 Too many arguments

Possible Cause: You have provided more parameters than required.

Action: The CLI does not allow more parameters than required for the function. Refer to the "Connecting to the Gateway Using a CLI" on page 25 or use vpnc -h before proceeding.

VPNCLIENT-CLI-274 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 "Using the Client with a CLI" on page 24. Specify the parameters as in the example **`vpnc -v -c profile`** for getting verbose details.

VPNCLIENT-CLI-275 Profile *profile name* does not exist.

Possible Cause: The specified profile does not exist.

Action: Specify a valid profile. If no valid profile exists, create a new one using the Profile Manager provided with the GUI. For details, refer to "Connection Profiles" on page 16.

VPNCLIENT-CLI-278 Certificate path *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 "Connection Profiles" on page 16.

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

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

VPNCLIENT-CLI-279 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.

VPNCLIENT-CLI-280 Profile is not valid.

Possible Cause: The specified profile is corrupt.

Action: Re-create the profile using the Profile Manager provided with the GUI. For details, refer to "Connection Profiles" on page 16.

VPNCLIENT-CLI-281 Failed to connect to IKE. Restart IKE.

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.

VPNCLIENT-CLI-282 Profile is not valid.

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

Action: Re-create the profile using the Profile Manager provided with the GUI. For details, refer to "Connection Profiles" on page 16.

VPNCLIENT-CLI-284 Profile is not valid.

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

Action: Edit the profile (using the Profile Manager provided with the GUI) to specify the correct IP address/gateway name.

VPNCLIENT-CLI-285 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.

VPNCLIENT-CLI-286 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 “IKE Log” on page 28.

VPNCLIENT-CLI-287 Profile does not exist. Create the profile using the GUI.

Possible Cause: There is no profile directory.

Action: Create a profile using the GUI. For details, refer to “Connection Profiles” on page 16.

VPNCLIENT-CLI-287 Authentication Failed. Verify your Credentials

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

Action: Specify the correct username and password.