Oracle® Communications Network Charging and Control

Virtual Private Network User's Guide

Release 12.0.0

December 2017

ORACLE®

Copyright

Contents

About This Document

Scope

The scope of this document includes all functionality a user must know in order to effectively operate the Virtual Private Network (VPN) application. It does not include detailed design of the service.

Audience

This guide is written primarily for VPN administrators. However, the overview sections of the document are useful to anyone requiring an introduction.

Prerequisites

Although there are no prerequisites for using this guide, familiarity with the target platform would be an advantage.

A solid understanding of Unix and a familiarity with IN concepts are an essential prerequisite for safely using the information contained in this guide. Attempting to install, remove, configure or otherwise alter the described system without the appropriate background skills, could cause damage to the system; including temporary or permanent incorrect operation, loss of service, and may render your system beyond recovery.

This manual describes system tasks that should only be carried out by suitably trained operators.

Related Documents

The following documents are related to this document:

- *CPE User's Guide*
- *VPN Technical Guide*

Document Conventions

Typographical Conventions

The following terms and typographical conventions are used in the Oracle Communications Network Charging and Control (NCC) documentation.

Formatting Convention	Type of Information
Special Bold	Items you must select, such as names of tabs. Names of database tables and fields.
Italics	Name of a document, chapter, topic or other publication. Emphasis within text.
Button	The name of a button to click or a key to press. **Example:** To close the window, either click **Close**, or press **Esc**.
Key+Key	Key combinations for which the user must press and hold down one key and then press another. Example: **Ctrl+P** or **Alt+F4**.
`Monospace`	Examples of code or standard output.
`Monospace Bold`	Text that you must enter.
variable	Used to indicate variables or text that should be replaced with an actual value.
menu option > menu option >	Used to indicate the cascading menu option to be selected. Example: **Operator Functions > Report Functions**
hypertext link	Used to indicate a hypertext link.

Specialized terms and acronyms are defined in the glossary at the end of this guide.

Chapter 1

System Overview

Overview

Introduction

This chapter provides an overview of the Virtual Private Network (VPN) service.

In this chapter

This chapter contains the following topics.

Virtual Private Network Service

Introduction

The Virtual Private Network (VPN) product provides a fully IN-based, feature-rich VPN solution with intuitive user interfaces, available on industry-standard platforms. Whilst being simple and easy to use, it also provides enhanced functionality for more experienced users.

The basic VPN service connects multiple locations together. Each VPN Network has its own private numbering plan which is used to map numbers in the private plan to the numbers required to correctly route the call through the PSTN (or mobile network). In addition to this simple number translation service, additional processing can be performed to further add value to the offered service.

Individual phone numbers can be provided with profiles that specify the operations available to them. The most obvious of these is outgoing call barring to prevent calls of certain types from being made. The following operations are also offered:

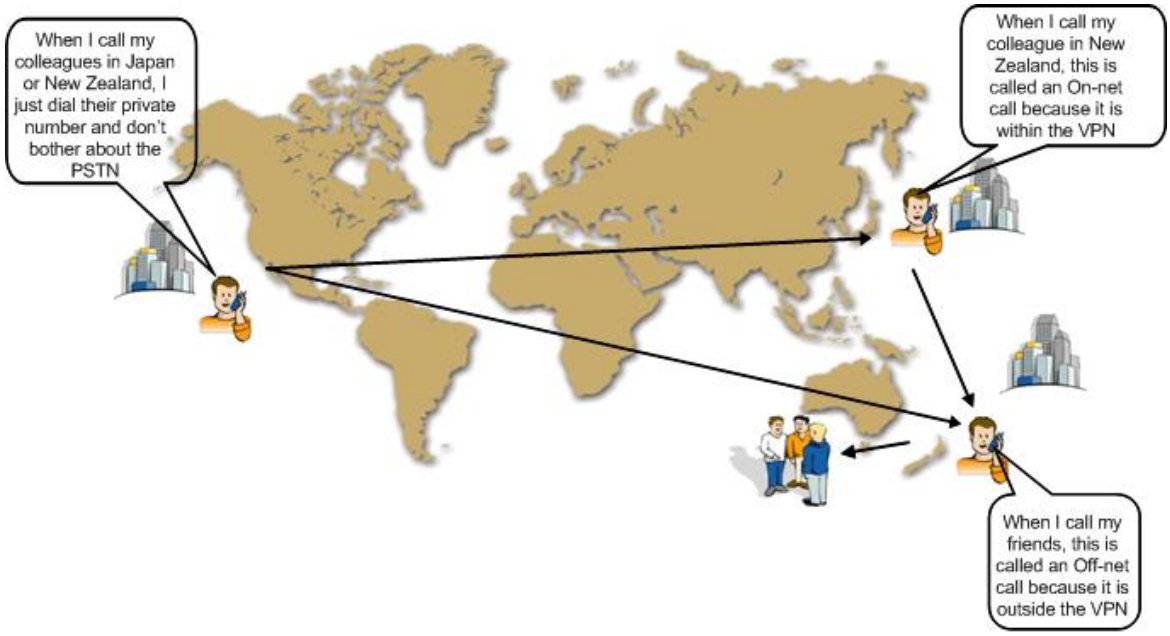
- Incoming call barring
- Call diversion
- Re-routing on busy (to another station or voice mail)
- PIN security for out-going calls
- Incoming call screening (with PIN override)

The facility to access a corporate VPN from points outside the VPN (off-net) is provided, effectively giving access to the corporate telephone network from any phone. Access to this very powerful feature requires rigorous security to prevent fraudulent use.

Users of off-net access can also inherit the features of the service they have in their office, for example, speed-dial codes, and the ability to divert calls from their office phone.

Key concepts

Here is an example VPN setup within a company.



Features of the VPN Service

Introduction

This topic describes the functionality and operation of the VPN application.

Off-net calling

For all originating station profiles, only calls to numbers within the VPN are allowed, unless the off-net calling feature is enabled in the setup for the *Adding a station* (on page 79).

Forced on-net calling

For off-net calls, a check is performed to determine whether the dialed number corresponds to a number that is within the VPN, that is, on-net. If it does, then the call is converted to an on-net call and processed and billed as an on-net call.

Speed dialing

Each originating profile has a configurable number of speed dial numbers. A speed dial number is a reserved private dialing plan number that is predefined on a per station basis. The typical implementation of a speed dial number uses a prefix to identify the number as a speed dial number, followed by the speed dial index.

For example, in a particular private numbering plan, '8' may be used as the speed dial prefix, therefore 800 could be the first speed dial number.

Non-prefixed speed dials are also supported. This means you can configure the VPN service to detect speed dials without needing to prefix them.

Speed dial numbers can be translated to any other private numbering plan number, including off-net numbers (for example, 912345678).

Preprogrammed speed dial numbers can be used as a mechanism to allow limited off-net calling for phones normally barred from off-net calls.

Allowed and barred lists

You can assign an allowed number list or a barred number list to any originating profile. The list is composed of a number of private numbering plan prefixes. Any dialed number for which the first digits match the list's prefix is either disallowed, or allowed, depending on whether the list is barred or allowed.

For example, to bar off-net calls to 900 (premium rate) numbers, a barred list would contain an entry ‘x900’ where x is the off-net number identifier.

Each VPN can have multiple allowed or barred lists that may contain multiple numbers.

Allowed/Barred lists may be both global and per station.

PIN coded security override

For stations where barred or allowed lists exist or were the off-net calling feature is not enabled, a user may enter an ID and PIN to override one or both of these blocks on making the call.

The PIN code override function is prefixed by specified digits to allow the application to distinguish it from a standard dialed number.

Account code

Dialed numbers may be prefixed by an account code that will be removed from the dialed number, but included in the billing information for the call. The account code is prefixed specified digits to allow the application to distinguish it from a standard dialed number.

Variable routing

For trunk and international calls, different routing algorithms may be specified, based on the destination of the call and a setting in the originating profile. This feature is intended to allow selection of different routes or carriers for long distance calls. A routing algorithm may result in different prefixes being appended to the existing dialed number to allow a call to route through alternative routes (for example, highly compressed speech routes, call back, land line only, internet, fax service). The algorithm used is determined by the leading dialed digits of the dialed number and a quality of service indication that may be set against each VPN network.

CLI restriction

It is possible to restrict the CLI presentation in VPN calls by selecting the CLI Restriction option at *Adding a network* (on page 41).

Calling line display

It is possible to select between the VPN address or the physical address to be displayed in the terminating station for calls between on-net stations.

Tariffing

VPN is able to set a special tariff for connections made among members of the same network (irrespective of whether the call was established as the result of dialing full subscriber's MSISDN number or abbreviated one).

Closed User Groups

The closed user group (CUG) facility allows you to define groups of stations within a network, and then place restrictions on the incoming and outgoing calls to and from the stations included in the group.

CUGs are defined at the network level. They can be one of the following:

- Restricted, where only calls between the stations included in the CUG are allowed
- Un-restricted, where calls between any stations, including stations not in the CUG, are allowed

Incoming calls to stations in a CUG are controlled through use of the CUG PIN. You must know the CUG PIN to make a call to a station in the CUG.

Station features

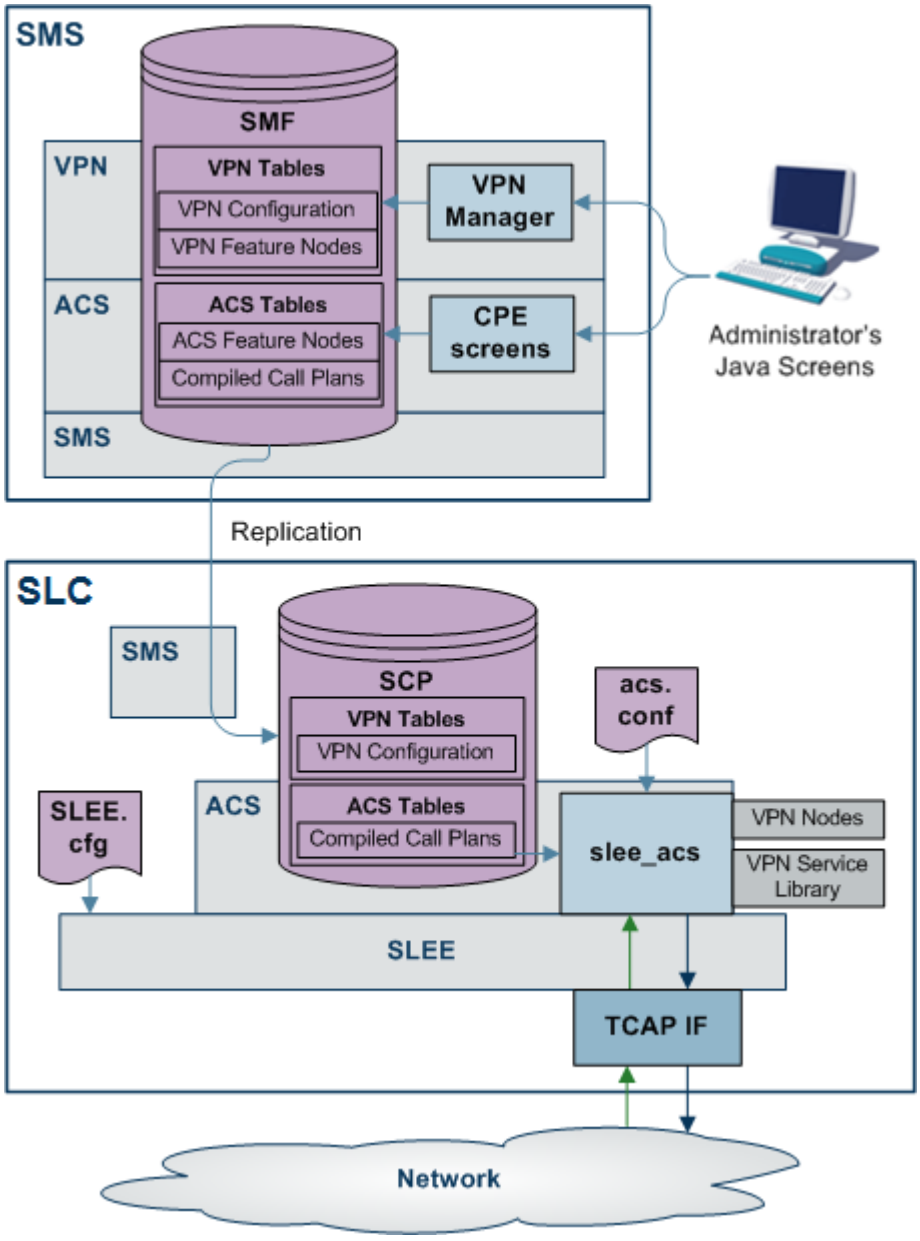
For each station, the following features are available:

- Incoming Call Barring
  Calls from a list of specified numbers can be barred.
- Call Forwarding
  A forward destination can be specified for incoming calls to a station.
- Divert On Busy/No Answer
  A forward destination can be specified for incoming calls to a station that is busy or not answered after a number of seconds.
- Hunting Functionality
  Hunting functionality is provided for terminating on-net calls to allow calls to be consecutively re-routed to different termination numbers each time a previous attempt fails.

Main Components of VPN

Introduction

Here is a high level diagram showing the main components of VPN in the context of NCC components.



VPN components

In this diagram, the components that are specific to VPN are:

- On the SMS:
  - VPN Tables in the SMF, replicated in the SCP
  - VPN Manager
- On the SLC:
  - VPN Nodes

- VPN Service Library

For more information, refer to *VPN Technical Guide*.

VPN Control Plans

Introduction

On installation of VPN, sample control plans are installed. These can be imported and modified as necessary.

You can view control plans using the ACS Control Plan Editor.

You can set which call plans to trigger which each network using the *Networks* (on page 39) tab of the VPN Network screen.

Note: To be visible on the VPN Network screen, VPN control plans must meet the following criteria:

- The control plan name must be prefixed with VPN
- The control plan must be successfully built
- The control plan must be for the effective ACS customer

Sample control plans

This topic describes the function of each sample control plan installed with VPN.

Originating

There are three sample Originating control plans.

Control Plan	Description
VPN_Originating_Fixed	Originating control plan most suitable for fixed lines.
VPN_Originating_Mobile	Originating control plan most suitable for mobile telephones.
VPN_Originating_Alternative	Similar to VPN_Originating_Fixed. Uses Set Tariff Code from Profile nodes to show how the network and station SCI fields may be used.

Terminating

There are two sample Terminating control plans.

Control Plan	Description
VPN_Terminating	To handle calls triggered towards a telephone within the VPN.
VPN_Terminating_Alternative	Similar to VPN_Terminating, but without terminating CUG functionality.

Management

There are two sample Management control plans.

Control Plan	Description
VPN_Management	Allows callers to manage their data interactively. This is the IVR control plan for managing:

Control Plan	Description
	• speed dials, • Follow me Number, • Alternative Routing Number. • Can also do breakout calls
VPN_Management_Alternative	As above, but slightly different style.

Chapter 2

Getting Started

Overview

Introduction

This chapter explains how to access the Virtual Private Network application and describes the contents of the Main Menu.

In this chapter

This chapter contains the following topics.

Accessing the VPN Service

Introduction

You can access the Virtual Private Network Service by using the following methods:

- *Accessing VPN using SMS* (on page 9)
- *Accessing VPN as a Standalone Application* (on page 10)

Accessing VPN using SMS

Introduction

You can access the application by logging into SMS and selecting it from the Service Management System **Services** menu.

For more information about logging into SMS, see *SMS User's Guide*.

Accessing VPN from SMS main screen

Follow these steps to open the VPN Service from the Service Management System main screen.

Step	Action
1	Select the **Services** menu from the Service Management System main screen.

Step	Action
	
2	Select **VPN Service**. **Result:** You see the *VPN main screen* (on page 14).

Accessing VPN as a Standalone Application

Introduction

You can access VPN directly using Java Webstart. See *Launching VPN using Webstart* (on page 10).

This provides access to the VPN Logon Dialog screen. See *Logging on to VPN* (on page 14).

Launching VPN using Webstart

Follow these steps to launch Virtual Private Network using Java Webstart.

Notes:

To launch GUI applications via Java Webstart, you must ensure that the Web server supports the jnlp file type. For more information, see *Setting up the Screens* in *SMS Technical Guide*.

Note that this process installs a shortcut to VPN on your desktop, allowing you to open the VPN GUI directly.

Step	Action
1	Using an Internet browser, open the VPN Webstart. There are two methods to do this: a. Navigating using the browser: ▪ Open the *Service Management System default page* (See example on page 12) on the *SMS_hostname*, then in the sentence below the heading **VPN Standalone Application**, click the here link. ▪ This opens the Virtual Private Network default page. Click the WebStart link. b. Open VPN Webstart directly. The address is in the format: `http://SMS_hostname/vpn.jnlp` Where *SMS_hostname* is the hostname of the SMS or the Primary Node cluster which is running the VPN application. **Result:** You see the Opening vpn.jnpl download screen.
2	Select **Open with** and click **OK**.

Step	Action

Result:
The following screens open:

a. A Java screen, for example:

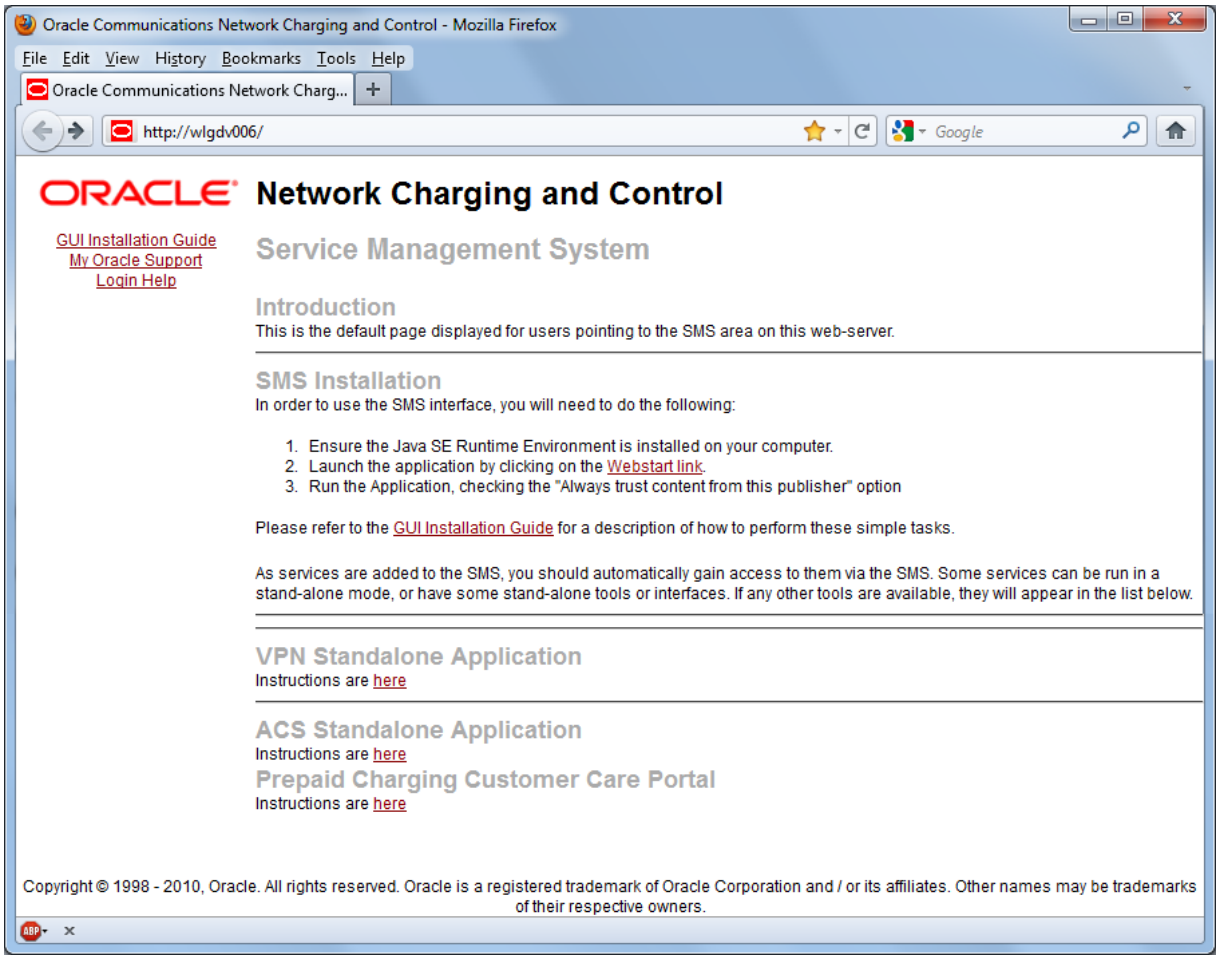
b. The VPN Logon Dialog screen will appear.
Refer to *Logging on to VPN* (on page 14).

Note: When launching VPN for the first time using Webstart, a shortcut icon is downloaded and displayed on the Desktop.

This enables you to open the VPN GUI directly by double-clicking the shortcut icon. The icon is removed every time you clear the system cache and downloads again when launching VPN through Webstart after clean up.

Service Management System default page

Here is an example Service Management System default page that is displayed for users navigating to the SMS on a web-server.



This page provides access to VPN Standalone Application. Click the here link to access the instructions. For more information, see Virtual Private Network default page.

Note: If you upgraded the NCC product from an earlier version, you will continue to have the option to launch the application using the vpn.html file.

Virtual Private Network default page

Here is an example Virtual Private Network default page. The format of the address of this page is http://*SMS_hostname*/Vpn_Service/index.html.

Note: If you upgraded the NCC product from an earlier version, you will continue to have the option to launch the application using the vpn.html file.

VPN Logon Dialog screen

Here is an example VPN Logon Dialog screen.

Logging on to VPN

Follow these steps to log on to VPN via the VPN Logon Dialog screen.

Step	Action
1	Type the name of the customer.
2	Type the valid username for the customer.
3	Type the password.
	Note: Passwords are case sensitive.
4	Click **OK**. **Result:** You see the *VPN main screen* (on page 14).

You can have three attempts to enter a correct username and password before the User ID is locked. If this happens, you must ask your System Administrator to re-activate it.

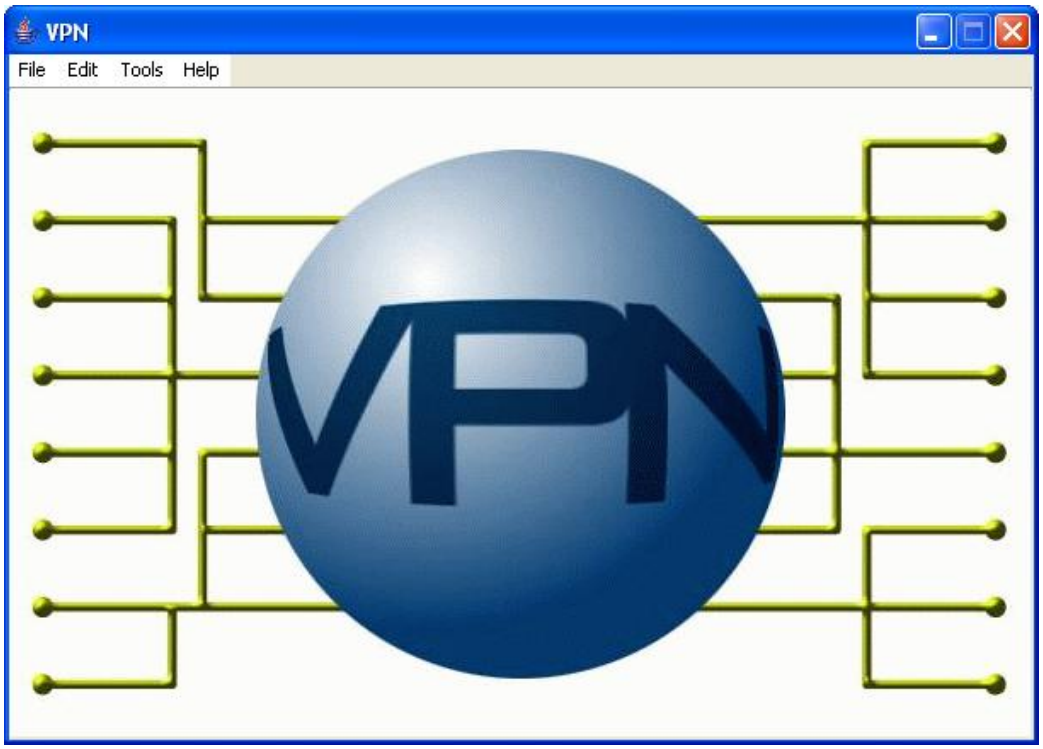
VPN Main Screen

Introduction

The VPN main screen is displayed when you successfully log in to the system. This screen provides access to the configuration screens, using the menus as described below.

VPN main screen

Here is the VPN main screen.



VPN screens

The VPN main screen provides access (depending upon your security privileges) to the following configuration screens, through the following menus:

- Edit:
  - *Network* (on page 35)
  - *Station* (on page 71)
  - *Customers and Users* (on page 23)
- Tools
  - *Accessing the VPN Configuration Module* (on page 17)

Security Privileges

Security

VPN has its own internal security mechanism that is used when VPN is run standalone or remotely. This security system is overridden by the SMS security mechanism when VPN is accessed through the SMS. When a user logs on using the Logon Dialog screen, access to the database is given. Each user has a privilege level set by the System Administrator. Privilege levels range from 1 to 7.

Security level privileges

Here are the privileges granted to each security level.

Level	User Type	Privilege
1	User	User may view all details of Network and Station for the customer they belong to.
2	User	Has access of privilege 1 and may change the following, for all stations: • Station Speed Dial lists • Hunting list scheduling
3	User	Has access of privilege 2 and can change all of the following: • Station Details • Allowed/Barred lists • Add/change/delete Stations Can also edit the following: • Divert allowed barred list • Station work zones
4	User	Has access of privilege 3 and can change the following: • Network Speed dial lists • Account Codes • Allowed/Barred lists • maintain Contacts for the Customer • network work zones Can add and delete the following: • CUG station • CUG (edit and delete only) • Inter-network prefix
5	User	Has access of privilege 4 and can perform the following actions:

Level	User Type	Privilege
		• Change all Network details • Change CUG station details • Add/change/delete Networks • Maintain users with permission 5 and below
6	System Administrator	Has access to add, delete and modify all aspects of VPN and the Global configuration, as well as Add and Change Customers and Address ranges. Cannot add or delete level 6 users.
7	Super User	Has System Administrator access and also may add, delete and modify all other users.

Process Overview

Logon details

To configure the VPN service for the first time, use the following logon parameters:

Customer Name Boss

User Name boss

Password ssob

You must change all these values once you have successfully logged on.

The password may be changed either in the VPN Customer screen, **User** tab or the SMS User Management screen.

Configuring announcements

The VPN Installation comes packaged with a number of public announcements which are grouped into sets for convenience. The VPN System Administrator creates and edits these public Announcement Sets, which are then used by all customers. To enable the Announcement Sets, you must configure Resource Names and IDs for them.

Chapter 3

Initial Configuration

Overview

Introduction

This chapter explains how to configure the VPN system for the first time.

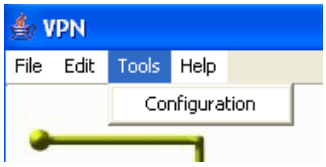
In this chapter

This chapter contains the following topics.

Accessing the VPN Configuration Module

Introduction

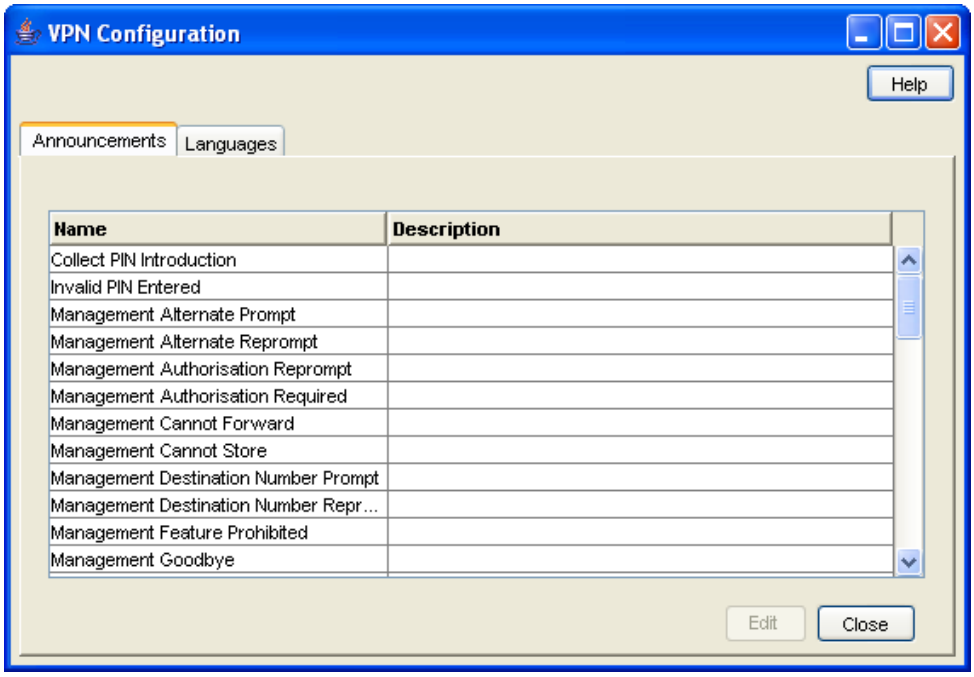
To access the VPN Configuration module, on the VPN main screen, select **Tools**, **Configuration**.



Note: This menu is only visible if you have a permission level of 6 or above.

VPN Configuration screen

Here is an example VPN Configuration screen.



Configuration screen tabs

The VPN Configuration screen contains the following tabs:

- *Announcements* (on page 18)
- *Languages* (on page 21)

Announcements

Introduction

The **Announcements** tab displays entries within the 'VPN Announcements' announcement set.

A complete set of announcements is installed with the application. You must select each announcement and assign a resource name and ID.

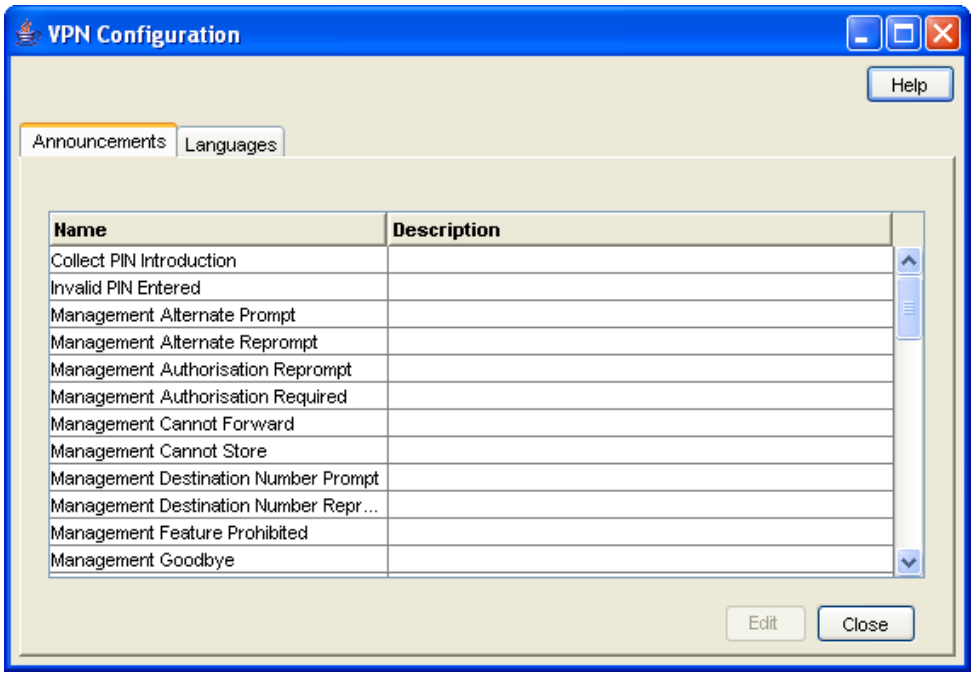
Note: The Resource Name and ID must exist and be configured in the **acs.conf** file, otherwise the announcements will not play. For more information about **acs.conf**, see *ACS Technical Guide*.

Privileges

This tab is available if you are using VPN standalone and have a permission level of 6; levels below this do not have access to this tab.

Announcements tab

Here is an example **Announcements** tab of the VPN Configuration screen.



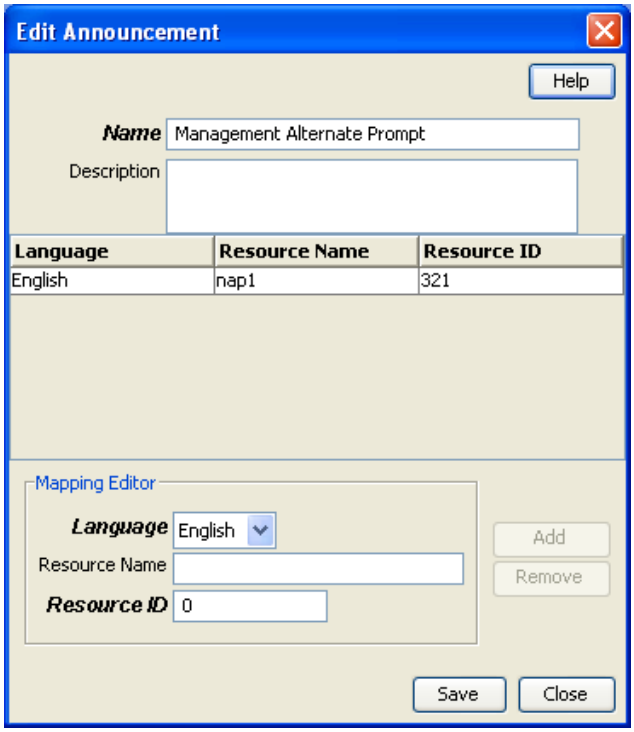
Configuring announcements

Follow these steps to configure an announcement. Repeat for each announcement required.

Step	Action
1	Select the **Announcements** tab on the VPN Configuration screen.
2	Select the announcement in the table and click **Edit**. **Result:** You see the *Edit Announcement screen* (See example on page 20).
3	Fill in the fields, as described in *Field descriptions* (on page 20).
4	Click **Add** to add the language to the Announcement set. **Note:** Only one language setting may be added for an announcement in each language.
5	To edit the language mappings, select the language in the table, then: • To modify a language mapping, make the changes to the fields in the Mapping Editor area and click **Add**. • To remove a language mapping, click **Remove**.
6	Click **Save**. **Result:** The announcement entry is updated.

Edit Announcement screen

Here is an example Edit Announcement screen.



Field descriptions

This table describes the function of each field on the Edit Announcements screen.

Field	Description
Name	Displays the name of the Announcement Record within the Announcement Set. This may be up to 50 characters in length and is required. An Announcement Entry Name must be unique within the Announcement Set.
Description	Lets you enter a text description for the Announcement. The description may be up to 250 characters in length and is optional.
Language	Lets you select the language in which the announcement is to be played. At least one instance of this announcement must be in the default language. Once the announcement mapping is added to the system, the selected language for that announcement mapping will be displayed in the Language column of the table.

Field	Description
Resource Name	Lets you enter the Resource Name of the announcement instance. The Resource Name is the name or location of the IP on which the announcement is stored. Once the announcement mapping is added to the system, the resource name for that announcement mapping will be displayed in the Resource Name column of the table.
Resource ID	Lets you enter the Resource ID of the announcement instance. The Resource ID is the identification on the IP that gives the exact location of the announcement. Once the announcement mapping is added to the system, the Resource ID for that announcement mapping will be displayed in the Resource ID column of the table.

Languages

Introduction

The **Languages** tab displays the languages set up for the system.

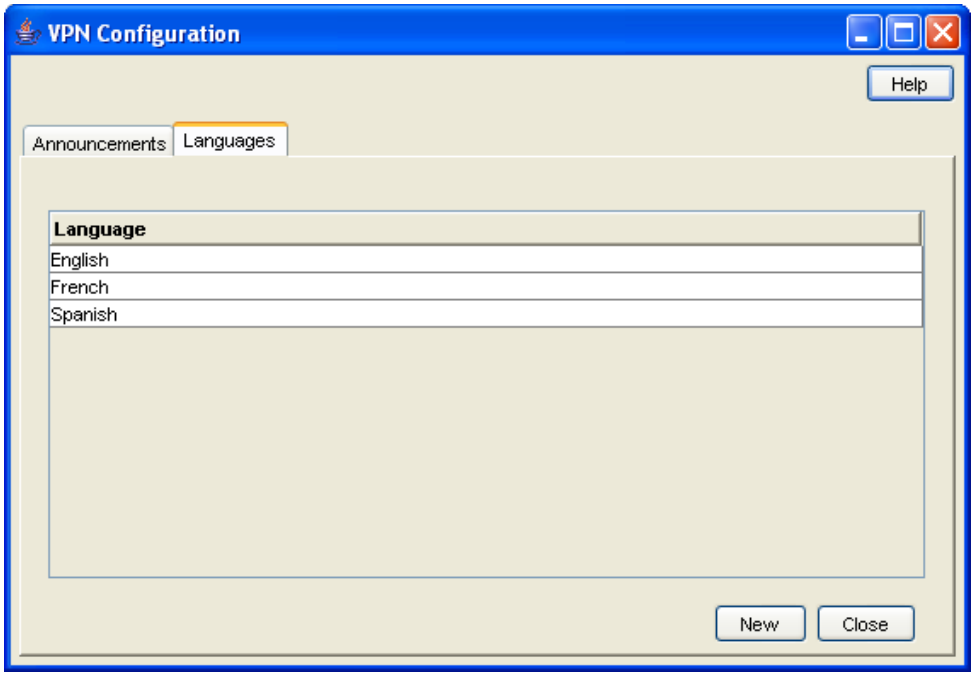
Ensure that the language you require for the announcements appears in this tab. If not, you must add it before configuring announcements.

Privileges

This tab is available if you are using VPN standalone and have a permission level of 6; levels below this do not have access to this tab.

Languages tab

Here is an example **Languages** tab of the VPN Configuration screen.



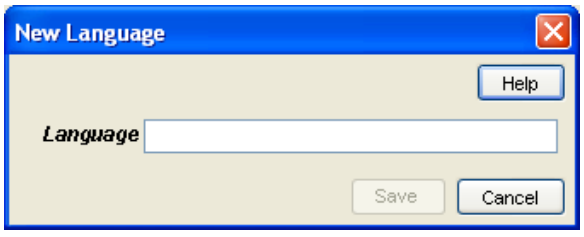
Adding a language

Follow these steps to add a new language.

Step	Action
1	Select the **Languages** tab on the VPN Configuration screen.
2	Click **New**. **Result:** You see the *New Language screen* (See example on page 22).
3	Enter the name of the language. **Note:** This must be unique.
4	Click **Save**.

New Language screen

Here is an example New Language screen.



Chapter 4

Customers and Users

Overview

Introduction

This chapter explains how to create customers and users for the VPN service.

In this chapter

This chapter contains the following topics.

Process Overview

Adding customers

The default system customer is BOSS. After adding a new customer, the system automatically creates a level 5 user as below:

User Name: Administrator

Password: Administrator

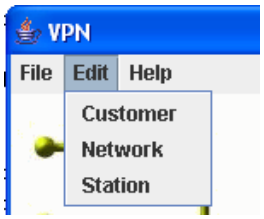
For security reasons, it is important to notify the customer to change their user name and password when they use the system for the first time.

Note: If you delete a customer, all users, VPN networks, and stations belonging to that customer are also deleted. Use with caution.

Accessing the Customer Module

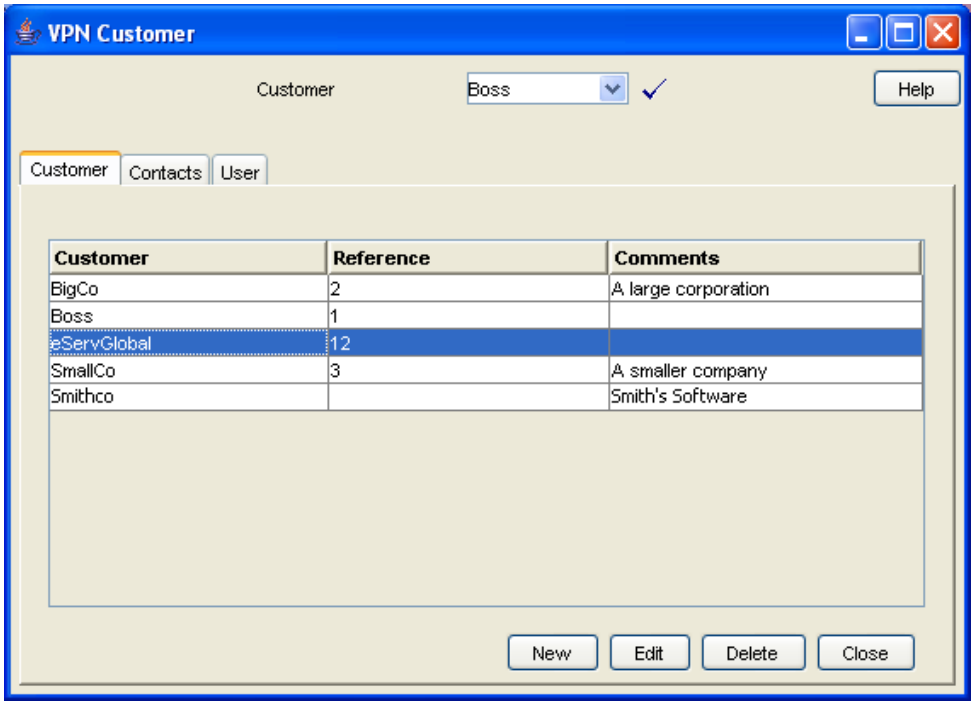
Introduction

To access the VPN Customer module, on the VPN main screen, select **Edit**, **Customer**.



VPN Customer screen

Here is an example VPN Customer screen.



Customer screen tabs

The VPN Customer screen contains the following tabs:

- *Customer* (on page 24)
- *Contacts* (on page 27)
- *User* (on page 30)

Customer

Introduction

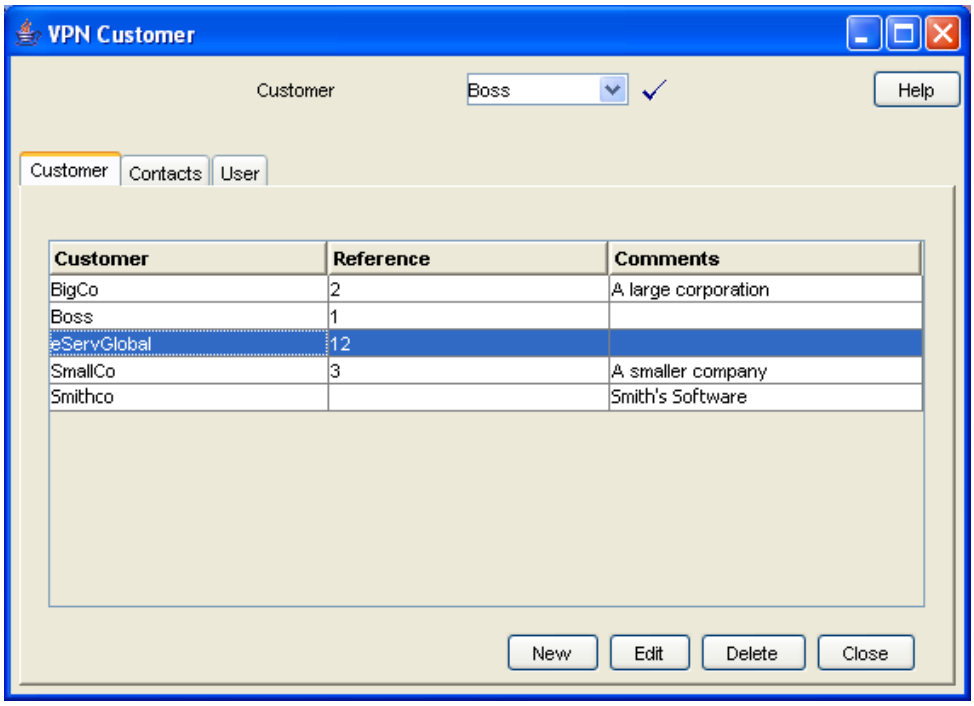
The **Customer** tab of the VPN Customer screen lists all the customers who are using VPN. One of these customers will be the telecommunications service provider (the VPN System Administrator).

Privileges

This tab is available if you are using VPN standalone and have a permission level of 6; levels below this do not have access to this tab.

Customer tab

Here is an example **Customer** tab of the VPN Customer screen.



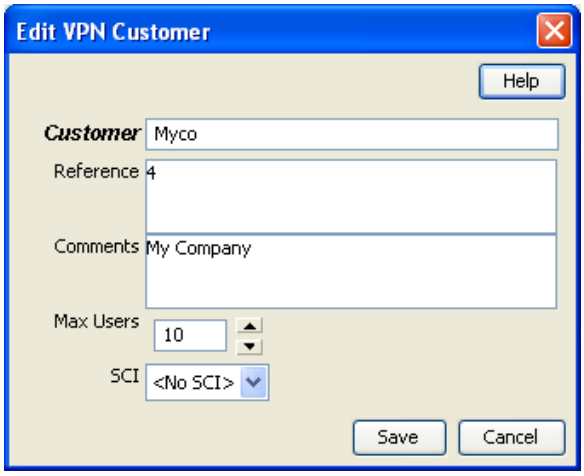
Field descriptions

This table describes each field of the New VPN Customer screen and Edit VPN Customer screen.

Field	Description
Customer	Displays the name of the selected customer. This will usually be the company name of the customer. This may be up to 20 alphanumeric characters long, but must be unique.
Reference	Displays a customer reference. This may be an address, or any other reference required. This may be up to 2000 text characters long and is optional.
Description / Comments	Displays a short description of the customer. It may be up to 2000 text characters long and is optional.
SCI	VPN is able to set special tariffs for connections made among members of VPNs. Send Charging Information (SCI) message is sent with appropriate Charging Zone value together with the termination attempt.
Max Users	Use to set the maximum number of users that the customer may have set up for them. This may be between 0 and 999.

VPN Customer screen

Here is an example VPN Customer screen.



Adding a VPN customer

Follow these steps to add a new VPN customer.

Step	Action
1	Select the customer from the drop down list on the VPN Customer screen.
2	Select the **Customer** tab.
3	Click **New**. **Result:** You see the New *VPN Customer screen* (See example on page 26).
4	Fill in the fields, as described in the *Field descriptions* (on page 25).
5	Click **Save**.

Changing VPN customer details

Follow these steps to change the details of a VPN customer, if required.

Step	Action
1	Select the customer from the drop down list, on the VPN Customer screen.
2	Select the **Customer** tab.
3	Select the customer in the table and click **Edit**. **Result:** You see the Edit *VPN Customer screen* (See example on page 26).
4	Change the details, as required. Refer to *Field descriptions* (on page 25).
5	Click **Save**. **Result:** The customer entry will be updated.

Deleting a customer

Follow these steps to delete a customer.

Warning: This will remove all user Networks and stations for the customer. Use with caution.

Step	Action
1	Select the customer from the drop down list on the VPN Customer screen.
2	Select the **Customer** tab.
3	Select the customer in the table and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes**. **Result:** The customer is removed from the system.

Contacts

Introduction

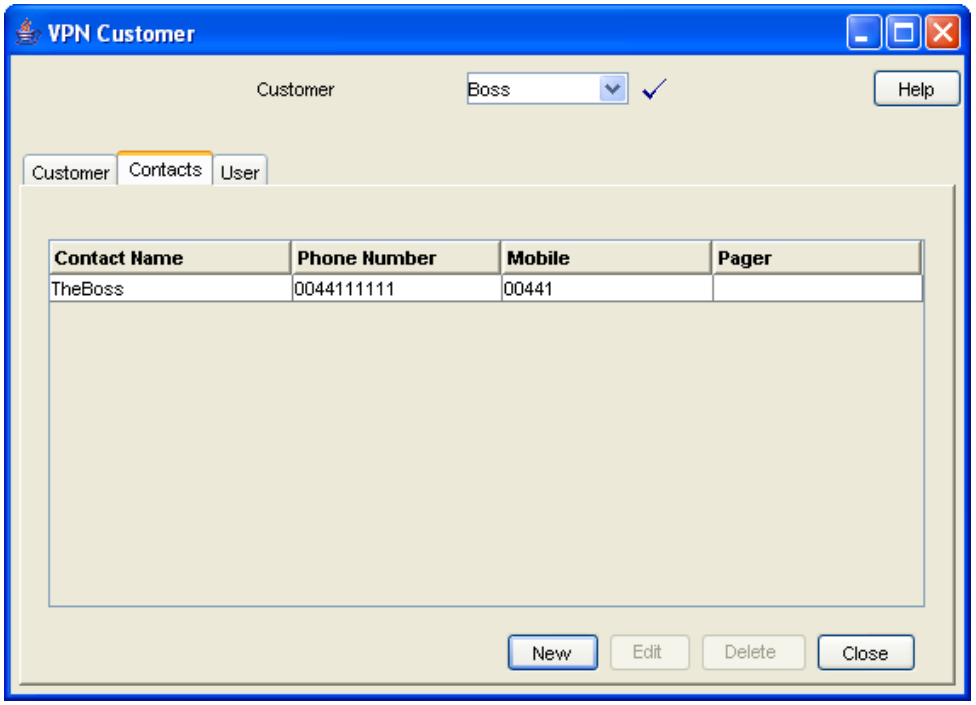
The **Contacts** tab of the VPN Customer screen displays the details of contact persons for each customer. There may be several contact persons for each VPN customer.

Privileges

This tab is available if you are using VPN standalone and have a privilege level of 4 or above; levels below this will not have access to this tab.

Contacts tab

Here is an example **Contacts** tab.



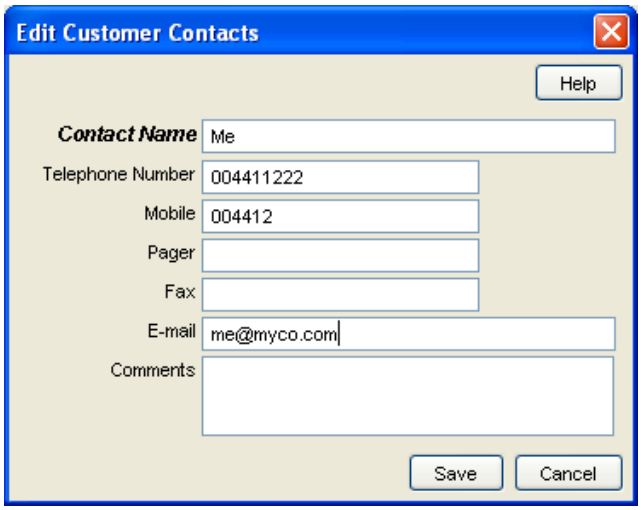
Field descriptions

This table describes each field of the New Customer Contacts screen and Edit Contacts screen.

Field	Description
Contact Name	The name of the Contact Person. This may be up to 30 text characters in length, but must be unique for the customer. This is a required field.
Telephone Number	The telephone number to be used to contact the contact person. This may be up to 32 digits in length. This field is optional, but you must complete at least one of the contact fields.
Mobile	The phone number of the contact person's mobile phone. This may be up to 32 digits in length. This field is optional, but you must complete at least one of the contact fields.
Pager	The pager number for the contact person. This may be up to 32 digits in length. This field is optional, but you must complete at least one of the contact fields.
Fax	The fax number of the contact person. This may be up to 32 digits in length. This field is optional, but you must complete at least one of the contact fields.
E-mail	E-mail of the contact person. This may be up to 50 characters in length. This field is optional, but you must complete at least one of the contact fields.
Comments	Any comments for the Contact. This may be up to 2000 text characters in length, and is optional.

Customer Contacts screen

Here is an example Customer Contacts screen.



Adding a customer contact

Follow these steps to add a new customer contact.

Step	Action
1	Select the customer from the drop down list on the VPN Customer screen.
2	Select the **Contacts** tab.
3	Click **New**. **Result:** You see the New *Customer Contacts screen* (See example on page 29).
4	Fill in the fields, as described in the *Field descriptions* (on page 28).
5	Click **Save**.

Changing customer contact details

Follow these steps to change the details of a customer, if required.

Step	Action
1	Select the customer from the drop down list, on the VPN Customer screen.
2	Select the **Contacts** tab.
3	Select the contact in the table and click **Edit**. **Result:** You see the Edit *Customer Contacts screen* (See example on page 29).
4	Change the details, as required. Refer to *Field descriptions* (on page 28).
5	Click **Save**. **Result:** The customer contact entry will be updated.

Deleting a customer contact

Follow these steps to delete a customer contact.

Step	Action
1	Select the customer from the drop down list on the VPN Customer screen.
2	Select the **Customer** tab.
2	Select the contact in the table and click **Delete**.
	Result: You see the Delete confirmation screen.
4	Click **Yes** to confirm.
	Result: The contact is removed from the system.

User

Introduction

The **User** tab of the VPN Customer screen displays the list users that are set up for each customer. Each user has a name, password, and privilege level.

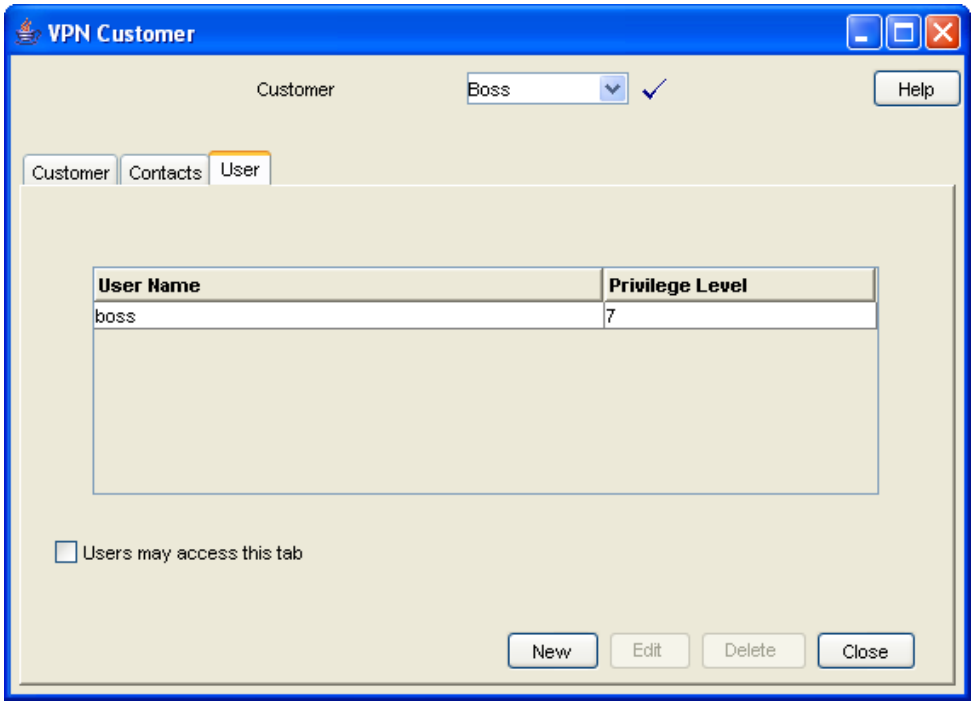
A user is an individual within the Company that may access the VPN management screens. A Customer is the person or company who purchases their telecommunication services from the Telco.

Privileges

This tab is available if you have a privilege level of 5 or above; levels below this will not have access to this tab. It is also available from the VPN standalone system.

User tab

Here is an example **User** tab.



Field descriptions

This table describes the fields on the New User screen and Edit User screen.

Field	Description
User Name	Displays the User Name of the user. A user name may be up to 50 alphanumeric characters in length, but may not be blank. The user name must be unique within that customer. There may be several customers with a user “Mary Smith”, but there may only be one user “Mary Smith” for each customer.
Privilege Level	The privilege level for the User. When creating new users, they may be assigned a privilege level. Level 5 and 6 users may create users of privilege levels 5. The VPN Super User (the Level 7 user) is installed at installation time. This user may add and delete all users, but in particular may create and delete level 6 users (VPN Administrators). When the Super User is creating users, the Privilege Levels that are available to them will be 6.
Password	The User's password. For security reasons, this will not display the characters that are actually entered; the password will display as a line of asterisks.
Confirm Password	The User's password must be entered for a second time, to confirm that the entry of the password is correct. If the entries in both the **Password** and the **Confirm Password** fields are not the same, then the user cannot be saved. You are informed that the passwords do not match and the edit screen remains open for the passwords to be re-entered. For security reasons, the password will display as a line of asterisks.

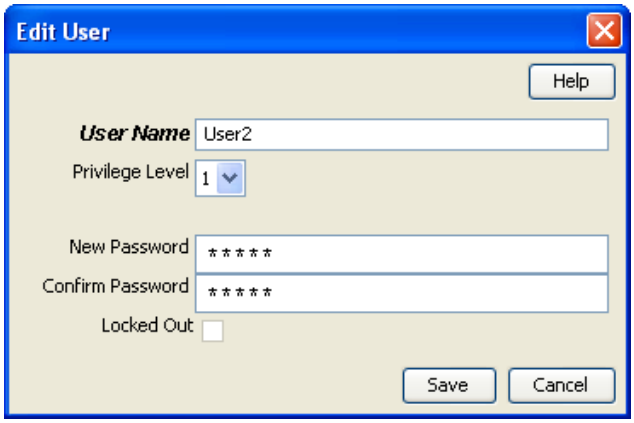
Edit User screen-only field

This table describes a field that is only on the Edit User screen.

Field	Description
User Locked	The check box indicates the lock status for the user. This check box has two functions: • It shows if the user is currently locked out of the system. A user may become locked out of the system if they have attempted to log on unsuccessfully three times. • It allows a user of privilege level 5 or above to manually unlock a user who has become locked out of the system if required. A user may not be manually locked. If it is necessary to prevent a user from accessing the system, it is suggested that the user be removed or that the System Administrator change their password.

User screen

Here is an example User screen.



Adding a user

Follow these steps to add a new user.

Step	Action
1	Select the customer from the drop down list on the VPN Customer screen.
2	Select the **User** tab.
3	Click **New**.
	Result: You see the New *User screen* (See example on page 32).
4	Fill in the fields, as described in the *Field descriptions* (on page 31).
5	Click **Save**.
	Note: If the entries in the **Password** and the **Confirm Password** fields are not the same, an error message will display. Re-enter as required.

Changing user details

Follow these steps to change the details of a user.

Step	Action
1	Select the customer from the drop down list on the VPN Customer screen.
2	Select the **User** tab.
3	Select the user in the table and click **Edit**.
	Result: You see the Edit *User screen* (See example on page 32).
4	Change the details, as required. Refer to *Field descriptions* (on page 31).
5	Click **Save**.
	Result: The user entry will be updated.

Deleting a user

Follow these steps to delete a user.

Step	Action
1	Select the customer from the drop down list on the VPN Customer screen.
2	Select the **User** tab.
3	Select the user in the table and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes** to confirm. **Result:** The user is removed from the system.

Chapter 5

Network

Overview

Introduction

This chapter lists the tasks and tabs available on the VPN Network screen.

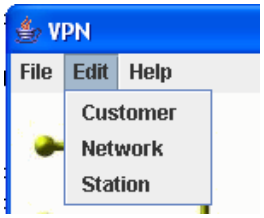
In this chapter

This chapter contains the following topics.

Accessing the Network Module

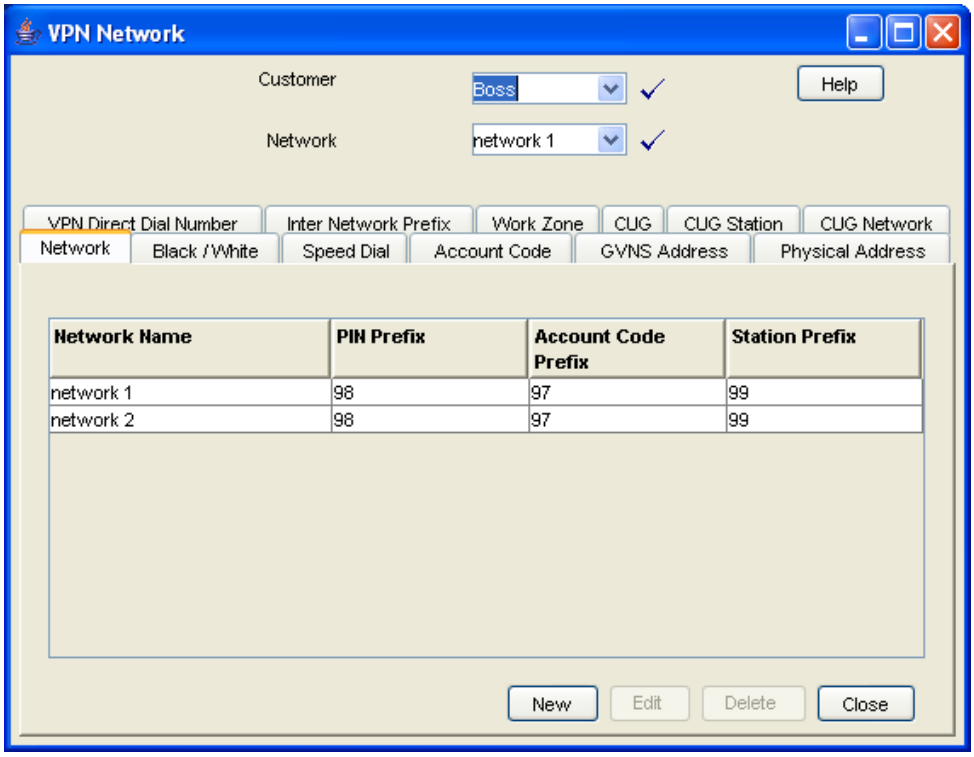
Introduction

To access the VPN Network module, on the VPN main screen, select **Edit**, **Network**.



VPN Network screen

Here is an example VPN Network screen.



Network screen tabs

The Network screen contains the following tabs:

- *Networks* (on page 39)
- *Black and White Network Number Lists* (on page 57)
- *Speed Dial* (on page 62)
- *Account Codes* (on page 55)
- *GVNS Address Ranges* (on page 46)
- *Physical Address Ranges* (on page 49)
- *VPN Direct Dial Number Ranges* (on page 51)
- *Inter Network Prefix* (on page 65)
- *Work Zone* (on page 67)
- *Closed User Groups* (on page 101)
- *CUG Stations* (on page 106)
- *CUG Networks* (on page 104)

Using the Network Screen

Network tasks

You can perform the following VPN network tasks from this screen.

- *Adding the Network* (on page 39)
- *Configuring the Network* (on page 55)

- *Defining Closed User groups* (on page 101)

Selecting a customer

Follow these steps to select a customer.

Step	Action
1	In the **Customer** field, type the first letters, or whole name.
2	Press **Enter**. **Result:** The name of the customer and the fields on the screen will be populated with the relevant data.

Finding a network

Follow these steps to find a network.

Step	Action
1	Select the network from the **Network** list field.
2	Press **Enter**. **Result:** The related records appear in the grid.

Chapter 6

Adding the Network

Overview

Introduction

This chapter explains how to add networks to the VPN service and maintain their details.

Add new network process

Networks must be created and deleted by the telecommunications provider. Once a new network is created, a customer with a privilege level of 5 may change the details of the Network. A customer may have several networks created for them.

When adding a new network follow the procedures, in the order given below:

1 *Adding a network* (on page 41) for the customer
2 *Adding a range* (on page 48)
3 *Adding a range* (on page 50)
4 *Adding a range* (on page 53)

To begin using VPN, the network must be configured. When configuring a new network, follow the procedures in the chapter *Configuring the Network* (on page 55).

In this chapter

This chapter contains the following topics.

Networks

Introduction

The **Network** tab of the Network screen displays the list of Network details.

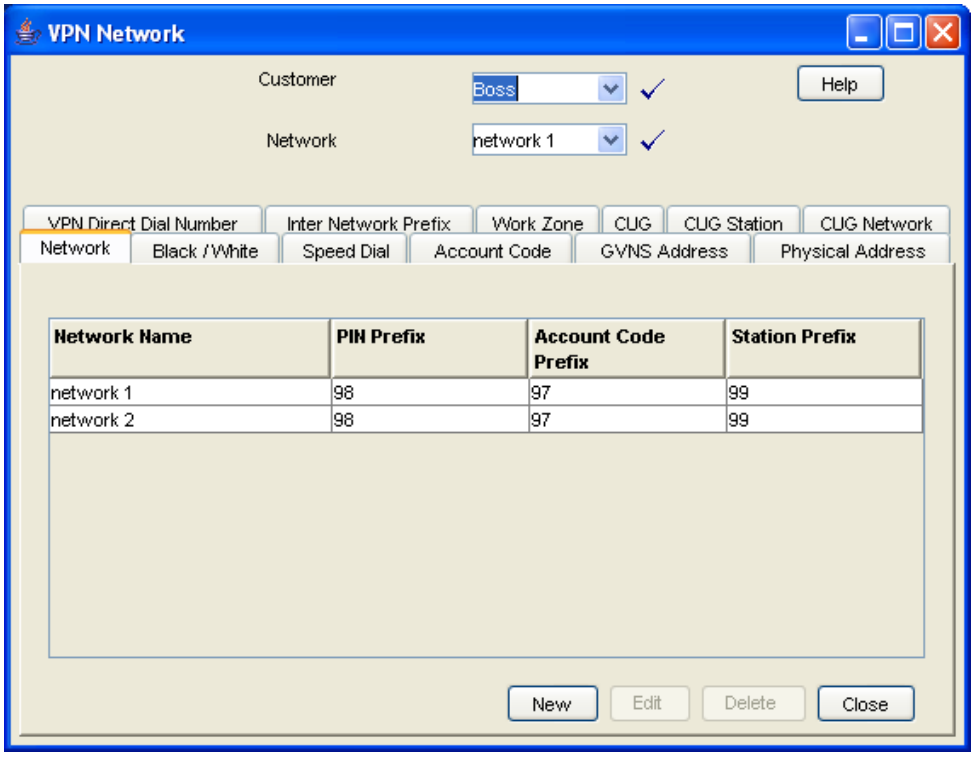
Each VPN customer may have several networks, and each network will support multiple stations.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 5 or above; levels below this will be able to view, but not edit this tab.

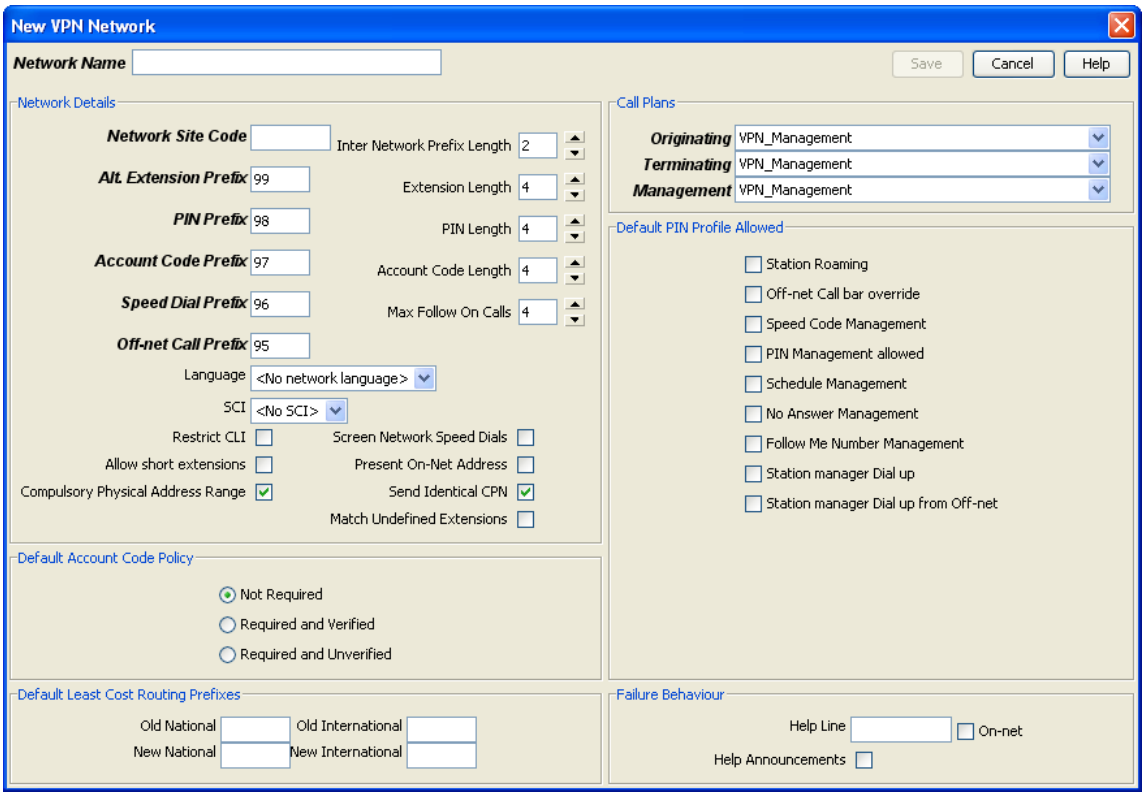
Network tab

Here is an example **Network** tab.



VPN Network screen

Here is an example VPN Network screen.



Adding a network

Follow these steps to add a new network.

Step	Action
1	Select the customer from the drop down list on the VPN Network screen.
2	Select the **Network** tab.
3	Click **New**. **Result:** You see the New *VPN Network screen* (See example on page 41).
4	Fill in the fields, as described in the *Field descriptions* (on page 41).
5	Click **Save**.

Field descriptions

This table describes each field of the New VPN Network screen and Edit Network screen.

Field	Description
Network Name	The name of the Network. A customer may have several networks, so all network names for a customer must be unique. This field may be up to 50 text characters in length and is a required field.

Network Details

Field	Description
Network Site Code	The site code for the network. Each network site code must be unique across all networks. This is a required field. It may be up to 10 DTMF digits (0-9,*,#,A-D) long.
Inter Network Prefix Length	The length of the inter network prefix defined for this network. This must be between 2 and 10.
Alt. Extension Prefix	The telephone digit/s (0-9, *, #) to be dialed before an alternate extension number is entered, (or the digit that all alternate extension number's should begin with). This may be up to 5 characters in length. The alternate extension number prefix must be unique for the network however is not a required field. **Note:** If the alternate extension number prefix is not set, users of this VPN network may not use the roaming profile features.
Extension Length	The length of the alternate extension number. This must be between 1 and 32.
PIN Prefix	The telephone digit/s (0-9, *, #) to be dialed before a PIN is entered. The PIN Prefix is an optional field. It must be unique for the network and may be up to 5 characters in length. **Note:** If the PIN prefix is not specified, a user will not be able to enter their PIN at the time of dialing the call; they will be prompted for it by the system, if required.
PIN Length	The length of the PIN. This must be between 1 and 32.
Account Code Prefix	The telephone digit/s (0-9, *, #) to be dialed before an account code is entered (or the digit that all account codes should begin with). This is an optional field. It must be unique for the network and may be up to 5 characters in length. **Note:** If the account code prefix is not specified, a user will not be able to enter an account code at the time of dialing the call; they will be prompted for it by the system if required.
Account Code Length	The length of the account code. This must be between 1 and 32.
Speed Dial Prefix	The telephone digit/s (0-9, *, #) to be dialed before a speed dial number is entered (or the digit that all speed dial numbers should begin with). This is an optional field. It must be unique for the network and may be up to 5 characters in length. **Note:** If no speed dial prefix is set, users of this VPN will not be able to use the speed dial features.
Max Follow On Calls	The number of calls that may be made from the station manager at any one dial-up. This must be between 1 and 32.

Field	Description
Off-net Call Prefix	The telephone digit/s (0-9, *, #) that are to be dialed before an off-net call is entered. This is an optional field. It must be unique for the network and may be up to 2 characters in length. **Note:** If no off-net prefix is set, users of this VPN may not make off-net calls.
Language	The default language for the Network. By default, all announcements played to users of this network will be played in this language. If the selected language is not available for an announcement, the announcement will play in the system default language. The default language is determined by ACS.
SCI	The tariff code associated with this network. **Note:** This only takes effect when used by a VPN set tariff code from profile node.
Restrict CLI	If selected , this option will restrict all caller line identifiers on the network.
Screen Network Speed Dials	If selected, this option will allow the user to enable speed dialing over the network. The network speed dials are screened against the allowed/barred list.
Allow short extensions	If selected, stations with extension numbers shorter than the network extension length can be defined within this network.
Present On-Net Address	If selected, this option will allow the user to display addresses on the network as caller line identifiers.
Compulsory Physical Address Range	If selected, stations within this network will require their physical address to be defined within one of the network physical address ranges.`
Send Identical CPN	If selected, send the calling party number in the connect, even if it is identical to the one in the initialDP.
Matched Undefined Extensions	If selected, there is no need to define the extensions for the site. If the dialed number site code plus it has the right number of digits is recognized, it will treat it like a station.

Default Account Code Policy

The default Account Code Policy determines if a station user must enter an Account Code when making off-net calls and, if required, whether these will be checked for validity or not.

The default Account Code Policy will be used for those stations in the network that do not have a specified Account Code Policy set for them. Select the required option to set the Account Code Policy.

Field	Description
Not Required	A VPN user will not be required to add an Account Code and will not be prompted to enter one.
Required and Verified	An Account Code is required and the user will be prompted for one if not supplied. The Account Code will then be checked against the list of valid account codes and the call may only proceed if the Account Code is valid.

Field	Description
Required and Unverified	An Account Code is required. The system will prompt for one if not supplied and will check number of digits entered, but will not check that the Account Code is valid.

Note: This is only relevant when the Account Code Entry node is used.

Default Least Cost Routing Prefixes

Field	Description
Old National	The Old National Routing Prefix in this field, which is to be used as a default if no prefix is specified for a network. The Least Cost Routing Prefix may be up to 32 digits in length, but is optional.
New National	The Old National Routing Prefix in this field, which is to be used as a default if no prefix is specified for a network. The Least Cost Routing Prefix may be up to 32 digits in length, but is optional.
Old International	The Old International Routing Prefix in this field, which is to be used as a default if no prefix is specified for a network. The Least Cost Routing Prefix may be up to 32 digits in length, but is optional.
New International	The International Least Cost Routing Prefix, which is to replace the Old International Routing Prefix in this field. The Least Cost Routing Prefix may be up to 32 digits in length, but is optional.

Call Plans

Field	Description
Originating	The control plan that is triggered when a call is originated from VPN. There are three sample Originating control plans: • VPN_Originating_Alternative • VPN_Originating_Fixed • VPN_Originating_Mobile
Terminating	The control plan that is triggered when a call is terminated at VPN. There are two sample Terminating control plans: • VPN_Terminating • VPN_Terminating_Alternative
Management	The management control plan that is triggered for all calls. There are two sample Management control plans: • VPN_Management • VPN_Management_Alternative

Refer to *VPN Control Plans* (on page 6) for details.

Note: The term Call Plan is the obsolete name for Control Plan.

Default PIN Profile Allowed

Select the appropriate check boxes that are required as the default PIN profile. This will set the default access given to a user by using a PIN.

An individual PIN profile may be set for each station. This is set in the Station screen.

The PIN profile allows a VPN user to dial up to manage aspects of their own profile.

You may select as many PIN profile check boxes as required.

Field	Description
Station Roaming	If selected, this will allow the user to move to another station and have it behave as if they were at their home station. For example; a user may move stations and have things that are set up for their station available to them (that is, their speed dial list, their allowed/barred lists), as if they were at their home station.
Off-net Call Bar override	If selected, this will allow the user to override the off-net call bar that may be set on a station.
Speed Code Management	If selected, the user may manage their speed code dial list.
PIN Management allowed	If selected, the user may manage their PIN. This will include changing their PIN and changing their own PIN profile.
Schedule Management	If selected, the user may manage their scheduling information.
No Answer Management	If selected, this will allow the user to manage and change their busy and no answer forwarding numbers.
Follow Me Number Management	If selected, this will allow the user to manage and change the follow me number for their station.
Station Manager Dial up	If selected, this will allow the user to dial up from within the VPN network and manage aspects of their own station profile.
Station Manager Dial up from Off-net	If selected, this will allow the user to dial up from a location that is not on the VPN network and manage aspects of their own station profile.

Failure Behaviour

Field	Description
Help line	The help number that calls are diverted to if the caller experiences difficulties. Enter the extension number if the help line number is on the network or enter the full number if the number if off the network.
On-net	Select this box if the Help line number is on the network.
Help Announcements	Select this if Help announcements are to play over the network. If this option is not checked the network will disconnect without playing an announcement.

Changing network details

Follow these steps to change the network details, if required.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Network** tab.
3	Select the network in the table and click **Edit**. **Result:** You see the Edit *VPN Network screen* (See example on page 41).
4	Change the details as required. Refer to *Field descriptions* (on page 41).
5	Click **Save**. **Result:** The network entry is updated.

Deleting a network

Follow these steps to delete a network.

Warning: This will also remove all stations belonging to the network. Use with caution.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Network** tab.
3	Select the network in the table and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes** to confirm. **Result:** The network is removed from the system.

GVNS Address Ranges

Introduction

The **GVNS Address** tab of the VPN Network screen displays the list of GVNS address ranges.

Each Station in a network may have a GVNS Address, but the Address that they use must be within the ranges that are assigned for the network.

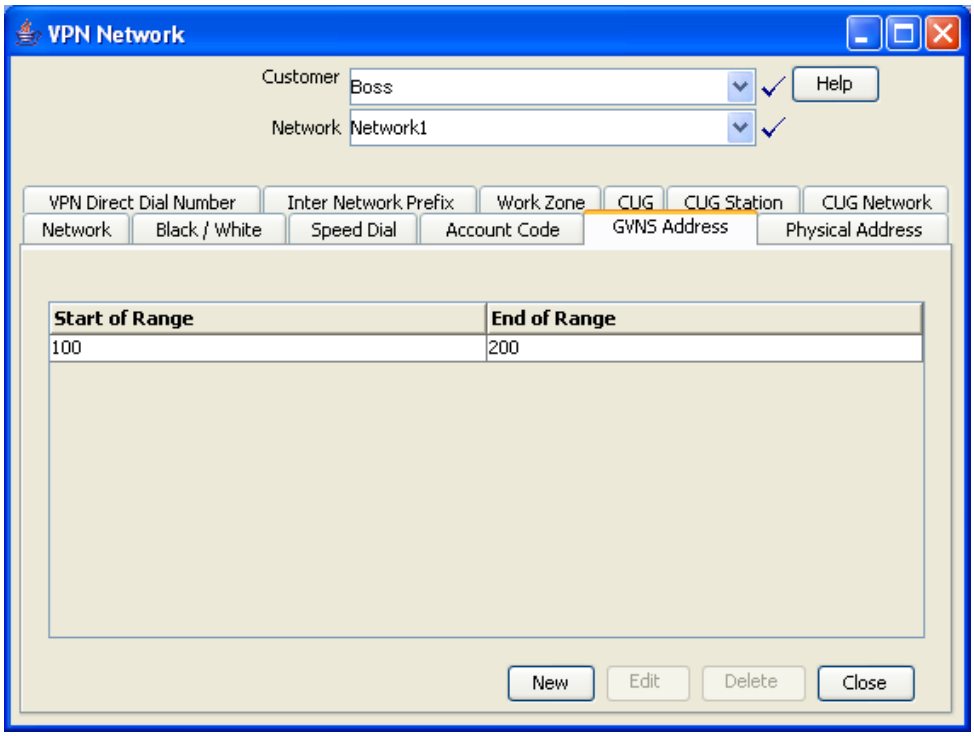
When multiple VPNs are in use by a customer, the capability to route calls between these VPNs requires a numbering scheme that uses destination addresses based on a customer ID and extension number. These GVNS addresses can then be interpreted to provide inter-VPN operation.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 6 or above; levels below this will be able to view, but not edit this tab.

GVNS Address tab

Here is an example **GVNS Address** tab.



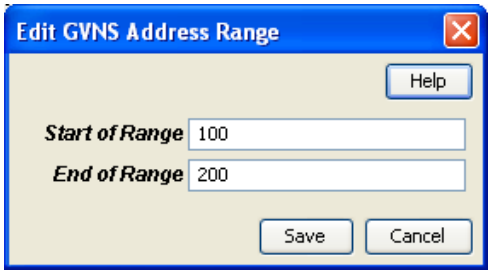
Field descriptions

This table describes each field of the New GVNS Address Range and Edit GVNS Address Range screen.

Field	Description
Start of range	Start of the number range that is allocated to the virtual network. This may be up to 32 characters in length (0-9).
End of range	End of the number range that is allocated to the virtual network. This may be up to 32 characters in length (0-9).

GVNS Address Range screen

Here is an example GVNS Address Range screen.



Adding a range

Follow these steps to add a GVNS address range.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **GVNS Address** tab.
3	Click **New**. **Result:** You see the New *GVNS Address Range screen* (See example on page 47).
4	Enter the numbers of the GVNS address range for the: • Start • End **Note:** Address ranges must not overlap. If a number is within another range in any network, you will see an error. If this occurs, check the GVNS address ranges of all of the customer's networks and create a unique range.
5	Click **Save**.

Changing range details

Follow these steps to change the details of a range, if required.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **GVNS Address** tab.
3	Select the range in the table and click **Edit**. **Result:** You see the Edit *GVNS Address Range screen* (See example on page 47).
4	Change the details, described in *Field descriptions* (on page 47), as required.
5	Click **Save**. **Result:** The entry will be updated.

Deleting a range

Follow these steps to delete a range.

Note: You cannot delete a range if the station uses the numbers within the range.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **GVNS Address** tab.
3	Select the range in the table and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes** to confirm.

Step	Action
	Result: The range is removed from the system.

Physical Address Ranges

Introduction

The **Physical Address** tab of the VPN Network screen displays the physical address ranges for the Network. Each Station in a network may have a Physical Address, but the Address that they use must be within the ranges that are assigned for the network.

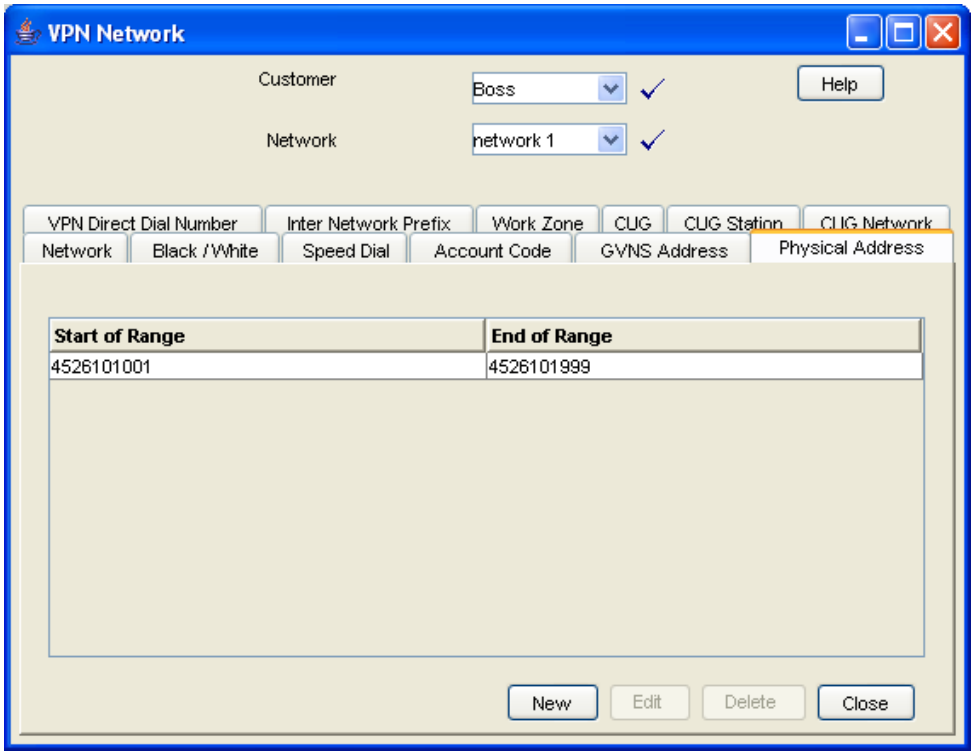
The Physical Address is the address of the Physical telephone line that a station uses.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 6 or above; levels below this will be able to view, but not edit this tab.

Physical Address tab

Here is an example **Physical Address** tab.



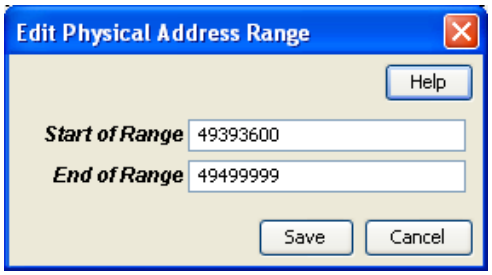
Field descriptions

This table describes each field of the New Physical Address Range screen and Edit Physical Address Range screen.

Field	Description
Start of range	Start of the physical address that is allocated to the virtual network. This may be up to 32 characters in length (0-9).
End of range	End of the physical address that is allocated to the virtual network. This may be up to 32 characters in length (0-9).

Physical Address Range screen

Here is an example Physical Address Range screen.



Adding a range

Follow these steps to add a physical address range.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Physical Address** tab
3	Click **New**. **Result:** You see the New *Physical Address Range screen.* (See example on page 50)
4	Enter the numbers of the range for the: • Start • End **Note:** Address ranges must not overlap. If a number is within another range in any network, you will see an error. If this occurs, check the Physical address ranges of all of the customer's networks and create a unique range.
5	Click **Save**.

Changing range details

Follow these steps to change the details of a range, if required.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.

Step	Action
2	Select the **Physical Address** tab.
3	Select the range in the table and click **Edit**. **Result:** You see the Edit *Physical Address Range screen.* (See example on page 50)
4	Change the details, as described in *Field descriptions* (on page 50), as required.
5	Click **Save**. **Result:** The entry will be updated.

Deleting ranges

Follow these steps to delete a range.

Note: You cannot delete a range if the station uses the numbers within the range.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Physical Address** tab.
3	Select the range in the table and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes** to confirm. **Result:** The range is removed from the system.

VPN Direct Dial Number Ranges

Introduction

The **VPN Direct Dial Number** tab of the VPN Network screen displays the VPN Direct Dial Number ranges for the network.

The VDDI (Virtual Direct Dial In) Address is the number that outside callers use to dial the station as a VPN call. It is the number that is dialled to reach the station using the VPN network.

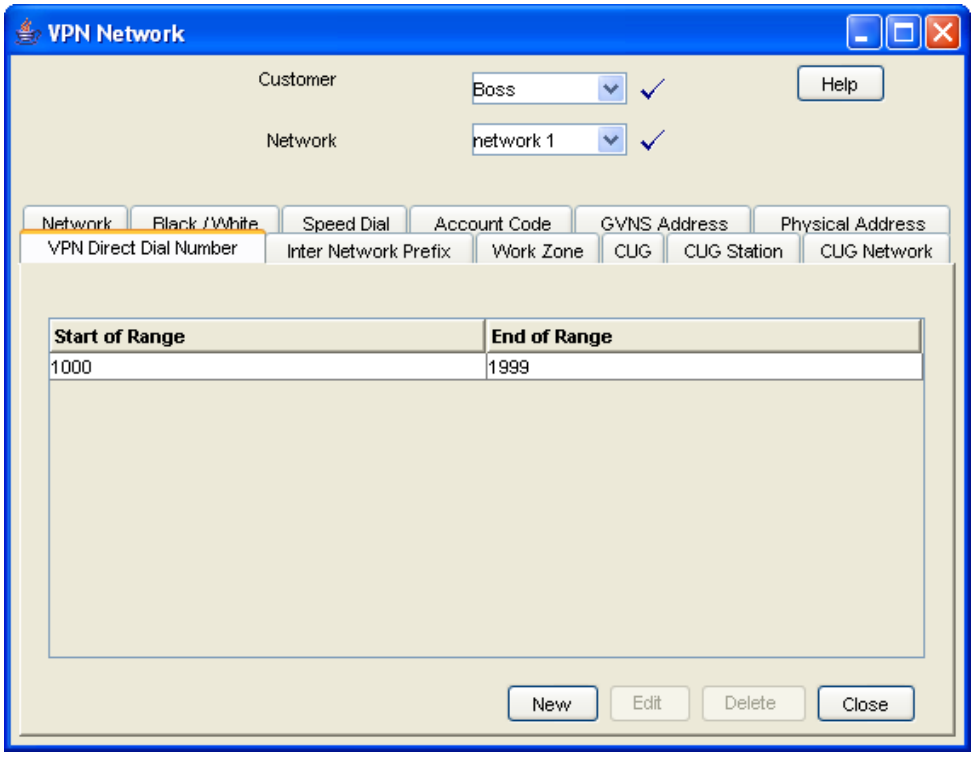
Each Station in a network may have a VDDI Address but the Address that they use must be within the ranges that are assigned for the network.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 6 or above; levels below this will be able to view, but not edit this tab.

VPN Direct Dial Number tab

Here is an example **VPN Direct Dial Number** tab.



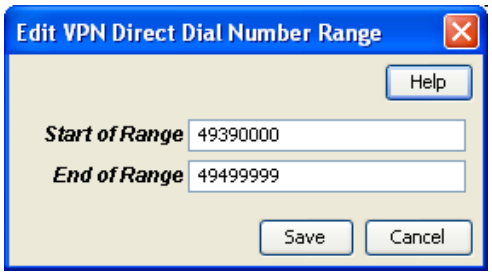
Field descriptions

This table describes each field of the New VPN Direct Dial Number Range screen and Edit VPN Direct Dial Number Range screen.

Field	Description
Start of range	Start of the DDI number that is allocated to the virtual network. This may be up to 32 characters in length (0-9).
End of range	End of the DDI number that is allocated to the virtual network. This may be up to 32 characters in length (0-9).

VPN Direct Dial Number Range screen

Here is an example VPN Direct Dial Number Range screen.



Adding a range

Follow these steps to add a VDDI number range.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **VPN Direct Dial Number** tab.
3	Click **New**. **Result:** You see the New *VPN Direct Dial Number Range screen* (See example on page 52).
4	Enter the numbers of the VDDI range for the: • Start • End **Note:** Address ranges must not overlap. If a number is within another range in any network, you will see an error. If this occurs, check the VDDI address ranges of all of the customer's networks and create a unique range.
5	Click **Save**.

Changing range details

Follow these steps to change the details of a range, if required.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **VPN Direct Dial Number** tab.
3	Select the range in the table and click **Edit**. **Result:** You see the Edit *VPN Direct Dial Number Range screen* (See example on page 52).
4	Change the details, as described in *Field descriptions* (on page 52), as required.
5	Click **Save**. **Result:** The entry will be updated.

Deleting ranges

Follow these steps to delete a range.

Note: You cannot delete a range if the station uses the numbers within the range.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **VPN Direct Dial Number** tab.
3	Select the range in the table and click **Delete**. **Result:** You see the Delete confirmation screen.

Step	Action
4	Click **Yes** to confirm. **Result:** The range is removed from the system.

Chapter 7

Configuring the Network

Overview

Introduction

This chapter explains how to configure a VPN network for a customer.

New network configuration process

To begin using VPN, the network must be configured. When configuring a new network, follow the procedures in the order below:

1. Enter *Account Codes* (on page 55) if required.
2. Enter *Black and White Network Number Lists* (on page 57).
3. Enter network *Speed Dial* (on page 62).
4. Set up *Stations* (on page 73) for network, including *Black/White lists for Stations* (on page 80) and *Divert A/B* (on page 87).
5. Customize the station, including *Speed Dial* (on page 84) and *Hunting Lists* (on page 89).
6. Define any *Defining Closed User groups* (on page 101), if required.

In this chapter

This chapter contains the following topics.

Account Codes

Introduction

The **Account Code** tab of the VPN Network screen displays the list of Account Codes for the VPN Network.

Account codes are required if either of the following is set to `Required and Verified`.:

- *Default Account Code Policy* (on page 43) in the VPN Network screen
- *Account Code Policy* (on page 76) in the VPN Station screen

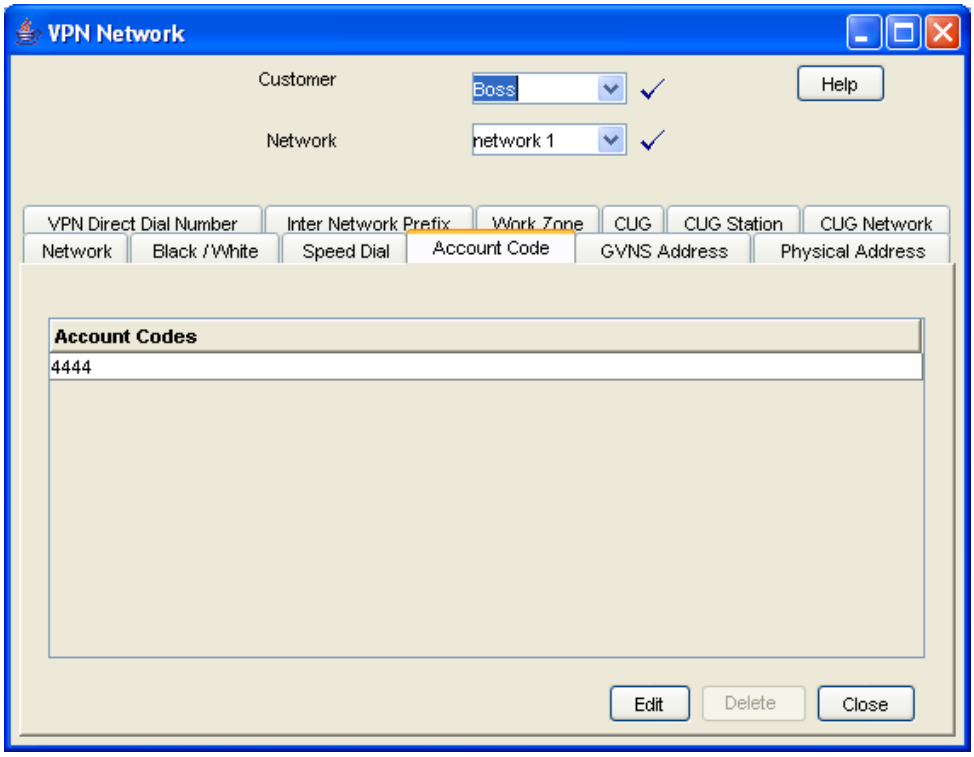
Note: These are only relevant when the Account Code Entry node is used.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 4 or above; levels below this will be able to view, but not edit this tab.

Account Code tab

Here is an example **Account Code** tab.



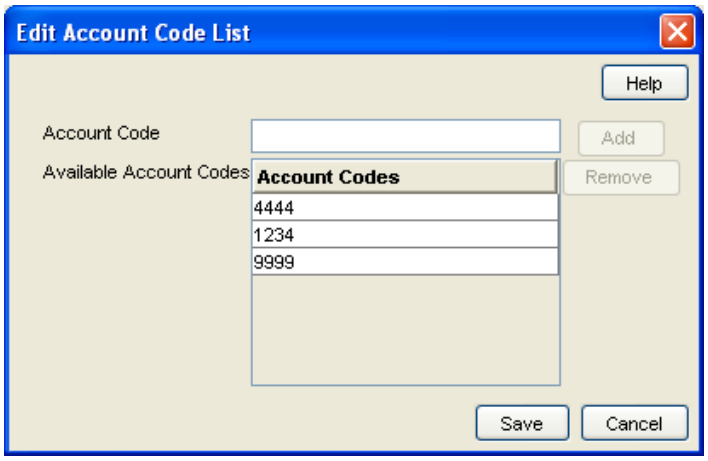
Editing the account code list

Follow these steps to edit the list of available account codes.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Account Code** tab.
3	Click **Edit**. **Result:** You see the *Edit Account Code List screen* (See example on page 57).
4	To: Add an account code to the list, fill in the **Account Code** field and click **Add**. **Note:** The length of Account Code may be up to the number of digits specified on the Network tab (Refer to *Network Details* (on page 42)) ((0-9, #, *). It is a required field and must be unique for a customer. There may be up to 10000 Account Codes set for each VPN. **Result:** The account code will appear in the list. • Remove an account code, select an account code from the table and click **Remove**. **Result:** The account code will disappear from the list.
5	Click **Save**.

Edit Account Code List screen

Here is an example Edit Account Code List screen.



Deleting an account code

Follow these steps to delete an account code.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Account Code** tab.
3	Select the account code from the table and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes** to confirm. **Result:** The account code is removed from the system.

Black and White Network Number Lists

Introduction

The **Black/White** tab of the VPN Network screen allows you to maintain the lists of numbers that are allowed (white lists) and numbers that are barred (black lists) for the VPN.

The black/white lists are global for all stations on the network. All calls are checked against the network black/white lists and then the station black/white lists.

You can maintain the following five types of black and white lists:

- Allowed/Barred
- On Net
- Off Net
- Pin Required
- Pin Not Required

There are two types of call lists that can be specified for each black/white list type:

- Incoming calls from
- Outgoing calls to

The different types of black/white lists for both types of call list may be set to either allowed or barred independently. See *Rules* (on page 58).

Note: An empty Allowed list means that *nothing* is allowed, all attempts to divert will fail. This is the default when a network is created. An empty Barred list means that *nothing* is barred.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 4 or above; levels below this will be able to view, but not edit this tab.

Rules

Black and white allowed and barred lists follow these rules:

- An empty allowed list means everything is barred (that is, nothing is allowed)
- An allowed list with numbers entered in it will allow only those numbers (or prefixes)
- An empty barred list will not bar any number (that is, every call is allowed)
- A barred list containing numbers will bar those numbers (or prefixes)
- For a number to be allowed, it must be allowed (or not barred) by both the station and the network Black/White lists
- For a number to be barred, it must be barred (or not allowed) by either the station or the network Black/White lists

Summary

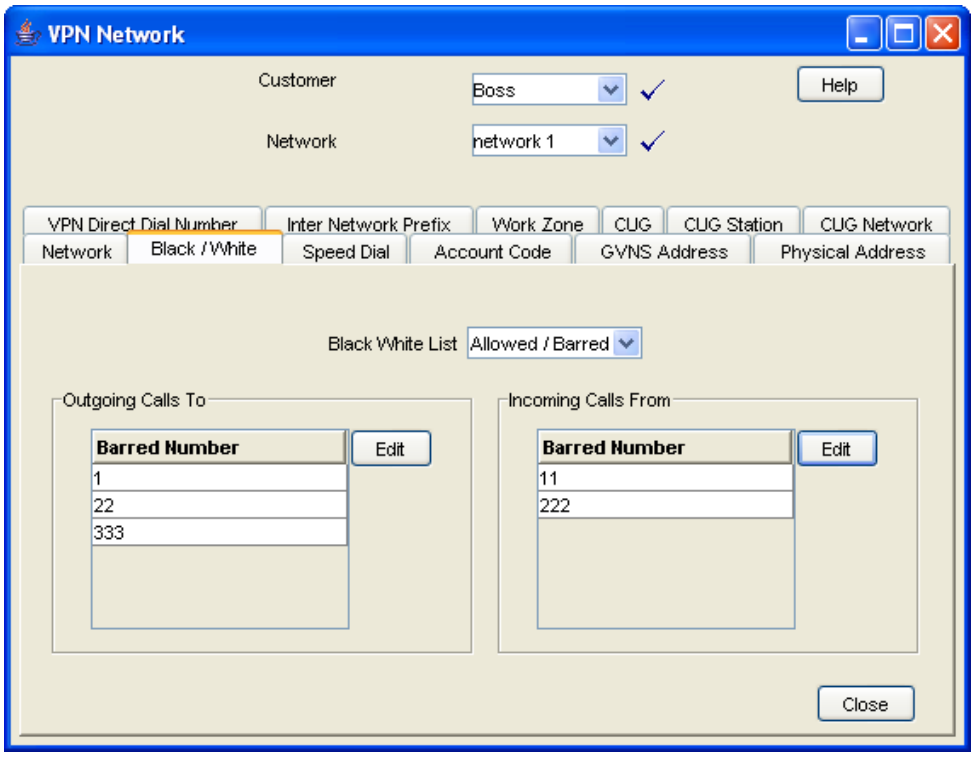
Black and White list rules may be more clearly understood from the following table:

			Network			
			Allowed List		Barred List	
			Empty List	Containing Numbers	Empty List	Containing Numbers
Station	Barred List	Containing Numbers	No calls allowed	Calls allowed: those on Network Allowed list except those on Station Barred list	All calls allowed except those on Station Barred list	All calls allowed except those on Network or Station Barred lists
		Empty List	No calls allowed	Only calls on Network allowed list	All calls allowed	All calls allowed except those on Network Barred list
	Allowed List	Containing Numbers	No calls allowed	Calls allowed: All calls on both the Network Allowed list and the Station Allowed list.	Only calls on Station Allowed list are allowed	Call allowed: All calls on Station Allowed list except those on Network Barred list
		Empty List	No calls allowed	No calls allowed	No calls allowed	No calls allowed

Note: These rules apply to a default control plan and may change if the control plan is modified.

Black/White tab

Here is an example **Black/White** tab.



Field descriptions

This table describes each field on the Edit (Inward or Outward) Calls screens.

Field	Description
Call List Type	This group contains two option buttons: • Allowed List • Barred List These allow you to select the list of either the numbers that users on the Network: • are allowed to call, or • may not call. The Allowed or Barred setting is for the entire list; either all the numbers (and only numbers on the list) are Allowed or they are Barred. The list may contain complete numbers, number prefixes, or a combination of both. **Example:** Barred list may contain 0900, 04 4773384 and 00. Users on this VPN Network will be barred from calling any numbers that begin with 0900 or 00 and the number 04 4773384. All other calls will be allowed. For Network Allowed lists, you must define the numbers in both the Network and Station screens. For the Barred list you define the numbers in the Network or Station screen. **Note:** If you change the list type from Allowed to Barred, or vice versa, the system will delete the entire list.
Edit List Details	Numbers in the Allowed/Barred list may be up to 32 digits in length and there may be up to 1000 numbers in the list. If there are no numbers defined in the Allowed list, this will mean that no calls are allowed, either incoming or outgoing. If there are no numbers defined in the Barred list, this will mean that nothing is barred.

Editing outgoing numbers

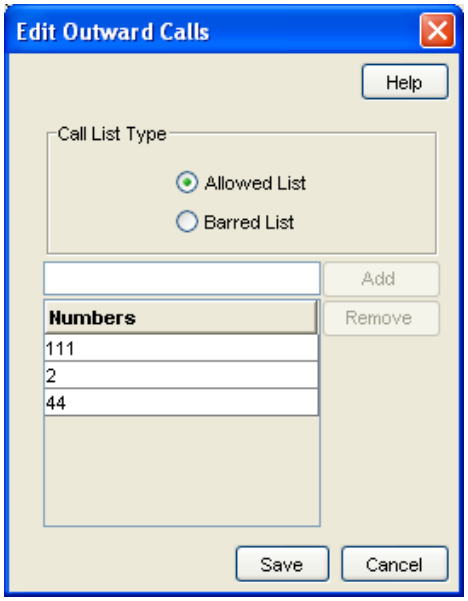
Follow these steps to add or remove an outgoing number to a black / white allowed or barred list.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Black/White** tab.
3	Select the **Black White List** type for the number to allow or bar.
4	Within the *Outgoing Calls To area* (See example on page 59), click **Edit**. **Result:** You see the *Edit Outward Calls screen* (See example on page 61).
5	Select the appropriate Call List Type (**Allowed List** or **Barred List**) option. See *Field descriptions* (on page 60) for details about the fields on this screen.
6	To: • Add a number, type the number or the number prefix that is to

Step	Action
	be specifically allowed or barred in the field and click **Add**. • Remove a number, select the number in the table and click **Remove**.
7	Repeat steps 3 to 6, as required.
8	Click **Save**.

Edit Outward Calls screen

Here is an example Edit Outward Calls screen.



Editing incoming numbers

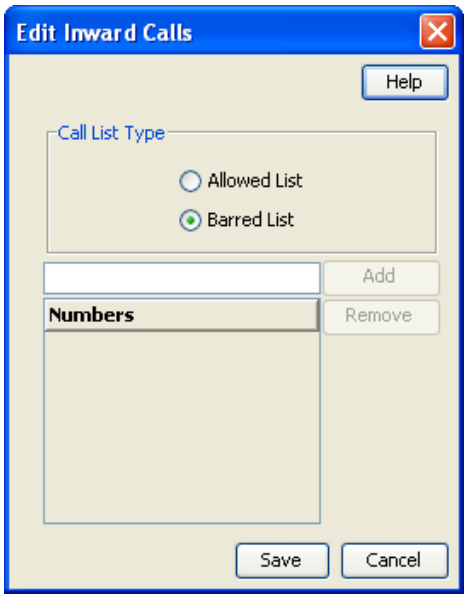
Follow these steps to add or remove an incoming number to a black / white allowed or barred list.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Black / White** tab.
3	Select the **Black White List** type for the number to allow or bar.
4	Within the *Incoming Calls From area* (See example on page 59), click **Edit**. **Result:** You see the *Edit Inward Calls screen* (See example on page 62).
5	Select the appropriate Call List Type (**Allowed** or **Barred**) option. See *Field descriptions* (on page 60) for details about the fields on this screen.
6	To: • Add a number, type the number or the number prefix that is to be specifically allowed or barred and click **Add**. • Remove a number, select the number in the table and click

Step	Action
	Remove.
7	Repeat steps 3 to 6, as required.
8	Click **Save**.

Edit Inward Calls screen

Here is an example Edit Inward Calls screen.



Speed Dial

Introduction

The **Speed Dial** tab of the VPN Network screen allows you to maintained the list of speed dial numbers for the network.

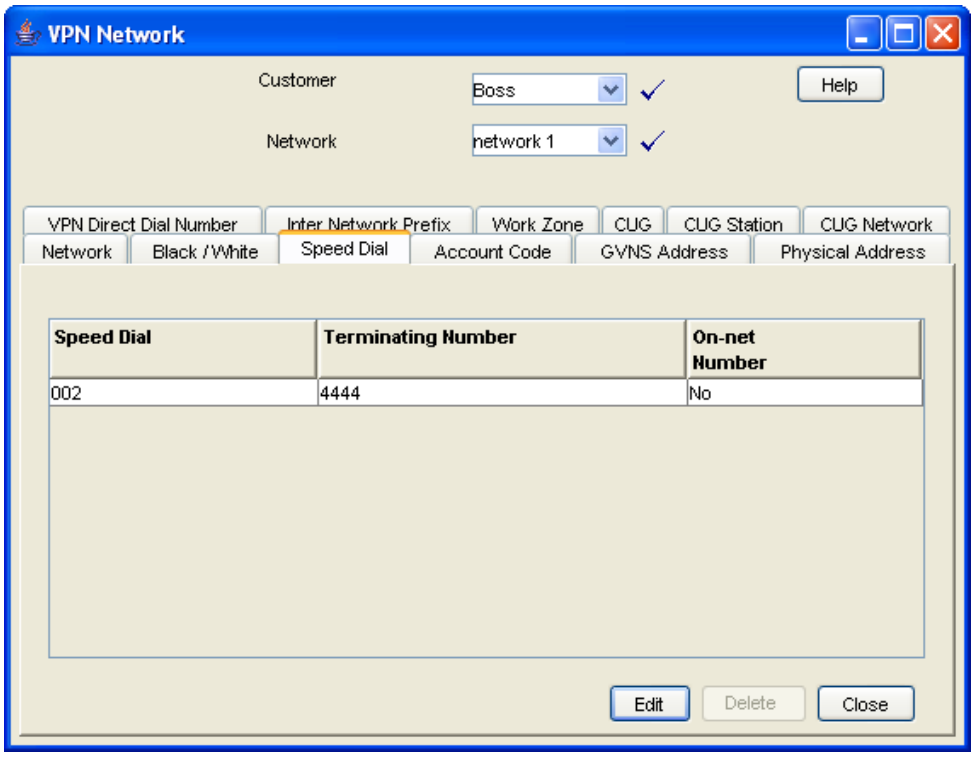
The Network Speed Dial list is global and may be used by all users on the network.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 4 or above; levels below this will be able to view, but not edit this tab.

Speed Dial tab

Here is an example **Speed Dial** tab.



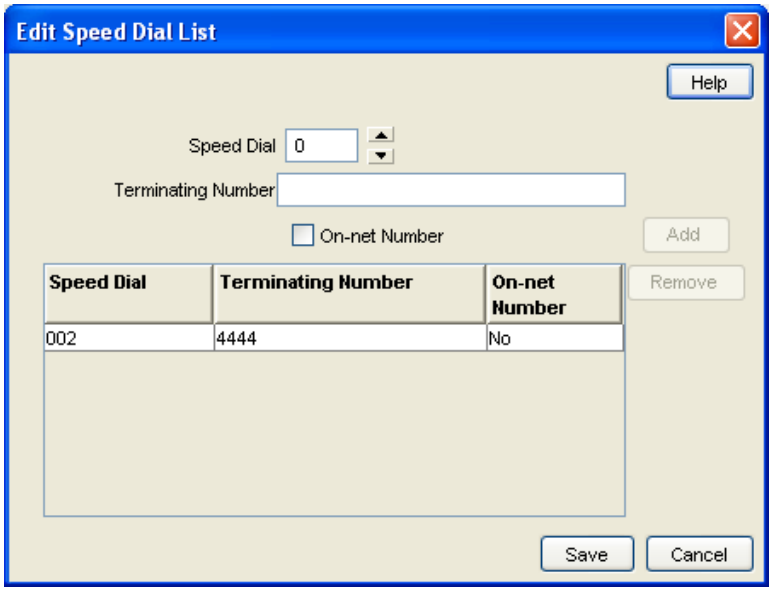
Editing the speed dial number list

Follow these steps to edit the speed dial number list.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Speed Dial** tab.
3	Click **Edit**. **Result:** You see the *Edit Speed Dial List screen* (See example on page 64).
4	To: • Add a number, complete the fields, as described in *Field descriptions* (on page 64) and click **Add**. **Result:** The number is added to the table. • Remove a number, select the speed dial record from the table and click **Remove**.
5	Repeat step 4, as required.
6	Click **Save**.

Edit Speed Dial List screen

Here is an example Edit Speed Dial List screen.



Field descriptions

This table describes each field in the Edit Speed Dial List screen.

Field	Description
Speed Dial	Network speed dial numbers are between 0 and 999. **Tip:** In the example management control plans, collect digit to sub-tag nodes, it is assumed that network speed dials are in the range 0 - 99 and station speed dials are in the range 100 - 199. The screens do not enforce these limits, but if one of these control plans is used unmodified, then the screen's users should use these ranges.
Terminating Number	The terminating number (0-9,*,#) for the speed dial. This number may be up to 32 digits in length and is required.
On-net Number	Used to indicate whether the terminating number for the speed dial is an on-net number or not. If the box is not selected, the system will assume that the terminating number is an off-net number and will prefix the number with an off-net prefix.

Deleting a speed network dial

Follow these steps to delete a speed dial from the list.

Note: You can also delete a speed dial using the *Edit Speed Dial List screen* (on page 63).

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Speed Dial** tab.
3	Select the speed dial from the table and click **Delete**.

Step	Action
	Result: You see the Delete confirmation screen.
4	Click **Yes** to confirm.
	Result: The speed dial is removed from the system.

Inter Network Prefix

Introduction

The **Inter Network Prefix** tab of the VPN Network screen allows you to maintain the list of Inter Network Prefixes for the network.

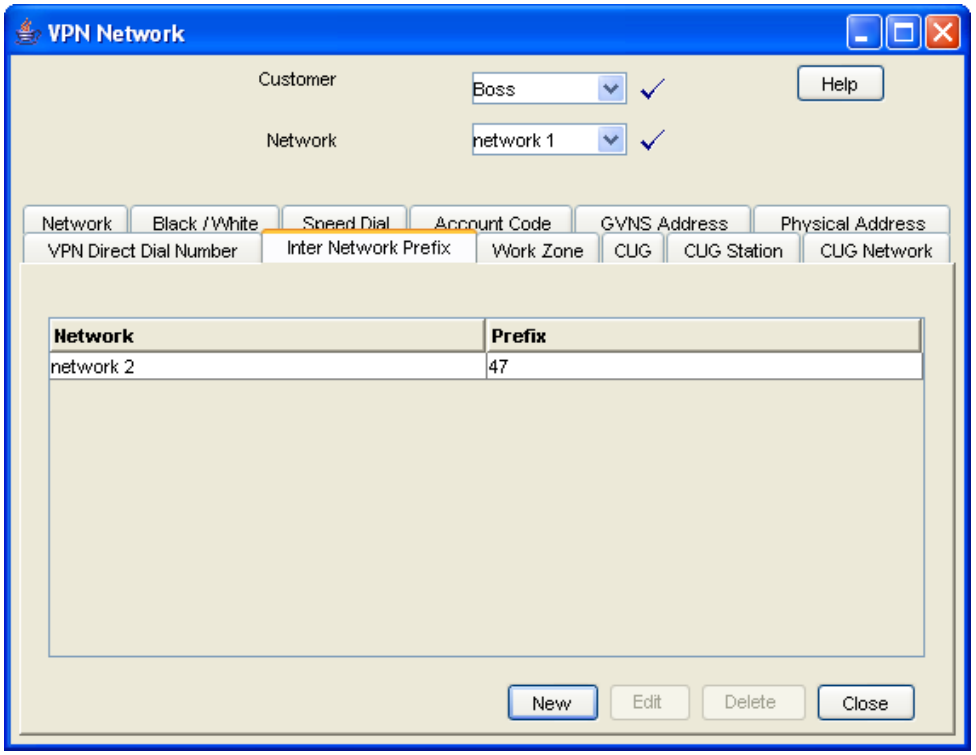
Note: The Inter Network Prefix list is global and may be used by all users on the network.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 6 or above; level 5 may edit but not add or delete; levels below this will be able to view, but not edit this tab.

Inter Network Prefix tab

Here is an example **Inter Network Prefix** tab.



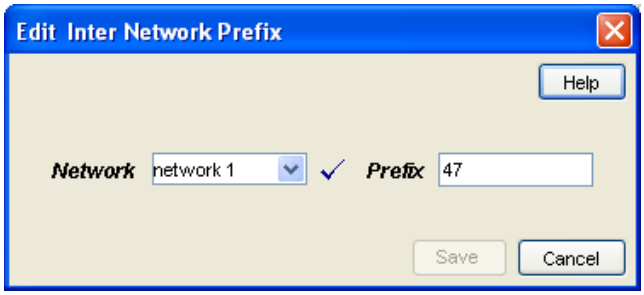
Field descriptions

This table describes each field in the New Inter Network Prefix and Edit Inter Network Prefix screens.

Field	Description
Network	The network name assigned to the prefix. Network names must correspond to defined VPN networks.
Prefix	The inter network prefix number DTMF digits (0-9,*,#,A-D). **Note:** This number must be the length specified for the *Network Details* (on page 42) on the Network screen.

Inter Network Prefix screen

Here is an example Inter Network Prefix screen.



Adding an Inter Network Prefix

Follow these steps to add an Inter Network Prefix.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Inter Network Prefix** tab.
3	Click **New**. **Result:** You see the New *Inter Network Prefix screen* (See example on page 66).
4	Select the **Network** from the drop down list.
5	Enter the **Prefix**.
6	Click **Save**.

Changing an Inter Network Prefix

Follow these steps to change an Inter Network Prefix.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Inter Network Prefix** tab.
3	Highlight the network prefix you want to modify on the table and click **Edit**. **Result:** You see the Edit *Inter Network Prefix screen* (See example on

Step	Action
	page 66).
4	Change the details, as described in *Field descriptions* (on page 66), as required.
5	Click **Save**. **Result:** The entry is updated.

Deleting an Inter Network Prefix

Follow these steps to delete an Inter Network Prefix.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Inter Network Prefix** tab.
3	Highlight the network prefix in the table and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes** to confirm. **Result:** The inter network prefix is removed from the system.

Work Zone

Introduction

The **Work Zone** tab of the VPN Network screen allows you to manage the list of shapes used to define the network work zone.

Notes:

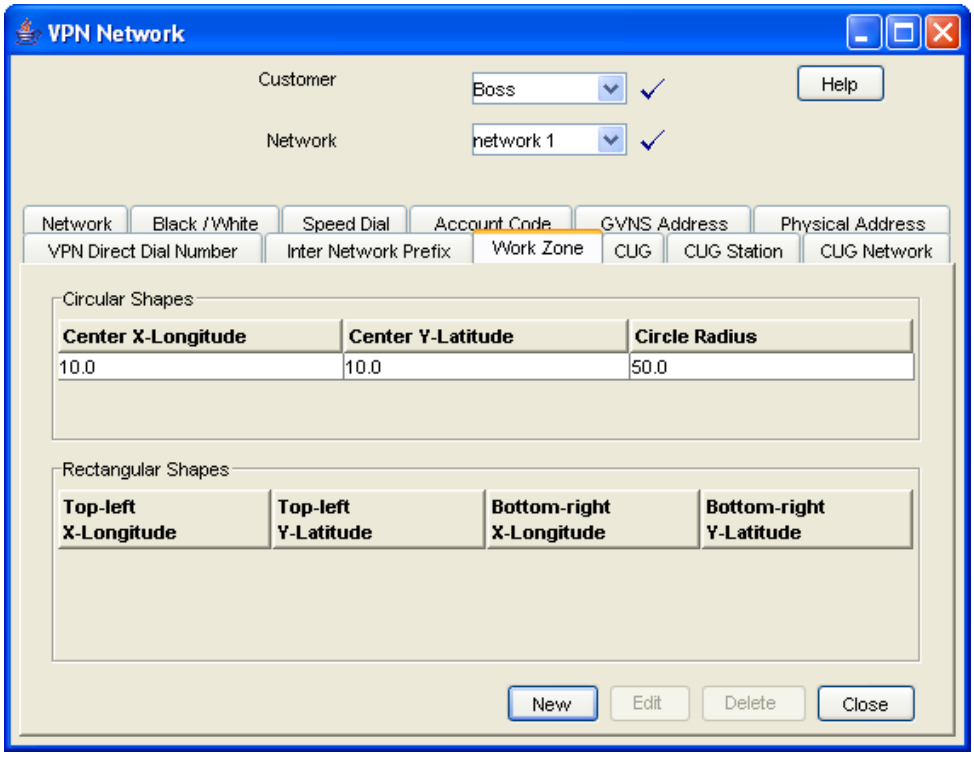
- The work zone functionality is only available if LCP is installed. For more information, see *Location Capabilities Pack Technical Guide*.
- ACS also needs to have profile fields of the zone type configured in the ACS Configuration screen. For more information about setting up profile fields, see *ACS User's Guide*.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 5 or above; level 4 may edit but not add or delete; levels below this will be able to view, but not edit this tab.

Work Zone tab

Here is an example **Work Zone** tab.



Field descriptions

This table describes each field in the New Work Zone Shape screen.

Field	Description
Circular Shape option	Select to define the attributes for a circular shape.
X (Deg)	Defines the x coordinate for the centre point of the circular shape. It is expressed in degrees longitude, in the range: -179.99999 to +179.99999.
Y (Deg)	Defines the y coordinate for the centre point of the circular shape. It is expressed in degrees latitude, in the range: -89.99999 to +89.99999.
R (Kms)	Defines the radius of the circular shape.
Rectangular Shape option	Select to define the attributes for a rectangular shape.
Top-left corner X (Deg)	Defines the x coordinate for the top left corner of the rectangular shape. It is expressed in degrees longitude, in the range: -179.99999 to +179.99999.
Top-left corner Y (Deg)	Defines the y coordinate for the top left corner of the rectangular shape. It is expressed in degrees latitude, in the range: -89.99999 to +89.99999.
Bottom-right corner X (Deg)	Defines the x coordinate for the the bottom left corner of the rectangular shape. It is expressed in degrees longitude, in the range: -179.99999 to +179.99999.

Field	Description
Bottom-right corner Y (Deg)	Defines the y coordinate for the bottom left corner of the rectangular shape. It is expressed in degrees latitude, in the range: -89.99999 to +89.99999.

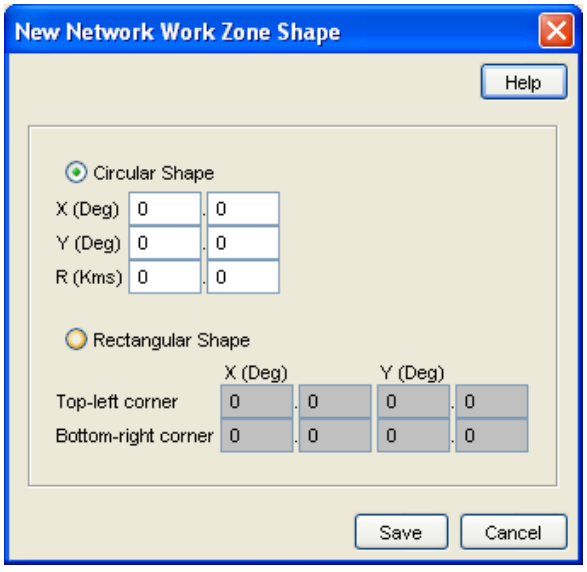
Adding a shape to a network work zone

Follow these steps to add a new shape to the work zone.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Work Zone** tab.
3	Click **New**. **Result:** You see the *New Network Work Zone screen* (See example on page 69).
4	Select the option for the type of shape you want to add (either circular or rectangular).
5	Enter the shape attributes in the appropriate fields, as described in *Field descriptions* (on page 68).
6	Click **Save**.

New Network Work Zone screen

Here is an example New Network Work Zone screen.



Changing a network work zone shape

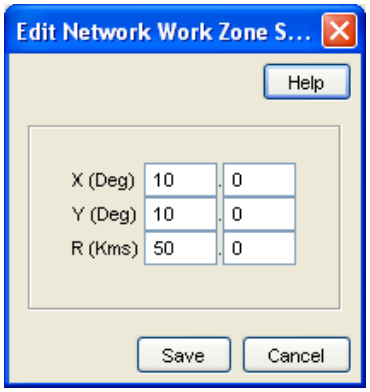
Follow these steps to change the details for a work zone shape.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.

Step	Action
2	Select the **Work Zone** tab.
3	Select the shape (circular or rectangular) in the *appropriate table* (See example on page 68).
4	Click **Edit**. **Result:** You see *Edit Network Work Zone Shape screen* (See example on page 70).
5	Modify the shape details, as described in *Field descriptions* (on page 68), as required.
6	Click **Save**.

Edit Network Work Zone Shape screen

Here is an example Edit Network Work Zone Shape screen.



Deleting a network work zone shape

Follow these steps to delete a network work zone shape.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Work Zone** tab.
3	Highlight the shape to delete (circular or rectangular) in the *appropriate table* (See example on page 68) and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes**. **Result:** The shape is removed from the work zone.

Chapter 8

Station

Overview

Introduction

This chapter explains how to add and maintain stations for the VPN service.

Add new station process

When adding a new station follow the procedures in the order given below:

1 *Adding a station* (on page 79) for the customer.
2 Add *Black/White lists for Stations* (on page 80) to the station.
3 *Editing the speed dial number list* (on page 85).
4 *Editing the divert number list* (on page 88).
5 *Adding a hunting list* (on page 91)
6 *Editing hunting planner* (on page 93)

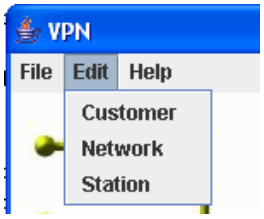
In this chapter

This chapter contains the following topics.

Accessing the Station Module

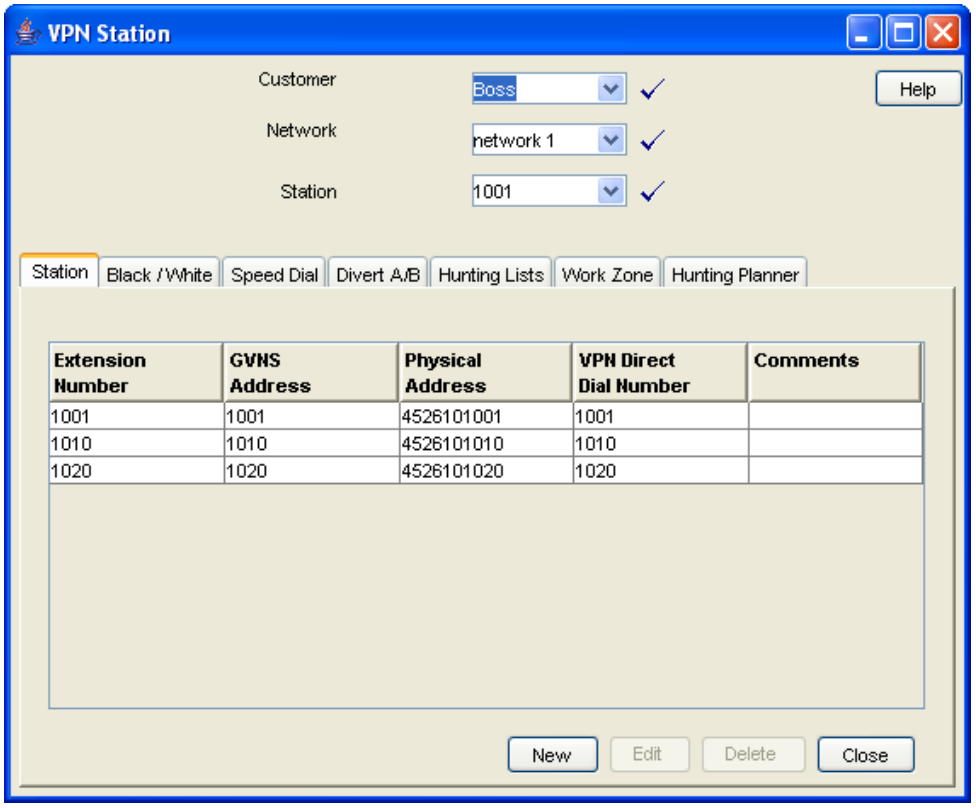
Introduction

To access the VPN Station module, on the VPN main screen, select **Edit**, **Station**.



Station screen

Here is an example VPN Station screen.



Station screen tabs

The VPN Station screen contains the following tabs:

- *Stations* (on page 73)
- *Black/White lists for Stations* (on page 80)
- *Speed Dial* (on page 84)
- *Divert A/B* (on page 87)
- *Hunting Lists* (on page 89)
- *Work Zone* (on page 95)
- *Hunting Planner* (on page 92)

Selecting a customer

Follow these steps to select a customer.

Step	Action
1	In the **Customer** field, type the first letters, or whole name.
2	Press **Enter**. **Result:** The name of the customer and the fields on the screen will be populated with the relevant data.

Finding a network

Follow these steps to find a network.

Step	Action
1	Select the network from the **Network** list field.
2	Press **Enter**. **Result:** The related records appear in the grid.

Finding a station

Follow these steps to find a station.

Step	Action
1	Select a station from the **Station** drop down list.
2	Press **Enter**. **Result:** Related stations will appear in the grid.

Stations

Introduction

The **Station** tab of the VPN Station screen displays the station records for the selected Network. This functionality is available from the VPN standalone system as well as if you are accessing VPN through the SMS system.

Stations are the equivalent of extension numbers on the network.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 4 or above; levels below this will be able to view, but not edit this tab.

Adding off-net hunt/forward numbers

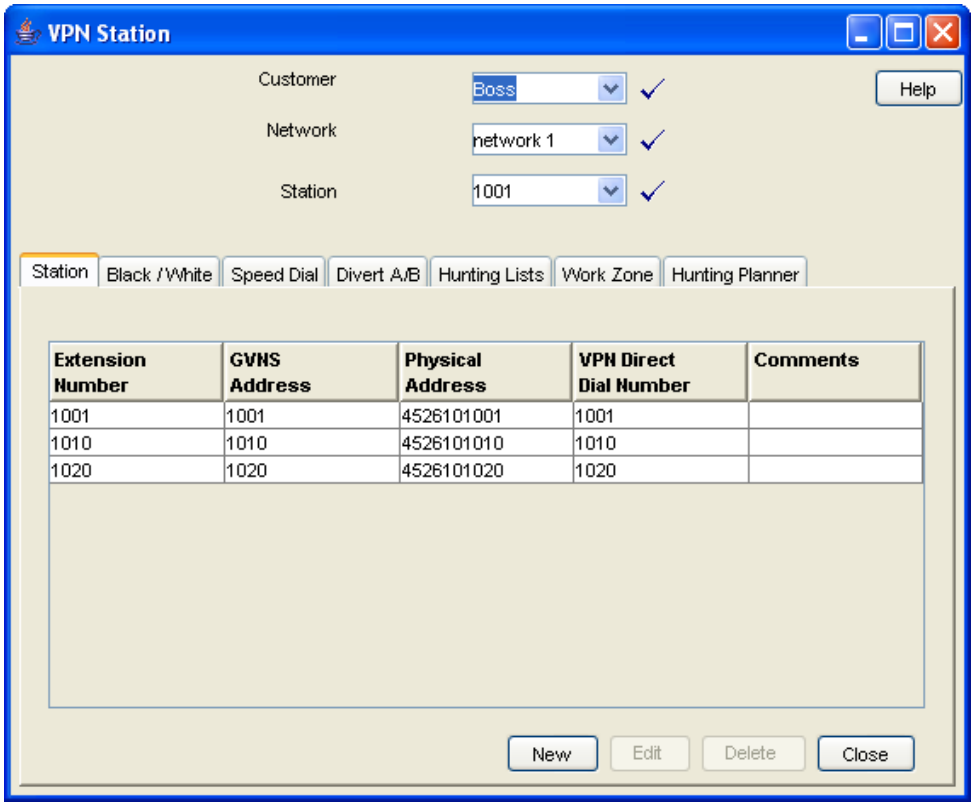
Follow these steps to add Follow Me or Alternative Routing numbers that are off-net after creating the Station as per the previous instructions.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Divert A/B** tab.
3	Create an Allowed list for Outward calls. Refer to *Editing the divert number list* (on page 88).
4	Add the off-net number that the Follow Me or Alternate Routing number is to use.
5	Save the Divert Allowed list.
6	Select the **Station** tab.
7	Edit the required station. Refer to *Changing station details* (on page 80).

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
8	Add the Follow-me or Alternative Routing number and leave the related **On-net Number** box clear.
9	**Save** the station.

Station tab

Here is an example **Station** tab.



Field descriptions

This table describes each field in the New VPN Station and Edit Station screens.

Station Details

Field	Description
Extension Number	The Extension Number (0-9, *, #) of the Station on the network. This may be up to 32 digits in length and must be unique for the network. This field is required.
GVNS Address	A GVNS (Global Virtual Numbering Scheme) Address for the station. This field is automatically populated with the network site code plus extension number. It must be within the range of GVNS Addresses that have been allocated for the network.

Field	Description
	The list of available ranges is available to all users on the *GVNS Address tab* (on page 47) of the Network screen. When multiple VPNs are in use by a customer, the capability to route calls between these VPNs requires a numbering scheme that uses destination addresses based on a customer ID and extension number. These GVNS addresses can then be interpreted to provide inter-VPN operation. The GVNS Address may be up to 32 digits in length. The GVNS address must be unique for all stations in a network, i.e. no two stations can have the same GVNS address.
Defined Address Range - GVNS	The GVNS range that has been defined for the network. When the 'Use Network Site Code' option is selected, the GVNS Address field is automatically populated with the value composed from the network site code plus the extension number. To manually enter the GVNS Address, select a different option from the GVNS Address Range.
Physical Address	A Physical Address for the station (this is the telephone number of the station). This may be up to 32 digits in length. This must be within the range of Physical Addresses that have been allocated for the network. The list of available ranges is available to all users on the *Physical Address tab* (on page 49) of the Network screen. The physical address must be unique for all stations in a network, that is, no two stations can have the same physical address.
Defined Address Range – Physical Address	The physical address range that has been defined for the network.
VPN Direct Dial Number	A VPN Direct Dial Number (0-9, *, #) for the station. This may be up to 32 digits in length. This must be within the range of VPN VPN Direct Dial Number Ranges that have been allocated for the network. The list of available ranges is available to all users on the *VPN Direct Dial Number tab* (on page 52) of the Network screen. The VDDI must be unique for all stations in a network, i.e. no two stations can have the same VDDI address.
Defined Address Range –VPN Direct Dial Number	The VPN Direct Dial Number range that has been defined for the network.
Language	The default language for the station.
Station is Station Manager	Selecting this box makes the Station's Extension Number the Dial up Management Address for the Network.
SCI	The Tariff Code associated to this station.
Allow Off-net Calls	Selecting this box allows the Station to make calls to locations off the VPN network.

Field	Description
Comments	Any comments required. This field may be up to 2000 text characters.
Fixed Station	Choose this radio button to unselect Mobile Station and set the station type to Fixed Station.
Mobile Station	Choose this radio button to unselect Fixed Station and set the station type to Mobile Station.

Hunt/Forward Settings

Field	Description
Follow-me Number	The follow-me number (0-9, *, #) of the station. This may be up to 32 digits in length. Upon creating a new station, the **On-net Number** check box to the right of the Follow Me number is automatically selected. If the Follow Me number is not entered, the on-net option disappears when you open the Edit Station screen. This ensures that at least initially, the Follow Me number for the station is on the network. To set the Follow Me number to be an off-net number, the Divert Allowed/Barred list must contain that number or prefix of the number to be allowed or barred. You cannot set the Follow Me number to be an off-net number if it is not allowed or is barred.
Alternate Routing Number	The Alternate Routing number (0-9, *, #) of the station. This may be up to 32 digits in length. This feature is not available if VPN is being run on an AIN network. Upon creating a new station, the **On-net Number** check box to the right of the Alternate Routing number (RSF) is automatically selected. If the RSF number is not entered, the on-net option disappears when you open the Edit Station screen. This ensures that at least initially, the RSF number for the station is on the network. To set the RSF number to be an off-net number, the Divert Allowed/Barred list must contain that number or prefix of the number to be allowed or barred. You cannot set the RSF number to be an off-net number if it is not allowed or is barred.

Note: To add an off-net number, see *Adding off-net hunt/forward numbers* (on page 73).

Account Code Policy

The default Account Code Policy determines if a station user must enter an Account Code when making off net calls and, if required, whether these will be checked for validity or not.

The default Account Code Policy will be used for those stations in the network that do not have a specified Account Code Policy set for them. The Account Code Policy option is set by selecting the required option.

Field	Description
Use Network Default	Use the Network Account Code policy for this station.
Not Required	A VPN user will not be required to add an Account Code and will not be prompted to enter one.
Required and Verified	An Account Code is required and the user will be prompted for one if not supplied. The Account Code will then be checked against the list of valid account codes and the call may only proceed if the Account Code is valid.
Required and Unverified	An Account Code is required. The system will prompt for one if not supplied and will check number of digits entered, but will not check that the Account Code is valid.

Incoming Call Barring

Field	Description
All incoming	Selecting this box will bar all incoming calls to the station.
All incoming off-net	Selecting this box will bar all incoming calls from an off-net number to the station.

Set PIN

Field	Description
Use Default PIN Profile	Selecting this box means the PIN will use the default profile for the Network. Selecting this box will disable all check boxes in the PIN Profile group.
PIN	The PIN for the station. The PIN length is set in the Network screen.

Allowed PIN Profiles

Select the boxes that are required as the PIN Profile for the station. This will set the access given to the station user by using a PIN.

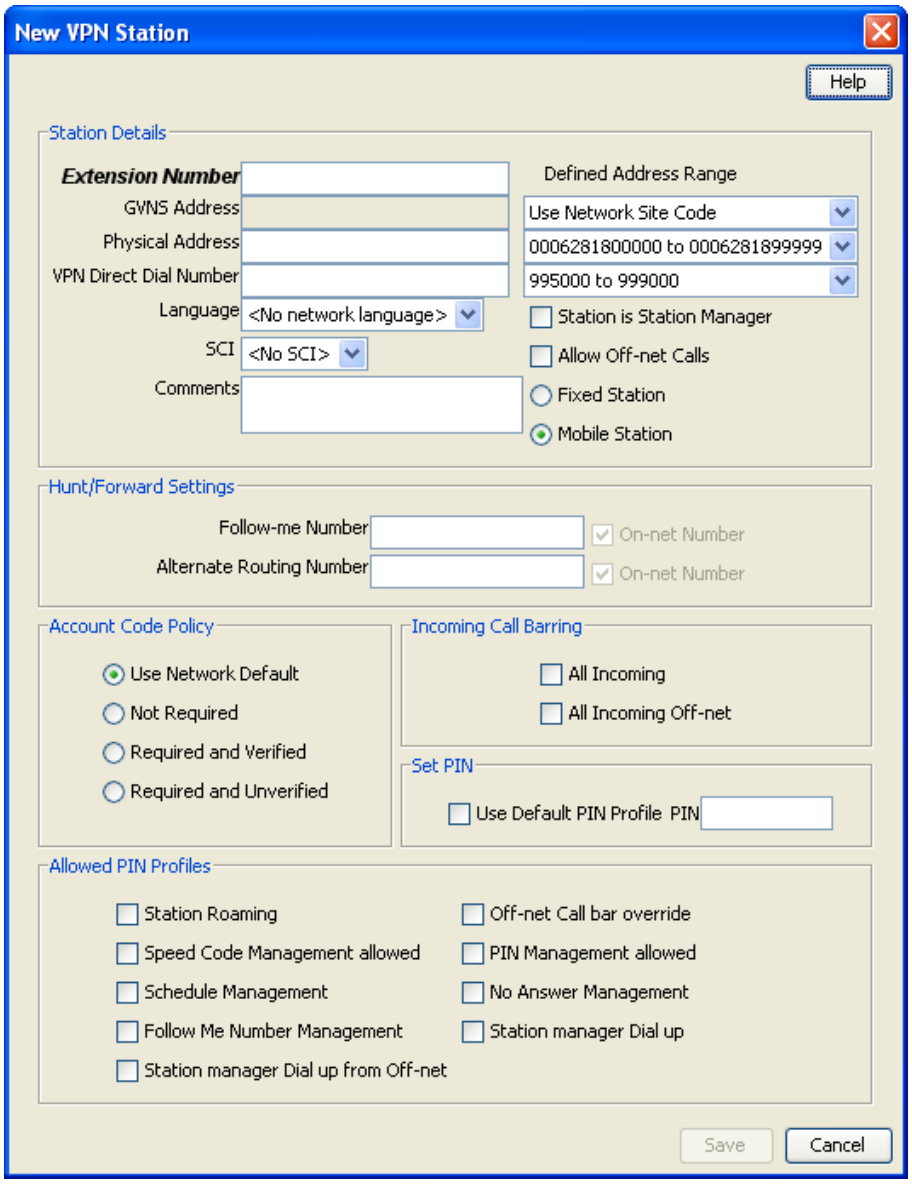
The PIN Profile allows a VPN user to Dial up to manage aspects of their own profile. As many PIN Profile check boxes as required may be selected.

Field	Description
Station Roaming	Selecting this box will allow the user to move to another station and have it behave as if they were at their home station. For example, a user may move stations and have things that are set up for their station available to them (i.e. their speed dial list, their allowed/barred lists), as if they were at their home station.

Field	Description
Speed Code Management allowed	Selecting this box will allow the user to manage their speed code dial list using the Dial In Station Manager.
Schedule Management	Selecting this box will allow the user to manage their scheduling information.
Follow Me Number Management	Selecting this box will allow the user to manage and change the Follow Me number for their station.
Station manager Dial up from Off-net	Selecting this box will allow the user to dial up from a location that is not on the VPN Network and manage aspects of their own station profile.
Off-net Call bar override	Selecting this box will allow the user to override the Off-net Call Bar that may be set on a station.
PIN Management allowed	Selecting this box will allow the user to manage their PIN. This will include changing their PIN and changing their own PIN Profile.
No Answer Management	Selecting this box will allow the user to manage and change the No Answer/Busy setting options for their station.
Station manager Dial up On-net	Selecting this box will allow the user to dial up from within the VPN Network and manage aspects of their own station profile.

VPN Station screen

Here is an example New VPN Station screen.



Adding a station

Follow these steps to add a new station.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
1	Select the **Station** tab.
2	Click **New**. **Result:** You see the New *VPN Station screen* (on page 79).
3	Fill in the fields, as described in the *Field descriptions* (on page 74).

Step	Action
4	Click **Save**.

Changing station details

Follow these steps to change the details of a station.

Step	Action
1	Select the customer, network and station from the drop down lists on the VPN Station screen.
2	Select the **Station** tab on the VPN Station screen.
3	Select the station in the table and click **Edit**.
	Result: You see the Edit *VPN Station screen* (on page 79).
4	Change the details, as required. Refer to *Field descriptions* (on page 74).
5	Click **Save**.

Deleting a station

Follow these steps to delete a station.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Station** tab.
3	Select the station in the table and click **Delete**.
	Result: You see the Delete confirmation screen.
4	Click **Yes** to confirm.
	Result: The station is removed from the system.

Black/White lists for Stations

Introduction

The **Black White** tab of the VPN Station screen allows you to maintain lists of numbers that are allowed (white lists) and numbers that are barred (black lists) for the VPN Station. You can maintain the following five types of black and white lists:

- Allowed/Barred
- On Net
- Off Net
- Pin Required
- Pin Not Required

There are two types of call lists that can be specified for each black/white list type:

- Incoming calls from
- Outgoing calls to

The different types of black/white lists for both types of call list may be set to either allowed or barred independently. See *Rules* (on page 58).

An empty Allowed list means that *nothing* its allowed, all attempts to divert will fail. This is the default when a station is created. An empty Barred list means that *nothing* is barred. A station owner may divert to any number. This may be a concern with respect to fraud.

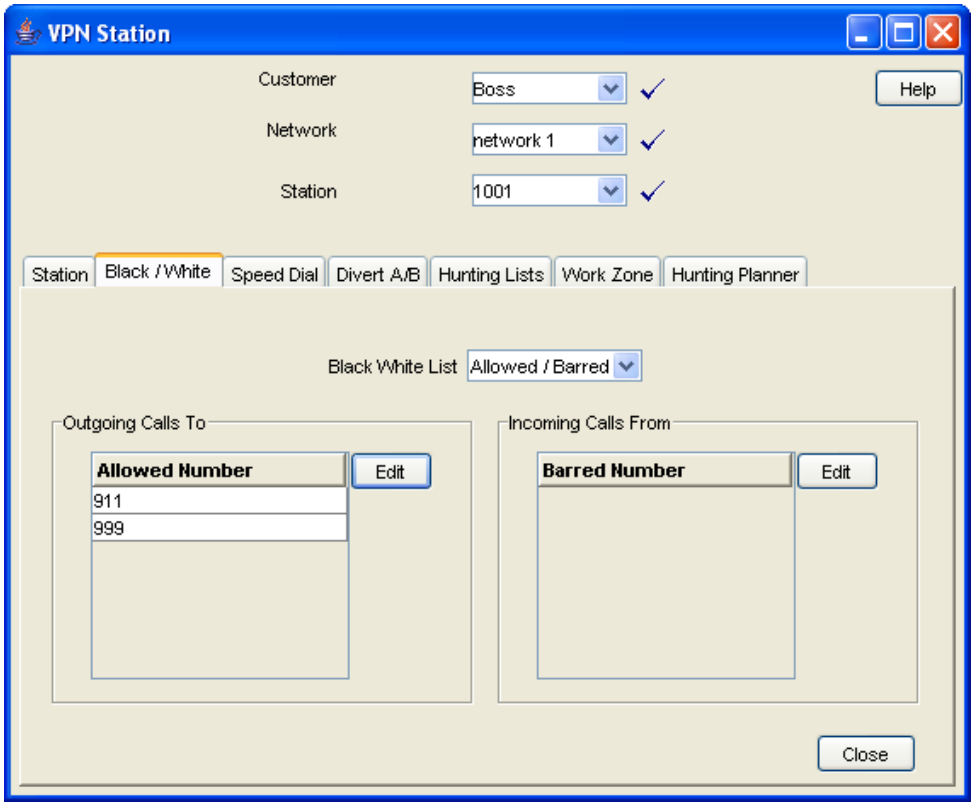
Note: The station black and white lists are checked after the network black and white lists for all calls. This may result in a call being barred by the Network that is allowed by the Station.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 4 or above; levels below this will be able to view, but not edit this tab. You can access this functionality from both the VPN standalone system and when accessing VPN through the SMS system.

Black / White tab

Here is an example Black / White tab for a VPN station.



Field descriptions

This table describes each field on the Edit (Inward or Outward) Calls screens.

Field	Description
Call List Type	This group contains two option buttons: • Allowed List • Barred List These allow you to select the list of either the numbers that users on the Station: • are allowed to call, or • may not call. The Allowed or Barred setting is for the entire list; either all the numbers (and only numbers on the list) are Allowed or they are Barred. The list may contain complete numbers, number prefixes, or a combination of both. **Example:** Barred list may contain 0900, 04 4773384 and 00. Users on this Station will be barred from calling any numbers that begin with 0900 or 00 and the number 04 4773384. All other calls will be allowed. The Outwards Calls and Inwards Calls Allowed/Barred lists may be set to either Allowed or Barred independently. If the list type is changed, the numbers in the list will be removed. If you change the list type from Allowed to Barred, or vice versa, the system will delete the entire list.
Edit List Details	Numbers in the Allowed/Barred list may be up to 32 digits in length and there may be up to 1000 numbers in the list. If there are no numbers defined in the Allowed list, this will mean that no calls are allowed, either incoming or outgoing. If there are no numbers defined in the Barred list, this will mean that nothing is barred.

Editing outgoing numbers

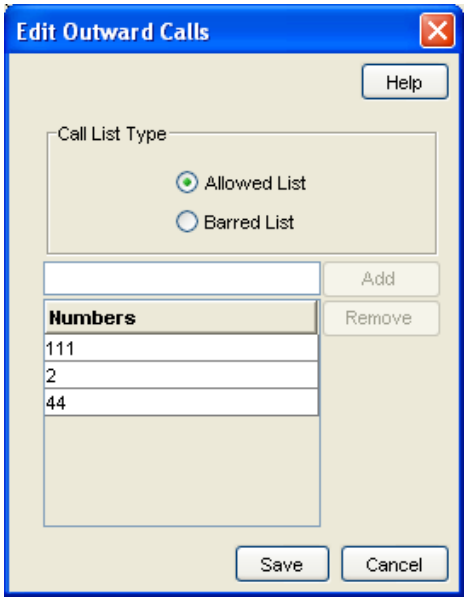
Follow these steps to add or remove an outgoing number to a black / white allowed or barred list.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Black / White** tab.
3	Select the **Black White List** type for the number to allow or bar.
4	Within the *Outgoing Calls To area* (See example on page 81), click **Edit**. **Result:** You see the *Edit Outward Calls screen* (See example on page 83).
5	Select the appropriate Call List Type (**Allowed List** or **Barred List**) option. See *Field descriptions* (on page 82) for details about the fields on this screen.
6	To: • Add a number, type the number or the number prefix that is to be specifically allowed or barred and click **Add**.

Step	Action
	• Remove a number, select the number in the table and click **Remove**.
7	Repeat steps 2 to 6, as required.
8	Click **Save**.

Edit Outward Calls screen

Here is an example Edit Outward Calls screen.



Editing incoming numbers

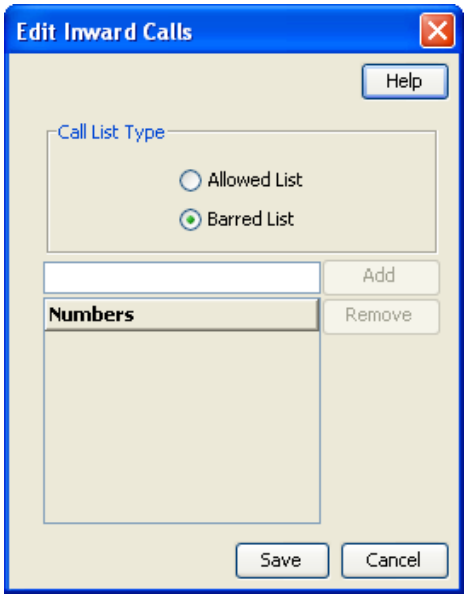
Follow these steps to add or remove an incoming number to a black/white allowed or barred list.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Black / White** tab.
3	Select the **Black White List** type for the number to allow or bar.
4	Within the *Incoming Calls From area* (See example on page 81), click **Edit**. **Result:** You see the *Edit Inward Calls screen* (See example on page 84).
5	Select the appropriate Call List Type (**Allowed List** or **Barred List**) option. See *Field descriptions* (on page 82) for details about the fields on this screen.
6	To: • Add a number, type the number or the number prefix that is to be specifically allowed or barred and click **Add**. • Remove a number, select the number in the table and click **Remove**.

Step	Action
7	Repeat steps 3 to 6, as required.
8	Click **Save**.

Edit Inward Calls screen

Here is an example Edit Inward Calls screen.



Speed Dial

Introduction

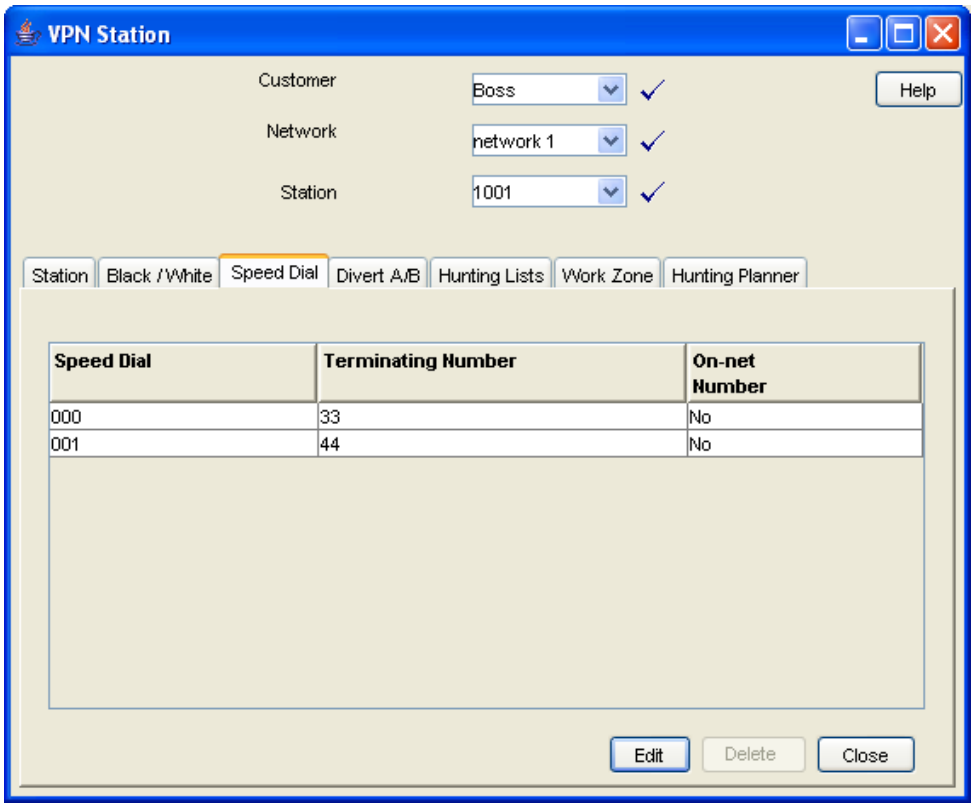
The **Speed Dial** tab of the VPN Station screen displays the list of speed dial numbers for the station.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 2 or above; level 1 will be able to view, but not edit this tab.

Speed Dial tab

Here is an example **Speed Dial** tab for a VPN station.



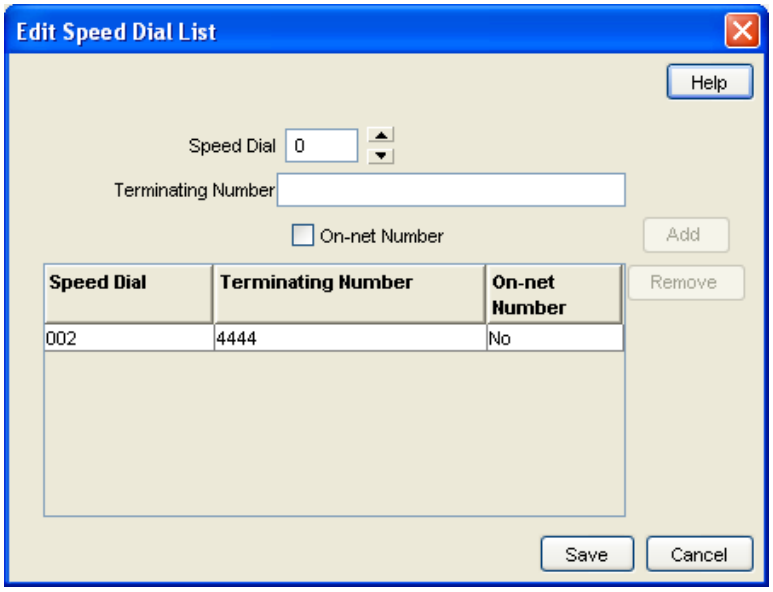
Editing the speed dial number list

Follow these steps to edit the speed dial number list for a VPN station.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Speed Dial** tab on the VPN Station screen.
3	Click **Edit**. **Result:** You see the *Edit Speed Dial List screen* (See example on page 86).
4	To: • Add a number, complete the fields, as described in *Field descriptions* (on page 86) and click **Add**. **Result:** The number is added to the table. • Remove a number, select the speed dial record from the table and click **Remove**.
5	Repeat step 4, as required.
6	Click **Save**.

Edit Speed Dial List screen

Here is an example Edit Speed Dial List screen.



Field descriptions

This table describes each field in the Edit Speed Dial List screen.

Field	Description
Speed Dial	Station speed dial numbers are between 0 and 999. **Tip:** In the example management control plans, collect digit to sub-tag nodes, it is assumed that network speed dials are in the range 0 - 99 and station speed dials are in the range 100 - 199. The screens do not enforce these limits, but if one of these control plans is used unmodified, then the screen's users should use these ranges.
Terminating Number	The terminating number (0-9,*,#) for the speed dial. This number may be up to 32 digits in length and is required.
On-net Number	Used to indicate whether the Terminating Number for the speed dial is an On-net Number or not. If the box is clear, the system assumes that the terminating number is an off-net number and prefixes it with an off-net prefix.

Deleting a station speed dial

Follow these steps to delete a speed dial from the list.

Note: You can also delete a speed dial using the *Edit Speed Dial List screen* (on page 85).

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **Speed Dial** tab.
3	Select the speed dial from the table and click **Delete**.

Step	Action
	Result: You see the Delete confirmation screen.
4	Click **Yes** to confirm.
	Result: The speed dial is removed from the system.

Divert A/B

Introduction

The **Divert A/B** tab of the VPN Station screen lists the allowed or barred numbers, to which a VPN Station can be diverted.

The Divert Allowed/Barred list is checked when any diversion numbers are entered, to ensure that they are not barred by the list. This may result in an error when a diversion number (that is, Alternate Routing Number or Scheduled Location number) that is barred by the Divert Allowed/Barred list is being saved.

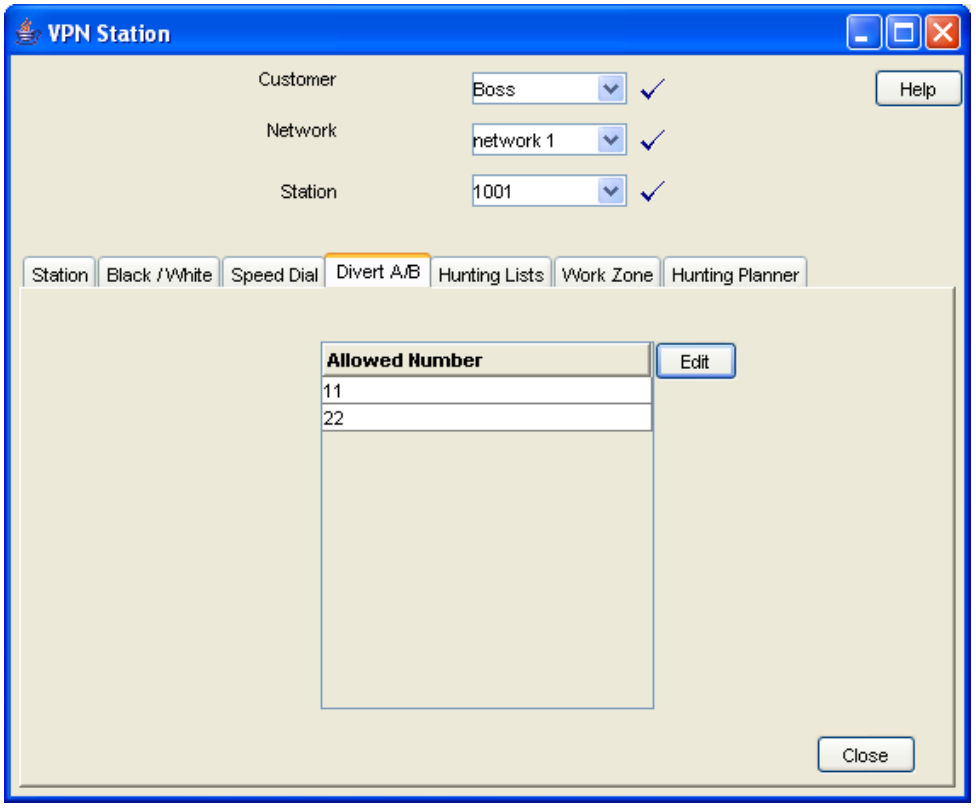
The Divert Allowed/Barred list may contain numbers that are barred or not allowed by either the Station or Network Black/White lists.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 3 or above; levels below this will be able to view, but not edit this tab.

Divert A/B tab

Here is an example **Divert A/B** tab in the VPN Station screen.



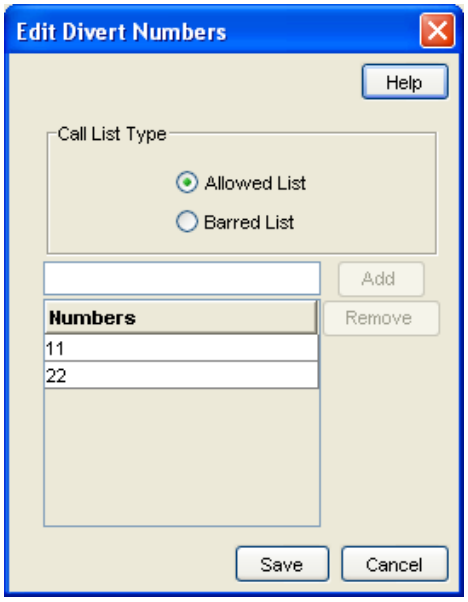
Editing the divert number list

Follow these steps to edit the divert number list for a VPN station.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Divert A/B** tab on the VPN Station screen.
3	Click **Edit**. **Result:** You see the *Edit Divert Numbers screen* (See example on page 89).
4	Select the appropriate Call List Type (**Allowed List** or **Barred List**) option. **Note:** You can maintain only one type of Call List. You cannot have an allowed list and a barred list. If you change type, the list is cleared.
5	To: • Add a number, type the number or the number prefix for the diversion that is to be specifically allowed or barred for a station and click **Add**. **Result:** The number is added to the table. • Remove a number, select the number from the table and click **Remove**.
6	Repeat steps 4 and 5, as required.
7	Click **Save**.

Edit Divert Numbers screen

Here is an example Edit Divert Numbers screen.



Hunting Lists

Introduction

The **Hunting Lists** tab of the VPN Station screen displays the hunting list entries for each hunting list that is set for the station. A hunting list consists of one or more hunting list entries. Each entry in a hunting list consists on a rank value, a terminating number, a short code number and a timeout value in seconds.

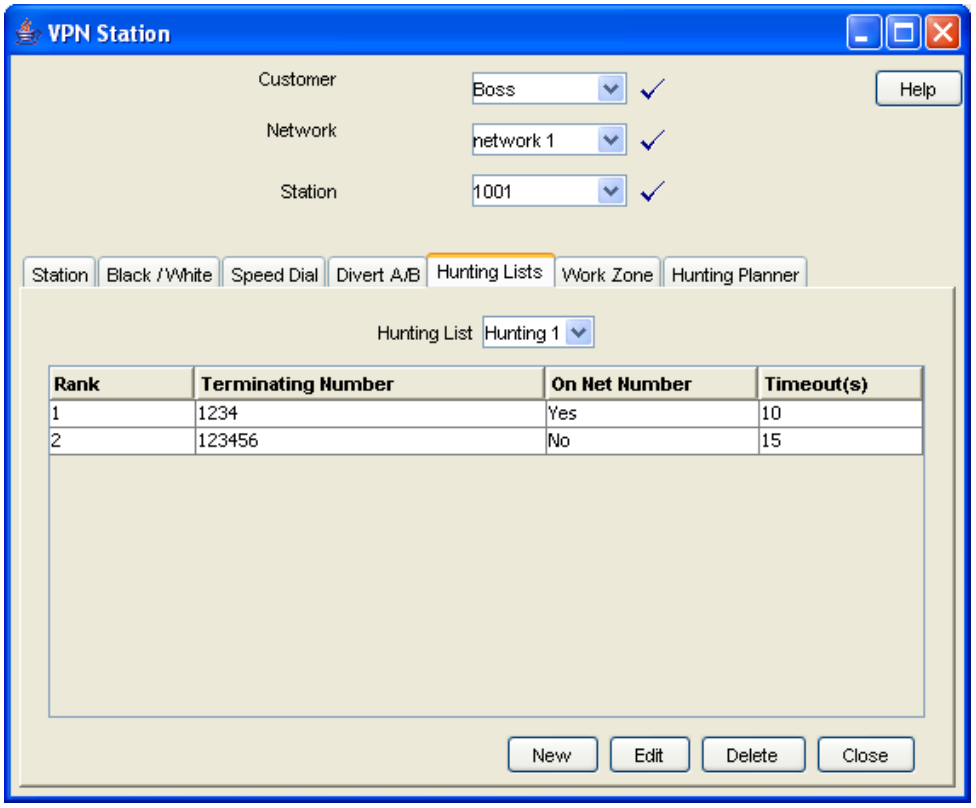
Hunting lists are used by hunting plans to establish what termination numbers will be attempted when hunting is taking place.

Privileges

This tab is available for editing if you are using VPN stand-alone and have a privilege level of 2 or above; level 1 will be able to view, but not edit this tab.

Hunting Lists tab

Here is an example **Hunting Lists** tab on the VPN Station screen.



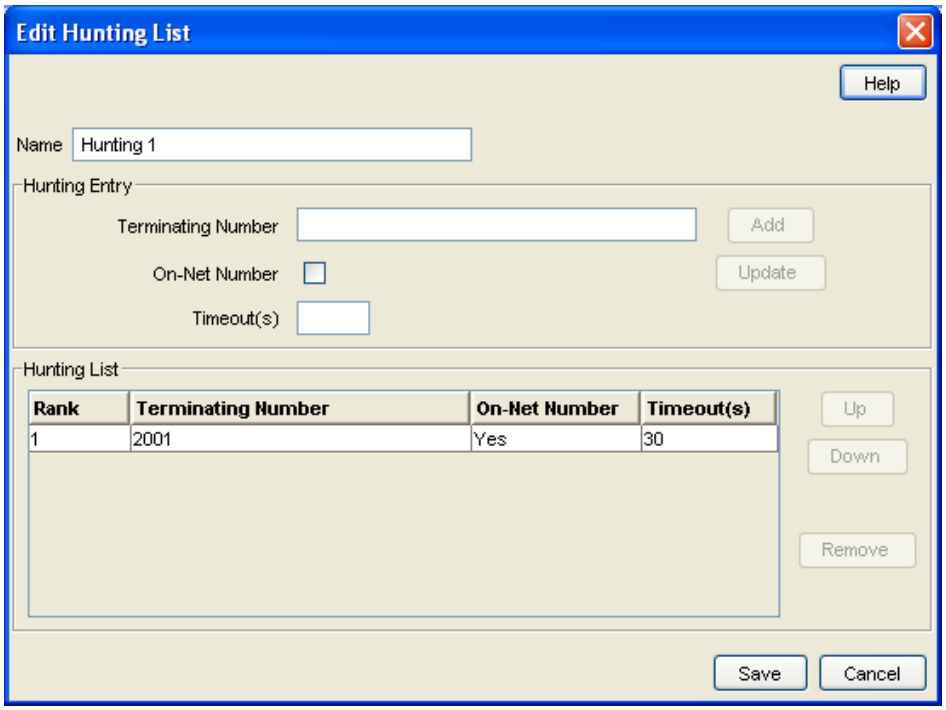
Field descriptions

This table describes each field in the New Hunting List screen and the Edit Hunting List screen.

Field	Description
Name	The name of the Hunting List.
Terminating Number	The Terminating Number for the next entry to be added to the new Hunting List.
On-Net Number	Used to indicate that the Termination Number is the on-net number of a VPN station.
Timeout(s)	Specifies the waiting time (in seconds) before next number in the list is attempted during hunting.
Hunting List	Displays the Rank, Terminating Number, Short Code Number and a Timeout for every entry in the Hunting List.

Hunting List screen

Here is an example Hunting List screen.



Adding a hunting list

Follow these steps to add a hunting list.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Hunting Lists** tab.
3	Click **New**. **Result:** You see the New *Hunting List screen* (See example on page 91).
4	Complete the fields, as described in *Field descriptions* (on page 90).
5	Click **Add**.
6	Repeat steps 4 and 5, as required.
7	Click **Save**.

Changing hunting list details

Follow these steps to change an existing hunting list for a station.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Hunting Lists** tab.
3	Click **Edit**.

Step	Action
	Result: You see the Edit *Hunting List screen* (See example on page 91).
4	Edit the name of the list, if required.
5	To modify an existing list entry, highlight it in the Hunting List table. **Result:** The values are displayed in the fields in the Hunting Entry area. Change its values as required, and click **Update**. Refer to *Field descriptions* (on page 90)
6	To add a new entry, in the Hunting Entry area, enter its values and click **Add**.
7	In the Hunting List area, to: • Change the rank of an entry in the list, click on a record in the table and use the **Up** and **Down** buttons. • Remove an entry, click on the record in the table and click **Remove**.
8	Click **Save**.

Deleting a hunting list

Follow these steps to delete a hunting list for a VPN station.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
1	Select the **Hunting Lists** tab.
3	Select a hunting list from the **Hunting List** drop-down box and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes** to confirm **Result:** The hunting list will be removed from the table.

Hunting Planner

Introduction

The **Hunting Plans** tab of the VPN Station screen displays the scheduled hunting information set for the station. It lists the different Hunting Plans set up for the station showing the Location, CLI and the time ranges for every Hunting Plan and its associated Hunting List.

A Hunting Plan allows a user to set their station to specify a Hunting List to use at set periods of time.

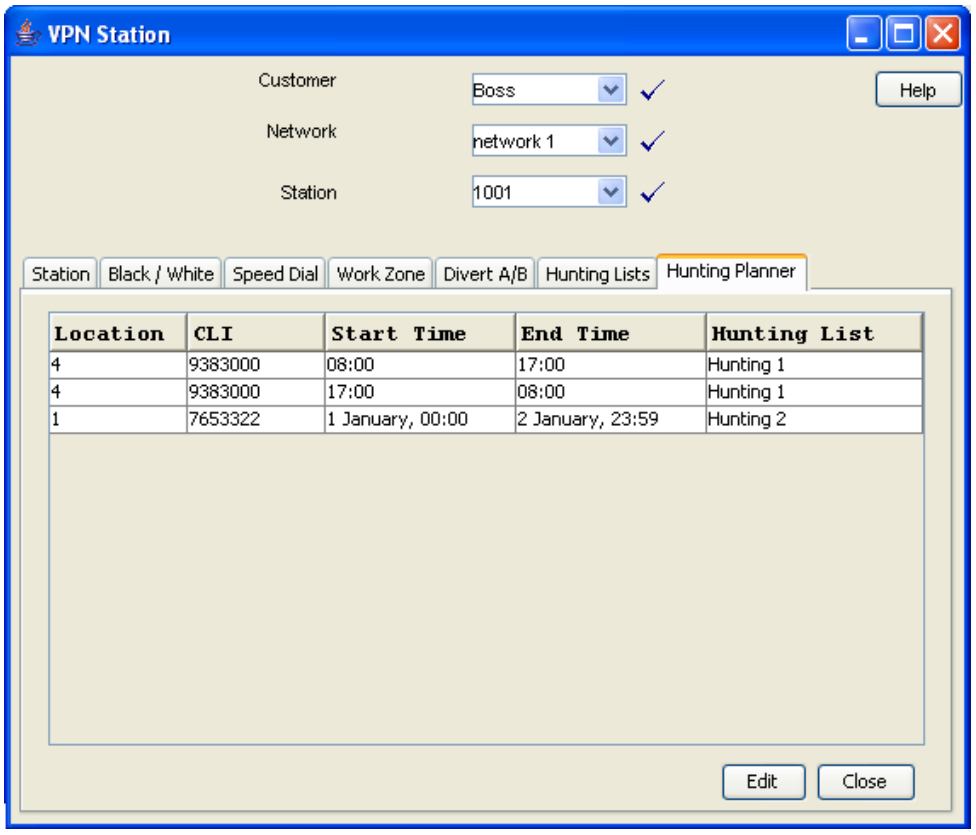
Example: A user may set a Hunting Plan that, from 5:00 pm on Friday to 8:00 am Monday, attempts to terminate all calls from a specific CLI and Location to the numbers in the Hunting List ‘Weekend’.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 2 or above; level 1 will be able to view, but not edit this tab.

Hunting Planner tab

Here is an example **Hunting Planner** tab.



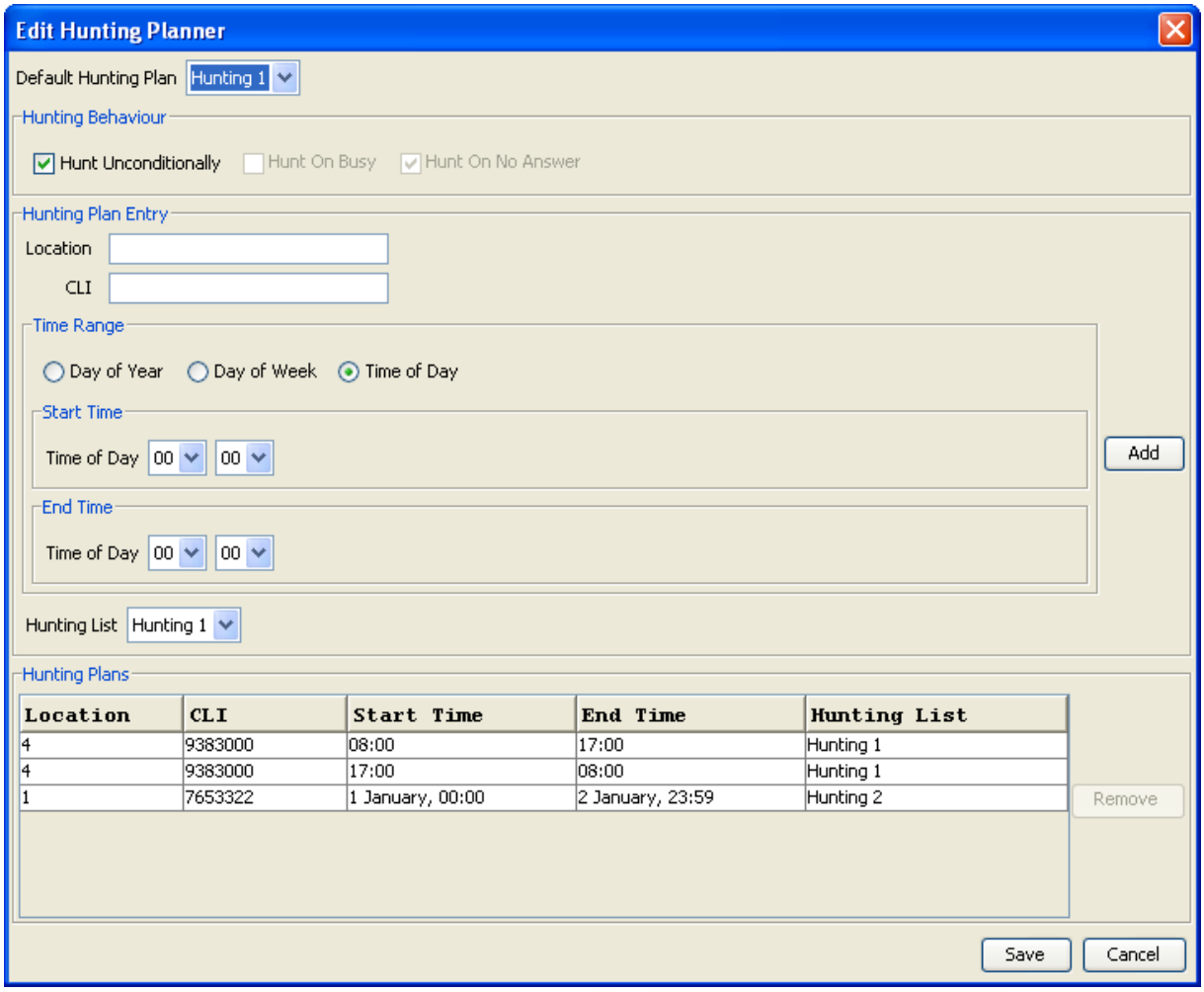
Editing hunting planner

Follow these steps to edit the hunting plans on the hunting planner for a VPN station.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Hunting Planner** tab.
3	Click **Edit**. **Result:** You see the *Edit Hunting Planner screen* (See example on page 94).
4	To: • Add a hunting plan to the planner, complete the fields, as described in *Field descriptions* (on page 94) and click **Add**. • Modify an existing plan: 1. Select the plan from the table. **Result:** The details of the plan will appear in the fields. 2. Change the details in the fields and click **Add**. **Result:** A new plan will appear in the table. The original plan will still appear in the table. You will need to remove it. • Remove a plan, select it from the table and click **Remove**.
5	Click **Save**.

Edit Hunting Planner screen

Here is an example Edit Hunting Planner screen



Field descriptions

This table describes each field in the Edit Hunting Planner screen.

Field	Description
Default Hunting Plan	Allows you to specify which Hunting List is used when hunting is enabled but no Hunting Plan is matched in terms of Location, CLI and time.
Hunt Unconditionally	Allows you to configure the station to perform hunting every time a call is received.
Hunt On Busy	Allows you to configure the station to perform hunting every time a call is received and the station is engaged.
Hunt On No Answer	Allows you to configure the station to perform hunting every time a call is received and the station is not answered after a timeout period.
Location	Allows you to specify a matching pattern for the calling party location.

Field	Description
	For example: A combination of Mobile Country Code, Mobile Network Code, Location Code and Cell ID can be used. A subset of the values can be also be specified, but the omission must start from the Cell ID, then the Location Code and so on. **Format:** *MccMncLacCellid* where: • Mcc: A 3-digit country code • Mnc: A 2 or 3-digit network code (starting with 0) • Lac: A 5-digit Location code with decimal value (starting with 0), and • Cellid: A 5-digit Cell ID with decimal value (starting with 0).
CLI	The CLI number for the Hunting Plan Entry being added or selected.
Time Range	These three option buttons allow you to select between the Time Range types for the Hunting Plan Entry being added or selected.
Start Time	Use the drop down lists to specify the Start Time for the Hunting Plan Entry. The label for the fields will be the selected Time Range option and the fields will be for: • Day of Year: Day of Month and Time of Day • Day of Week: Day of Week and Time of Day • Time of Day: Time of Day
End Time	Use the drop down lists to specify the End Time for the Hunting Plan Entry. The label for the fields will be the selected Time Range option and the fields will be as described in Start Time.
Hunting List	This list sets the Hunting Plan for the current Hunting Plan Entry.
Hunting Plans	The table lists all the Hunting Plans set for the station. The displayed fields for every plan are Location, CLI, start and end times of a Hunting Plan and the associated Hunting List.

Work Zone

Introduction

The **Work Zone** tab of the VPN Station screen allows you to manage the list of shapes used to define the station work zone.

Notes:

- The work zone functionality is only available if LCP is installed. For more information, see *Location Capabilities Pack Technical Guide*.

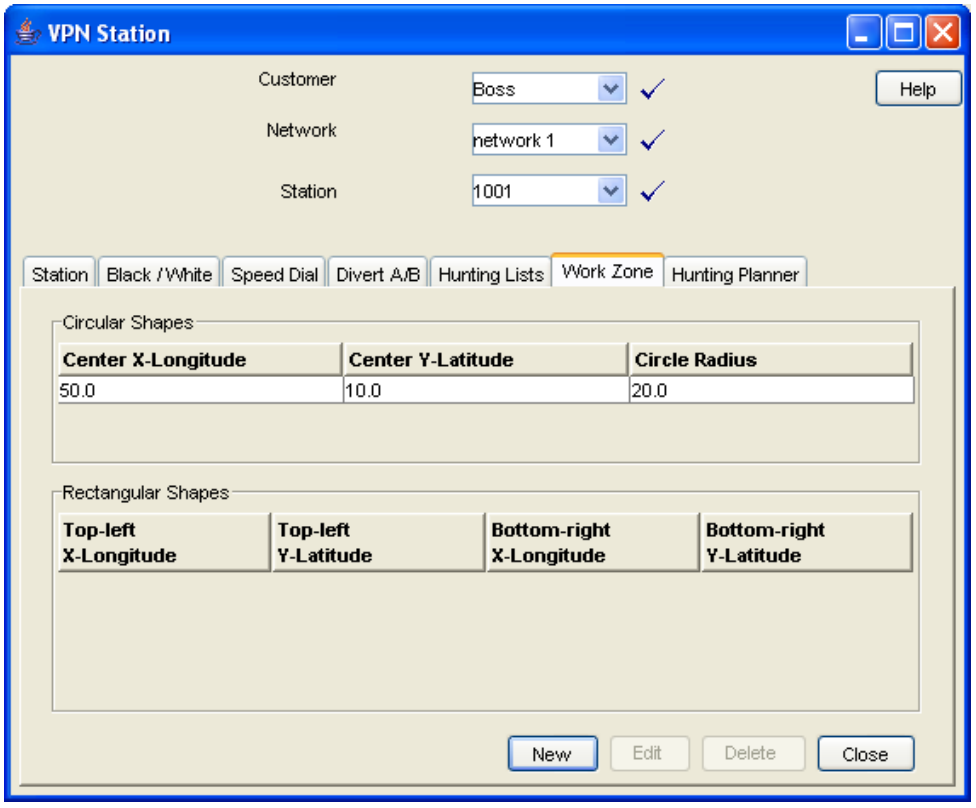
- ACS also needs to have profile fields of the zone type configured in the ACS Configuration screen. For more information about setting up profile fields, see *ACS User's Guide*.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 3 or above; levels below this will be able to view, but not edit this tab. It can be accessed both from the VPN standalone system and from the VPN service available through the SMS screens.

Work Zone tab

Here is an example **Work Zone** tab for VPN stations.



Field descriptions

This table describes each field in the New Work Zone Shape screen.

Field	Description
Circular Shape option	Select to define the attributes for a circular shape.
X (Deg)	Defines the x coordinate for the centre point of the circular shape. It is expressed in degrees longitude, in the range: -179.99999 to +179.99999.
Y (Deg)	Defines the y coordinate for the centre point of the circular shape. It is expressed in degrees latitude, in the range: -89.99999 to +89.99999.
R (Kms)	Defines the radius of the circular shape.
Rectangular Shape option	Select to define the attributes for a rectangular shape.

Field	Description
Top-left corner X (Deg)	Defines the x coordinate for the top left corner of the rectangular shape. It is expressed in degrees longitude, in the range: -179.99999 to +179.99999.
Top-left corner Y (Deg)	Defines the y coordinate for the top left corner of the rectangular shape. It is expressed in degrees latitude, in the range: -89.99999 to +89.99999.
Bottom-right corner X (Deg)	Defines the x coordinate for the the bottom left corner of the rectangular shape. It is expressed in degrees longitude, in the range: -179.99999 to +179.99999.
Bottom-right corner Y (Deg)	Defines the y coordinate for the bottom left corner of the rectangular shape. It is expressed in degrees latitude, in the range: -89.99999 to +89.99999.

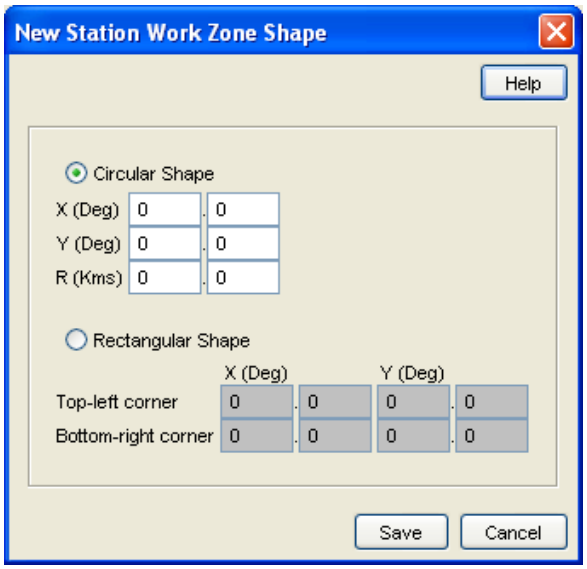
Adding a shape to a station work zone

Follow these steps to add a new shape to the station work zone.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Work Zone** tab.
3	Click **New**. **Result:** You see the *New Station Work Zone Shape screen* (See example on page 97).
4	Click the option for the type of shape you want to add (either circular or rectangular).
5	Enter the shape attributes in the appropriate fields, as described in *Field descriptions* (on page 68).
6	Click **Save**.

New Station Work Zone Shape screen

Here is an example New Station Work Zone Shape screen.



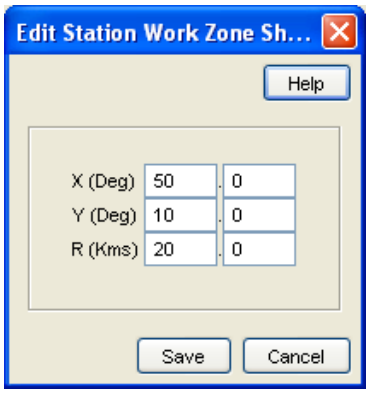
Changing a station work zone shape

Follow these steps to change the details for a VPN station work zone shape.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Work Zone** tab.
3	Select the shape (circular or rectangular) in the *appropriate table* (See example on page 96).
4	Click **Edit**. **Result:** You see *Edit Station Work Zone Shape screen* (See example on page 98).
5	Modify the shape details as required. For details see *Field descriptions* (on page 68).
6	Click **Save**.

Edit Station Work Zone Shape screen

Here is an example Edit Station Work Zone Shape screen.



Deleting a station work zone shape

Follow these steps to delete a VPN station work zone shape.

Step	Action
1	Select the customer, network, and station from the drop down lists on the VPN Station screen.
2	Select the **Work Zone** tab.
3	Select the shape to delete (circular or rectangular) in the *appropriate table* (See example on page 96) and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes**. **Result:** The shape is removed from the work zone.

Chapter 9

Defining Closed User groups

Overview

Introduction

This chapter explains how to define Closed User Groups (CUG).

Defining CUGs process

When defining a CUG, you must follow the procedures listed below, in the given order:

1 *Adding a CUG* (on page 103) to the network.
2 *Editing the CUG network list* (on page 105) (the networks from which the CUG stations may be selected).
3 *Editing the CUG station list* (on page 107).

Note: You must set up the networks and stations you want to include in the CUG before you begin defining the CUG.

In this chapter

This chapter contains the following topics.

Closed User Groups

Introduction

The **CUG** tab on the VPN Network screen allows you to define the Closed User Group (CUG) for the network. To define a CUG, you select the stations to include, and specify the restrictions on the incoming and outgoing calls to and from the stations included in the group.

CUGs are defined at the network level. The CUG type is one of the following:

- Restricted, where only calls between the stations included in the CUG are allowed
- Un-restricted, where calls between any stations, including stations not in the CUG, are allowed

Calls

Calls to and from stations in the CUG are controlled in the following ways:

- Incoming calls are controlled through use of the CUG PIN.
- Outgoing calls are controlled by the CUG type.

CUG stations

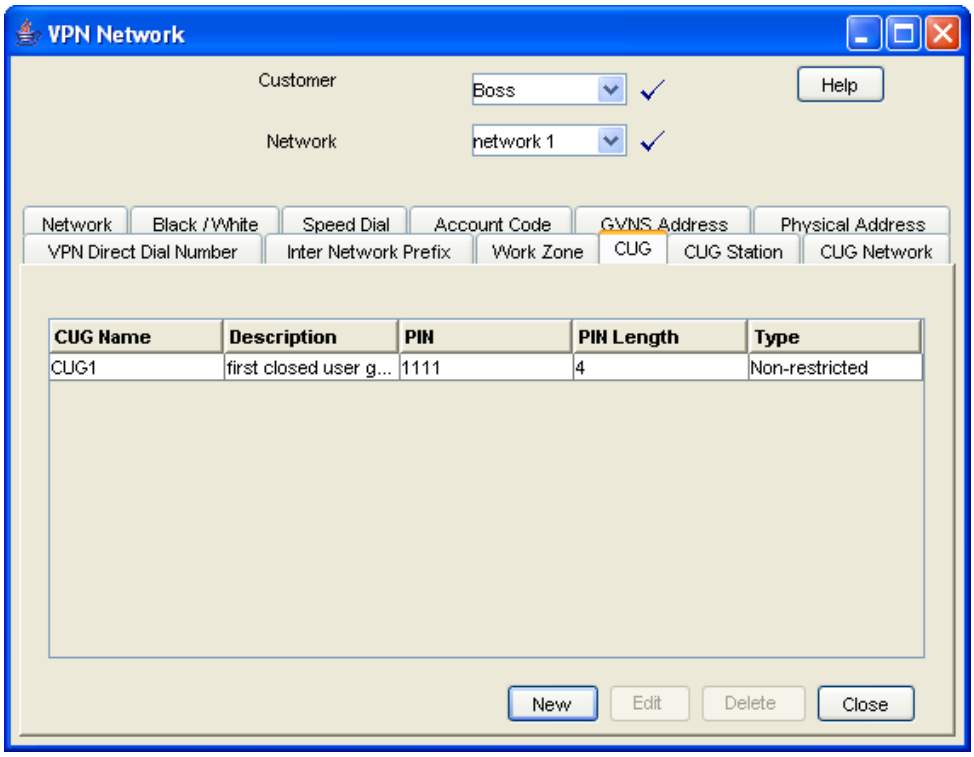
Stations can be in more than one CUG. If a station is in more than one CUG, one of which is an un-restricted group, then the station will be able to make un-restricted calls.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 5 or above; level 4 may edit or delete, but not add; levels below this will be able to view, but not edit this tab.

CUG tab

Here is an example **CUG** tab.



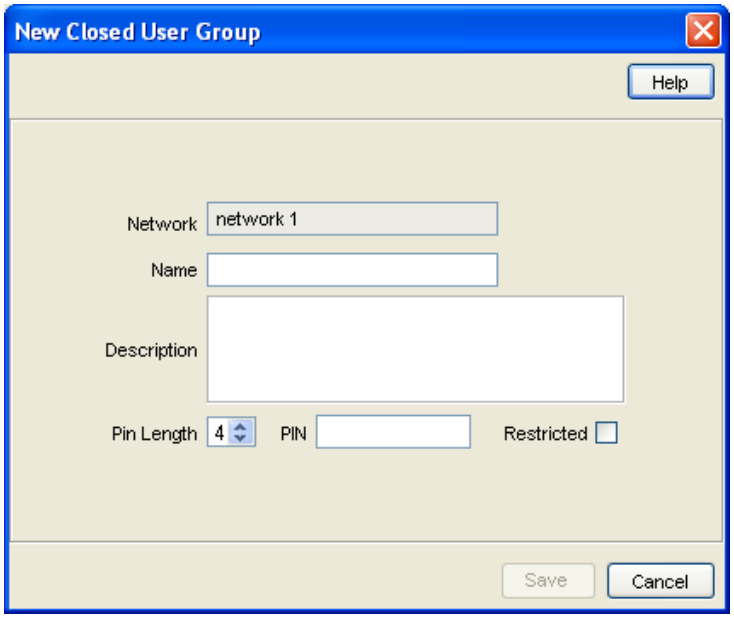
Field descriptions

This table describes each field in the New Closed User Group and Edit Closed User Group screens.

Field	Description
Name	The name of the closed user group.
Description	Text describing the closed user group.
Pin Length	Defines the length of the PIN that is used to control access to stations in the CUG. The default PIN length is four; use the up and down arrows to specify a different length if required. **Note:** The minimum PIN length is one.
PIN	The PIN that is used to control access to stations in the CUG. This is a required field.
Restricted	Select this check box to set the CUG type to restricted. **Note:** Stations in: • A restricted CUG can only call other stations in the same CUG. • An unrestricted CUG can call any other station.

Closed User Group screen

Here is an example Closed User Group screen.



Adding a CUG

Follow these steps to add a Closed User Group for a network.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **CUG** tab.
3	Click **New**. **Result:** You see the New *Closed User Group screen* (See example on page 103).
4	Fill in the fields as described in *Field descriptions* (on page 102).
5	Click **Save**.

Changing a CUG

Follow these steps to change the details of a CUG.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **CUG** tab.
3	Select the CUG in the table and click **Edit**. **Result**: You see the Edit *Closed User Group screen* (See example on page 103).
4	Change the details, as described in *Field descriptions* (on page 102),

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen. as required.
5	Click **Save**.

Deleting a CUG

Follow these steps to delete a CUG.

Note: Before you can delete a CUG, you must first delete any stations defined for the CUG, and then delete any networks defined for the CUG.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **CUG** tab.
3	Select the CUG to delete in the table, and click **Delete**. **Result:** You see the Delete confirmation screen.
4	Click **Yes** to confirm. **Result:** The Closed User Group is removed from the system.

CUG Networks

Introduction

The **CUG Network** tab on the VPN Network screen allows you to specify the networks from which you want to select the stations to include in a CUG.

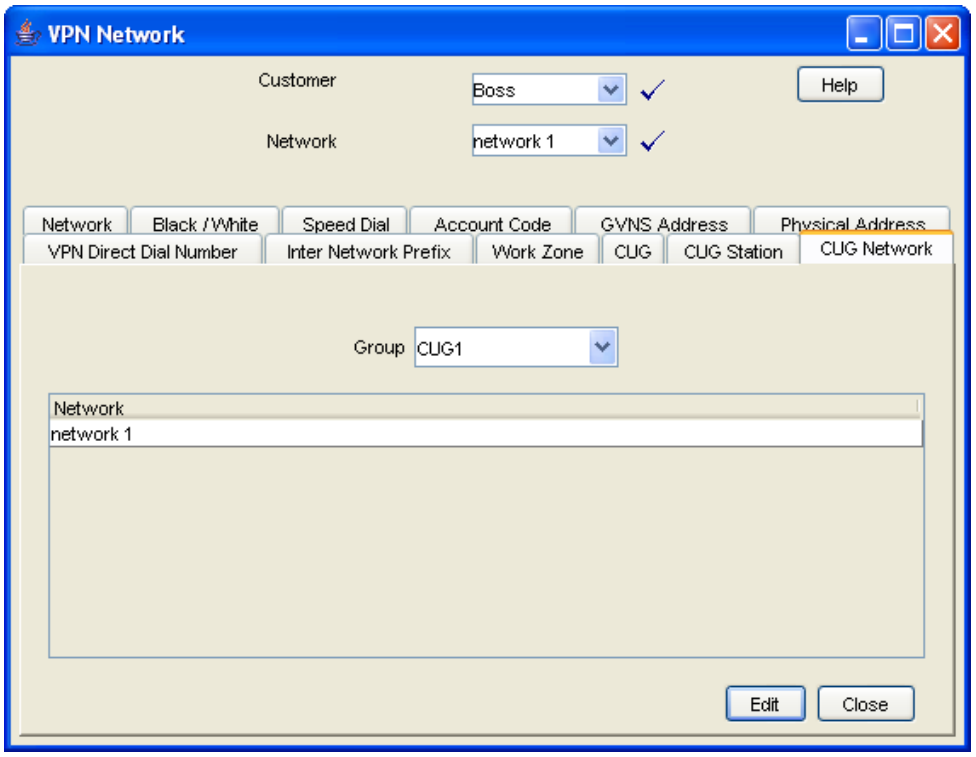
Note: You can include stations from more than one network in the same CUG.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 5 or above; levels below this will be able to view, but not edit this tab.

CUG Network tab

Here is an example **CUG Network** tab.



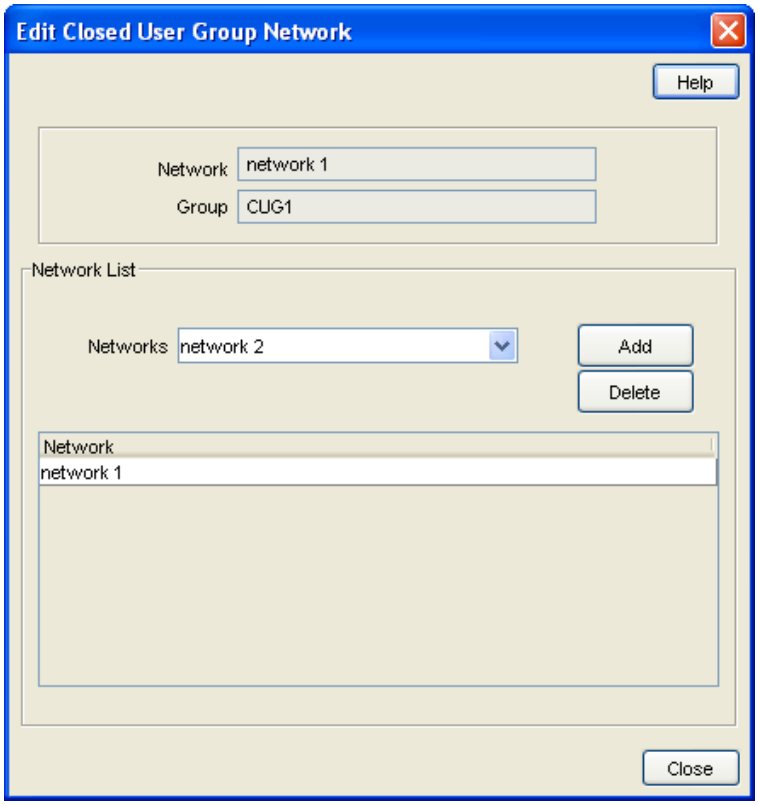
Editing the CUG network list

Follow these steps to edit the list of networks in a closed user group.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **CUG Network** tab.
3	Select the CUG from the **Group** drop down list and click **Edit**. **Result:** You see the *Edit Closed User Group Network screen* (See example on page 106).
4	To: • Add a network to the CUG, select the network from the **Networks** field drop down list and click **Add**. **Result:** The network is added to the table. • Remove a network, select the record from the table and click **Delete**. **Note:** Before you can delete a network from a CUG, you must first delete all the CUG stations for the CUG network.
5	Repeat step 4 as required.
6	Click **Close**.

Edit Closed User Group Network screen

Here is an example Edit Closed User Group Network screen.



Field descriptions

This table describes each field in the Edit Closed User Group Network screen.

Field	Description
Network	The name of the network in which the closed user group is defined. This field is for reference only.
Group	The name of the closed user group. This field is for reference only.
Networks	Choose networks from which to select the stations you want to include in the CUG.
Network table	Displays the networks included in the CUG.

CUG Stations

Introduction

The **CUG Station** tab allows you to specify which stations to include in a closed user group.

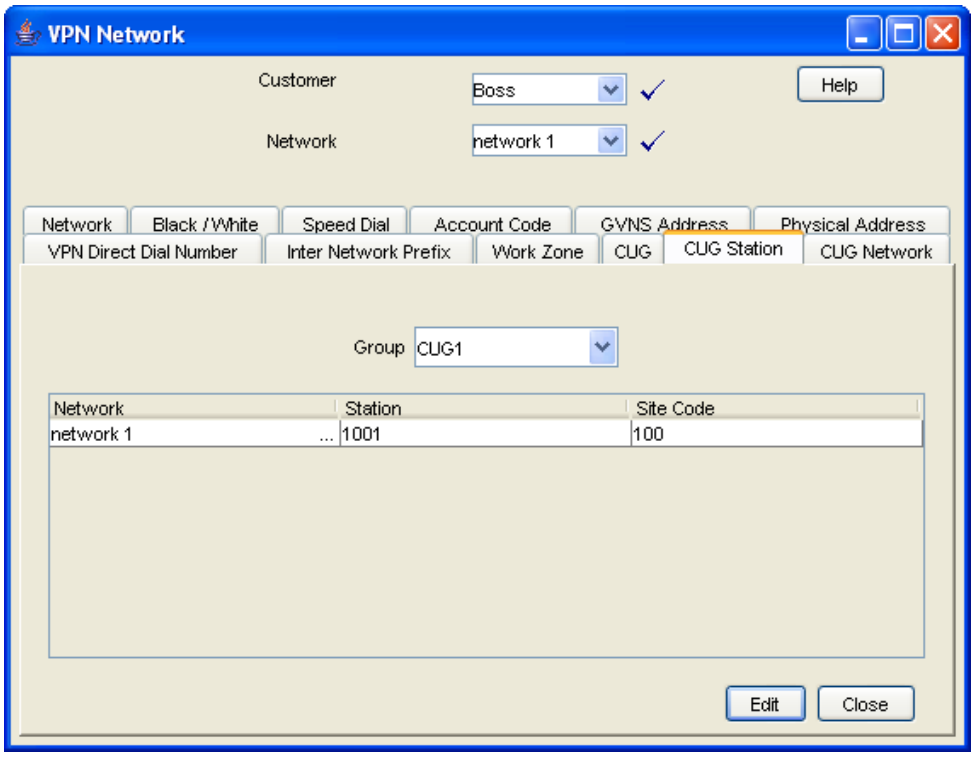
Note: Before you add a station to a CUG, check that the network the station belongs to has already been added to the CUG.

Privileges

This tab is available for editing if you are using VPN standalone and have a privilege level of 4 or above; levels below this will be able to view, but not edit this tab.

CUG Station tab

Here is an example **CUG Station** tab.



Editing the CUG station list

Follow these steps to edit the list of stations in a closed user group.

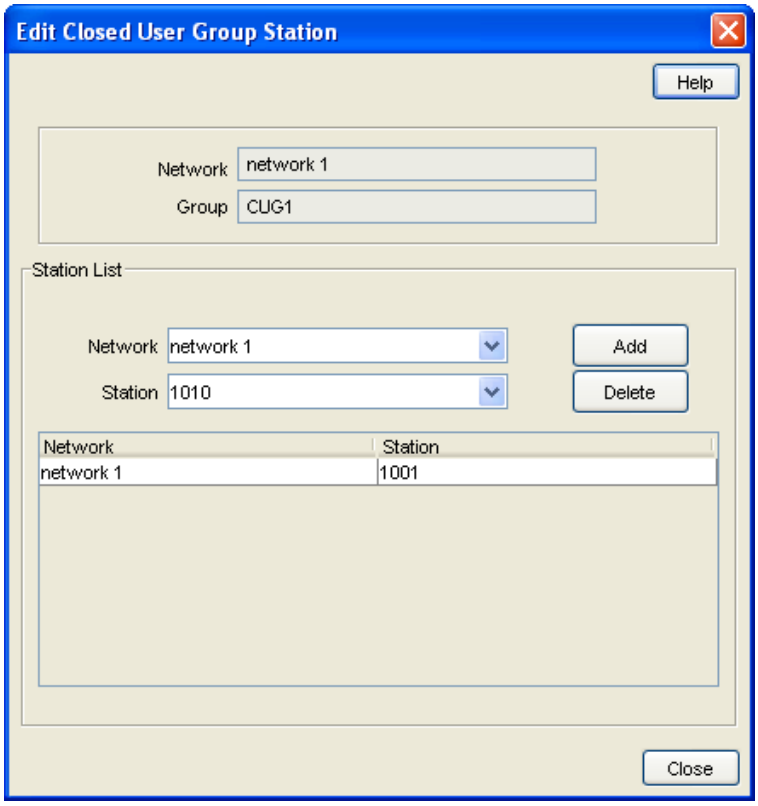
Note: You can add stations from more than one network to the same CUG.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
2	Select the **CUG Station** tab.
3	Select the CUG from the **Group** drop down list and click **Edit**. **Result:** You see the *Edit Closed User Group Station screen* (See example on page 108).
4	In the **Station List** area, select the **Network**. **Result:** The list of available stations for that network appear in the **Station** drop down list and any stations already in the GUG appear in the table.

Step	Action
1	Select the customer and network from the drop down lists on the VPN Network screen.
5	To: • Add a station, select the Station from the **Station** field drop down list and click **Add**. **Result:** The network and station are added to the table. • Remove a station, select the record from the table and click **Delete**.
6	Repeat steps 4 and 5 as required for each network in the CUG.
7	Click **Close**.

Edit Closed User Group Station screen

Here is an example Edit Closed User Group Station screen.



Field descriptions

This table describes each field in the Edit Closed User Group Station screen.

Field	Description
Network	The name of the network where the CUG is defined. This field is for reference only.
Group	The name of the selected CUG. This field is for reference only.
Network	Lists the networks included in the CUG. Select the network you want from the list.

Field	Description
Station	Lists the stations in the selected network. Select the station you want from the list.
Station List table	Displays the network stations currently included in the CUG.

Glossary of Terms

ACS

Advanced Control Services configuration platform.

AIN

Advanced Intelligent Network

ANI

Automatic Number Identification - Term used in the USA by long-distance carriers for CLI.

CC

Country Code. Prefix identifying the country for a numeric international address.

CLI

Calling Line Identification - the telephone number of the caller. Also referred to as ANI.

CPE

Control Plan Editor (previously Call Plan Editor) - software used to define the logic and data associated with a call -for example, "if the subscriber calls 0800 *nnnnnn* from a phone at location *xxx* then put the call through to *bb bbb bbbb*".

DTMF

Dual Tone Multi-Frequency - system used by touch tone telephones where one high and one low frequency, or tone, is assigned to each touch tone button on the phone.

GUI

Graphical User Interface

GVNS

Global Virtual Numbering Scheme - When multiple VPNs are in use by a customer, the capability to route calls between these VPNs requires a numbering scheme that uses destination addresses based on a customer id and extension number. These GVNS addresses can then be interpreted to provide inter VPN operation.

Hunting

A terminating call feature where a subscriber may request a list of alternate destination addresses. If their mobile station is not attached, or does not answer a call, then the service logic should attempt to reach the supplied alternate destinations in sequence.

IN

Intelligent Network

INAP

Intelligent Network Application Part - a protocol offering real time communication between IN elements.

IP

1) Internet Protocol

2) Intelligent Peripheral - This is a node in an Intelligent Network containing a Specialized Resource Function (SRF).

ISDN

Integrated Services Digital Network - set of protocols for connecting ISDN stations.

IVR

Interactive Voice Response - systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words or, more commonly, DTMF signalling.

LCP

Location Capabilities Pack - set of software components used by other applications to look up the location of mobile devices.

MSISDN

Mobile Station ISDN number. Uniquely defines the mobile station as an ISDN terminal. It consists of three parts; the country code (CC), the national destination code (NDC) and the subscriber number (SN).

PIN

Personal Identification Number

PSTN

Public Switched Telephone Network - a general term referring to the variety of telephone networks and services.

SCI

Send Charging Information. An INAP operation sent from ACS to the SSP to control real time charging by the SSP.

SCP

Service Control Point. Also known as SLC.

SLC

Service Logic Controller (formerly UAS).

SMS

Depending on context, can be:

- Service Management System hardware platform
- Short Message Service
- Service Management System platform
- NCC Service Management System application

SN

Service Number

SRF

Specialized Resource Function – This is a node on an IN which can connect to both the SSP and the SLC and delivers additional special resources into the call, mostly related to voice data, for example play voice announcements or collect DTMF tones from the user. Can be present on an SSP or an Intelligent Peripheral (IP).

SSP

Service Switching Point

System Administrator

The person(s) responsible for the overall set-up and maintenance of the IN.

Telco

Telecommunications Provider. This is the company that provides the telephone service to customers.

Telecommunications Provider

See Telco.

Termination Number

The final number that a call terminates to. Can be set in control plan nodes such as Attempt Termination and Unconditional Termination for re-routing numbers such as Toll Free or Follow Me numbers.

VDDI

Virtual Direct Dial In

VPN

The Virtual Private Network product is an enhanced services capability enabling private network facilities across a public telephony network.

Index

F

G

H

I

K

L

M

N

O

P