Contents

1. Preface ......................................................................................................................... 4
   1.1 HOW THIS GUIDE IS ORGANISED ...................................................................... 4
2. What is CMI? .................................................................................................................... 5
   2.1 ADMINISTRATOR MAINTENANCE ................................................................. 5
   2.2 IP ALLOCATION AND AUTHENTICATION .............................................. 5
   2.3 REPORTING .......................................................................................................... 5
3. What’s New .................................................................................................................... 7
   3.1 LOOK AND FEEL ............................................................................................... 7
   3.2 LOGIN & AUTHENTICATION ........................................................................... 7
   3.3 VRF PANEL ....................................................................................................... 7
   3.4 MANAGED BY ..................................................................................................... 7
   3.5 REALM SUPPORT .............................................................................................. 7
4. Interface Basics ............................................................................................................. 8
   4.1 REQUIREMENTS FOR ACCESS TO CMI ..................................................... 8
   4.2 ACCESSING CMI ............................................................................................... 8
      Figure 1 - CMI Web URL .................................................................................... 8
      Figure 2 - Login Screen ..................................................................................... 9
   4.3 CUSTOMER PANEL ........................................................................................... 9
      Figure 3 - Customer and VRFs Panels ............................................................. 10
   4.4 VRF PANEL ...................................................................................................... 10
      Figure 4 - VRFs Panel with a Highlighted Service ......................................... 11
      Figure 5 - Customer, VRFs, APN and Devices Panels .................................. 11
   4.5 APN PANEL ...................................................................................................... 12
5. Administrator Maintenance .............................................................................................. 13
   5.1 ADMINISTRATOR ACCOUNT TYPES ....................................................... 13
   5.2 USING THE TOOL ............................................................................................ 13
      Figure 6 - Admins Panel ................................................................................... 13
   5.3 CREATING ADMINISTRATORS ..................................................................... 13
      Figure 7 - New Admin Form ........................................................................... 13
   5.4 EDITING ADMINISTRATORS .......................................................................... 14
      Figure 8 - Highlighted Admin Record .............................................................. 14
      Figure 9 - Administrator form ........................................................................ 14
   5.5 DELETING ADMINISTRATORS ....................................................................... 14
6. Device Administration .................................................................................................... 16
   6.1 END USER DEVICE MAINTENANCE ......................................................... 16
      Figure 10 - Devices Panel ............................................................................... 16
   6.2 CREATING END USER DEVICES .............................................................. 16
      Figure 11 - New Device Form ........................................................................ 16
      Figure 12 - Create End User Device Form .................................................... 17
      Figure 13 - New End Use /Device Created ................................................... 17
   6.3 EDIT END USER DEVICES ............................................................................... 18
      Figure 14 - Edit End User Device Selection .................................................. 18
      Figure 15 - Edit End User Device Form ........................................................ 18
6.4 DELETING END USER DEVICES ................................................................. 18
6.5 BULK MAINTENANCE ........................................................................... 19
6.6 BULK ACTIVATION ............................................................................... 19

Figure 16 – APNs Panel ........................................................................... 19
Figure 17 - Bulk Activation Form and Instructions .................................... 19
Figure 18 – Downloaded activation template ............................................. 20
Figure 19 – Activation template with sample data filled in ....................... 20
Figure 20 - Sample Bulk Activation Error ............................................... 20
6.7 BULK REPLACE ................................................................................... 21

Figure 21 - Bulk Replace ......................................................................... 21

7. Reporting .............................................................................................. 22
7.1 AUTHENTICATION REPORTS ............................................................... 22
7.2 AUTHENTICATION DETAILED REPORTS .............................................. 22

Figure 22 - Authentication Detailed Report Form .................................... 23
Figure 23 - Authentication Detailed Report Form with results ................ 23
Figure 24 – Report in Excel format ........................................................... 24
Figure 25 – Report in Text (tab delimited) format ..................................... 24
7.3 AUTHENTICATION SUMMARY REPORTS ............................................ 24

Figure 26 - Authentication Summary Report Form .................................. 25
Figure 27 - Authentication Summary Report Form with results ............... 25
Figure 28 - Sample Printable Authentication Summary Report ................ 26
7.4 ACCOUNTING REPORTS ...................................................................... 26
7.5 ACCOUNTING DETAILED REPORTS .................................................... 26

Figure 29 - Accounting Detailed Report Form ......................................... 27
7.6 ACCOUNTING SUMMARY REPORTS ................................................... 28

Figure 30 - Accounting Summary Report Form ....................................... 28
Figure 31 - Sample Printable Accounting Summary Report .................... 29

8. Appendix A. Glossary ........................................................................... 30
9. Appendix B. Troubleshooting ............................................................... 32
10. Appendix C. Fields .............................................................................. 34
11. Table of Figures .................................................................................. 35
1. Preface

This document has been developed as a technical how-to guide for administrator users of the Optus Wireless IP VPN Customer Management Interface (or CMI for short) platform.

This document will guide you through all the features of the CMI platform allowing you to effectively manage your Optus Wireless IP VPN mobile fleet.

1.1 HOW THIS GUIDE IS ORGANISED

This guide is broken up into a number of logical sections:

- **What is CMI?** – A brief overview of the CMI platform,
- **What’s New** – For existing users, describing the recent enhancements to the CMI platform,
- **Interface Basics** – A brief overview of the user interface for beginners,
- **Administrator Maintenance** – Maintaining administrator user access to the platform,
- **Device Administration** – Maintaining end users’ services and devices,
- **Reporting** – End user authentication and accounting report generation.

The following appendixes are also included for your reference:

- **Glossary**
- **Troubleshooting**
- **Fields**
- **Table of Figures**

If you are a beginner to the Optus CMI platform, it is suggested you read this guide from start to finish before utilising the platform.

Advanced users can skip ahead to the What’s New, Administrator Maintenance, Device Administration and Reporting sections. These sections relate to the recent interface enhancements and how to use the interface for the most common administrative tasks.
2. What is CMI?

CMI stands for Customer Management Interface. The CMI platform is provided to Optus customers for the benefit of self-administration and reporting of the Optus Wireless IP VPN and Wireless IP VPN Plus products that are provided as an additional feature of the Optus GPRS, 3G and 4G mobile data services. It provides a convenient web based interface to manage your fleet without having to call Optus to make individual changes to your mobile phones and devices.

The CMI platform provides the following three main functions:

- **Administrator Maintenance**
- **End User Device IP Allocation and Authentication**
- **Reporting**

2.1 ADMINISTRATOR MAINTENANCE

Access to the Optus CMI platform is controlled via Administrator user accounts; only users with administrator account logins can access the web interface to manage mobile services.

There are two types of administrator accounts that can be setup:

- **Administrator**, and
- **Super User**

Administrator users with Super User access can add, modify and delete Administrator Accounts via the CMI platform directly. Only a limited number of administrator accounts can be created; this limit is defined when your Optus CMI customer account is created (by default 5 administrators are allocated to a customer account).

2.2 IP ALLOCATION AND AUTHENTICATION

The Optus CMI platform provides you with the functionality to manage individual end user mobile services depending on a number of criteria:

- **MSISDN** - Phone number of the device (known as the MSISDN),
- **Username, Password** - Username and password supplied when logging onto the network,
- **Both** - A secure combination of both.

For example, you may wish to allocate a Static IP address to a particular mobile number (also known as MSISDN) that is being used in a particular device. With CMI, you can not only allocate this IP address yourself, but also change it later on to a new IP address within your IP Address range if you wish.

Another applicable example is where you are frequently changing mobile devices and wish to carry the same IP address with you between devices. With CMI you can allocate an IP address to a particular username and password to ensure that no-one can take that IP without proper authentication.

A combination of the two authentication methods means that a would-be hacker cannot just steal the mobile service and device and expect it to work. Not only do you ensure that your MSISDN is the only device to obtain an IP address – but also you can ensure that only proper credentials can be used to gain access to your private corporate network.

2.3 REPORTING

As a part of the CMI platform, Optus also provides you with the ability to generate reports on end device authentication and basic traffic usage for Optus GPRS, 3G and 4G mobile data connections.
The reports are broken into two broad categories:

- **Authentication Based Reports:**
  - Detailed Authentication Reports - Showing failure and success for each mobile data connection attempt.
  - Summary Authentication Reports - Showing graphs to give a clear idea of how many authentication successes and failures have been made over the specified time.

- **Account Based Reports:**
  - Detailed Accounting Reports - Showing the details of a mobile data session after it has been disconnected.
  - Summary Accounting Reports - Showing traffic utilization, length of the connection and number of data sessions.

These reports can be used for your own internal back-billing purposes, network debugging or for general growth analysis.

The reports are all accessible through the CMI platform and can be dynamically generated and customised based on your specific needs via the various filter options available.
3. What’s New

3.1 LOOK AND FEEL

The Optus CMI platform has been enhanced with a new intuitive design that lets you access relevant information without having to navigate through several pages and menu items.

Various sections are now organised in self-contained panels on a single page rather than individual pages with many panels only displayed on request from selecting a particular option. After logging into the platform the following panels are initially visible (please see figure 3 for a system screenshot).

- Customer [Titled with your Company Name] Panel
- VRF Panel

The following panels are displayed on request and if the administrator user account has the appropriate privileges:

- Admins – Exposed by selecting the Maintain Admins option,
- APNs – Exposed by selecting the relevant VRF,
- Devices – Exposed by selecting the relevant VRF,
- Reports – Exposed by selecting the Reports option.

3.2 LOGIN & AUTHENTICATION

With the recent enhancements to the CMI platform, selected customers will now log into the platform via a Realm instead of the usual APN. If you’re currently logging into the CMI platform via an APN, you will continue do so. Please select APN as Authentication Type on the login screen as described in the following section (see figure 2 in Interface Basics section).

3.3 VRF PANEL

The VRF (Virtual Routing and Forwarding) panel is configured for you by Optus staff. Some strings, such as IP Range and Authentication method have been moved from the APN level to the VRF level. Your existing APN name will be identical to your VRF name. Please see the following section for more details on this new panel.

3.4 MANAGED BY

A new Managed By identification flag has been added to each VRF, this flag denotes who is able to administrate the end user devices. There are three possible options:

- Customer – You are able to view, modify and delete the end user devices associated with the selected VRF as your require.
- Alphawest – Alphawest manage the end user devices associated with the selected VRF, however you will still be able to view the end user device details.
- Optus – Optus manage the end user devices associated with the selected VRF, however you will still be able to view the end user device details.

3.5 REALM SUPPORT

To provide support for services that use a common APN (such as the Wireless IP VPN Plus product) a new grouping identification ‘Realm’ has been added. This allows the logical separation of services using a common APN in the same way a traditional private APN is used to separate services and their particular access.

Please Note: The functionality of your existing service will not be affected by any of the enhancements to the CMI platform and will continue to operate in the same manner as it did before.
4. Interface Basics

The CMI platform is provided as a secure web-based interface for access from a PC with public Internet access. Here we will provide you with an introduction to the interface and give you the basics on how to get started.

4.1 REQUIREMENTS FOR ACCESS TO CMI

Before you can begin, you need to ensure that you have met the following minimum system requirements.

**Browser:** Latest version of major browsers including Internet Explorer 8 and higher are supported. Browser cookies and JavaScript features must be enabled for full functionality.

4.2 ACCESSING CMI

Accessing CMI is simple and can be done from a PC with access to the Internet.

**Step 1**
Open your Internet browser.

**Step 2**
In the address bar, type in the address [https://wirelessip.optus.com.au](https://wirelessip.optus.com.au)

![CMI Web URL](https://wirelessip.optus.com.au/)

**Figure 1 - CMI Web URL**

**Step 3**
You will be prompted to enter your CMI account Username, Password and APN or Realm, depending on your account authentication type. This information will have been provided to you when the Wireless IP VPN link was first setup.
WIRELESS IP VPN

Welcome to the Wireless IP VPN Customer Management Interface (CMI). CMI is an optional service designed to manage and deliver user authentication and static IP allocation. CMI may only be accessed by the IT Manager(s) nominated by your organisation.

![Login Screen](image)

© Optus Administration Pty Ltd 2015

**Figure 2 - Login Screen**

**Step 4**

Click the **Login** button to continue, you will be then presented with an overview of your service.

Finally, if you wish to logout of the system, simply click the button labelled **Logout** in the top right corner.

**4.3 CUSTOMER PANEL**

Once logged in you’ll be presented with an overview of your services. The top panel titled with your company name, in this case **Pub Internet** is the Customer panel.
4.4 VRF PANEL

The VRF (Virtual Routing and Forwarding) panel contains information about your services, as they have been configured for you by Optus.

There are a number of options that are set up for you by Optus in the VRF panel. Some of these options impact the way your service works.

- **Status** – [Active | Suspended], If the VRF is “Suspended”, all services associated to the VRF are considered Suspended and will not authenticate / connect to mobile data services.
- **VRF** – The name assigned to the particular VRF.
- **Managed By** – [Customer | Optus | Alphawest], Denotes weather you as the customer manages the end device or whether it’s Optus or Alphawest in the case of Managed services (such as the Optus Wireless IP VPN Plus Managed Service option). In the case of Optus or Alphawest Managed services you will only be able to view end user device details you will not be able to modify or delete them.
- **APNs** – List of all APNs (Mobile Access Point Names) associated to the particular VRF.
- **Realm** – Realm associated with this particular VRF. Used for authentication with the Optus Wireless IP VPN Plus service.
- **Auth Method** – (Username / Password | MSISDN | MSISDN / Username / Password), You will notice that with only MSISDN authentication for example, there will be no field to enter the Username or Password for an end device in the Devices Panel.
- **Static IP** – [Yes | No], If Static IP is set to “Yes” then each connecting device is assigned their own unique IP address, if set to “No” then each connecting end device is dynamically assigned an IP address upon each mobile data connection request.
- **IP Ranges** – List of IP Ranges setup for this VRF. You will not be able to assign IP addresses for your devices outside of these specified IP Ranges.
- **Devices** – [Number of used / total number of devices]. The total number of devices is calculated as a sum of all usable IP addresses in all IP Ranges setup for this VRF.
- **Product Type** – The Product Type of the associated VRF.
- **Mobile Network** – [GPRS / 3G | GPRS / 3G / 4G], The Mobile Networks supported by the VRF.
- **Network Connectivity** – The Network Connectivity used by the VRF.
- **DNS** – DNS (Domain Name Service) configuration.
- **WINS** – WINS (Windows Internet Name Service) configuration.

Moving the mouse pointer over the VRF details in the VRFs panel, highlights the service in yellow colour, as can be seen in the following image.

![Figure 4 - VRFs Panel with a Highlighted Service](image)

Clicking the highlighted VRF details changes the highlighted colour to orange and opens the APNs and Devices panels as shown below. These panels are described later in the document.

![Figure 5 - Customer, VRFs, APN and Devices Panels](image)

A number of restrictions will have been set for your VRF. These include:

- Account Status
- Managed By
- Authentication Method
- Static IP
- Number of end devices you can allocate on the system
- Number of CMI account Administrators you can allocate on the system

All of these restrictions can only be changed by Optus.
4.5 APN PANEL

The APN or Access Point Name will have been given to you upon ordering the Optus Wireless IP VPN service.

An APN is important because it designates a company configuration and separates your services from all other companies configured on the Optus network. Without an APN, all customers would be a part of the same configuration pool – and this would be unacceptable.

The APN is configured on both the Optus network, and your end device. Before using an APN you must ensure that the mobile device you are using has been configured correctly.

Any mobile service ordered from Optus for use with your Wireless IP VPN service is provisioned to only work with the APNs / Realms assigned to your company. No other company will be able to use your APNs / Realms unless you have given Optus permission to do so.
5. Administrator Maintenance

The Administrator Maintenance panel is used to manage additional CMI administrator users.

5.1 ADMINISTRATOR ACCOUNT TYPES

There are two CMI account types:

- **Administrator**
- **Super User**

The difference between the two is that only **Super Users** can access the Administrator Maintenance panel, an **Administrator** cannot.

The **Administrator** account is usually given to the helpdesk or operational department of your company.

**Super User** access should be reserved for senior administrators or management personnel.

Both the **Super User** and **Administrator** account types can add, delete and modify end user devices and generate reports as required.

5.2 USING THE TOOL

Assuming you are already logged into the CMI platform, click the **Maintain Admins** link on the right hand side of the Customer panel header. The **Admins** panel should then appear below the Customer panel. **Note**: Only Super Users can see the Maintain Admins link.

![Figure 6 - Admins Panel](image)

5.3 CREATING ADMINISTRATORS

**Step 1**

Click the **Add Admin** link on the left side of the Admins panel header. A new Admin user form appears at the bottom of the Admins panel.

![Figure 7 - New Admin Form](image)
Step 2
Enter the new user’s login credentials, select account type and click **Save**.

The fields are explained here:
- **Username** - The username must be unique and is case sensitive. It can only contain alphanumeric characters, full stops, hyphens (-), at characters (@) and underscores (_).
- **Password** - The password has to be either mixed case or numbers and letters. An error will be returned if the username or password is rejected.
- **Comment** - The comment field can be used for whatever you like. This can be either the person’s name or a note about the user. This field is only used by the interface and does not affect any CMI account configurations.

5.4 EDITING ADMINISTRATORS
You may edit an Admin user and modify its comment and password.

Step 1
Moving the mouse pointer over an Admin user’s details highlights the respective row in yellow colour.

![Figure 8 - Highlighted Admin Record](image)

Step 2
Clicking the highlighted row changes the highlight colour to orange and shows a form with the Admin user’s details at the bottom of the Admins panel.

![Figure 9 - Administrator form](image)

Step 3
Make the desired changes and click the **Save** button.

5.5 DELETING ADMINISTRATORS
Step 1
Select the desired Administrator user and make sure the Admin user’s details form is open as if you wanted to edit the user.
Step 2

Click the Delete this Admin link at the bottom right corner of the Admin user’s details form, as can be seen in the previous image.

The user is removed from the system.

**Note:** If the Admin user is currently logged in, the next action they perform on the interface will cause that user to be logged out with a session timed out message.
6. Device Administration

The Device Administration capabilities of CMI allow you to provision and configure your mobile user devices for use with the CMI system and its Reporting facilities.

The CMI facility allows two methods for updating this information:

- End User Device Maintenance
- Bulk Maintenance

Combined, these methods allow a very flexible means of modifying your mobile end user device fleet.

6.1 END USER DEVICE MAINTENANCE

End User Device Maintenance is provided for the provision and modification of single mobile devices.

The following are instructions on how to use the interface. The service used in the following examples is configured for Username, Password and MSISDN authentication to show all possible options. Your display options may vary depending on your own service configuration.

Individual devices are managed in the Devices panel. Open the Devices panel by selecting a VRF as shown in Figure 5.

If you haven’t added any end user devices yet, your Devices panel should look as follows.

![Figure 10 - Devices Panel](image)

When you first access the tool, it’s likely there will be no end devices displayed.

6.2 CREATING END USER DEVICES

Creating an end user device is a simple task, and is performed from the Devices panel.

![Figure 11 - New Device Form](image)
Step 1
Click the **Add Devices** link on the left side of the Devices panel header. A new Device form will appear at the bottom of the Devices panel.

Step 2
Enter the desired new end user device credentials and click **Save**.

![Figure 12 - Create End User Device Form](image)

The fields are explained here:

- **VRF / APN** - The VRF / APN will be pre-populated based on the VRF that has been previously selected.
- **Route Type** - If available set the Router Type to the desired option, if Framed is selected you will need to enter in the required LAN – Subnet details.
- **Device Status** - Ensure Device Status is set to Active for the new device to be able to authenticate to the VRF / APN.
- **Username** - The username must be unique and is case sensitive. It can only contain alphanumeric characters, full stops, hyphens (-), at characters (@) and underscores (_).
- **Password** - The password has to be either mixed case or numbers and letters. An error will be returned if the username or password is rejected.
- **MSISDN** - For VRF’s / APN configured for MSISDN authentication options enter the required end user devices mobile number.
- **WAN-IP / WAN-Netmask** - For VRFs / APNs configured for Static IP address select the desired WAN-IP address and WAN-Netmask from the available list.
- **Comments** - The comments field can be used for whatever you like. This can be either the person's name or a note about the user. This field is only used by the interface and does not affect any CMI account configurations.

Step 3
Click **Save** to create the end user device.

The end user device should now be created and you should be able to see it in the Devices Panel, this new end user device can be used straight away.

![Figure 13 - New End User /Device Created](image)
6.3 editar dispositivos de usuario final

**Paso 1**
Moviendo el puntero del mouse sobre los detalles de un dispositivo de usuario final, se resalta la respectiva fila en el color amarillo.

![Imagen 14 - Selección de dispositivo de usuario final para editar](image)

**Paso 2**
Al hacer clic sobre la fila resaltada, la coloración de resaltado cambia a naranja y muestra una forma con los detalles del dispositivo del usuario final en el panel Devices.

![Imagen 15 - Forma de dispositivo de usuario final para editar](image)

**Paso 3**
Realice los cambios deseados y haga clic en el botón **Guardar**.

6.4 elimina dispositivos de usuario final

**Paso 1**
Seleccionar el dispositivo de usuario final deseado asegurándose de que el formulario de detalles de dispositivos esté abierto como si quisiera editar el dispositivo de usuario final.

**Paso 2**
Haga clic en el enlace **Eliminar este dispositivo** en el extremo inferior derecho del formulario de detalles de dispositivos, como se puede ver en la imagen anterior.

El configuración del dispositivo de usuario final se eliminará de la plataforma.

**Nota:** Si el dispositivo está actualmente conectado a una sesión de datos móvil, no se desconectará automáticamente. Si el dispositivo se desconecta y trata de volver a conectarse, fallará.
6.5 BULK MAINTENANCE

The Bulk Maintenance functionality is provided in CMI to allow flexibility in the way you can provision end user devices.

The platform allows you to use a Microsoft Excel spreadsheet to modify or add new devices and upload this spreadsheet to the CMI system for automated provisioning. This can come in very handy when attempting to provision any more than a few end user devices at a time.

There are two options in the Bulk Maintenance tool in CMI:

- Bulk Activation
- Bulk Replace

6.6 BULK ACTIVATION

This tool allows you to add an additional number of end user devices to your APN / Realm configuration in one go, using a Microsoft Excel template provided by CMI.

All existing configuration will stay the same, and not be overwritten by the use of this tool.

This method of provisioning is useful when activating a large number of devices or SIMs at once.

Step 1
Select a VRF in VRFs panel.

Step 2
Click Bulk Active in the APNs panel.

Figure 16 – APNs Panel

Step 3
Follow the step-by-step instructions provided in the Bulk Activate. Remember to download the activation template first – you cannot use your own template.

Figure 17 - Bulk Activation Form and Instructions
By selecting the **Auto allocate blank IP addresses** option, you will be able to leave IP addresses blank in your spreadsheet and let them be automatically chosen by the system. This saves you having to worry about allocating IP addresses that may have already been taken. Unless you have a specific reason, please make sure **WAN Netmask** is set to **32**.

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Username</td>
<td>Password</td>
<td>MSISDN</td>
<td>WAN IP</td>
<td>WAN Netmask</td>
<td>Comment</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 18 – Downloaded activation template*

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Username</td>
<td>Password</td>
<td>MSISDN</td>
<td>WAN IP</td>
<td>WAN Netmask</td>
<td>Comment</td>
</tr>
<tr>
<td>2</td>
<td>publntnetA</td>
<td>Password1</td>
<td>6142102082</td>
<td></td>
<td>32</td>
<td>Device A</td>
</tr>
<tr>
<td>3</td>
<td>publntnetB</td>
<td>Password2</td>
<td>6142102083</td>
<td></td>
<td>32</td>
<td>Device B</td>
</tr>
<tr>
<td>4</td>
<td>publntnetC</td>
<td>Password3</td>
<td>6142102084</td>
<td></td>
<td>32</td>
<td>Device C</td>
</tr>
</tbody>
</table>

*Figure 19 – Activation template with sample data filled in*

**Step 4**

Click **Submit**.

Analyse errors that are returned by the system. These will appear in Red at the top of the screen. No activation will occur until these errors are cleared.

Here is an example of an error that may occur:

*Figure 20 - Sample Bulk Activation Error*

Once you have successfully submitted the spreadsheet, the end user device configuration becomes active within one minute.

If you realise you have made a mistake on an individual device, modify the device using the **End User Device Maintenance** instead of using the Bulk Maintenance. This way, it will be much quicker to make the change.
6.7 BULK REPLACE

This method of bulk maintenance allows you to download a complete list of currently provisioned end user devices, modify that list and then resubmit for reconfiguration.

This tool can come in handy in a number of situations:

- You wish to modify all device passwords offline.
- You need to modify the subnet allocated to the APN.
- You need to remove a number of devices quickly.
- You simply need a list of devices for your own records.

This tool can however be dangerous as it replaces your entire configuration. Be very careful with this facility, and ensure you backup any spreadsheet configurations before you modify them.

Here are the step-by-step instructions on how to use the replace method:

**Step 1**
Select a **VRF** in the VRFs panel.

**Step 2**
Click **Bulk Replace** in the APNs panel.

**Step 3**
Follow the step-by-step instructions provided on this page. Make sure you back-up the downloaded Microsoft Excel spreadsheet file before modification.

By selecting the **Auto allocate blank IP addresses** option, you will be able to leave IP addresses blank in your spreadsheet, and let them be automatically chosen by the system. This saves you having to worry about inputting IP addresses that may have already been taken by other end user devices.

**Step 4**
Complete the steps by clicking **Submit**.

Analyse any errors that are returned by the system. These will appear in Red at the top of the screen. No replacement will occur until these errors are cleared.

Once the replace has occurred, all of your entries will have been replaced by the entries contained on the spreadsheet within one minute.
7. Reporting

The reporting facility allows you to generate summary and detailed reports on both authentication and session accounting of your GPRS, 3G and 4G mobile end user devices.

These reports are provided to help you with troubleshooting and for querying individual usage of the service.

As before, you will only be able to generate reports that apply to your particular APN / Realm. No one else will be able to see your information.

The report section is broken down into two categories:

- **Authentication**
- **Accounting**

Authentication reports show information regarding the initial connection of the device. Accounting reports show data session information.

Reporting data is processed in near real time however ensure that if you are looking to report on a particular data session that the session has ended as accounting information is only sent for processing at the end of an end user device data session for reporting purposes.

Returned reporting data is limited to the first 2,000 records when displayed within the platform interface, to display all returned data (if more than 2,000 records) the report must be exported via the Printable format, Excel, CSV or Text export options.

### 7.1 AUTHENTICATION REPORTS

When a device first establishes a data connection to the mobile network, this is called establishing a data session. Within the CMI system, this data session establishment is when authentication occurs and an IP address is assigned to a particular mobile end user device.

When a data session occurs depends on the device itself, some devices will establish a data session upon start-up, others will await the first initial request for data access before connecting. Please consult the user manual of your particular mobile device for this information.

Authentication reports reflect information about that initial connection. Using the CMI platform you can either generate **Detailed Reports**, showing each individual connection or a **Summary Report** – which will report on activity over time.

### 7.2 AUTHENTICATION DETAILED REPORTS

Detailed Authentication Reports break down information for each data session establishment.

To generate a detailed authentication report, follow these steps:

**Step 1**
Click the **Reports** link from the page top banner. A new Reports form will appear at the bottom of the page.

**Step 2**
Choose **Authentication Detailed** from the available reporting options.

**Step 3**
Fill in the form depending on what results you want returned to you.
The fields are explained here:

- **Username** – Search for a username that was used during an attempted data session establishment.
- **MSISDN** – Searches for a particular MSISDN or mobile number that attempted a data session establishment.
- **WAN-IP** – Search for a particular WAN IP address that was assigned to a device.
- **APN** – Searches for connections to a particular APN / Realm.
- **From / To** – Performs the query, and returns data session attempts that occurred during the specified from and to times.
- **Show** – This will limit the results to those that are either Successes, Failures or Both.
- **Sort By** – Sorts the results, ascending or descending depending on the sort option chosen.

**Step 4**

Click **Submit** to generate the report.

Here is an explanation of each field in the returned report:

- **Time** – The time of the data session attempt.
- **Outcome** – Success or Failure depending on whether the device was authenticated or not.
• **Reason** – The reason for a failed authentication. This will be blank if the authentication was a success.
• **APN** – The APN that the data session was attempted on. Should not differ from the APN you are reporting on.
• **Username** – The username used for authentication (if Username and Password authentication are enabled for this APN).
• **MSISDN** – The MSISDN or phone number of the device that attempted the data session.
• **WAN-IP** – The IP address that was given to the successfully authenticated device. This will be blank if the authentication failed.

**Step 5**

If you wish to print the report, open the report in a Printable format. You can also download the report in a Microsoft Excel, CSV and Text format by clicking the relevant button.

<table>
<thead>
<tr>
<th>Time</th>
<th>Outcome</th>
<th>Username</th>
<th>MSISDN</th>
<th>WAN-IP</th>
</tr>
</thead>
</table>

**Figure 24 – Report in Excel format**

<table>
<thead>
<tr>
<th>Time</th>
<th>Outcome</th>
<th>Username</th>
<th>MSISDN</th>
<th>WAN-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-09-19</td>
<td>Success</td>
<td>whtb</td>
<td>61423990780</td>
<td>192.168.200.80</td>
</tr>
</tbody>
</table>

**Figure 25 – Report in Text (tab delimited) format**

**7.3 AUTHENTICATION SUMMARY REPORTS**

Summary authentication reports show authentication success and failure over time.

To generate a summary authentication report, follow these steps:

**Step 1**  
Click the **Reports** link from the page top banner. A new Reports form will appear at the bottom of the page.

**Step 2**  
Choose **Authentication Summary** from the available reporting options.

**Step 3**  
Fill in the form depending on what results you want returned to you.
figure 26 - authentication summary report form

the fields are explained here:

- **username** – search for a username that was used during an attempted data session establishment.
- **msisdn** – searches for a particular msisdn or mobile number that attempted a data session establishment.
- **apn** – searches for connections to a particular apn / realm.
- **from / to** – performs the query, and returns data session attempts that occurred during the specified from and to times.
- **granularity** – in the graph and tabulated report, summarises the amount of successes and failures into this period of time. note: avoid generating a large table by specifying a low granularity over a large period of time.
- **display** – you can either display the graph, the tabulated report or both depending on how you want the report to be displayed.

**step 4**

click submit to generate the report.

figure 27 - authentication summary report form with results

**step 5**

if you wish to print the report, open the report in a printable format. you can also download the report in a microsoft excel, csv and text format by clicking the relevant button.

here is a sample printable report.
The graph shows successes in red, and failures in green. The fields of the tabulated report are explained here:

- **Date** – Date of analysis,
- **Successes** – Number of successful authentications for that time period,
- **Failures** – Number of failed authentications for that time period.

### 7.4 ACCOUNTING REPORTS

Accounting Reports are provided to analyse data session information. CMI can provide you with detailed reports, that break down each data connection or summary reports showing trends over time.

### 7.5 ACCOUNTING DETAILED REPORTS

Detailed Accounting Reports break down session information for each data session.

To generate a detailed account report, follow these steps:

**Step 1**
Click the **Reports** link from the page top banner. A new Reports form will appear at the bottom of the page.
Step 2
Choose Accounting Detailed from the available reporting options.

Step 3
Fill in the form depending on what results you want returned to you.

![Figure 29 - Accounting Detailed Report Form]

The fields are explained here:

- **Username** – Search for a username that was used during an attempted data session establishment.
- **MSISDN** – Searches for a particular MSISDN or mobile number that attempted a data session establishment.
- **WAN-IP** – Search for a particular WAN IP address that was assigned to a device.
- **APN** – Searches for connections to a particular APN / Realm.
- **Session Start** – Performs the query, and returns data session attempts that occurred during the specified time.
- **Session End** – Performs the query, and returns data session attempts that occurred during the specified time.
- **Usage** – Generates the report output for sessions that used the specified amount of data during the session. This can be specified as greater than or less than.
- **Duration** – The report output will be generated for sessions that had a duration length as specified. This can be specified as greater than or less than.
- **Sort By** – Sort the results, ascending or descending depending on the column chosen.

**Step 4:**
Click Submit to generate the report.

**Step 5:**
If you wish to print the report, open the report in a printable format. You can also download the report as a Microsoft Excel file. The paragraph above the report explains how to do this, also see the circled items in the graphic below.

Here is an explanation of each field in the report:

- **Start Time** – The time that the session started.
- **End Time** – The time that the session ended.
- **Duration (min)** – The total duration of the session in minutes.
- **APN** – The APN that the data session was established on. This should not differ from the APN you are reporting on.
- **Username** – The username used for authentication (if Username and Password authentication is enabled for this APN).
- **MSISDN** – The MSISDN or phone number of the device that attempted the data session.
- **IP** – The IP address used during the session. This will either be a static IP address, or in the case of dynamic allocation – it will be the dynamically allocated address.
- **Usage (bytes)** – The total usage (in and out) used by this connection.
7.6 ACCOUNTING SUMMARY REPORTS

Summary accounting reports can display the following information:

- Average Session Length over time
- Session connections over time
- Average Bandwidth Utilisation over time
- Session disconnections over time

This information is provided in a number of graphs, and a single table format.

Each graph and each column of the tables shows the required information over time. To generate a summary authentication report, follow these steps:

**Step 1**
Click the Reports link from the page top banner. A new Reports form will appear at the bottom of the page.

**Step 2**
Choose Accounting Detailed from the available reporting options.

**Step 3**
Fill in the provided form.

![Figure 30 - Accounting Summary Report Form](image)

The fields are explained here:

- **Username** – Search for a username that was used during an attempted data session establishment.
- **MSISDN** – Searches for a particular MSISDN or mobile number that attempted a data session establishment.
- **APN** – Searches for connections to a particular APN / Realm.
- **Report** – The report information to display.
- **From / To** – Performs the query, and returns data session attempts that occurred during the specified from and to times.
- **Granularity** – In the graph and tabulated report, summarises the amount of Successes and Failures into this period of time. Note: avoid generating a large table by specifying a low granularity over a large period of time.
- **Display** – You can either display the graph, the tabulated report or both depending on how you want the report to be displayed.

**Step 4**
Click Submit to generate the report.
Step 5

If you wish to print the report, open the report in a printable format. You can also download the report as a Microsoft Excel file. The paragraph above the report explains how to do this, also see the circled items in the graphic below.

A sample printable report is shown below.

![Sample Printable Accounting Summary Report](image-url)
8. Appendix A. Glossary

3G – 3G or 3rd Generation. This is the short form pertaining to the third generation of Wireless Data Systems. This system was developed to satisfy the needs of users for higher data bandwidth across a wireless connection with the ability to roam.

4G – 4G or 4th Generation. This is the short form pertaining to the fourth generation of Wireless Data Systems that use LTE technology. This system was developed to satisfy the needs of users for higher data bandwidth than the 3rd Generation Wireless Data Systems across a wireless connection.

Accounting – Account relates to RADIUS or session accounting. This term is used to describe the facilities to account for traffic utilisation and duration for sessions.

APN – Access Point Name. This is a GPRS term, similar to the concept of a domain or RADIUS realm. The APN is used to segregate customers or classes of customers from each other – and is usually given to a subscriber for network authentication and access. The APN must be configured on a device before the device may be used.

Authentication – Authentication is the process of ensuring that a user or device is identified. This identification is then used to give the user or device access to particular services, and may be used to ensure that the user is allowed to access a particular APN. Although commonly authentication is performed with a username and password, in the case of CMI it can be the MSISDN or mobile number of the device as well.

CMI – Customer Management Interface. This interface allows the modification of users, end devices or devices for a particular APN. It also allows an IT manager to generate custom reports for accounting and authentication of devices.

CSV – Comma Separated Values.

Data Session -This term determines that either an active GPRS/3G PDP-Context or LTE EPS Bearer mobile data connection has taken place and confirms that a virtual network connection has been successfully established between the mobile device and the mobile network.

EPS Bearer -Evolved Packet System, is a connection-oriented transmission network that requires the establishment of a “virtual” connection between two endpoints between the mobile device and the mobile network.

GPRS – General Packet Radio Service, is a packet-based mobile data service, with the ability to roam.

IP address – IP stands for Internet Protocol. An IP address is a unique identifier given to participants on the Internet. This unique identifier is used to ensure that traffic is sent to the correct recipient.

LAN – Local Area Network

LTE – Long Term Evolution is the technology behind the 4th Generation of Wireless Data Systems. LTE, commonly marketed as 4G LTE, is a standard for wireless communications of high-speed data for mobile phones and data terminals.

MSISDN – Mobile Subscriber ISDN number. This is the technical term for a mobile number. For example: 61421029081.

PDP Context – Packet Data Protocol Context. This term pertains to an active GPRS or 3G data connection, the term context is used to indicate that it covers the start to the end of the connection.
RADIUS – Remote Access Dial In User Service. This technology became a popular means for authentication for dial up service within ISP’s. Today it is used for many different authentication systems including GPRS and VPN technology. Along with authentication, the RADIUS protocol will also provide network connection information to end devices or terminal servers.

Realm – Realm is a concept to provide customer and VRF isolation for a shared APN based product such as Wireless IP VPN Plus.

Session – We use this terminology in this document to describe a “period of connection” much like a PDP Context. A session consists of a connection from start to finish.

VRF – Virtual Routing and Forwarding

WAN-IP – Wide Area Network - IP

WIP VPN – Wireless Internet Protocol Virtual Private Network
9. Appendix B. Troubleshooting

I am unable to login to the user interface; instead I get an error “Session Failed”. My login credentials are correct.

The browser you are using must be capable of supporting cookies. Most browsers today will support this, however you can manually switch off this capability which will limit your ability to access some websites.

Check your browser to ensure it supports cookies, and that cookie support is enabled.

If you still fail to login, either ask a super-user of CMI within your company to try and change your password. If you are a super-user already, contact Optus Technical Support for further assistance.

When I attempt to connect, I get the error “Authentication Failed” on my device.

This is due to either invalid credentials when logging in or the end user account is currently suspended. This may be due to an incorrect mobile number (MSISDN), username or password. Or it may apply to the combination of both. Or the end user mobile account is currently suspended.

First check that your credentials are correct for the device by ensuring that you’re MSISDN, username and password are set correctly and the device status is currently active within in CMI Platform. Remember that you’re APN / Realm may not require all of this information – check the associated VRF within the CMI interface to check the APN / Realm configuration that applies to you.

Try changing the password for the device in the interface to see if this helps also.

An authentication report can help with determining what information was sent by the device to ensure that it matches the End User Device configuration. You should see a failed authentication attempt every time you try to connect.

Otherwise, if you fail to see an authentication attempt (either successful or not) perhaps you have configured the incorrect APN on your device. Double - check your device configuration.

When I attempt to connect, I get the error “Temporary Failure” on my device.

This can sometimes be the same as an “Authentication Failure”. Check the above help description before doing anything else.

Also, ensure that you are using a valid SIM card on the Optus network. If you are attempting to use another provider to connect to your Optus APN / Realm, this may not work unless the provider has a roaming relationship with SingTel Optus.

Finally, the error may be a network related error – so after attempting everything in the above few paragraphs, you may wish to call Optus Technical Support for further assistance.

I connect, but I keep getting the incorrect IP address.

This may be for a number of reasons. If the invalid IP address is constant, perhaps you are authenticating with the wrong credentials. Double check the End User Device configuration within the CMI user interface to ensure that is correct.

Check the Authentication reports to see what IP address you are being allocated. If the IP address in the report, and the one being allocated to your device do not match, you could be specifying an IP address in the network configuration of your device or laptop – check the configuration of both to ensure this is not the case.
If the IP address appears to be random, you may be attempting to configure an APN that is not set-up for Static IP. Check with Optus Technical Support to ensure your APN is configured correctly to use statically assigned IP Addresses.

**When I connect, I am unable to send data.**

This symptom can be due to various reasons. Ensure that the platform initially gives you an IP address correctly and that it matches what you expect. An invalid IP address will not route correctly and so expected traffic will not flow.

As the IP address is allocated to the connecting end user device, in most cases a corporate firewall may block you from accessing the data you require. If there is a firewall in place, check with your firewall manager to ensure your IP address is allowed to access the required information.

To see if any traffic is passing through the mobile end user device, you may wish to run an Accounting report on your session. Analyse the traffic utilisation to see if traffic is being generated during the data connection session.

**When I attempt to generate a report, nothing is displayed.**

Ensure that if you are looking to report on a particular session that the session has ended. Accounting information is only sent at the end of a session for reporting purposes.

Perhaps your check is too rigid, try not specifying a check item such as usage or username when generating the report. If you can see the item you are looking for in a more general report than you are probably being too rigid in your query and specifying invalid check items within the report form.

Ensure that the time span is correct when performing the query. Also, try widening the timestamp by a few hours or days. Sometimes a session may have started earlier than you expected.

**When I attempt to do a bulk replace, I can download the file but am unable to open it to modify it.**

The file downloaded is a Microsoft Excel 97 format file. You will need a version of Microsoft Excel that is equal to or greater than Microsoft Excel 97 to open the file and modify it.

**The application keeps rejecting a password as invalid when attempting to set a user’s password.**

The password allocated to devices has strict requirements for security as would be expected in password-only based authentication.

Please see section 6.2 CREATING END USER DEVICES of this guide for end user device password requirements.

**I attempt to set an MSISDN but it is rejected as already taken.**

This is probably because it is! You cannot use the same MSISDN for two different IP addresses. Each APN / Realm must have a unique list of MSISDN’s to operate.
## 10. Appendix C. Fields

The interface checks all inputs for fields. Requirements for each type of field with the interface are outlined below:

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>A username is made up of alphabetical and numerical characters including a hyphen (-) and a full stop (.). A username must be between 3 and 32 characters long.</td>
</tr>
<tr>
<td>Comment</td>
<td>The comment field is made up of mixed characters that are available on a normal US-ASCII keyboard. The string must not be any longer than 64 characters and does allow the use of spaces.</td>
</tr>
<tr>
<td>Password</td>
<td>The password field is a string of characters with no spaces that includes numbers, symbols and alphabetical characters. There must be at least 2 characters of different groups. The password must be between 6 and 32 characters.</td>
</tr>
<tr>
<td>MSISDN</td>
<td>This is strictly a numerical field that is 11 characters long. An example would be: 61421029081. Note the country code and the lack of the trailing 0 before the 421.</td>
</tr>
<tr>
<td>WAN-IP</td>
<td>A single IP address field in the format 'aaa.bbb.ccc.ddd'. An example would be 192.168.1.2.</td>
</tr>
<tr>
<td>APN / Realm</td>
<td>A string between 3 and 64 characters. This string must consist of either alphabetical or numerical characters including the hyphen (-), the underscore (_), and a dot (.). No spaces are allowed for an APN / Realm.</td>
</tr>
</tbody>
</table>
11. Table of Figures

Figure 1 - CMI URL 8
Figure 2 - Login Screen 9
Figure 3 - Customer and VRFs Panels 10
Figure 4 - VRFs Panel with a Highlighted Service 11
Figure 5 - Customer, VRFs, APN and Devices Panels 11
Figure 6 - Admins Panel 13
Figure 7 - New Admin form 13
Figure 8 - Highlighted Admin record 14
Figure 9 - Administrator form 14
Figure 10 - Devices Panel 16
Figure 11 - New Device form 16
Figure 12 - Create End User Device Form 17
Figure 13 - New End User Device Created 17
Figure 14 - Edit End User Device Selection 17
Figure 15 - Edit End User Device Form 18
Figure 16 - APNs panel 19
Figure 17 - Bulk Activation Form and Instructions 19
Figure 18 - Downloaded activation template 20
Figure 19 - Activation template with sample data filled in 20
Figure 20 - Sample Bulk Activation Error 20
Figure 21 - Bulk Replace 21
Figure 22 - Authentication Detailed Report Form 23
Figure 23 - Authentication Detailed Report Form with results 23
Figure 24 - Report in Excel format 24
Figure 25 - Report in Text (tab delimited) format 24
Figure 26 - Authentication Summary Report Form 25
Figure 27 - Authentication Summary Report Form with results 25
Figure 28 - Sample Printable Authentication Summary Report 26
Figure 29 - Accounting Detailed Report Form 27
Figure 30 - Accounting Summary Report Form 28
Figure 31 - Sample Printable Accounting Summary Report 29