Oracle® Communications Convergent Charging Controller

Virtual Private Network Help

Release 15.0.0
F83551-01
October 2023

Oracle Communications Convergent Charging Controller Virtual Private Network Help, Release 15.0.0

F83551-01

Contents

1 Initial Configuration

Accessing the VPN Configuration Module 1-1
- Configuration screen tabs 1-1

Announcements 1-1
- Configuring announcements 1-1
- Field descriptions - Edit Announcements 1-2

Languages 1-3
- Adding a language 1-3

2 Customers and Users

Adding customers 2-1

Accessing the Customer Module 2-1
- Customer screen tabs 2-1

Customer 2-1
- Field descriptions - Customer 2-2
- Adding a VPN customer 2-2
- Changing VPN customer details 2-2
- Deleting a customer 2-3

Contacts 2-3
- Field descriptions - Contacts 2-3
- Adding a customer contact 2-4
- Changing customer contact details 2-4
- Deleting a customer contact 2-5

User 2-5
- Field descriptions - User 2-5
- Edit User screen-only field 2-6
- Adding a user 2-6
- Changing user details 2-7
- Deleting a user 2-7

3 Adding the Network

Networks 3-1
- Adding a network 3-1
- Field descriptions - New VPN Network 3-2
  - Network Details 3-2
  - Default Account Code Policy 3-4
  - Default Least Cost Routing Prefixes 3-4
  - Call Plans 3-5
  - Default PIN Profile Allowed 3-5
  - Failure Behaviour 3-6
  - Changing network details 3-6
- Deleting a network 3-7

GVNS Address Ranges 3-7
- Field descriptions - GVNS Address Ranges 3-7
- Adding a range 3-8
- Changing range details 3-8
- Deleting a range 3-9

Physical Address Ranges 3-9
- Field descriptions - Physical Address Ranges 3-9
- Adding a range 3-9
- Changing range details 3-10
- Deleting ranges 3-10

VPN Direct Dial Number Ranges 3-11
- Field descriptions - VPN Direct Dial Number Ranges 3-11
- Adding a range 3-11
- Changing range details 3-12
- Deleting ranges 3-12

4 Configuring the Network

Account Codes 4-1
- Editing the account code list 4-1
- Deleting an account code 4-2

Black and White Network Number Lists 4-2
- Rules - Black and White Network Number Lists 4-3
- Field descriptions - Black and White Network Number Lists 4-3
- Editing outgoing numbers 4-4
- Editing incoming numbers 4-5

Speed Dial 4-5
- Editing the speed dial number list 4-5
- Field descriptions - Edit Speed Dial List screen 4-6

Deleting a speed network dial 4-6
Inter Network Prefix 4-7
Field descriptions - Inter Network Prefix 4-7
Adding an Inter Network Prefix 4-7
Changing an Inter Network Prefix 4-8
Deleting an Inter Network Prefix 4-8
Work Zone 4-8
Field descriptions - Work Zone 4-9
Adding a shape to a network work zone 4-9
Changing a network work zone shape 4-10
Deleting a network work zone shape 4-10

5 Station

Accessing the Station Module 5-1
Station screen tabs 5-1
Selecting a customer 5-2
Finding a network 5-2
Finding a station 5-2
Stations 5-2
Adding off-net hunt/forward numbers 5-2
Field descriptions - Stations 5-3
Station Details 5-3
Hunt/Forward Settings 5-5
Account Code Policy 5-5
Incoming Call Barring 5-6
Set PIN 5-6
Allowed PIN Profiles 5-6
Adding a station 5-7
Changing station details 5-7
Deleting a station 5-8
Black/White lists for Stations 5-8
Field descriptions - Black/White lists for Stations 5-9
Editing incoming numbers 5-9
Editing outgoing numbers 5-10
Speed Dial 5-10
Editing the speed dial number list 5-11
Field descriptions - Edit Speed Dial List screen 5-11
Deleting a station speed dial 5-11
Divert A/B 5-12
Editing the divert number list 5-12

Hunting Lists 5-13
Field descriptions - Hunting Lists 5-13
Adding a hunting list 5-13
Changing hunting list details 5-14
Deleting a hunting list 5-14
Hunting Planner 5-14
Editing hunting planner 5-15
Field descriptions - Edit Hunting Planner screen 5-15
Work Zone 5-16
Field descriptions - Work Zone 5-17
Adding a shape to a station work zone 5-17
Changing a station work zone shape 5-18
Deleting a station work zone shape 5-18

6 Defining Closed User groups

Closed User Groups 6-1
Field descriptions - Closed User Groups 6-2
Adding a CUG 6-2
Changing a CUG 6-2
Deleting a CUG 6-3
CUG Networks 6-3
Editing the CUG network list 6-3
Field descriptions - Edit Closed User Group Network 6-4
CUG Stations 6-4
Editing the CUG station list 6-4
Field descriptions - Edit Closed User Group Station screen 6-5

7 Feature Nodes

Available Feature Nodes 7-1
Profile Blocks and Fields 7-2
Primary tags 7-3
Nodes using profile blocks 7-3
Profile block availability 7-3
Profile block list 7-3
ACS primary tags 7-5
VPN primary tags 7-6
Zones 7-8
VPN Analyze 7-8
VPN Network Site Code 7-8

Mapped Network Prefix 7-8
Optional Prefixes 7-8
Termination Number 7-9
Availability 7-9
Node exits - VPN Analyze 7-9
Configuring the node - VPN Analyze 7-9
VPN Originating CUG 7-10
Availability 7-10
Node exits - VPN Originating CUG 7-10
Configuring the node 7-11
VPN Load Station 7-11
Availability 7-12
Node exits - VPN Load Station 7-12
Configuring the node - VPN Load Station 7-12
VPN Lookup 7-13
Availability 7-13
Node exits - VPN Lookup 7-13
Configuring the node 7-13
VPN CLI Lookup 7-13
Availability 7-14
Node exits - VPN CLI Lookup 7-14
Configuring the node - VPN CLI Lookup 7-14
VPN Mobile Analyze 7-14
Network Site Code 7-15
Mapped Network prefix 7-15
Stripping off number prefixes 7-15
Global Special Numbers 7-15
Availability 7-15
Node exits - VPN Mobile Analyze 7-15
Configuring the node - VPN Mobile Analyze 7-16
VPN Caller is On-Net 7-16
Availability 7-16
Node exits - VPN Caller is On-Net 7-16
Configuring the node 7-17
VPN Get Hunting Number 7-17
Availability 7-17
Node exits - VPN Get Hunting Number 7-17
Configuring the node - VPN Get Hunting Number 7-17
VPN Redirection Counter Branching 7-17
Availability 7-17
Node exits - VPN Redirection Counter Branching 7-18

Configuring the node - VPN Redirection Counter Branching 7-18
VPN Set Redirection Counter 7-18
Availability 7-18
Node exits - VPN Set Redirection Counter 7-18
Configuring the node - VPN Set Redirection Counter 7-19
VPN Set Tariff Code From Profile 7-19
Availability 7-19
Node exits - VPN Set Tariff Code From Profile 7-19
Configuring the node - VPN Set Tariff Code From Profile 7-19
VPN Subscriber Lookup 7-19
Node exits - VPN Subscriber Lookup 7-20
Configuring the node - VPN Subscriber Lookup 7-20
VPN Voice Mail Number Configuration 7-20
Availability 7-21
Node exits - VPN Voice Mail Number Configuration 7-21
Configuring the node - VPN Voice Mail Number Configuration 7-21
VPN Terminating CUG 7-21
Availability 7-21
Node exits - VPN Terminating CUG 7-21
Configuring the node - VPN Terminating CUG 7-22

1

Initial Configuration

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

This chapter contains the following topics.

Accessing the VPN Configuration Module

Announcements

Languages

Accessing the VPN Configuration Module

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.

Configuration screen tabs

The VPN Configuration screen contains the following tabs:

- Announcements
- Languages

Announcements

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.

Configuring announcements

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

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.

3. Fill in the fields, as described in Field descriptions - Edit Announcements.
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.

Related topic

Announcements

Field descriptions - Edit Announcements

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.
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.

Field	Description
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

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.

Adding a language

Follow these steps to add a new language.

1. Select the **Languages** tab on the VPN Configuration screen.
2. Click **New**.

   Result: You see the New Language screen.
3. Enter the name of the language.

   Note: This must be unique.
4. Click **Save**.

Related topic

Languages

2

Customers and Users

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

This chapter contains the following topics.

Adding customers

Accessing the Customer Module

Customer

Contacts

User

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

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

Customer screen tabs

The VPN Customer screen contains the following tabs:

- Customer
- Contacts
- User

Customer

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.

Field descriptions - Customer

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.

Adding a VPN customer

Follow these steps to add a new VPN customer.

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.
4. Fill in the fields, as described in the Field descriptions - Customer.
5. Click **Save**.

Related topic

Customer

Changing VPN customer details

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

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.
4. Change the details, as required. Refer to Field descriptions - Customer.
5. Click **Save**.

   Result: The customer entry will be updated.

Related topic

Customer

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.

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.

Related topic

Customer

Contacts

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.

Field descriptions - Contacts

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.

Field	Description
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.

Adding a customer contact

Follow these steps to add a new customer contact.

1. Select the customer from the drop down list on the VPN Customer screen.
2. Select the **Contacts** tab.
3. Click **New**.
4. **Result:** You see the New Customer Contacts screen.
5. Fill in the fields, as described in the Field descriptions - Contacts.
6. Click **Save**.

Related topic

Contacts

Changing customer contact details

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

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.

4. Change the details, as required. Refer to Field descriptions - Contacts.

5. Click **Save**.

   Result: The customer contact entry will be updated.

Related topic

Contacts

Deleting a customer contact

Follow these steps to delete a customer contact.

1. Select the customer from the drop down list on the VPN Customer screen.
2. Select the **Customer** tab.
3. 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.

Related topic

Contacts

User

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.

Field descriptions - User

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.

Field	Description
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.

Adding a user

Follow these steps to add a new user.

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.
4. Fill in the fields, as described in the Field descriptions - User.
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.

Related topic

User

Changing user details

Follow these steps to change the details of a user.

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.
4. Change the details, as required. Refer to Field descriptions - User.
5. Click **Save**.

   Result: The user entry will be updated.

Related topic

User

Deleting a user

Follow these steps to delete a user.

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.

Related topic

User

3
Adding the Network

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

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 for the customer
2. Adding a range
3. Adding a range
4. Adding a range

To begin using VPN, the network must be configured. When configuring a new network, follow the procedures in the chapter Configuring the Network.

This chapter contains the following topics.

Networks

GVNS Address Ranges

Physical Address Ranges

VPN Direct Dial Number Ranges

Networks

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.

Adding a network

Follow these steps to add a new network.

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.
4. Fill in the fields, as described in the Field descriptions - New VPN Network.
5. Click **Save**.

Related topic

Networks

Field descriptions - New VPN Network

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.

Field	Description
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.
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.

Field	Description
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.
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.

Field	Description
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 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.

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.
4. Change the details as required. Refer to Field descriptions - New VPN Network.
5. Click **Save**.

   Result: The network entry is updated.

Related topic

Networks

Deleting a network

Follow these steps to delete a network.

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

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

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.

Field descriptions - GVNS Address Ranges

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).

Field	Description
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).

Adding a range

Follow these steps to add a GVNS address range.

1. 1 Select the customer and network from the drop down lists on the VPN Network screen.
2. 2 Select the **GVNS Address** tab.
3. 3 Click **New**.

   Result: You see the New GVNS Address Range screen.
4. 4 Enter the numbers of the GVNS address range for the:
   - Start
   - End
5. **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.
6. 5 Click **Save**.

Related topic

GVNS Address Ranges

Changing range details

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

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.
4. Change the details, described in Field descriptions - GVNS Address Ranges, as required.
5. Click **Save**.

   Result: The entry will be updated.

Related topic

GVNS Address Ranges

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.

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.

   Result: The range is removed from the system.

Related topic

GVNS Address Ranges

Physical Address Ranges

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.

Field descriptions - Physical Address Ranges

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).

Adding a range

Follow these steps to add a physical address range.

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.
4. Enter the numbers of the range for the:

- Start
- End

5. **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.

6. Click **Save**.

Related topic

Physical Address Ranges

Changing range details

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

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 **Edit**.

   Result: You see the Edit Physical Address Range screen.

4. Change the details, as described in Field descriptions - Physical Address Ranges, as required.
5. Click **Save**.

   Result: The entry will be updated.

Related topic

Physical Address Ranges

Deleting ranges

Follow these steps to delete a range.

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

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.

Related topic

Physical Address Ranges

VPN Direct Dial Number Ranges

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.

Field descriptions - VPN Direct Dial Number Ranges

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).

Adding a range

Follow these steps to add a VDDI number range.

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.
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**.

Related topic

VPN Direct Dial Number Ranges

Changing range details

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

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.
4. Change the details, as described in Field descriptions - VPN Direct Dial Number Ranges, as required.
5. Click **Save**.

   Result: The entry will be updated.

Related topic

VPN Direct Dial Number Ranges

Deleting ranges

Follow these steps to delete a range.

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

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.
4. Click **Yes** to confirm.

   Result: The range is removed from the system.

Related topic

VPN Direct Dial Number Ranges

4

Configuring the Network

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

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 if required.
2. Enter Black and White Network Number Lists.
3. Enter network Speed Dial.
4. Set up Stations for network, including Black/White lists for Stations and Divert A/B.
5. Customize the station, including Speed Dial and Hunting Lists.
6. Define any closed user groups, if required. See Defining Closed User groups.

This chapter contains the following topics.

Account Codes

Black and White Network Number Lists

Speed Dial

Inter Network Prefix

Work Zone

Account Codes

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 in the VPN Network screen
- Account Code Policy 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.

Editing the account code list

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

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.

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) ((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.

1. Click **Save**.

Related topic

Account Codes

Deleting an account code

Follow these steps to delete an account code.

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.

Related topic

Account Codes

Black and White Network Number Lists

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 - Black and White Network Number Lists.

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 Network Number Lists

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

Field descriptions - Black and White Network Number Lists

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.

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, click **Edit**.

   Result: You see the Edit Outward Calls screen.
5. Select the appropriate Call List Type (**Allowed List** or **Barred List**) option.

   See Field descriptions - Black and White Network Number Lists 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 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**.

Related topic

Black and White Network Number Lists

Editing incoming numbers

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

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, click **Edit**.

   Result: You see the Edit Inward Calls screen.
5. Select the appropriate Call List Type (**Allowed** or **Barred**) option.

   See Field descriptions - Black and White Network Number Lists 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**.
7. Repeat steps 3 to 6, as required.
8. Click **Save**.

Related topic

Black and White Network Number Lists

Speed Dial

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.

Editing the speed dial number list

Follow these steps to edit the speed dial number list.

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.
4. To:
   - Add a number, complete the fields, as described in Field descriptions - Edit Speed Dial List screen 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**.

Related topic

Speed Dial

Field descriptions - Edit Speed Dial List screen

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 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.

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**.

   Result: You see the Delete confirmation screen.

4. Click **Yes** to confirm.

   Result: The speed dial is removed from the system.

Related topic

Speed Dial

Inter Network Prefix

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.

Field descriptions - Inter Network Prefix

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 the Network screen.

Adding an Inter Network Prefix

Follow these steps to add an Inter Network Prefix.

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.

4. Select the **Network** from the drop down list.
5. Enter the **Prefix**.
6. Click **Save**.

Related topic

Inter Network Prefix

Changing an Inter Network Prefix

Follow these steps to change an Inter Network Prefix.

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.
4. Change the details, as described in Field descriptions - Inter Network Prefix, as required.
5. Click **Save**.

   Result: The entry is updated.

Related topic

Inter Network Prefix

Deleting an Inter Network Prefix

Follow these steps to delete an Inter Network Prefix.

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.

Related topic

Inter Network Prefix

Work Zone

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.

Field descriptions - Work Zone

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.
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.

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**.
4. **Result:** You see the New Network Work Zone screen.
5. Select the option for the type of shape you want to add (either circular or rectangular).
6. Enter the shape attributes in the appropriate fields, as described in Field descriptions - Work Zone.
7. Click **Save**.

Related topic

Work Zone

Changing a network work zone shape

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

1. Select the customer and network from the drop down lists on the VPN Network screen.
2. Select the **Work Zone** tab.
3. Select the shape (circular or rectangular) in the appropriate table.
4. Click **Edit**.

   Result: You see Edit Network Work Zone Shape screen.
5. Modify the shape details, as described in Field descriptions - Work Zone, as required.
6. Click **Save**.

Related topic

Work Zone

Deleting a network work zone shape

Follow these steps to delete a network work zone shape.

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 and click **Delete**.

   Result: You see the Delete confirmation screen.
4. Click **Yes**.

   Result: The shape is removed from the work zone.

Related topic

Work Zone

5
Station

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

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

1. Adding a station for the customer.
2. Add Black/White lists for Stations to the station.
3. Editing the speed dial number list.
4. Editing the divert number list.
5. Adding a hunting list
6. Editing hunting planner

This chapter contains the following topics.

Accessing the Station Module

Stations

Black/White lists for Stations

Speed Dial

Divert A/B

Hunting Lists

Hunting Planner

Work Zone

Accessing the Station Module

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

Station screen tabs

The VPN Station screen contains the following tabs:

- Stations
- Black/White lists for Stations
- Speed Dial
- Divert A/B
- Hunting Lists
- Work Zone
- Hunting Planner

Selecting a customer

Follow these steps to select a customer.

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.

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.

1. Select a station from the **Station** drop down list.
2. Press **Enter**.

   Result: Related stations will appear in the grid.

Stations

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.

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.
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.
8. Add the Follow-me or Alternative Routing number and leave the related **On-net Number** box clear.
9. **Save** the station.

Field descriptions - Stations

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. The list of available ranges is available to all users on the GVNS Address tab 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.

Field	Description
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 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 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.
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.

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.

Field	Description
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.
Speed Code Management allowed	Selecting this box will allow the user to manage their speed code dial list using the Dial In Station Manager.

Field	Description
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.

Adding a station

Follow these steps to add a new station.

1. Select the customer, network, and station from the drop down lists on the VPN Station screen.
2. Select the **Station** tab.
3. Click **New**.

   Result: You see the New VPN Station screen.
4. Fill in the fields, as described in the Field descriptions - Stations.
5. Click **Save**.

Related topic

Stations

Changing station details

Follow these steps to change the details of a station.

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.
4. Change the details, as required. Refer to Field descriptions - Stations.

5. Click **Save**.

Related topic

Stations

Deleting a station

Follow these steps to delete a station.

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.

Related topic

Stations

Black/White lists for Stations

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 - Black and White Network Number Lists.

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.

Field descriptions - Black/White lists for Stations

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 incoming numbers

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

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, click **Edit**.

   Result: You see the Edit Inward Calls screen.

5. Select the appropriate Call List Type (**Allowed List** or **Barred List**) option.

   See Field descriptions - Black/White lists for Stations 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**.
7. Repeat steps 3 to 6, as required.
8. Click **Save**.

Related topic

Black/White lists for Stations

Editing outgoing numbers

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

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, click **Edit**.

   Result: You see the Edit Outward Calls screen.
5. Select the appropriate Call List Type (**Allowed List** or **Barred List**) option.

   See Field descriptions - Black/White lists for Stations 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**.
7. Repeat steps 2 to 6, as required.
8. Click **Save**.

Related topic

Black/White lists for Stations

Speed Dial

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.

Editing the speed dial number list

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

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.
4. To:
   - Add a number, complete the fields, as described in Field descriptions - Edit Speed Dial List screen 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**.

Related topic

Speed Dial

Field descriptions - Edit Speed Dial List screen

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.

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**.

   Result: You see the Delete confirmation screen.
4. Click **Yes** to confirm.

   Result: The speed dial is removed from the system.

Related topic

Speed Dial

Divert A/B

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.

Editing the divert number list

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

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.
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**.

Related topic

Divert A/B

Hunting Lists

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.

Field descriptions - Hunting Lists

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.

Adding a hunting list

Follow these steps to add a hunting list.

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.
4. Complete the fields, as described in Field descriptions - Hunting Lists.
5. Click **Add**.
6. Repeat steps 4 and 5, as required.
7. Click **Save**.

Related topic

Hunting Lists

Changing hunting list details

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

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**.

   Result: You see the Edit Hunting List screen.
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 - Hunting Lists.
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**.

Related topic

Hunting Lists

Deleting a hunting list

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

1. Select the customer, network, and station from the drop down lists on the VPN Station screen.
2. 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.

Related topic

Hunting Lists

Hunting Planner

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.

Editing hunting planner

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

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.
4. To:
   - Add a hunting plan to the planner, complete the fields, as described in Field descriptions - Edit Hunting Planner screen and click **Add**.
   - Modify an existing plan:

   a. Select the plan from the table.

      Result: The details of the plan will appear in the fields.

   b. 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**.

Related topic

Hunting Planner

Field descriptions - Edit Hunting Planner screen

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.

Field	Description
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. **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

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.

Field descriptions - Work Zone

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.
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.

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.

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 - Work Zone.
6. Click **Save**.

Related topic

Work Zone

Changing a station work zone shape

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

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.
4. Click **Edit**.

   Result: You see Edit Station Work Zone Shape screen.
5. Modify the shape details as required. For details see Field descriptions - Work Zone.
6. Click **Save**.

Related topic

Work Zone

Deleting a station work zone shape

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

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 and click **Delete**.

   Result: You see the Delete confirmation screen.
4. Click **Yes**.

   Result: The shape is removed from the work zone.

6

Defining Closed User groups

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

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

1. Adding a CUG to the network.
2. Editing the CUG network list (the networks from which the CUG stations may be selected).
3. Editing the CUG station list.

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

This chapter contains the following topics.

Closed User Groups

CUG Networks

CUG Stations

Closed User Groups

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.

Field descriptions - Closed User Groups

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.

Adding a CUG

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

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.
4. Fill in the fields as described in Field descriptions - Closed User Groups.
5. Click **Save**.

Related topic

Closed User Groups

Changing a CUG

Follow these steps to change the details of a CUG.

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.

4. Change the details, as described in Field descriptions - Closed User Groups, as required.
5. Click **Save**.

Related topic

Closed User Groups

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.

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.

Related topic

Closed User Groups

CUG Networks

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.

Editing the CUG network list

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

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.
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**.

5. **Note:** Before you can delete a network from a CUG, you must first delete all the CUG stations for the CUG network.
6. Repeat step 4 as required.
7. Click **Close**.

Related topic

CUG Networks

Field descriptions - Edit Closed User Group Network

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

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.

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.

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.
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.
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**.

Related topic

CUG Stations

Field descriptions - Edit Closed User Group Station screen

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.
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.

7

Feature Nodes

This chapter describes the VPN feature nodes.

You can configure these nodes through the ACS Control Plan Editor management screens, available through the ACS service control plans.

This chapter contains the following topics.

Available Feature Nodes

Profile Blocks and Fields

VPN Analyze

VPN Originating CUG

VPN Load Station

VPN Lookup

VPN CLI Lookup

VPN Mobile Analyze

VPN Caller is On-Net

VPN Get Hunting Number

VPN Redirection Counter Branching

VPN Set Redirection Counter

VPN Set Tariff Code From Profile

VPN Subscriber Lookup

VPN Voice Mail Number Configuration

VPN Terminating CUG

Available Feature Nodes

This topic lists all the feature nodes that are available to VPN within the Control Plan Editor. In some cases, additional nodes may have been created and installed to fit a specific customer need. These custom feature nodes do not appear in this list.

Node name	Node description	Reference
VPN Analyze	Used to break down the digits contained in the Pending TN Buffer.	VPN Analyze
VPN Load Station	Used to load an alternate calling station profile.	VPN Load Station

Node name	Node description	Reference
VPN Lookup	Used to translate an OnNet number to the corresponding Network address from VPN_STATION in the database.	VPN Lookup
VPN CLI Lookup	Used to set the Originating Network ID for the current service interaction.	VPN CLI Lookup
VPN Mobile Analyze	Used to break down the digits contained in the Pending Termination Number Buffer.	VPN Mobile Analyze
VPN Caller is On-Net	Used to check if the incoming caller is on-net.	VPN Caller is On-Net
VPN Get Hunting Number	Used to search a list of termination numbers and timeout pairs.	VPN Get Hunting Number
VPN Redirection Counter Branching	Allows comparison of the Redirection Information Counter received in the invoking message.	VPN Redirection Counter Branching
VPN Set Redirection Counter	Allows an integer constant to be set as the redirection information counter.	VPN Set Redirection Counter
VPN Set Tariff Code From Profile	Used to add network charging data to the next outgoing TCAP primitive.	VPN Set Tariff Code From Profile
VPN Subscriber Lookup	Allows you to look up a number buffer and load the VPN network and station profiles associated with that number.	VPN Subscriber Lookup
VPN Voice Mail Number Configuration	Allows modification of the Pending Termination Number to provide compatibility with voicemail systems.	VPN Voice Mail Number Configuration
VPN Originating CUG	Analyses the calling and called numbers contained in the Calling Private Network or Logical Calling Buffer, and the PendingTN Buffer, respectively.	VPN Originating CUG
VPN Terminating CUG	Analyses the calling and called numbers contained in the Calling Private Network or Logical Calling Buffer, and the PendingTN Buffer respectively.	VPN Terminating CUG

Profile Blocks and Fields

A profile block is a piece of binary data which is usually stored in the database. Profile blocks are usually stored in the database in a "long raw" column type. For example, the profile block containing data relevant to an ACS customer is held in the PROFILE field of the ACS_CUSTOMER table.

Profile blocks store data used during call processing.

Primary tags

Profile blocks contain a series of different pieces of data called primary tags. Each tag is indexed by a hex tag. Some feature nodes enable you to specify which tag to use. For example, the Profile Branch feature node enables you to compare the value of a specific primary tag with a specified value, and branch on the result.

Profiles are generally maintained by editing the relevant screens in the application, for example, Edit Customer Details. They can also store data from the session or call context, or be updated by a feature node (for example, Store Profile).

Nodes using profile blocks

The following VPN nodes use the profile blocks listed below:

- VPN Analyze
- VPN Mobile Analyze
- VPN Set Tariff Code From Profile

Profile block availability

The service loader you are using determines the profile blocks that are available to the control plan and whether they are read-only or can be updated. All service loaders include the Global Profile.

For example, you can read the VPN Network Profile, VPN Station Profile and Customer Profile if the VPN service loader is used.

The VPN service loader specifies the Station Profile as updateable and the Network Profile as read-only. This means that any nodes that can write back to a profile can update the VPN Station Profile in the database.

The service loader also specifies the uses of Application Specific profiles 1-8. Some of these will be specified as temporary profiles, which are never written back to the database and are cleared at the end of the call. They can be used for such things as moving data from one application to another within the control plan (for example between a USSD node and a DAP node).

Profile block list

Here are the profile blocks.

Name	Description
VPN Network Profile	Contains most of the information you can specify in the VPN edit network, for example: • Account code maximum length • Outgoing barred/allowed list type • Incoming barred/allowed list type • VPN network SD no check • VPN present private address **Note:** Only relevant if you have the VPN service installed.

Name	Description
VPN Station Profile	Contains most of the information you can specify in the VPN edit station, for example: • Outgoing barred/allowed list type • Incoming barred/allowed list type • VPN bar all incoming • VPN bar off network incoming **Note:** Only relevant if you have the VPN service installed.
Customer Profile	Contains customer information, for example: • Incoming barred/allowed list type • Incoming barred/allowed list • PIN rights • Default language • Incoming barred/allowed ignore • Termination number ranges • Termination number range policy
Control Plan Profile	This profile contains current switch node exits only.
Global Profile	Contains global information, for example: • PIN rights • Multi-lingual announcements • Default language • Control plan version hiding
CLI Subscriber Profile	Contains most of the information you can specify in the **CLI** tab of the Numbers screen, for example: • Account Code • Language • Follow me number **Note:** Only relevant to the 0800 service.
Service Number Profile	Contains most of the information you can specify in the **Service Number** tab of the Numbers screen, for example: • Account code • Language • Follow me number **Note:** Only relevant to the 0800 service.
App Specific Profile 1 App Specific Profile 2 App Specific Profile 3 App Specific Profile 4 App Specific Profile 5 App Specific Profile 6 App Specific Profile 7 App Specific Profile 8	Contains information specific to an application (for example, Messaging Manager or CCS). **Note:** Unless it is in use by a specific application, these profiles, for example, App Specific Profile 7 can be specified as a temporary profile (where nothing is written back to the database) in order to pass information from one application to another, for example between USSD and DAP).
Any Valid Profile	Allows you to search for tags in all profiles that have been loaded.

ACS primary tags

Here is a list of ACS primary tags.

Description	Hex	Decimal
DO NOT USE	0x0000	0
PIN Prefix	0x0001	1
PIN Length	0x0002	2
Account Code Prefix	0x0003	3
Account Code Max Length	0x0004	4
A/S Prefix	0x0005	5
A/S Length	0x0006	6
Off Net Prefix	0x0007	7
S/D Prefix	0x0008	8
Outgoing Barred/Allowed List Type	0x0009	9
Outgoing Barred/Allowed List	0x000a	10
Incoming Barred/Allowed List Type	0x000b	11
Incoming Barred/Allowed List	0x000c	12
Account Code Values	0x000d	13
Account Code Policy	0x000e	14
-RESERVED-	0x000f	15
Divert RSF	0x0010	16
Divert Busy	0x0011	17
Divert No Answer	0x0012	18
Divert Follow Me	0x0013	19
Divert TOW Schedule	0x0014	20
PIN Digits	0x0015	21
PIN Rights	0x0016	22
Off Net Bar	0x0017	23
Follow on Break Out Sequence	0x0018	24
Station is Manager	0x0019	25
Speed List	0x001a	26
Divert Barred/Allowed List Type	0x001b	27
Divert Barred/Allowed List	0x001c	28
Divert Locations	0x001d	29
Break Limit	0x001e	30
LCR Old National	0x001f	31
LCR New National	0x0020	32
LCR Old International	0x0021	33
LCR New International	0x0022	34
Multi Lingual Announcements	0x0023	35
Number Lists	0x0024	36
Language	0x0025	37

Description	Hex	Decimal
Switch Configuration	0x0026	38
Virtual Message List	0x0027	39
Number Of Messages	0x0028	40
GUI Language	0x0029	41
Carrier Code	0x002a	42
Barred Categories	0x002b	43
Outgoing Barred/Allowed Ignore	0x002c	44
Incoming Barred/Allowed Ignore	0x002d	45
Divert Barred/Allowed Ignore	0x002e	46
Account Code Minimum Length	0x002f	47
Timezone Geographical Map	0x0030	48
PIN Encryption Method	0x0031	49
Silent Disconnect	0x0032	50
Postpaid Flag	0x0033	51
Hunt On Busy	0x0034	52
Hunt On No Answer	0x0035	53
Hunt Always	0x0036	54
Hunt RESERVED	0x0037	55
Help Line Address	0x0038	56
Legacy	0x0039	57
Disable	0x003a	58
VARS	0x003b	59
VARS Mapping	0x003c	60
Toll Free Beep ID	0x003d	61
Toll Free Beep Type	0x003e	62
Termination Number Ranges	0x003f	63
Termination Number Range Policy	0x0040	64
Control Plan Version Hiding	0x0041	65
Toll Free Beeps Required	0x0042	66
Bar Pay Phone Callers	0x0043	67
Bar Cell Phone Callers	0x0044	68

Note: Each service may have its own specific tags in a separate tag range.

VPN primary tags

Here is a list of the VPN primary tags, used in the VPN service.

Description	Hex	Decimal
Network SD No Check	0x30001	196609
Present Private Address	0x30002	196610
Bar All Incoming	0x30003	196611
Bar Off Network Incoming	0x30004	196612

Description	Hex	Decimal
PIN Prefix	0x30005	196613
Account Code Prefix	0x30006	196614
Alternate Station Prefix	0x30007	196615
Off Network Prefix	0x30008	196616
Speed Dial Prefix	0x30009	196617
PIN Length	0x3000a	196618
Account Code Length	0x3000b	196619
Station Length	0x3000c	196620
Off Network Call Barred	0x3000d	196621
Station Is Manager	0x3000e	196622
Restrict Calling Address	0x3000f	196623
Allow Short Extensions	0x30010	196624
Hunting List 1	0x30011	196625
Hunting List 2	0x30012	196626
Hunting List 3	0x30013	196627
Hunting List 4	0x30014	196628
Hunting List 5	0x30015	196629
Hunting List Default	0x30016	196630
Hunting To List 1	0x30017	196631
Hunting To List 2	0x30018	196632
Hunting To List 3	0x30019	196633
Hunting To List 4	0x3001a	196634
Hunting To List 5	0x3001b	196635
Hunting To List Default	0x3001c	196636
Send Identical CPN	0x3001d	196637
Match Undefined Extensions	0x3001e	196638
Hunting Configuration	0x30020	196640
Hunting Scheduling	0x30060	196704
SCI ID	0x30100	196864
SCI Data	0x30101	196865
Dialing Prefix Length	0x30200	197120
Calling On Network List	0x30310	197392
Calling On Network List Type	0x30311	197393
Calling Off Network List	0x30320	197408
Calling Off Network List Type	0x30321	197409
Calling PIN Always List	0x30330	197424
Calling PIN Always List Type	0x30331	197425
Calling PIN Never List	0x30340	197440
Calling PIN Never List Type	0x30341	197441
Called On Network LIST	0x30350	197456
Called On Network List Type	0x30351	197457
Called Off Network List	0x30360	197472
Called Off Network List Type	0x30361	197473
Called PIN Always List	0x30370	197488

Description	Hex	Decimal
Called PIN Always_List Type	0x30371	197489
Called PIN Never List	0x30380	197504
Called PIN Never List Type	0x30381	197505

Zones

VPN work zone functionality relies on profile fields of the zone type being set up in ACS. For more information about zone profile fields, see *ACS User's Guide* and *Location Capabilities Pack User's Guide*.

VPN Analyze

The VPN Analyze node allows you to break down the digits contained in the Pending TN Buffer. It parses the optional VPN prefix fields, placed into dedicated buffers, and the content and type of the actual termination number, placed in Pending TN Buffer. Depending on the outcome, it may replace the original content of the Pending TN Buffer.

VPN Analyze checks the following:

- VPN Network Site Code
- Mapped Network Prefix
- Optional Prefixes
- Termination Number

VPN Network Site Code

The first digits in the Pending TN Buffer are compared with the site codes for all defined VPNs. If a match is found, then the network id for the VPN of the matched site code is compared with the network id for the current VPN. If the ids are the same, then the Pending TN Type is set to 'Private' (called number is on-net). If they are different, then the Pending TN Type is set to 'Public' (called number is off-net).

Mapped Network Prefix

If no match is found for the VPN site code, then VPN Analyze tries to match the first digits of the Pending TN Buffer against all the mapped network prefixes of the owning VPN. If a match is found then the site code of the VPN of the matched network prefix is replaced in the Pending TN Buffer by the mapped network prefix. The network id of the VPN for the matched network prefix is compared with the network id for the current VPN. If the ids are the same, then the Pending TN Type is set to 'Private' (called number is on-net). If they are different, then the Pending TN Type is set to 'Public' (called number is off-net).

Optional Prefixes

The dialed digits can be prefixed with one or more of the following components. They can appear in any order.

Prefix	Description
PIN Number:	Indicated by the PIN Prefix. If present, this is placed in the PIN Buffer.
Account Code:	Indicated by the Account Code prefix. If present, this is placed in the Account Code Buffer.
Alternate Station ID:	Indicated by the Alternate Station prefix. If present, this is placed in the Calling OnNet Address Buffer.

Termination Number

Only one of the following must be present. This must be the last item in the digits string.

Termination Number	Description
Speed Dial:	Indicated by the Speed Dial prefix. There must be at least one and at most three digits remaining. The remaining digits are taken as the speed dial number and are copied into the Sub-Tag Buffer as a numeric value.
Off-Net:	Indicated by the Off Net prefix. The remaining digits are taken off net number and are copied into the Pending TN Buffer.
On-net:	In the absence of either of the above prefixes, the remaining digits are considered to be an On-Net address and are copied into the Pending TN Buffer.

Availability

Available in VPN.

Node exits - VPN Analyze

This node has one entry and four exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The decode did not fail and no alternate station was found.
2	AltStation	An alternate station has been found
3	DecodeFail	A decode failure has occurred.
4	CollectFail	A collect info failure has occurred.

Configuring the node - VPN Analyze

Follow these steps to set prefix numbers.

1. Options can be excluded using the following values in the **Exclude Flags** box. Exclude:
   - Alternate Station = 0x1
   - PIN number = 0x2
   - Account Code = 0x4
   - Off-Net number = 0x8

- Speed-Dial number = 0x10

2. The **Get More Digits** box lets you specify that CollectInformation should be used if there are insufficient digits for parsing.
3. The **Buffer ID** value for the Speed Dial Buffer must be 5, to match the Collect To SubTag buffers (which are currently fixed at 5 and cannot be modified).
4. Click **Save**.

Note: Decode failure occurs when:

- Insufficient digits are present to decode an optional prefix.
- Field already parsed.
- Excluded fields are present.

VPN Originating CUG

The Originating CUG node analyzes the calling and called numbers contained in the calling private network or logical calling buffer, and the pending TN buffer, respectively.

It determines whether the calling and called numbers are in the same logical CUG, and it determines the CUG type. The following rules apply:

- If the calling number is in a restricted CUG, then the called number must be in the same CUG. If it is not in the same CUG, then the CUG failure branch of the node is followed.
- If a VPN station is in more than one CUG, one of which is non-restricted, then the VPN station is also deemed to be non-restricted.
- If the calling number is not in a CUG or it is in a non-restricted CUG, then the success branch of the node is followed.

Availability

Available in VPN.

Node exits - VPN Originating CUG

This node has one entry and three exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	Decode succeeded as follows: 1. Calling number is not in CUG or it is in a non-restricted CUG. 2. Calling number is in a restricted CUG, called number is on-net and both numbers are in the same CUG.

Exit	Cause	Description
2	Error	General errors: 1. ACS engine pending context PendingTN or Logical Address buffer may not contain enough digits. 2. Error returned from Oracle.
3	CUG Error	Decode failed as follows: 1. Calling number is in a restricted CUG, called number is on-net and the numbers are in different CUGs. 2. Calling number is in a restricted CUG and called number is not in the same CUG (the called number may be on-net, off_net, on a different VPN, or a non VPN number).

Configuring the node

This node requires no configuration data. You may change the **Node name**, if required.

VPN Load Station

The VPN alternate station allows you to load an alternate calling station profile.

If defined, the network address of the station to call is in Calling On-Net Address. If it is not defined, then the VPN alternate station node prompts you to enter a station ID, using the specified announcements. You are prompted up to a defined maximum number of times before following the Not Loaded exit.

The Load Station process is described below.

Stage	Description
1	Calling on-net address is defined? If there is a value currently defined in the calling on-net address, then skip directly to stage 3.

Stage	Description
2	Prompt for Input. • Check if max iterations reached (follow Not Loaded). • Collect a digit string, between 2 and 16 digits in length. • On input failure, increment the iteration counter and restart this stage (stage 2). • Also check here for Canceled (follow Not Loaded) or Abandoned (follow Abandoned).
3	Load the profile? • Load the specified station profile from the database. • Go to stage 4 on success. • If the data is not found and max iterations are reached then follow the Not Loaded branch. • Otherwise return to stage 2 for re-prompt.
4	Success. Update the callingOnNetAddress in the engine context to correspond to the new station profile.

Notes:

- If you were prompted, then the collected digits are not placed in the engine context callingOnNetAddress buffer until the profile has been successfully loaded.
- If max iterations is set to 0, then the you should never be prompted. In this case the announcement ids may not actually be defined. This is permitted by the editor and compiler.
- This feature does not check the PIN for the remote profile, or any specific access rights. A subsequent PIN authorization feature node is typically required.

Availability

Available in VPN.

Node exits - VPN Load Station

This node has one entry and four exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	See node description.
2	Not Loaded	See node description.
3	Abandoned	See node description.
4	Collected	See node description.

Configuring the node - VPN Load Station

Follow these steps to edit the node

1. Select the Initial and Reprompt Announcements to set the initial prompt and re-prompt announcement.
2. Set the **Max Iterations** value to the number of retries.
3. Click **Save**.

VPN Lookup

The VPN Lookup allows you to translate an On-Net number to the corresponding Network address from VPN_STATION in the database. The node uses the PendingTN type to determine if a lookup should be performed.

The VPN Lookup process is described below.

Stage	Description
1	If the PendingTN type is: • OffNet, or Unknown, return Success • SpeedDial, return Failure • OnNet, then go to stage 2
2	Look up the corresponding NETWORK address from VPN_STATION in the database using the current network ID. If: • Found, replace the pending TN with that OffNet address, and return Success • Otherwise, return Failure

Availability

Available in VPN.

Node exits - VPN Lookup

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	See node description.
2	Failure	See node description.

Configuring the node

This node requires no configuration data. You may change the **Node name**, if required.

VPN CLI Lookup

The VPN CLI Lookup node allows you to set the Originating Network ID for the current service interaction. The node matches a calling number buffer with the physical address of a VPN station.

Availability

Available in VPN.

Node exits - VPN CLI Lookup

This node has one entry and four exits. The number of exits cannot be changed.

Exit	Cause	Description
1	On This Net	The value matched the physical address of a VPN station in this network.
2	On Another Net	The value matched the physical address of a VPN station in another network.
3	Off Net	The value did not match any known VPN station physical address.
4	Macro Fail	There was a failure.

Configuring the node - VPN CLI Lookup

Follow these steps to configure the VPN CLI Lookup.

1. You can set the node to check the:
   - **Calling Logical** number buffer,
   - **Calling Network** value, or
   - **Calling Party ID**
2. from the invoking message.

   Note: If multiple buffers have been selected, the first will be used.
3. Click **Save**.

   Result: The node will then branch based on the result.

VPN Mobile Analyze

The VPN Mobile Analyze node allows you to break down the digits contained in the Pending Termination Number Buffer. This node differs from the VPN Analyze node in that it does not use the network defined prefixes to analyze the type of call being made, unless the option to strip prefixes is enabled in the configuration file.

The logic of the node is to check, in order:

- Network Site Code
- Mapped Network Prefix
- Global Special Numbers
- Network Speed Dial

- Station Speed Dial
- Network Station Extensions.

If a match is:

- Found, the number type is set accordingly and the node exits through the appropriate exit.
- Not found, the number of digits needed to make the shortest possible match is used to collect more digits and the whole process is started again.

This matching process is repeated until a valid match is found. If no match is found, then the number is assumed to be off-net and the off-net branch is taken.

Network Site Code

VPN Mobile Analyze compares the first digits in the pending TN buffer with the site codes for all defined VPNs. If a match is found, then the network ID of the VPN for the matched site code is compared with the network ID of the current VPN. If the IDs are the same, then the pending TN type is set to 'Private' (on-net), if they are different, it is set to 'Public' (off-net).

Mapped Network prefix

If there is no match for the network site code, then the first digits of the pending TN buffer are compared with all the mapped network prefixes of the owning VPN. If a match is found, then the site code of the VPN for the matched network prefix is replaced in the pending TN buffer by the mapped network prefix. In addition, the network ID of the VPN for the matched network prefix is compared with the network ID for the current VPN. If the IDs are the same, then the pending TN type is set to 'Private' (on-net), otherwise it is set to 'Public' (off-net).

Stripping off number prefixes

When the corresponding configuration option in the **eserv.config** file is enabled, the node strips off the VPN network speed dial or off-net prefix prior to number matching. If a match is found, the node exits via the appropriate branch, depending on the applicable number match.

Global Special Numbers

The global special number check, network speed dial check, and station speed dial checks can be enabled and disabled using the check boxes in the node.

Availability

Available in VPN.

Node exits - VPN Mobile Analyze

This node has one entry and six exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Global Special	Match has been made with Global Special number.

Exit	Cause	Description
2	Network Speed Dial	Match has been made with Network Speed Dial number.
3	Station Speed Dial	Match has been made with Station Speed Dial number.
4	On Net	Match was made with extension number of a VPN station on the same VPN Network as the caller.
5	Off Net	No match was made.
6	Error	General failure

Configuring the node - VPN Mobile Analyze

Follow these steps to configure the node.

1. Select the following check boxes to enable or disable the check comparisons against specific number lists:
   - **Global Special**
   - **Network Speed Dial**
   - **Station Speed Dial**
2. Enter the decimal value of the tag for the profile block in the text box below any selected box.

   Note: The tag for Speed Dial is 26. Refer to Profile Blocks and Fields.
3. Click **Save**

VPN Caller is On-Net

The VPN Caller is On-Net node allows you to check if the incoming caller is on-net.

Availability

Available in VPN.

Node exits - VPN Caller is On-Net

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Yes	A private calling and called address is defined and the calling network ID matches the called network ID.
2	No	no match

Configuring the node

This node requires no configuration data. You may change the **Node name**, if required.

VPN Get Hunting Number

Warning: This feature node has now been deprecated and should no longer be used. This feature node will still function in existing control plans. For new control plans please use the **Get Hunting Number** feature node.

The VPN Get Hunting Number feature node allows you to search a list of termination numbers and timeout pairs. On each iteration, the node sets the PendingTN and timeout using the next number on the list until no numbers remain.

Availability

Available in VPN.

Node exits - VPN Get Hunting Number

This node has one entry and three exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Next Number	A number is found
2	No More Numbers	No numbers remain
3	Failure	General failure

Configuring the node - VPN Get Hunting Number

The hunting numbers and timeouts are set for every station through the VPN Station Hunting Planner screen.

This node requires no configuration data. You may change the **Node name**, if required.

VPN Redirection Counter Branching

The Redirection Counter branching node allows you to compare the Redirection Information Counter received in the invoking message. The node lets you define an integer constant for the comparison. One of the following branches is taken, as appropriate:

- Less than
- Equal to
- More than

Note: If no value is supplied for the redirection counter, then the error branch is taken.

Availability

Available in VPN.

Node exits - VPN Redirection Counter Branching

This node has one entry and four exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Less Than	The redirection counter was less than the value.
2	Equal To	The redirection counter was equal to the value.
3	More Than	The redirection counter was more than the value.
4	Fail	The redirection counter was not supplied.

Configuring the node - VPN Redirection Counter Branching

Follow these steps to configure the node.

1. Enter the number in the **Compare with value** field, against which the Redirection Information is compared.
2. Click **Save**.

VPN Set Redirection Counter

The Set Redirection Counter node allows you to set an integer constant as the redirection information counter. This value is then used as the redirection information counter in the next Connect message sent by the system.

You can also configure the following redirection information for inclusion in the Connect message:

- Indicator (for example, call was diverted)
- Original reason (for example, no reply)
- Redirection reason (for example, mobile subscriber busy)

Availability

Available in VPN.

Node exits - VPN Set Redirection Counter

The VPN Set Redirection Counter feature node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	Redirection succeeded
2	Failure	Redirection failed

Configuring the node - VPN Set Redirection Counter

Follow these steps to configure the Set Redirection Counter feature node.

1. From the **Redirection Counter** list, select the number of redirections to send in the connect message.
2. From the **Redirection Indicator** list, select the redirection indicator to send in the connect message.
3. From the **Original Redirection Reason** list, select the original reason for the redirection to send in the connect message.
4. From the **Redirection Reason** list, select the redirection reason to send in the connect message.
5. Click **Save**.

VPN Set Tariff Code From Profile

The Set Tariff Code node allows you to add network charging data to the next outgoing TCAP primitive. The node first looks at the station profile, then the network profile and finally the customer profile, and selects the network charging data, based on the first successful match.

The SCI/FCI data for the Customer/Network/Station can be accessed and set through the VPN Customer/Network/Station provisioning screens.

Availability

Available in VPN.

Node exits - VPN Set Tariff Code From Profile

This node has one entry and three exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Tariff Set	Tariff successfully set
2	No Tariff Found	Tariff not found
3	Error	General failure message

Configuring the node - VPN Set Tariff Code From Profile

Follow these steps to configure the node.

1. Select the Tariff From Profile from the list.
2. Click **Save**.

VPN Subscriber Lookup

The VPN Subscriber Lookup node allows you to look up a number buffer and load the VPN network and station profiles associated with that number. This will store them in chassis

context so that other nodes (for example, Set Pending TN from Profile, Profile Branching) can use the information.

Note: This can be used with any service library, not just VPN.

Node exits - VPN Subscriber Lookup

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	Profile was successfully retrieved from the database.
2	Failure	Profile was not retrieved from the database.

Configuring the node - VPN Subscriber Lookup

Follow these steps to edit the node configuration.

1. Select the number buffer from the **Which Number?** drop down list. Available buffers are:
   - Dialed Service Number
   - Calling Logical Number
   - Calling Network Address
   - Calling Party ID
   - Pending Termination Number
   - Original Called Number
2. Click **Save**.

Note: For more information on number buffers, refer to the *CPE User's Guide*.

VPN Voice Mail Number Configuration

The Voice Mail Number Configuration node allows you to modify the Pending Termination Number to provide compatibility with voicemail systems. The node allows you to modify a selected number buffer by inserting some defined digits at an offset, also defined in the feature node.

Example:

Insert At Position: 5

Insert What (Pattern): 888

Buffer (Call Context Number): pendingTN (01473200)

In this case the final number would be 01473888200.

The final number is copied to the pendingTN buffer and the node is exited through the SUCCESS branch.

If the length of the final number is too long (typically 32 digits or more), or if there is no number available for the selected buffer under the processing call, then no number is copied to the pendingTN buffer and the node is exited though the ERROR branch.

Availability

Available in VPN.

Node exits - VPN Voice Mail Number Configuration

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	See node description.
2	Error	See node description.

Configuring the node - VPN Voice Mail Number Configuration

Follow these steps to configure the node.

1. Enter the offset where the pattern list should be inserted in the **Insert At Position** field.
2. Enter the string to be inserted in the **Pattern List** field.
3. Select the buffer to use to form the final voice mail number from **The Call Context Number** drop down list.

   Note: For a definition of each buffer, refer to the *CPE User's Guide*.
4. Click **Save**.

VPN Terminating CUG

The VPN Terminating CUG node analyzes the calling and called numbers contained in the Calling Private Network or Logical Calling Buffer, and the PendingTN Buffer respectively.

The node determines whether the calling and called numbers are in the same logical CUG, and also determines the CUG type. If required, it also collects the PIN for the called number's CUG. The following rules apply:

- If the CUG PIN is required, and the called number is in a CUG, and the calling number is not in a CUG, and the maximum number of retry attempts is reached, then the CUG PIN failure branch of the node is followed.
- If the called number is in a CUG, and the calling number is not in a CUG, and the correct PIN has been entered, then the success branch of the node is also followed.

Availability

Available in VPN.

Node exits - VPN Terminating CUG

This node has one entry and three exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	Decode succeeded as follows: 1. Called number is not in a CUG. 2. Calling and called numbers are in the same CUG. 3. Called number is in a CUG, calling number is not in a CUG and correct PIN has been collected.
2	Error	General errors: 1. ACS Engine context PendingTN or Logical Address buffer may not contain enough digits. 2. Error returned from Oracle.
3	CUG Error	Decode failed as follows: 1. Available for future enhancements.
4	CUG PIN Error	Decode failed as follows: 1. Called number is in a CUG, calling number is not in a CUG and number of retry attempts for collecting the PIN has been exceeded.

Configuring the node - VPN Terminating CUG

Follow these steps to configure the node.

1. Enter the number of retry attempts for collecting the PIN in the **Number of PIN Attempts** field.
2. Select the **Collect PIN Introduction** announcement from the lists.
3. Select the **Invalid PIN Entered** announcement from the lists.
4. Select the **Maximum PIN Attempts Reached** announcement from the lists.
5. Click **Save**.