



CMS6100 - Central Management Appliance

VCMS - Virtual Central Management Appliance

User Manual

Rev: 1.1

June 23rd 2010

INDEX

INTRODUCTION	4
1.1 Manual Organization	4
Manual Conventions	5
INSTALLATION	7
2.1 CMS6100 Installation	7
2.1.1 <i>CMS6100 kit components</i>	7
2.1.2 <i>CMS6100 power connection</i>	7
2.1.3 <i>CMS6100 network components</i>	8
2.2 VCMS Deployment	8
2.2.1 <i>System Requirements</i>	8
2.2.2 <i>Distributed Files</i>	8
2.2.3 <i>Example of cloud deployment (ElasticHosts)</i>	9
2.2.4 <i>Configuring CMS</i>	10
CONFIGURATION	11
3.1 Connect to the management console	11
3.1.1 <i>Connected PC/workstation set up</i>	11
3.1.2 <i>Browser connection</i>	12
3.2 Enter Passwords	13
3.2.1 <i>Enter Call Home Password</i>	14
3.2.2 <i>Enter License Key (VCMS only)</i>	14
3.3 Configure Local Network Settings	14
3.3.1 <i>IPv6 configuration</i>	15
3.3.2 <i>Dynamic DNS (DDNS) configuration</i>	16
3.4 Configure Managed Console Servers	17
3.4.1 <i>Connecting CMS/VCMS and console servers on separate private or firewalled networks</i>	20
3.5 Call Home	21
3.5.1 <i>Setting up console server as a management candidate on CMS</i>	22
3.5.2 <i>Call Home to a generic central SSH server</i>	23
3.6 Authorize Automatically Added Users	24
3.7 Upgrade Firmware	25
3.8 Configure Date and Time	26
3.9 Key Exchange	26
3.10 Authentication Configuration	28
3.10.1 <i>Local authentication</i>	28
3.10.2 <i>TACACS authentication</i>	28
3.10.3 <i>RADIUS authentication</i>	29
3.10.4 <i>LDAP authentication</i>	30
3.11 SSL Certificate	31
3.12 Support Report	33
3.13 System Reset	34
STATUS & MANAGED ACCESS	35
4.1 Access Managed Console Servers	35
4.2 Command Console Servers	36
CURRENT STATUS, REPORTS & SYSTEM	39
5.1 Monitor	39
5.1.1 <i>Tactical Overview</i>	39
5.1.2 <i>Hosts</i>	40
5.1.3 <i>Services</i>	41

5.1.4	<i>Problems</i>	42
5.1.5	<i>Connecting with SDT Connector</i>	43
5.2	Reports and system	46
5.2.1	<i>Notifications</i>	46
5.3	Extended Nagios	46
5.3.1	<i>Adding custom checks + scripting/config set up</i>	47
5.3.2	<i>Introducing NagVis</i>	47
5.3.3	<i>Notifications</i>	48
5.3.4	<i>Notification Elevation</i>	49
5.3.5	<i>An example showing you how to add new check programs</i>	50
	SDT CONNECTOR CONFIGURATION	53
6.1	Configuring for SSH Tunneling to Hosts	54
6.2	SDT Connector client installation and configuration	54
6.2.1	<i>SDT Connector client installation</i>	55
6.2.2	<i>Configuring a new gateway in the SDT Connector client</i>	56
6.2.3	<i>Auto-configure SDT Connector client with the user's access privileges</i>	57
6.2.4	<i>Make an SDT connection through the gateway to a host</i>	58
6.2.5	<i>Manually adding hosts to the SDT Connector gateway</i>	59
6.2.6	<i>Manually adding new services to the new hosts</i>	60
6.2.7	<i>Adding a client program to be started for the new service</i>	62
6.2.8	<i>Dial in configuration</i>	63
6.3	SDT Connector to Management Console	64
6.4	SDT Connector - telnet or SSH connect to serially attached devices	65
6.5	Using SDT Connector for out-of-band connection to the gateway	66
6.6	Importing (and exporting) preferences	68
6.7	SDT Connector Public Key Authentication	68
6.8	Setting up SDT for Remote Desktop access	69
6.8.1	<i>Enable Remote Desktop on the target Windows computer to be accessed</i>	69
6.8.2	<i>Configure the Remote Desktop Connection client</i>	71
6.9	SDT SSH Tunnel for VNC	74
6.9.1	<i>Install and configure the VNC Server on the computer to be accessed</i>	74
6.9.2	<i>Install, configure and connect the VNC Viewer</i>	75
6.10	Using SDT to IP connect to hosts that are serially attached to the gateway	77
6.10.1	<i>Establish a PPP connection between the host COM port and console server</i>	77
6.10.2	<i>Set up SDT Serial Ports on console server</i>	81
6.10.3	<i>Set up SDT Connector to ssh port forward over the console server Serial Port</i>	82
6.11	SSH Tunneling using other SSH clients (e.g. PuTTY)	82

APPENDIX

- A. CLI Commands and Source Code
- B. Hardware Specification
- C. Safety and Certifications
- D. Terminology
- E. End User License Agreement
- F. Service and Warranty

This Users Manual walks you through installing and configuring the Opengear's CMS6100 Central Management Appliance and the VCMS Virtual Central Management Appliance. These are referred to generically in this manual as *CMS*.

Once configured, *CMS* allows you to securely manage devices that are serially or network connected to the Opengear console servers (ACM500, CM4000, IM4200, IMG4000 or KCS6000 models) distributed across your network. With *CMS*'s web user interface, you have access to overviews, network maps, status, and detailed service checks for every *Managed Console Server*.

To quickly remedy identified problems, *CMS* gives you the ability to connect directly from the web UI to a *Managed Console Server* or to its downstream *Managed Devices* (computers, routers, switches, power and environmental devices). With a click, your browser will launch the *SDT Connector* Java application and run the correct text-based tool (such as SSH, telnet, SoL) to access the serially *Managed Devices* or graphical tool (such VNC, RDP, HTTPS, HTTP, X11, VMware, RSA, DRAC, iLO) for network *Managed Devices*. *SDT Connector* tunnels this over SSH to the target console server for maximum access security.

CMS has Nagios (www.nagios.org) at its core and is extensible for customized monitoring applications. Nagios is the leading open source IT infrastructure monitoring system so it will be very familiar to many system administrators and network managers.

1.1 Manual Organization

This manual contains the following chapters:

- | | |
|------------------|--|
| 1. Introduction | |
| 2. Installation | Installation of CMS6100 hardware or VCMS virtual appliance software |
| 3. Configuration | Initial configuration and connection to the <i>Managed Console Servers</i> |
| 4. Operation | Details the status displays and reports and connecting with hosts |
| 5. Nagios | Customization of the Nagios monitoring |
| 6. SDT Connector | Extended configuration options for the Java application |

The latest update of this manual can be found online at www.opengear.com/download.html

This documentation mainly covers using your browser to configure and operate the *CMS* and monitor all the connected hosts. However *CMS* runs a Linux 2.6 operating system (www.ucdot.org) and Nagios (www.nagios.org). Experienced Linux/Nagios users may prefer to operate *CMS* at the command line.

Manual Conventions

This manual uses different fonts and typefaces to show specific actions:

Note Text presented like this indicates issues to take note of



Text presented like this highlights important issues and it is essential you read and take heed of these warnings

- Text presented with an arrow head indent indicates an action you should take as part of the procedure

Bold text indicates text that you type, or the name of a screen object (e.g. a menu or button)

Italic text is also used to indicate a text command to be entered at the command line level.

Publishing history

Date	Revision	Update details
Nov 2009	0.9	Initial pre-release (V3.0 firmware)
Aug 2010	1.0	3.2 features + Call Home + VCMS model + Proxy access/manage
June 2011	1.1	

Copyright

©Opengear Inc. 2011. All Rights Reserved.

Information in this document is subject to change without notice and does not represent a commitment on the part of Opengear. Opengear provides this document “as is”, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose.

Opengear may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time. This product could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes may be incorporated in new editions of the publication.

Proper back-up systems and necessary safety devices should be utilized to protect against injury, death or property damage due to system failure. Such protection is the responsibility of the user.



This CMS device is not approved for use as a life-support or medical system.

Any changes or modifications made to this CMS device without the explicit approval or consent of Opengear will void Opengear of any liability or responsibility of injury or loss caused by any malfunction.

This equipment is for indoor use and all the communication wirings are limited to inside of the building.

Opengear's CMS runs on both physical (CMS6100) and virtual (VCMS) platforms. This chapter describes the physical installation of the CMS6100 hardware appliance and the initial deployment and configuration of the VCMS software appliance.

2.1 CMS6100 Installation

2.1.1 CMS6100 kit components



Part # 50903x CMS6100 unit



Part # 440001 AC power cable

Part #539000 Quick Start Guide and CD-ROM

- Unpack your CMS6100 kit and verify you have all the parts shown above, and that they all appear in good working order
- If you are installing your CMS6100 in a rack you will need to attach the rack mounting brackets supplied with the unit, and install the unit in the rack. Take care to heed the Safety Precautions listed in Appendix C
- Proceed to connect your CMS6100 to the network and to power as outlined below



To avoid physical and electrical hazard please read Appendix C on Safety

2.1.2 CMS6100 power connection

The CMS6100 has a built-in universal auto-switching AC power supply. This power supply accepts AC input voltage between 100 and 240 VAC with a frequency of 50 or 60 Hz and the power consumption is less than 40W.

The CMS6100 has an IEC AC power socket located at the rear of the metal case. This IEC power inlet uses a conventional IEC AC power cord, and the power cords for various regions are available as accessories.



Do take note of the warning notice printed on the back of each unit:



To avoid electrical shock the power cord grounding conductor must be connected to ground

2.1.3 CMS6100 network components

The RJ45 10/100 Ethernet LAN port is located on the rear panel of the CMS6100 and is labeled *NETWORK*. All physical connections are made using industry standard Cat5 cabling and connectors.

Ensure you only connect the LAN port to an Ethernet network that supports 10Base-T/100Base-T. For the initial configuration you must connect a PC or workstation to the *CMS*'s network port.

Note Care should be taken in handling all *CMS* products. There are no operator serviceable components inside, so please do not remove covers, and do refer service to qualified personnel

2.2 VCMS Deployment

VCMS can be run as a guest virtual appliance under:

- Linux Kernel-based Virtual Machine (Linux KVM) or
- VMware ESX, VMware ESXi or VMware Server

The host may be a physical machine that you administer, or a managed server or a cloud hosting service from a hosting provider.

2.2.1 System Requirements

At a minimum, the VCMS requires the following reserved resources:

- 500MHz CPU core
- 256MB RAM
- 4GB disk space

In addition, the following virtual devices are required:

- Disk device SATA (VMware) or IDE (Linux KVM)
- E1000 compatible Ethernet NIC, bridged

2.2.2 Distributed Files

The Opengear VCMS is released as a firmware upgrade file (*.bin) and a full image (*.gz). The full image is used for the initial deployment. Firmware upgrade files are used thereafter for upgrades.

Upgrades and full images are available from:

<http://www.opengear.com/firmware/>

Which full disk image you deploy depends on your virtualization solution:

- For Linux KVM, use: `vcms-x.y.z-kvm.hdd.gz`
- For VMware ESX/ESXi, use: `vcms-x.y.z-vmware-ovf.tar.gz`
- For VMware server, use: `vcms-x.y.z-vmware.tar.gz`

Which upgrade file you use also depends on your virtualization solution:

- For Linux KVM, use: `vcms-x.y.z-kvm.bin`
- For VMware, use: `vcms-x.y.z-vmware.bin`

Uncompress the full image using *gunzip*, *Winzip* or similar before deployment.

Refer to the online `faqs.html` for instructions provided by your virtualization management suite to deploy the *ovf*, *vmx* or *hdd* file as appropriate.

2.2.3 Example of cloud deployment (ElasticHosts)

(These instructions are current as of 19 August 2010.)

- Browse to `http://www.elastichosts.com` and create an account at your preferred peer location.
- You may wish to use the 5 day free hosting trial, otherwise add a subscription that meets the reserved resource requirements outlined under System Requirements in this document.

Ensure you set 'Committed data transfer' to 10 GB or higher and/or have a pre-pay balance to cover monthly data transfer. Data usage by VCMS will vary with usage patterns, but will generally not be heavy.

We recommend you purchase a static IP address, otherwise you must also configure *CMS* to use a dynamic DNS service.

- Upload `vcms-x.y.z-kvm.hdd` as a drive using any of the methods described in:

`http://www.elastichosts.com/cloud-hosting/faq#uploadQ`

If you are deploying from a Linux or POSIX compliant system, we recommend using the drive upload tool script:

`http://www.elastichosts.com/downloads/elastichosts-upload.sh`

Your secret API key is available on your Profile page:

```
export EAUTH="xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

Your API endpoint URI is the hostname of account's peer location, preceded by "api.", e.g. for San Antonio Peer 1:

```
export EHURI=https://api.sat-p.elastichosts.com/
```

After setting these in your environment, run:

```
./elastichosts-upload.sh vcms-x.y.z-kvm.hdd
```

- From the Elastic Hosts Control Panel, select Server in 'Add server or drive'. Enter a Name, e.g. "VCMS". Select the Type of 'Boot from existing drive'. Select the Drive you uploaded in the previous step, e.g. "vcms-x.y.z-kvm.hdd". Click Add.
- Click Edit on the Server you have just added. Select the static IP address to use if available, and set the VNC password. Click Start.
- Deployment is now complete. You can now monitor the VCMS boot progress using VNC, or proceed to the next step to begin configuration.

2.2.4 Configuring CMS

Once the virtual appliance has booted, *CMS* configuration is performed by browsing to the IP address of the virtual NIC. The virtual NIC obtains an address using DHCP and has a static IP address of:

192.168.0.1

The default username and password are:

root / default

Configuration instructions for the VCMS are identical to the CMS6100 and are detailed in the following chapter.

This chapter provides instructions for the initial configuration of your *CMS*. You will need to configure the following in order to have a usable unit:

1. Connect to the *CMS* management console
2. Change the default administration password on the *System Administration* page
3. Configure the local network settings on the *Network Settings* page
4. Configure console servers to be managed on the *Managed Console Servers* page
5. Authorize automatically added users on the *User Authorization* page

This chapter also discusses other *Configure* menu items that the *Administrator* may use in managing the *CMS* (such as setting Time/Date and upgrading the firmware).

3.1 Connect to the management console

Your *CMS* comes configured with a default IP address of 192.168.0.1 and Subnet Mask 255.255.255.0

- Directly connect a PC or workstation to the *CMS*

Note For initial configuration it is recommended that the *CMS* be connected directly to a single PC or workstation. However, if you choose to connect your LAN before completing the initial setup steps, it is important that:

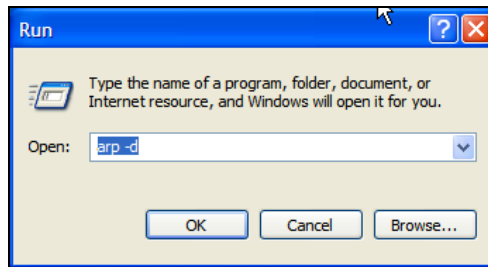
- you ensure there are no other devices on the LAN with an **address of 192.168.0.1**
 - the *CMS* and the PC/workstation are on the same LAN segment, with no interposed router appliances
-

3.1.1 Connected PC/workstation set up

To configure the *CMS* with a browser, the connected PC/workstation should have an IP address in the same range as the *CMS* (e.g. 192.168.0.100):

- To configure the IP Address of your Linux or Unix PC/workstation simply run *ifconfig*
- For Windows PCs (Win9x/Me/2000/XP/Vista/7/NT):
 - Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections**
 - Right click on **Local Area Connection** and select **Properties**
 - Select **Internet Protocol (TCP/IP)** and click **Properties**
 - Select **Use the following IP address** and enter the following details:
 - IP address: **192.168.0.100**
 - Subnet mask: **255.255.255.0**

- If you wish to retain your existing IP settings for this network connection, click **Advanced** and **Add** the above as a secondary IP connection.
- If it is not convenient to change your PC/workstation network address, you can use the *ARP-Ping* command to reset the *CMS* IP address. To do this from a Windows PC:
 - Click **Start** -> **Run** (or select **All Programs** then **Accessories** then **Run**)
 - Type *cmd* and click **OK** to bring up the command line
 - Type *arp -d* to flush the ARP cache
 - Type *arp -a* to view the current ARP cache which should be empty



Now add a static entry to the ARP table and *ping* the *CMS* to have it take up the IP address. In the example below we have a *CMS* with a MAC Address 00:13:C6:00:02:0F (designated on the label on the bottom of the unit) and we are setting its IP address to 192.168.100.23. Also the PC/workstation issuing the *arp* command must be on the same network segment as the *CMS* (i.e. have an IP address of 192.168.100.xxx)

- Type *arp -s 192.168.100.23 00-13-C6-00-02-0F* (Note: for UNIX the syntax is: *arp -s 192.168.100.23 00:13:C6:00:02:0F*)
- Type *ping -t 192.18.100.23* to start a continuous ping to the new IP Address.
- Turn on the *CMS* and wait for it to configure itself with the new IP address. It will start replying to the ping at this point
- Type *arp -d* to flush the ARP cache again

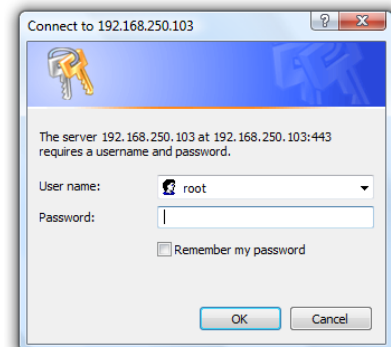
3.1.2 Browser connection

The *CMS* supports all current versions of the popular browsers (Netscape, Internet Explorer, Mozilla Firefox, Gnome, Apple Safari and more)

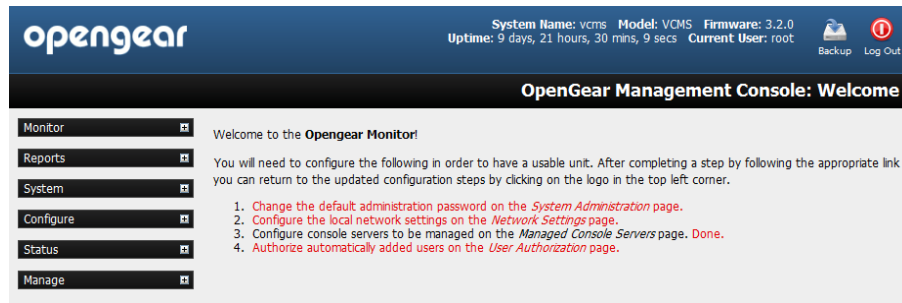
- Activate your preferred browser on the connected PC/workstation and enter **https://192.168.0.1**
- You will be prompted to log in. Enter the default administration username and administration password:

Username: **root**

Password: **default**

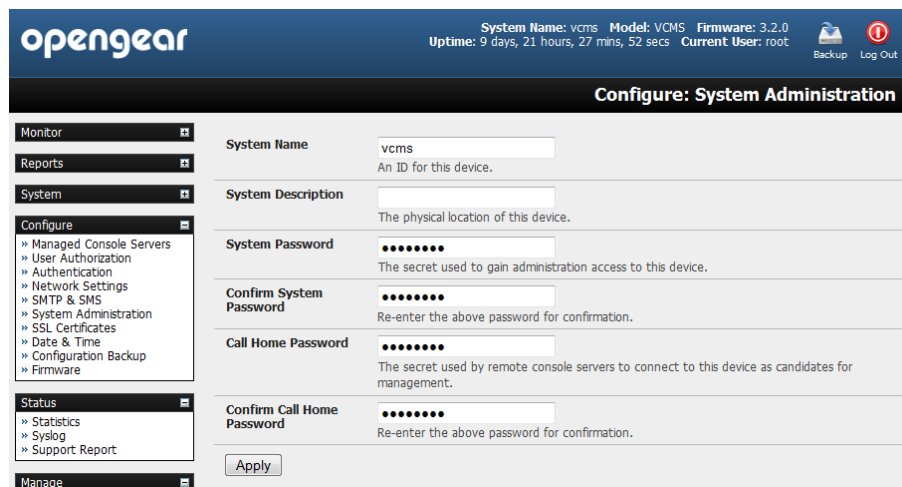


On successful log in you will be presented with a **Welcome** screen.



3.2 Enter Passwords

Initially only the administration user named **root** can log into your *CMS*. The default root password is “**default**” so it is essential that you create a new system password for the root user



- Select **Configure: System Administration**
- Enter a new **System Password** then re-enter it in **Confirm System Password**. This is the new password for **root**, the main administrative user account, so it is important that you choose a complex password, and keep it safe
- At this stage you may also wish to enter a **System Name** and **System Description** for the *CMS* to give it a unique ID and make it simple to identify

Note The System Name can contain from 1 to 64 alphanumeric characters. You can also use the special characters "-", "_", and ".". Similarly there are no restrictions on the characters that can be used in the System Description or the System Password. Each of these can contain up to 254 characters, but only the first eight password characters are used to make the *password hash*.

- Click **Apply**. As you have changed the password you will be prompted to log in again. This time use the new *System Password*

3.2.1 Enter Call Home Password

If you wish to monitor *console servers* that are connected via Call Home, you will need a Call Home password:

- Enter a new **Call Home Password** then re-enter it in **Confirm Call Home Password** and click **Apply**

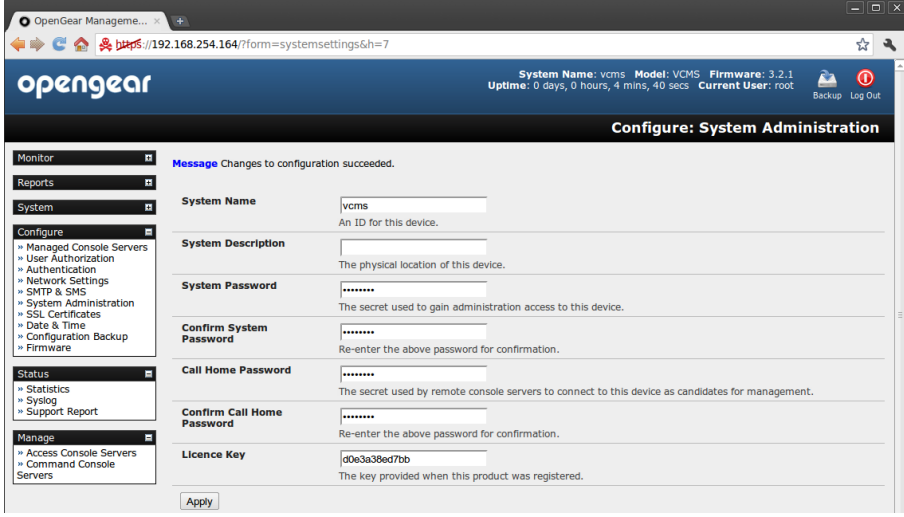
This password is used for a system account used solely for accepting Call Home connections. It is safe to change this password, without affecting currently established Call Home connections.

For details on the Call Home feature, see the section entitled Call Home later in this document.

3.2.2 Enter License Key (VCMS only)

When you commercially license VCMS you will be emailed a *VCMS License Key*. To install the *Key*:

- Copy the *Key* from the email into the **License Key** field and click **Apply**



The screenshot shows the OpenGear Management web interface. The browser address bar shows the URL: 192.168.254.164/?form=systemsettings&h=7. The page title is "opengear". The system status bar shows: System Name: vcms, Model: VCMS, Firmware: 3.2.1, Uptime: 0 days, 0 hours, 4 mins, 40 secs, Current User: root. The main content area is titled "Configure: System Administration". A message at the top says "Changes to configuration succeeded." The form contains the following fields:

- System Name:** vcms (An ID for this device.)
- System Description:** (The physical location of this device.)
- System Password:** (The secret used to gain administration access to this device.)
- Confirm System Password:** (Re-enter the above password for confirmation.)
- Call Home Password:** (The secret used by remote console servers to connect to this device as candidates for management.)
- Confirm Call Home Password:** (Re-enter the above password for confirmation.)
- Licence Key:** d0e3a38ed7bb (The key provided when this product was registered.)

An "Apply" button is located at the bottom of the form.

This *Key* provides you with a commercial license to use the VCMS software appliance, and entitles you to 12 months free technical support and upgrades. You will need to renew your *Key* annually to receive ongoing support and upgrades. If you have to contact support, they will ask you to quote the License Key number from this page.

3.3 Configure Local Network Settings

The next step is to enter an IP address and network settings for the *Network* port on the *CMS*, or to enable its DHCP client so that it automatically obtains an IP address from a DHCP server on the network it is to be connected to

- On the **Configure: Network Settings** menu select the **Network Interface** page then check **DHCP** or **Static** for the **Configuration Method**

- If you selected **Static** you must manually enter the new **IP Address, Subnet Mask, Gateway** and **DNS** server details. This selection automatically disables the DHCP client

- If you selected **DHCP** the *CMS* will look for configuration details from a DHCP server on your management LAN. This selection automatically disables any static address. The *CMS* MAC address can be found on a label on the base plate

Note In its factory default state (with no Configuration Method selected) the *CMS* has its DHCP client enabled, so it automatically accepts any network IP address assigned by a DHCP server on your network. In this initial state, the *CMS* will then respond to both its Static address (192.168.0.1) and its newly assigned DHCP address

- By default the *CMS* Network port auto detects the Ethernet connection speed. However you can use the **Media** menu to lock the Ethernet to 10 Mb/s or 100Mb/s and to Full Duplex (FD) or Half Duplex (HD)

Note If you have changed the *CMS* IP address, you may need to reconfigure your PC/workstation so it has an IP address that is in the same network range as this new address

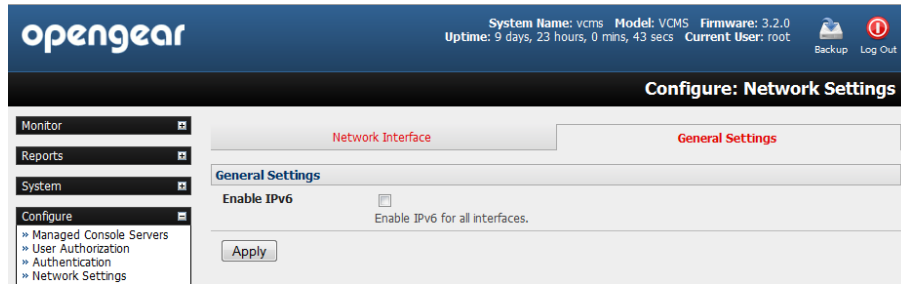
- Click **Apply**
- You will need to reconnect the browser on the PC/workstation that is connected to the *CMS* by entering **http://new IP address**

Note If you selected the DHCP configuration method, and plan to use Call Home **it is strongly recommended** that you use a dynamic DNS service. So at this point, you may also configure dynamic DNS. For detailed setup instructions, see the sections entitled Call Home and Dynamic DNS later in this document.

3.3.1 IPv6 configuration

The *CMS* Network interface can also be configured for IPv6 operation:

- On the **Configure: Network Settings** menu select **General Settings** page and check **Enable IPv6**



3.3.2 Dynamic DNS (DDNS) configuration

With Dynamic DNS (DDNS), an appliance whose IP address is dynamically assigned (and that may change from time to time) can be located using a fixed host or domain name.

- The first step in enabling DDNS is to create an account with the supported DDNS service provider of your choice. Supported DDNS providers include:
 - DyNS www.dyns.cx
 - dyndns.org www.dyndns.org
 - GNUDip gnudip.cheapnet.net
 - ODS www.ods.org
 - TZO www.tzo.com
 - 3322.org (Chinese provider) www.3322.org

Upon registering with the DDNS service provider, you will select a username and password, as well as a hostname that you will use as the DNS name (to allow external access to your machine using a URL).

The Dynamic DNS service providers allow the user to choose a hostname URL and set an initial IP address to correspond to that hostname URL. Many Dynamic DNS providers offer a selection of URL hostnames available for free use with their service. However, with a paid plan, any URL hostname (including your own registered domain name) can be used. By default DDNS is disabled. To enable:

- On the **Configure: Network Settings** menu select the **Network Interface** page then select the DDNS service provider from the drop down **Dynamic DNS** list

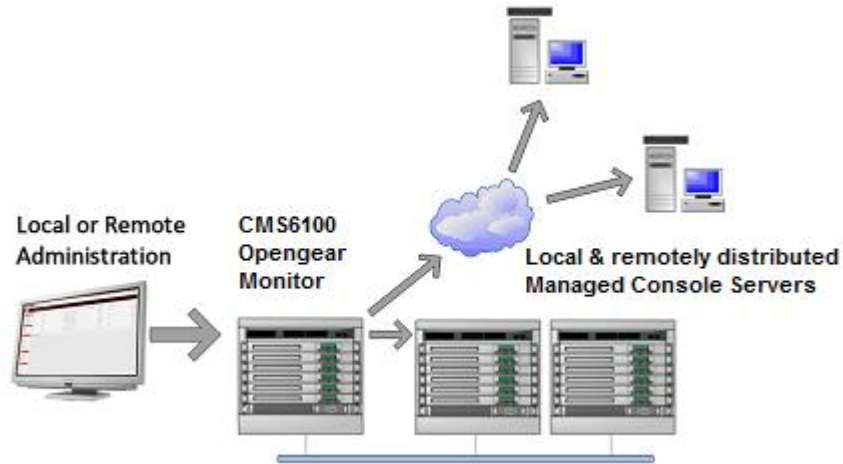
Dynamic DNS	
Dynamic DNS	None - DDNS disabled Update a DNS server when IP address is changed.
DDNS Hostname	The Fully Qualified DNS hostname assigned to this interface.
DDNS Username	The username for the account to manage this interface.
DDNS Password	The password for the account to manage this interface.
Confirm DDNS Password	Re-enter the password for confirmation.
Maximum interval between updates	Maximum interval between updates in days. DDNS update will be sent even if the address has not changed. <i>Defaults to 25.</i>
Minimum interval between checks	Minimum interval between checks for changed addresses, in seconds. Updates will still only be sent if the address has changed. <i>Defaults to 1800.</i>
Maximum attempts per update	Number of times to attempt an update before giving up. <i>Defaults to 3.</i>
<input type="button" value="Apply"/>	

- In **DDNS Hostname** enter the fully qualified DNS hostname for your console server e.g. *your-hostname.dyndns.org*
- Enter the **DDNS Username** and **DDNS Password** for the DDNS service provider account
- Specify the **Maximum interval between updates** - in days. A DDNS update will be sent even if the address has not changed
- Specify the **Minimum interval between checks** for changed addresses - in seconds. Updates will still only be sent if the address has changed
- Specify the **Maximum attempts per update** i.e. the number of times to attempt an update before giving up (defaults to 3)

3.4 Configure Managed Console Servers

CMS maintains public key authenticated SSH connections to each of its *Managed Console Servers*. These connections are used for monitoring, commanding and accessing the *Managed Console Servers* and the *Managed Devices* connected to the *Managed Console Server*.

To manage Local Console Servers, or console servers that are reachable from the *CMS*, the SSH connections are initiated by *CMS*. To manage Remote Console Servers, or console servers that are firewalled, not routable, or otherwise unreachable from the *CMS*, the SSH connections are initiated by the *Managed Console Server* via an initial Call Home connection. This ensures secure, authenticated communications and enables *Managed Console Server* units to be distributed locally on a LAN, or remotely around the world.



➤ Select **Configure: Managed Console Servers**

The *Managed Console Servers* list displays all the console servers which are currently being monitored by the CMS:

- The *Host Last Retrieved* field shows when each console server's configuration information (such as user and *Managed Device* details, alert settings etc) was last updated in the CMS. To update this information check the *Managed Console Server(s)* to be updated and click **Retrieve Hosts**
- The *IP Address/DNS Name* shows how the CMS is accessing this *Managed Console Server*:
 - For a Local Console Server, it shows the network address and SSH server port that CMS is connected to
 - For a Remote Console Server, it shows the local redirected port, and the remote IP address from which the connection has originated. The local redirected port matches the Listening Port as displayed in the Call Home connection on the Remote Console Server

The screenshot shows the 'Configure: Managed Console Servers' page in the Opengear CMS. The top navigation bar includes the Opengear logo, system information (System Name: vcms, Model: VCMS, Firmware: 3.2.0, Uptime: 9 days, 23 hours, 21 mins, 28 secs, Current User: root), and Backup/Log Out buttons. A left sidebar contains navigation menus for Monitor, Reports, System, Configure, Status, and Manage. The main content area is titled 'Configure: Managed Console Servers' and contains the following sections:

- Managed Console Servers:** A table with the following data:

Name	IP Address/DNS Name	Description	Hosts Last Retrieved
<input type="checkbox"/> im4216-25	192.168.254.152:22	im4216-25	Wed Aug 18 16:52:31 2010

 Below the table are 'Retrieve Hosts' and 'Delete' buttons, and a 'Select/unselect all nodes' link.
- Detected Console Servers:**
 - Local Console Servers:** A dropdown menu showing '192.168.254.23'. Below it, text states: 'These console servers have been detected on the local network as candidates for management.' Below this are 'Add' and 'Refresh' buttons.
 - Remote Console Servers:** A dropdown menu showing 'Port 58231 (localhost:58231 → 192.168.254.149)'. Below it, text states: 'These console servers have been detected on the remote network as candidates for management.' Below this are 'Add' and 'Refresh' buttons.
- New Console Server:** A section with the text 'Manually enter the details of a console server to manage.'

The *Detected Console Servers* list displays all the *console servers* which are currently not being monitored by the *CMS*:

- The *Local Console Servers* drop down list shows all the *console servers* which are on the same subnet as the *CMS*, and are not currently being monitored. Click **Refresh** to update
- The *Remote Console Servers* drop down list shows all the *console servers* that have established a Call Home connection (so are candidates) but are not currently being monitored. Click **Refresh** to update

Note When adding a (Detected) Remote Console Server, the IP Address will appear as localhost. This is the loopback listening port created by the Call Home connection

- To add a *console server* to the *Managed Console Servers* list, either select it from the Local or Remote Console Servers drop down list, and click **Add**

Note Alternately you can manually add a *console server* to the *Managed Console Server* list by entering its details in the **New Console Server** section. You may wish to do this if the *console server* is at a remote address, but is reachable from the *CMS* – and you do not wish to use Call Home. Simply specify the SSH server address and port of the *console server* and click **Add**

- Enter the IP Address and SSH Port if these fields have not been auto-completed
- Enter a **Description** and unique **Name** for the *Managed Console Server* you are adding (e.g. “Boston”)

The screenshot shows the OpenGear web interface. At the top, the system name is 'vcms', model is 'VCMS', and firmware is '3.2.0'. The uptime is '10 days, 2 hours, 13 mins, 20 secs' and the current user is 'root'. There are 'Backup' and 'Log Out' links. The main heading is 'Configure: Managed Console Servers'. On the left is a navigation menu with 'Monitor', 'Reports', 'System', 'Configure', and 'Status'. The 'Configure' menu is expanded to show 'Managed Console Servers', 'User Authorization', 'Authentication', 'Network Settings', 'SMTP & SMS', 'System Administration', 'SSL Certificates', 'Date & Time', 'Configuration Backup', and 'Firmware'. The main form has the following fields: 'IP Address/DNS Name' with value 'localhost' and a description 'The managed console server's IP address or DNS name.'; 'SSH Port' with value '57452' and a description 'The managed console server's SSH server port.'; 'Description' with value 'Engineering Test Room 3' and a description 'A brief description of the managed console server.'; 'Name' with value 'Boston' and a description 'Short name to identify the managed console server.'; and 'Remote Root Password' which is masked with dots and has a description 'The root password set on the managed console server. This password will not be stored, but used to propagate SSH keys and then forgotten.' An 'Apply' button is at the bottom of the form.

- Enter the **Remote Root Password** (i.e. System Password that has been set on this *Managed Console Server*)

Note This password is used by the *CMS* to propagate auto generated SSH keys and then forgotten. This password will not be stored

- Click **Apply**.

The *CMS* will now set up secure SSH connections to and from the *Managed Console Server*. “Boston” will be included in the *Managed Console Servers* list (which displays all the console servers which are currently being monitored by the *CMS*). And the *CMS* will retrieve its *Managed Devices*, user account details and configured alerts.

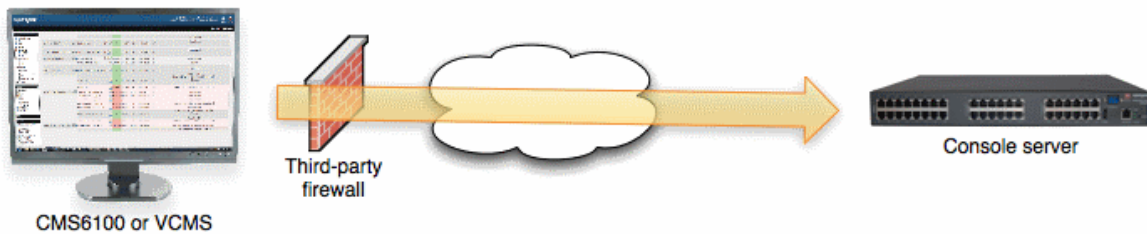
3.4.1 Connecting CMS/VCMS and console servers on separate private or firewalled networks

To set up the Often, console servers or the CMS itself will be on a private, firewalled network and unable to connect to each other.

Whatever the topology, if either CMS can SSH to the console server, or the console server can SSH to CMS, the CMS can manage the console server.

There are three main scenarios:

I. The console server has a public address, the CMS has a private or firewalled address.



In this case, ensure the third-party firewall allows outbound connections the distributed console server's SSH port (outbound destination TCP port 22). This is the default behavior of most firewalls. The distributed console server will not be detected by the CMS, but can be added manually at the CMS using *Configure -> Managed Console Servers -> New Console Server -> Add* as described above.

II. The console server has a private or firewalled address and the CMS has a public address.



This is a common for console servers using cellular connections. On the console server, use *Serial & Network -> Call Home* to connect the console server to the CMS public address. The distributed console server will then be detected by the CMS and can be added using *Configure -> Managed Console Servers -> Remote Console Servers* as described in the next section

III. Both the console server and CMS have a private or firewalled address.

There are two options in this scenario:

(a) Make CMS accessible by the console servers

This is usually the preferable option if there are multiple console servers with private or firewalled addresses - common with console servers using cellular connections connecting to a CMS on a central private operations network.



Configure the third-party firewall to port forward (PAT) from its public address to the CMS's private address, targeting TCP port 22. The public forwarded port may be any port, e.g. 2222.

Configure the CMS with the external IP or DNS address of the third-party firewall. Connect to the CMS command line using SSH and run:

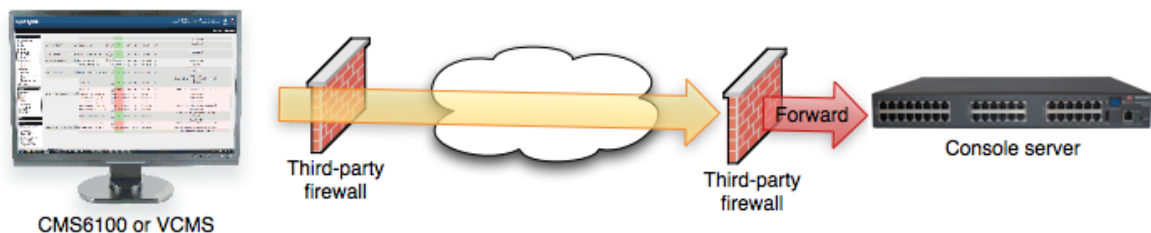
```
config -s config.cms.address=4.3.2.1 config -s config.cms.sshport=2222
```

.. where 4.3.2.1 is public address of the third-party firewall, and 2222 is the public forwarded port.

Once this is done, the managed console server can Call Home to the CMS using the forwarded port as per scenario 2 above.

(b) Make the console server accessible by CMS

Configure the third-party firewall to port forward (PAT) from its public address to the console server's private address, targeting TCP port 22.



The public forwarded port may be any port, e.g. 1022, 2022 - this allows for multiple console servers to be managed behind a single firewall. Once this is done, add the managed console server to CMS as described in the earlier section.

3.5 Call Home

To manage a console server, the *CMS* must be able to connect to it using SSH. Sometimes this is not possible, e.g. if a console server is behind a third party firewall, or has a private, non-routable IP address. This is often the case when the console server is connected via a Cellular Modem connection.

In this situation, a Call Home connection is initiated from the console server to the *CMS*. This creates an SSH listening port on the *CMS*, that is redirected back across the Call Home connection to the console server. This allows the *CMS* to connect to the console server using SSH, and thereby manage it.

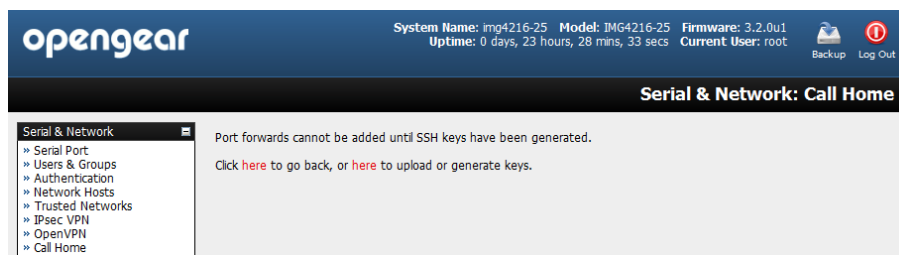
Any *console server* with Firmware V3.2 or later, has *Call Home* support.

Note To Call Home, the console server must be able to connect to the *CMS* using SSH. It is also important that the *CMS* has a static IP address. If this is not possible, you must configure the *CMS* to use a dynamic DNS service (refer Dynamic DNS section later in this manual).

3.5.1 Setting up console server as a management candidate on CMS

To set up the *console server* as a Call Home management candidate on the *CMS*:

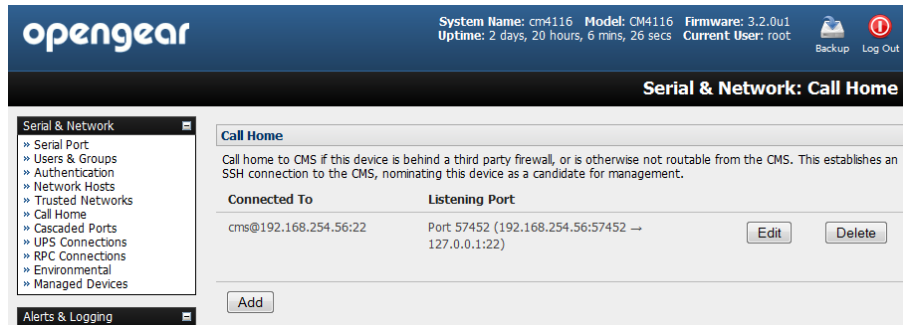
- Browse to the *console server's* management console and select **Call Home** on the **Serial & Network** menu



- If you have not already generated or uploaded an SSH key pair for this *console server*, you will need to do so before proceeding. Details on this procedure are outlined in the Opengear User Manual in the section entitled *Automatically generate and upload SSH keys*
- Click **Add**



- Enter the IP address or DNS name (e.g. the dynamic DNS address) of the *CMS*
- Enter the Password that you configured on the *CMS* as the **Call Home Password**
- Click **Apply**



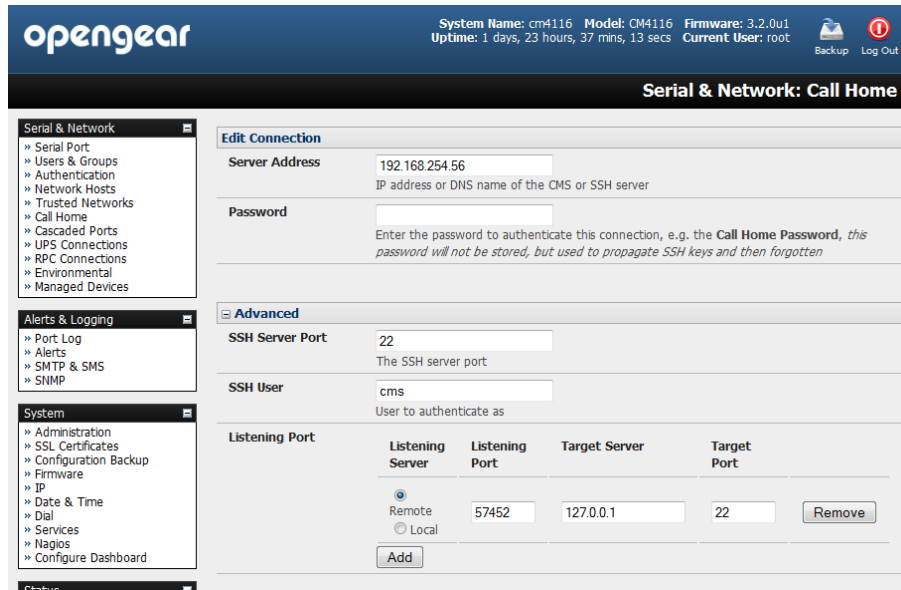
These steps initiate the Call Home connection from the *console server* to the *CMS*. An SSH listening port is created on the *CMS*, and the *console server* is set up as a candidate to be accepted as a *Managed Console Server*.

Once the candidate has been accepted on the *CMS* (as outlined in the previous section), an SSH tunnel to the *console server* is then redirected back across the Call Home connection. The *console server* has now become a *Managed Console Server* and the *CMS* can connect to and monitor it through this tunnel.

3.5.2 Call Home to a generic central SSH server

If you are connecting to a generic SSH server (not a *CMS*), you may configure *Advanced* settings:

- Enter the **SSH Server Port** and SSH User to authenticate as
- Enter the details for the SSH port forward(s) to create



By selecting *Listening Server*, you may create a **Remote** port forward from the Server to this unit, or a **Local** port forward from this unit to the Server:

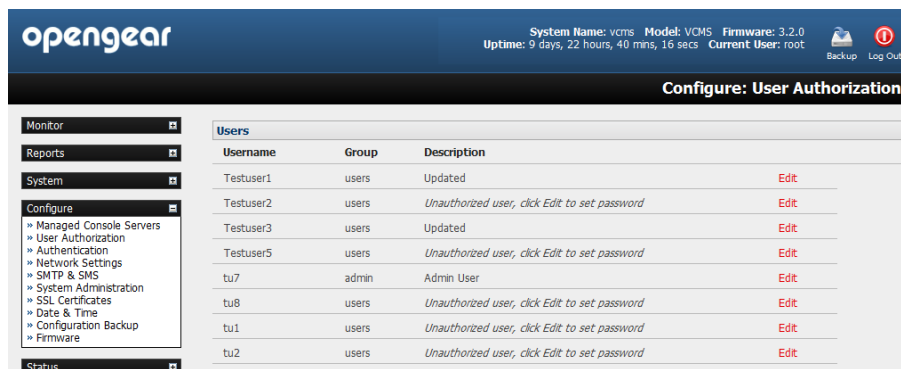
- Specify a Listening Port to forward from, leave this field blank to allocate an unused port
- Enter the Target Server and Target Port that will be the recipient of forwarded connections

3.6 Authorize Automatically Added Users

CMS retrieves and aggregates user accounts that are locally configured on *Managed Console Servers*. This way, a user with accounts across multiple *Managed Console Servers* has a single pane of glass from which they can monitor and access all the *Managed Console Servers* and subordinate *Managed Devices* the user has permissions to access.

Once a user account has been retrieved for the first time, it must be explicitly authorized on the CMS before that user can log in to the CMS.

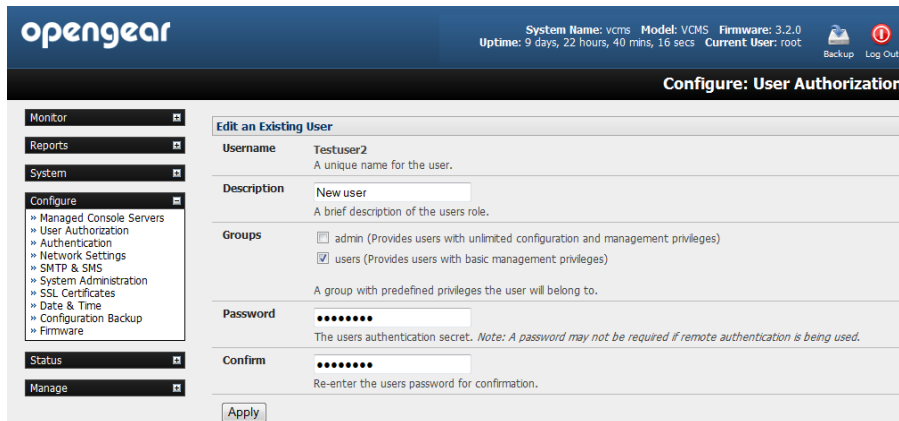
- Select **Configure: User Authorization**. This will display a list of all the users which have been set up on all the *Managed Console Servers* currently being monitored by the CMS



- For any user, select **Edit** and enter a new password that will be used by that user when accessing CMS
- At this stage, you can also modify the *Group* membership and *Description* associated with that particular user. Users in the **user** group can access the *Current Status* menus, the *Reports* menus and the *System* menu (basically all the monitoring screens) whereas users in the **admin** group have this access plus the ability to reconfigure the CMS using the *Configure* menu

Note Group membership on the CMS is distinct from group members on *Managed Console Servers*. Groups set on CMS, control access to the CMS only, and are not retrieved from or propagated to *Managed Console Servers*.

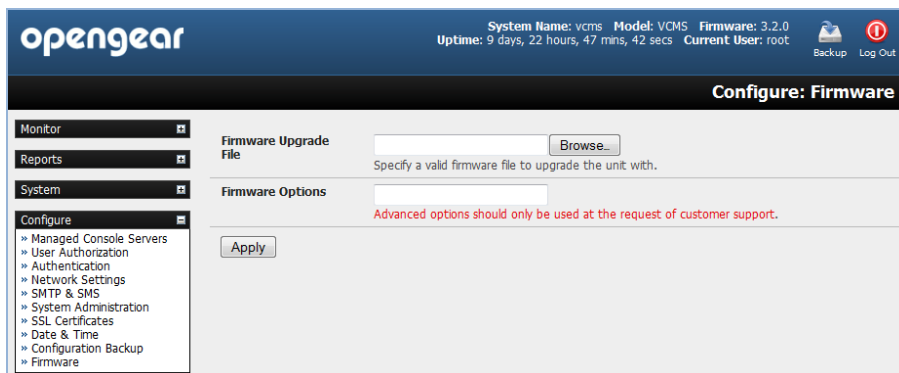
- Click **Apply**



3.7 Upgrade Firmware

Before upgrading, you should ascertain if you are already running the most current firmware in your gateway. Your CMS will not allow you to upgrade to the same or an earlier version.

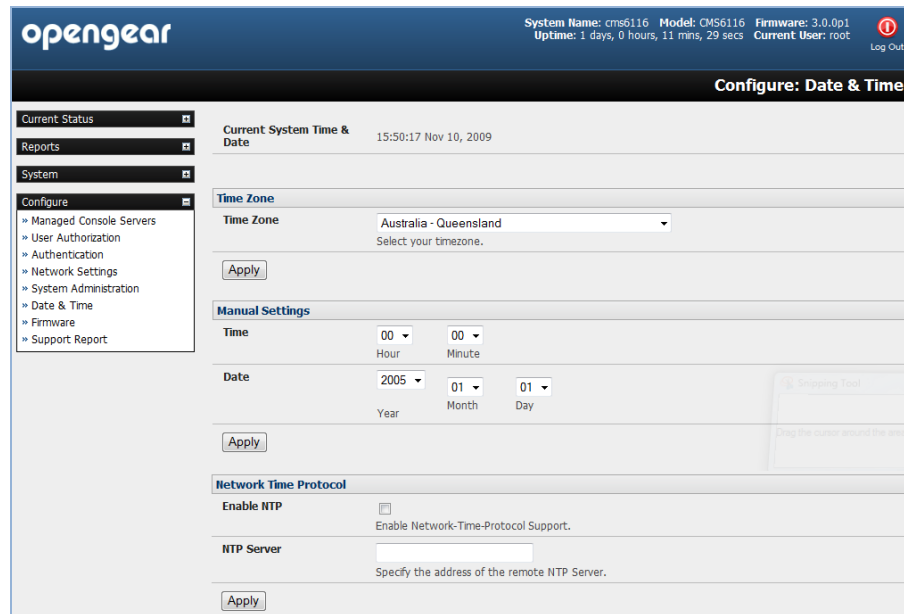
- The *Firmware* version is displayed in the header of each page or you can select **Configure: Support Report** and note the *Firmware Version* listed there
- To upgrade, first download the latest firmware image from `ftp://ftp.opengear.com` –
 - `cms6100-x.y.x.bin` for CMS6100 appliances
 - `vcms-x.y.z.bin` for VCMS installs
- Save this downloaded firmware image file on to a system on the same subnet as the CMS



- Also download and read the `release_notes.txt` for the latest information
- To upload the firmware image file to your CMS select **Configure: Firmware**
 - **Browse** the local subnet and locate the downloaded file
 - Click **Apply** and the CMS appliance will undertake a soft reboot and commence upgrading the firmware. This process will take several minutes
- After the firmware upgrade has completed, click **here** to return to the Management Console. Your CMS will have retained all its pre-upgrade configuration information

3.8 Configure Date and Time

It is recommended that you set the local Date and Time in the *CMS* as soon as it is configured. Many of the *CMS* logging features use the system time for time-stamping log entries, while certificate generation depends on a correct *Timestamp* to check the validity period of the certificate



- Select the **Configure: Date & Time** menu option
- Set your appropriate region/locality in the **Time Zone** selection box (not UTP) and click **Apply**
- Manually set the **Year, Month, Day, Hour** and **Minute** using the **Date** and **Time** selection boxes, then click **Apply**

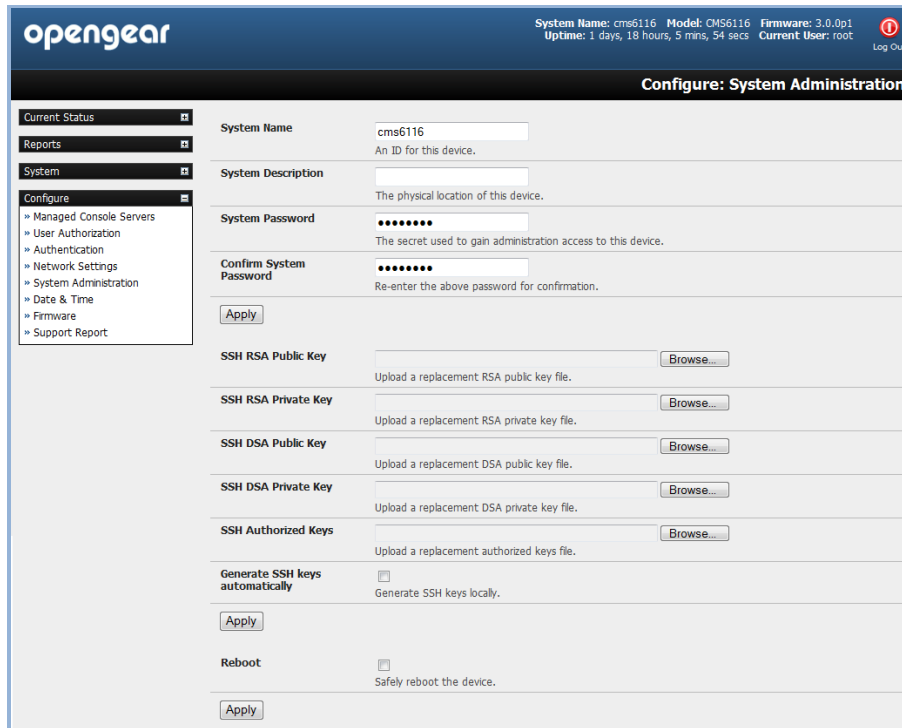
Alternately, the *CMS* can synchronize its system time with a remote time server using the Network Time Protocol (NTP). Configuring the NTP time server ensures that the *CMS* clock will be accurate soon after the Internet connection is established. To set the system time using NTP:

- Select the **Enable NTP** checkbox under **Network Time Protocol**
- Enter the IP address of the remote **NTP Server** and click **Apply**

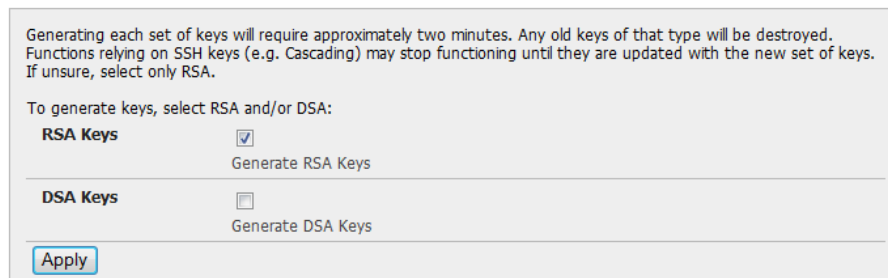
3.9 Key Exchange

The *CMS* automatically generates the SSH keys used to communicate with each of its *Managed Console Servers*.

However, you can additionally generate or manually enter RSA or DSA key pairs and SSH Authorized keys that will be used for other SSH connections with the *CMS*.



- Select **Configure: System Administration**
- Check **Generate SSH keys automatically** and click **Apply**



Next you must select whether to generate keys using RSA and/or DSA (and if unsure check only **RSA Keys**). Generating each set of keys will require approximately two minutes and the new keys will destroy any old keys of that type that may have previously been uploaded. To generate keys:

- Select **RSA Keys** and/or **DSA Keys**
- Click **Apply**
- Once the new keys have been successfully generated simply click **here** to return

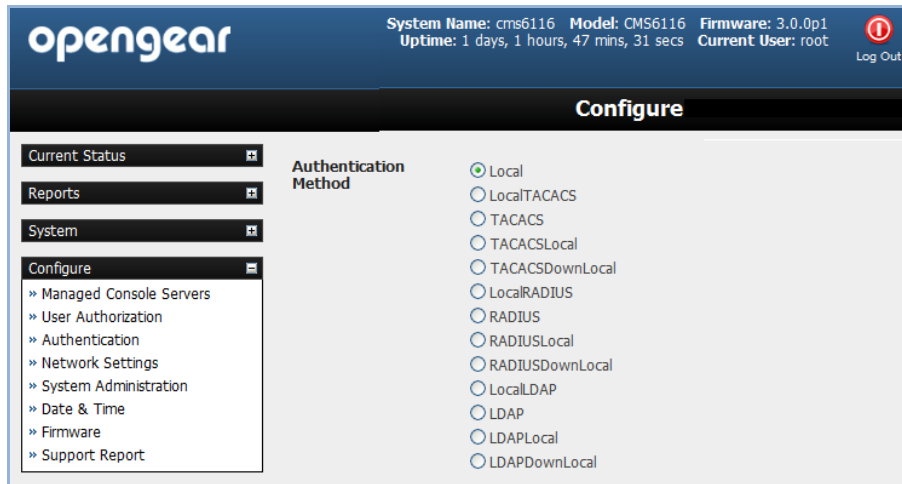
Alternately if you have a RSA or DSA key pair you can manually upload them to the CMS:

- Select **Configure: System Administration** on the CMS
- Browse to the location you have stored RSA (or DSA) Public Key and upload it to **SSH RSA (DSA) Public Key**
- Browse to the stored RSA (or DSA) Private Key and upload it to **SSH RSA (DSA) Private Key**

- Click **Apply**

3.10 Authentication Configuration

Authentication can be performed locally, or remotely using an *LDAP*, *Radius* or *TACACS+* authentication server. The default authentication method for the *CMS* is *Local*.



Any authentication method that is configured will be used for authentication of any user who attempts to log in through HTTPS or SSH to the *CMS*.

The *CMS* can be configured to the default (**Local**) or an alternate authentication method (**TACACS**, **RADIUS** or **LDAP**) with the option of a selected order in which local and remote authentication is to be used:

Local TACACS /RADIUS/LDAP: Tries local authentication first, falling back to remote if local fails

TACACS /RADIUS/LDAP Local: Tries remote authentication first, falling back to local if remote fails

TACACS /RADIUS/LDAP Down Local: Tries remote authentication first, falling back to local if the remote authentication returns an error condition (e.g. the remote authentication server is down or inaccessible)

3.10.1 Local authentication

- Select **Configure: Authentication** and check **Local**
- Click **Apply**

3.10.2 TACACS authentication

Perform the following procedure to configure the TACACS+ authentication method to be used whenever the *CMS* or any of its serial ports or hosts is accessed:

- Select **Configure: Authentication** and check **TACAS**, **LocalTACACS**, **TACACSLocal** or **TACACSDownLocal**

TACACS	
Authentication and Authorisation Server Address	<input type="text"/> Comma separated list of remote authentication and authorisation servers.
Accounting Server Address	<input type="text"/> Comma separated list of remote accounting servers. If unset, Authentication and Authorisation Server Address will be used.
Server Password	<input type="text"/> The shared secret allowing access to the authentication server.
Confirm Password	<input type="text"/> Re-enter the above password for confirmation.

- Enter the **Server Address** (IP or host name) of the remote Authentication/Authorization server. Multiple remote servers may be specified in a comma separated list. Each server is tried in succession.
- In addition to multiple remote servers, you can also enter separate lists of Authentication/Authorization servers and Accounting servers. If no Accounting servers are specified, the Authentication/Authorization servers are used instead.
- Enter the **Server Password**
- Click **Apply**. TACAS+ remote authentication will now be used for all user access to *CMS* and serially or network attached devices

TACACS+ The Terminal Access Controller Access Control System (TACACS+) security protocol is a recent protocol developed by Cisco. It provides detailed accounting information and flexible administrative control over the authentication and authorization processes. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting services independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. There is a draft RFC detailing this protocol. Further information on configuring remote TACACS+ servers can be found at the following sites:

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a00800eb6d6.html

http://cio.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt2/sctplus.htm

3.10.3 RADIUS authentication

Perform the following procedure to configure the RADIUS authentication method to be used whenever the *CMS* or any of its serial ports or hosts is accessed:

- Select **Configure: Authentication** and check **RADIUS, LocalRADIUS, RADIUSLocal** or **RADIUSDownLocal**

RADIUS	
Authentication and Authorisation Server Address	<input type="text"/> Comma separated list of remote authentication and authorisation servers.
Accounting Server Address	<input type="text"/> Comma separated list of remote accounting servers. If unset, Authentication and Authorisation Server Address will be used.
Server Password	<input type="text"/> The shared secret allowing access to the authentication server.
Confirm Password	<input type="text"/> Re-enter the above password for confirmation.

- Enter the **Server Address** (IP or host name) of the remote Authentication/Authorization server. Multiple remote servers may be specified in a comma separated list. Each server is tried in succession
- In addition to multiple remote servers, you can also enter separate lists of Authentication/Authorization servers and Accounting servers. If no Accounting servers are specified, the Authentication/Authorization servers are used instead
- Enter the **Server Password**
- Click **Apply**. RADIUS remote authentication will now be used for all user access to *CMS* and serially or network attached devices

RADIUS

The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises as an access server authentication and accounting protocol. The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms. Further information on configuring remote RADIUS servers can be found at the following sites:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/d4fe8248-eeed-49e4-88f6-9e304f97fetc.mspx>

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml

<http://www.freeradius.org/>

3.10.4 LDAP authentication

Perform the following procedure to configure the LDAP authentication method to be used whenever the *CMS* or any of its serial ports or hosts is accessed:

- Select **Configure: Authentication** and check **LDAP, LocalLDAP, LDAPLocal** or **LDAPDownLocal**

LDAP	
Server Address	<input type="text"/> Comma separated list of remote servers.
Server Password	<input type="password"/> The shared secret allowing access to the authentication server.
Confirm Password	<input type="password"/> Re-enter the above password for confirmation.
LDAP Base DN	<input type="text"/> The distinguished name of the search base. For example: dc=my-company,dc=com
LDAP Bind DN	<input type="text"/> The distinguished name to bind to the server with. The default is to bind anonymously.
<input type="button" value="Apply"/>	

- Enter the **Server Address** (IP or host name) of the remote Authentication server. Multiple remote servers may be specified in a comma separated list. Each server is tried in succession.
- Enter the **Server Password**

Note To interact with LDAP requires that the user account exists on our *CMS* to work with the remote server i.e. you can't just create the user on your LDAP server and not tell the *CMS* about it. You need to add the user account.

- Click **Apply**. LDAP remote authentication will now be used for all user access to *CMS* and serially or network attached devices

LDAP The Lightweight Directory Access Protocol (LDAP) is based on the X.500 standard, but significantly simpler and more readily adapted to meet custom needs. The core LDAP specifications are all defined in RFCs. LDAP is a protocol used to access information stored in an LDAP server. Further information on configuring remote RADIUS servers can be found at the following sites:

http://www.ldapman.org/articles/intro_to_ldap.html

<http://www.ldapman.org/servers.html>

<http://www.linuxplanet.com/linuxplanet/tutorials/5050/1/>

<http://www.linuxplanet.com/linuxplanet/tutorials/5074/4/>

3.11 SSL Certificate

The *CMS* uses the Secure Socket Layer (SSL) protocol for encrypted network traffic between itself and a connected user. During the connection establishment the *CMS* has to expose its identity to the user's browser using a cryptographic certificate. The default certificate that comes with the *CMS* device upon delivery is for testing purposes only and should not be relied on for secured global access.



The System Administrator should not rely on the default certificate as the secured global access mechanism for use through the Internet

- Activate your preferred browser and enter `https:// IP address`. Your browser may respond with a message that verifies the security certificate is valid but notes that it is not necessarily verified by a certifying authority. To proceed you need to click *yes* if you are using Internet Explorer or select *accept this certificate permanently (or temporarily)* if you are using Mozilla Firefox.
- You will then be prompted for the *Administrator* account and password as normal.

However, it is recommended you generate and install a new base64 X.509 certificate that is unique for a particular *CMS*.

To do this the *CMS* must be enabled to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a Certification Authority (CA). A certification authority verifies that you are the person who you claim you are, and signs and issues a SSL certificate to you. To create and install a SSL certificate for the *CMS*:

- Select **System: SSL Certificate** and fill out the fields as explained below:

Common name This is the network name of the *CMS* once it is installed on the network (usually the fully qualified domain name). It is identical to the name that is used to access the *CMS* with a web browser (without the “`http://`” prefix). In case the name given here and the actual network name differ, the browser will pop up a security warning when the *CMS* is accessed using HTTPS

Organizational Unit This field is used for specifying to which department within an organization the *CMS* belongs

Organization The name of the organization to which the *CMS* belongs

Locality/City The city where the organization is located

State/Province The state or province where the organization is located

Country The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the USA. (Note: the country code has to be entered in CAPITAL LETTERS)

Email The email address of a contact person that is responsible for the *CMS* and its security

Challenge Password Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is 4 characters

Confirm Challenge Password Confirmation of the Challenge Password

Key length This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the *CMS* during connection establishment

- Once this is done, click on the button **Generate CSR** which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the **Download** button
- Send the saved CSR string to a Certification Authority (CA) for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA)
- Upload the certificate to the *CMS* using the **Upload** button as shown below

After completing these steps the *CMS* will have its own certificate that is used for identifying the *CMS* to its users.

The screenshot shows the OpenGear web interface. At the top, the system name is 'cms6116', model is 'CMS6116', and firmware is '3.0.0p2'. The current user is 'root'. The page title is 'Configure: SSL Certificates'. On the left, there is a navigation menu with options like 'Current Status', 'Reports', 'System', 'Configure', 'Managed Console Servers', 'User Authorization', 'Authentication', 'Network Settings', 'System Administration', 'SSL Certificates', 'Date & Time', 'Firmware', and 'Support Report'. The main content area contains a form with the following fields:

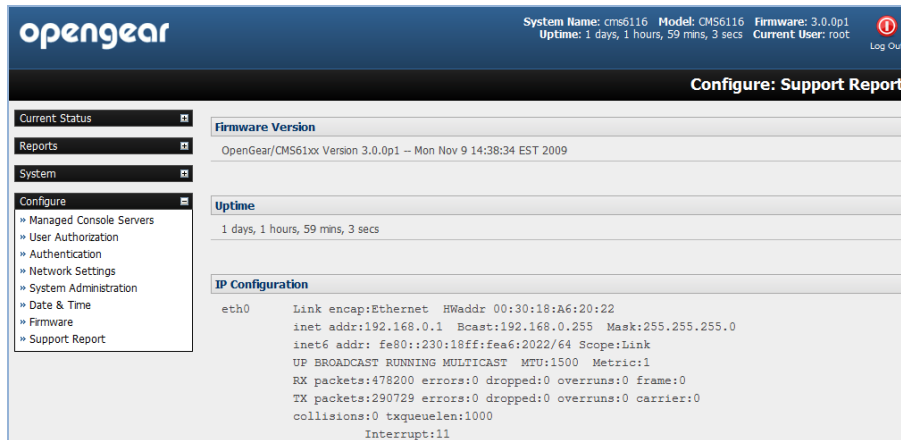
Common name	192.168.250.103 The full canonical name for this device.
Organizational unit	testing The group overseeing this device.
Organization	testing The name of the organization to which the device belongs.
Locality/City	brisbane The City where the organization is located.
State/Province	queensland The State or Province where the organization is located.
Country	AU The country where the organization is located.
Email	tamar.mccullough@opengear.com The email address of a contact person for this device.
Challenge Password	***** An optional (dependant on CA) password.
Confirm Password	***** Confirmation of the challenge password.
Key Length (bits)	512 Length of generated key in bits.

At the bottom of the form, there are two buttons: 'Download' and 'Cancel CSR'.

3.12 Support Report

The Support Report provides useful status information that will assist the OpenGear technical support team to solve any problems you may experience with your *CMS*.

If you do experience a problem and have to contact support, ensure you include the Support Report with your email support request. The Support Report should be generated when the issue is occurring, and attached in plain text format.



- Select **Configure: Support Report** and you will be presented with a status snapshot
- Save the file as a text file and attach it to your support email

3.13 System Reset

The *Administrator* can reboot or reset the gateway to default settings.

A *soft* reset is affected by:

- Selecting **Reboot** in the **Configure: System Administration** menu and clicking **Apply**



The *CMS* reboots with all settings (*e.g.* the assigned network IP address) preserved. However this *soft* reset does disconnect all users and ends any SSH sessions that had been established.

A *soft* reset will also be affected when you switch OFF power from the *CMS*, and then switch the power back ON. However, if you cycle the power and the unit is writing to flash you could corrupt or lose data, so the software reboot is the safer option.

A *hard* erase (*hard reset*) is effected by:

- Pushing the *Erase* button on the rear panel **twice**. A ball point pen or bent paper clip is a suitable tool for performing this procedure. Do not use a graphite pencil. Depress the button gently **twice** (within a couple of second period) while the unit is powered ON.

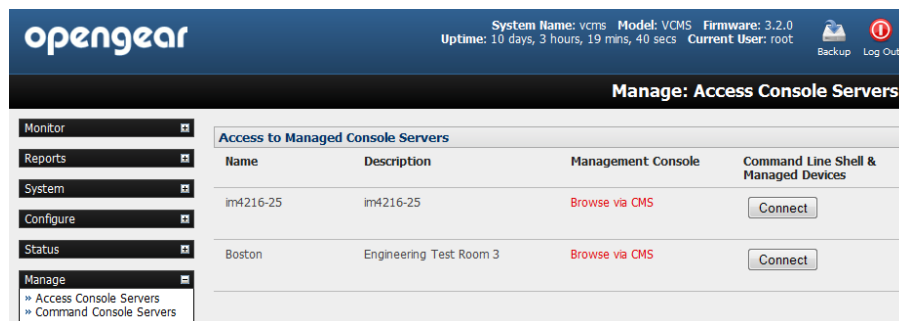
This will reset the *CMS* back to its factory default settings and clear the *CMS*'s stored configuration information.

The *hard* erase will clear all custom settings and return the unit back to factory default settings (*i.e.* the IP address will be reset to 192.168.0.1). You will be prompted to log in and must enter the default administration username and administration password (Username: **root** Password: **default**)

The CMS provides a selection of paths for accessing *Managed Console Servers* (and attached *Managed Devices*). SDT Connector access points are embedded in many of the Monitor screens and with the SDT Connector applet running on your client PC you can *point-n-click* connect specific applications on your client PC to the *Managed Console Servers* and *Managed Devices* (covered in Chapters 5 and 6). This chapter covers the browser and SDT proxy connection facilities; and the scheduled batch command facilities embedded in the CMS itself.

4.1 Access Managed Console Servers

CMS provides a simple way to access *Managed Console Servers*.



- Click **Manage -> Access Console Servers**. The *console servers* that the current user has access to are listed under *Access to Managed Console Servers*.

Note If the current user has 'user' or 'admin' group access on a console server, they are deemed to have access to that console server

There are then two paths to access *console servers*:

- In the **Management Console** column click **Browse via CMS** to connect to the *console server's* web Management Console UI.

This connection is proxied via *CMS*, so the *console server* is still accessible even if firewalled, failed over to a private connection or otherwise inaccessible from the WAN. When browsing via a proxied connection, the following message is display in the Management Console header:

This Console Server is being accessed via CMS [Click here to return to CMS](#)

- Click **Connect** in the *Command Line Shell & Managed Devices* column. This will download a configured *SDT Connector* applet to your client PC and connect to the console server.

This also launches a command line shell session through the *SDT Connector* connection to the console server.

As with Management Console connections, this connection is proxied via *CMS*.

The *SDT Connector* uses the credentials of the current user to connect to the console server. The *Managed Devices* and hosts that the current user has access to are retrieved, and displayed in the left hand column. For each host, connection buttons for the services the current user is permitted to access are available in the right hand Services pane. Click a service's button to launch a connection to it via *CMS*

Note When you click **Connect** it opens *SDT Connector* and launches a shell to the console server. this is exactly the same as when you click **Connect** for the "Command Line Shell" service on Monitor - > Services screen as described in Chapter 6

4.2 Command Console Servers

Using *CMS* you may schedule batch commands to run on one or more *Managed Console Servers*.

- Select **Manage: Command Console Servers** to display the list of *Managed Console Servers* that can be commanded by the current user. These are the *console servers* on which the current user has 'admin' group privileges

Note Only if the current user has 'admin' group privileges on a *console server*, are they deemed to be allowed to command that *console server*

- Select the **Managed Console Server(s)** to command
- Select the **Command** to schedule:
 - **Reboot:** Soft reboot the selected console servers
 - **Shutdown:** Halt the selected console servers. After being shut down, manual intervention in the form of a physical power cycle is required before the console server becomes available again
 - **Firmware Upgrade:** Perform a firmware upgrade, loading firmware from a given http:// URL, e.g. <http://www.opengear.com/firmware/acm500x-x.y.z.flash>
 - **Modify User:** Specify the *Username* to modify, the *Modification* to apply. Currently supported *Modifications* are *Lock Account* and *Unlock Account* where *Lock Account* prevents a user from logging in to the *console server* itself, or accessing *Managed Devices* using *SDT Connector* via the console server. Use *Unlock Account* to undo this modification.

The screenshot shows a web interface for scheduling commands on console servers. It is divided into two main sections: 'Command' and 'Arguments'.
The 'Command' section has four radio button options:

- Reboot:** Safely reboot the selected console servers.
- Shutdown:** Safely halt the selected console servers.
- Firmware Upgrade:** Perform a firmware upgrade on the selected console servers.
- Modify User:** Modify a user account on the selected console servers. This option is selected with a blue dot.

The 'Arguments' section contains:

- Modification:** A dropdown menu currently set to 'Lock Account'. Below it is the text: 'The modification to apply to the selected user account.'
- Username:** An empty text input field. Below it is the text: 'Username of the account to modify.'

- Click **Schedule Command**. The results of the schedule commands are displayed under **Monitor: Services** in the *Status Information* of the *Managed Console Server's Console server command*

Monitor: Services

- Monitor
 - Tactical Overview
 - Map
 - Hosts
 - Services
 - Host Groups
 - Summary
 - Grid
 - Service Groups
 - Summary
 - Grid
 - Problems
 - Services
 - Unhandled Services
 - Hosts
 - Unhandled Hosts
 - Outages
- Reports
- System
- Configure
 - Managed Console Servers
 - User Authorization
 - Authentication
 - Network Settings
 - SMTP & SMS
 - System Administration

Current Network Status		Host Status Totals				Service Status		
Up	Down	Unreachable	Pending	Ok	Warning	Unknown		
4	0	0	0	9	0	0		
All Problems		All Types		All Problems				
0		4		0				

Last Updated: Thu Aug 19 19:52:58 EDT 2010
 Updated every 90 seconds
 Nagios® 3.1.2 - www.nagios.org
 Logged in as root

View History For all hosts
 View Notifications For All Hosts
 View Host Status Detail For All Hosts

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Boston	Alert 1 - Login	PENDING	N/A	0d 1h 36m 2s+	1/1	Service is not scheduled to be checked... TCP OK - 0.020 second response time on port 23 Connect
	Command line shell	OK	2010-08-19 19:51:18	0d 1h 34m 41s	1/1	
	Console server command	PENDING	N/A	0d 1h 36m 2s+	1/1	Service is not scheduled to be checked...
	Firmware version	OK	2010-08-19 19:50:18	0d 1h 35m 41s	1/1	OpenGear/CM41xx Version 3.2.0u1 -- Mon Aug 16 01:00:12 EST 2010

Chapter 5 Monitor, Reports, System & Nagios Extensions

5.1 Monitor

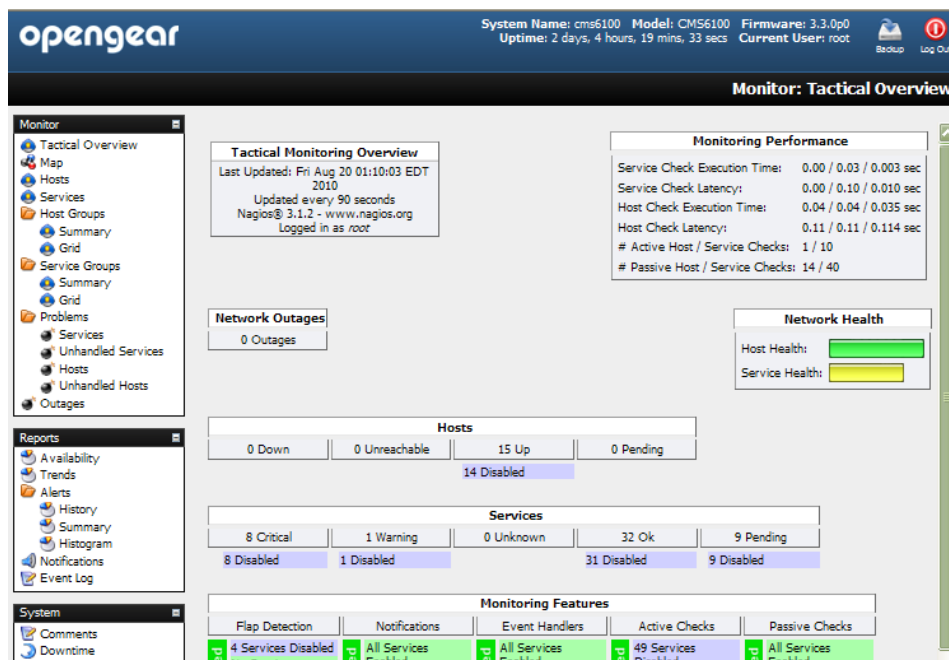
This section covers the Monitor menu options. All status screens under Monitor automatically refresh every 30 seconds, so there is no need to reload them (and this refresh time can be changed to even lower values in the *CMS Nagios* configuration files).

5.1.1 Tactical Overview

This screen gives you an overview of the current status of the monitored services and hosts.

Look at the *Hosts* and you see that you are currently monitoring 15 hosts (i.e. these will be the *Managed Console Servers* and their attached *Managed Devices*) and they are all *Up*. In the *Services* line you see that many of the services you are monitoring are disabled and report various levels of warning/critical status.

As a summary the *Network Health - Host* health bar on right is filled completely with green, indicating all configured hosts are OK while the *Service* health bar is filled with yellow.



Most fields on this page are links to more specific views e.g. if you wanted to see more details about your monitored services you can either click on the *8 Critical* field within the *Services* table (as shown below) or select *Problems: Services* from the Monitor menu:

The screenshot shows the Nagios web interface with the following components:

- System Information:** System Name: cms6100, Model: CMS6100, Firmware: 3.3.0p0, Uptime: 2 days, 4 hours, 50 mins, 48 secs, Current User: root.
- Host Status Totals:**

Up	Down	Unreachable	Pending
15	0	0	0
All Problems		All Types	
0		15	
- Service Status Totals:**

Ok	Warning	Unknown	Critical	Pending
32	1	0	8	9
All Problems		All Types		
9		50		
- Current Network Status:** Last Updated: Fri Aug 20 01:30:44 EDT 2010, Updated every 90 seconds, Nagios® 3.1.2 - www.nagios.org, Logged in as root.
- Display Filters:**
 - Host Status: All
 - Types: Any
 - Host Properties: Critical
 - Service Status: Active Checks Disabled
- Service Status Details For All Hosts:**

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ACM5004 - CVS	Permitted Service - 1494/tcp - ica	CRITICAL	2010-08-20 01:28:53	2d 1h 30m 32s	1/1	Connection refused
	Permitted Service - 23/tcp - telnet	CRITICAL	2010-08-20 01:28:53	2d 1h 30m 32s	1/1	Connection refused
	Permitted Service - 3389/tcp - rdp	CRITICAL	2010-08-20 01:27:53	2d 1h 28m 32s	1/1	Connection refused
	Permitted Service - 5900/tcp - vnc	CRITICAL	2010-08-20 01:29:53	0d 21h 33m 17s	1/1	Connection refused
CM4001 - CVS	Permitted Service - 1494/tcp - ica	CRITICAL	2010-08-20 01:29:33	2d 1h 27m 19s	1/1	Connection refused
	Permitted Service - 23/tcp - telnet	CRITICAL	2010-08-20 01:29:33	2d 1h 27m 19s	1/1	Connection refused
	Permitted Service - 3389/tcp - rdp	CRITICAL	2010-08-20 01:28:33	2d 1h 25m 21s	1/1	Connection refused
	Permitted Service - 5900/tcp - vnc	CRITICAL	2010-08-20 01:30:32	0d 21h 32m 50s	1/1	Connection refused

5.1.2 Hosts

This screen shows the details of all the monitored hosts (i.e. all the *Managed Console Servers* in your distributed network and all the *Managed Devices* that are attached to them at the local and remote sites). You will see all configured hosts and have the choice to select one to get more information about it.

The screenshot shows the Nagios web interface. At the top, system information includes: System Name: cms6100, Model: CMS6100, Firmware: 3.3.0p0, Uptime: 2 days, 4 hours, 45 mins, 42 secs, and Current User: root. The page title is 'Monitor: Hosts'. The sidebar on the left contains sections for Monitor (Tactical Overview, Map, Hosts, Services, Host Groups, Service Groups, Problems, Services, Unhandled Services, Hosts, Unhandled Hosts, Outages), Reports (Availability, Trends, Alerts, History, Summary, Histogram, Notifications, Event Log), and System (Comments, Downtime). The main content area features 'Current Network Status' (Last Updated: Fri Aug 20 01:27:08 EDT 2010, Updated every 90 seconds, Nagios® 3.1.2 - www.nagios.org, Logged in as root), 'Host Status Totals' (Up: 15, Down: 0, Unreachable: 0, Pending: 0), and 'Service Status Totals' (Ok: 32, Warning: 1, Unknown: 0, Critical: 8, Pending: 9). Below these are 'Host Status Details For All Host Groups' and a table listing individual hosts.

Host	Status	Last Check	Duration	Status Information
ACMS004	UP	2010-08-20 01:26:54	2d 1h 26m 56s	OK
ACMS004 - CVS	UP	2010-08-20 01:26:54	2d 1h 26m 56s	OK
ACMS004 - Eaton	UP	2010-08-20 01:26:54	2d 1h 26m 56s	OK
ACMS004 - baytech	UP	2010-08-20 01:26:54	2d 1h 24m 56s	OK
CM4001	UP	2010-08-20 01:26:32	2d 1h 23m 43s	OK
CM4001 - Baytech	UP	2010-08-20 01:26:32	2d 1h 21m 45s	OK
CM4001 - CVS	UP	2010-08-20 01:26:32	2d 1h 23m 43s	OK
CM4001 - Level_2_Rm44_Port_1_EMD	UP	2010-08-20 01:26:32	2d 1h 23m 43s	OK
CM4116	UP	2010-08-20 01:26:51	2d 1h 22m 15s	OK
IM4004	UP	2010-08-20 01:26:31	2d 1h 25m 37s	OK

As we saw in the Tactical screen, here are the fifteen hosts we monitor right now. You can see basic information about each host on this page:

- **Host** shows all the hosts which are configured (If this field is marked red, the host itself is down, if it's just grey the server is up and reachable with ping, and if green then the host is OK)
- **Status** shows the current status of the hosts (OK = green, Warning = yellow, Critical = red, Unknown = orange)
- **Last Check** shows date and time when it has been checked the last time
- **Duration** shows for how long the service in this status
- **Status Information** is the output from the check program itself

And if you want to know more about a single host you select it by its name and you are redirected to a more detailed page about it.

5.1.3 Services

Similar to the *Hosts* view, *Services* shows the details of all the monitored screens. Again you see all configured services and have the choice to select one to get more information about it.

The screenshot shows the OpenGear Nagios Services monitor interface. At the top, the system name is 'cms6100', model is 'CMS6100', and firmware is '3.3.0p0'. The uptime is '2 days, 4 hours, 34 mins, 45 secs' and the current user is 'root'. The page title is 'Monitor: Services'.

Current Network Status:
 Last Updated: Fri Aug 20 01:14:41 EDT 2010
 Updated every 90 seconds
 Nagios® 3.1.2 - www.nagios.org
 Logged in as root

Host Status Totals:

Up	Down	Unreachable	Pending
15	0	0	0
All Problems		All Types	
0		15	

Service Status Totals:

Ok	Warning	Unknown	Critical	Pending
32	1	0	8	9
All Problems		All Types		
9		50		

Service Status Details For All Hosts:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ACMS004	Alert 1 - test	WARNING	2010-08-18 00:28:33	2d 0h 46m 32s	1/1	1 alert current User root performed a logout on port02 (/dev/port02)
	Command line shell	OK	2010-08-20 01:13:53	2d 1h 14m 28s	1/1	TCP OK - 0.025 second response time on port 23 Connect
	Console server command	PENDING	N/A	2d 1h 8m 13s+	1/1	Service is not scheduled to be checked...
	Firmware version	OK	2010-08-20 01:12:53	2d 1h 12m 28s	1/1	OpenGear/ACMS00x: Version 3.3.0p0 -- Wed Aug 18 07:52:39 EST 2010 TCP OK - 0.017 second response time on port 80
	Management Console	OK	2010-08-20 01:11:53	2d 1h 13m 28s	1/1	Connect

The screen fields are also similar to *Hosts* (and all being well, the screen will all be grey and green - indicating there are no service problems). Only one additional field is displayed:

- **Attempt** shows how many attempts were needed for the check

5.1.4 Problems

These screens show the current problems with the hosts and services being monitored e.g. whenever a service reports a failure (like a connection alerts as shown below) you will get the information on this page.

The screenshot shows the OpenGear Nagios Services monitor interface with a 'WARNING' status for 'Alert 1 - test' on host ACMS004. The system name is 'cms6100', model is 'CMS6100', and firmware is '3.3.0p0'. The uptime is '2 days, 5 hours, 7 mins, 59 secs' and the current user is 'root'. The page title is 'Monitor: Services'.

Current Network Status:
 Last Updated: Fri Aug 20 01:47:54 EDT 2010
 Updated every 90 seconds
 Nagios® 3.1.2 - www.nagios.org
 Logged in as root

Host Status Totals:

Up	Down	Unreachable	Pending
15	0	0	0
All Problems		All Types	
0		15	

Service Status Totals:

Ok	Warning	Unknown	Critical	Pending
32	1	0	8	9
All Problems		All Types		
9		50		

Display Filters:

Host Status Types: All
 Host Properties: Any
 Service Status Types: All Problems
 Service Properties: Any

Service Status Details For All Hosts:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ACMS004	Alert 1 - test	WARNING	2010-08-18 00:28:33	2d 1h 19m 46s	1/1	1 alert current User root performed a logout on port02 (/dev/port02)

The browser refreshes every 30 seconds so you get the current list of failed services. Also CMS checks the hosts and services at regular (programmable) intervals. So if an error was reported, but on the next

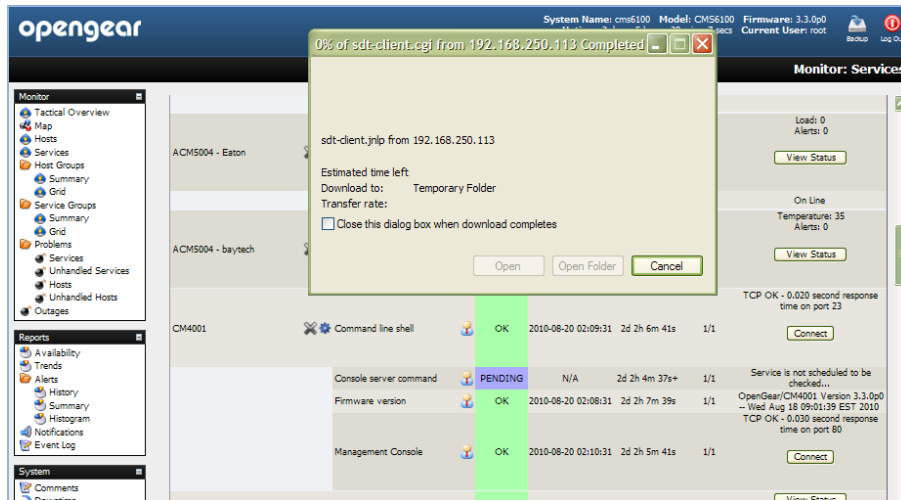
check reports that everything is okay for that service, the status will be updated. For example, *CMS* connects to each of the configured *Managed Console Servers* and their attached *Managed Devices* using all the services it was told are configured. If a service (like HTTP or SSH access) is momentarily disabled on a particular *Managed Device*, then the *Problems: Current Status: Services* will report a *Connection Refused* error, and this report will be removed when the service has been re-enabled.

5.1.5 Connecting with SDT Connector

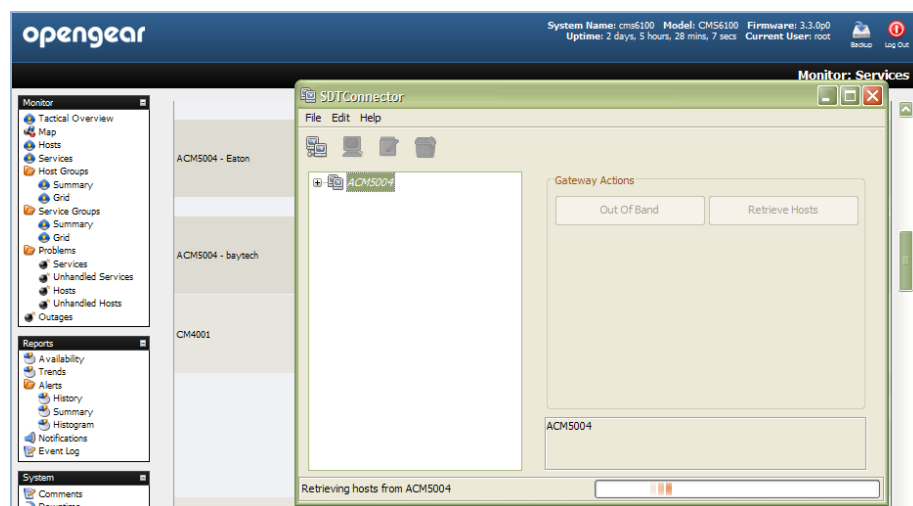
Many of the hosts displayed on the Monitor: Services screen have a **Connect**, **Manage Power**, **View Status** or **View Logs** button in the *Status Information* field as shown below.

ACM5004 - Eaton	UPS Eaton Log	OK	2010-08-20 02:06:52	2d 2h 5m 50s	1/1	Load: 0 Alerts: 0	View Status
	UPS Eaton Power	OK	2010-08-20 02:07:51	2d 2h 7m 50s	1/1	On Line	
ACM5004 - baytech	RPC baytech	OK	2010-08-20 02:06:52	2d 2h 5m 50s	1/1	Temperature: 35 Alerts: 0	View Status
CM4001	Command line shell	OK	2010-08-20 02:06:31	2d 2h 3m 39s	1/1	TCP OK - 0.020 second response time on port 23	Connect
	Console server command	PENDING	N/A	2d 2h 1m 35s+	1/1	Service is not scheduled to be checked...	
	Firmware version	OK	2010-08-20 02:05:32	2d 2h 4m 37s	1/1	OpenGear/CM4001 Version 3.3.0p0 -- Wed Aug 18 09:01:39 EST 2010 TCP OK - 0.080 second response time on port 80	
	Management Console	OK	2010-08-20 02:07:31	2d 2h 2m 39s	1/1		Connect
CM4001 - Baytech	RPC Baytech	OK	2010-08-20 02:07:31	2d 2h 2m 39s	1/1		View Status

- Click on this button and you will be connected to the relevant screen on that *Managed Device* or *Managed Console Server*
 - Your browser will download a configured *SDT Connector* Java application from the *CMS* and it will run on your computer. This *SDT Connector* is preconfigured with the *gateway* details (that being the *Managed Console Server*) and the host details (which will be one of the *Managed Devices* attached to the *Managed Console Server*, or the *Managed Console Server* itself)

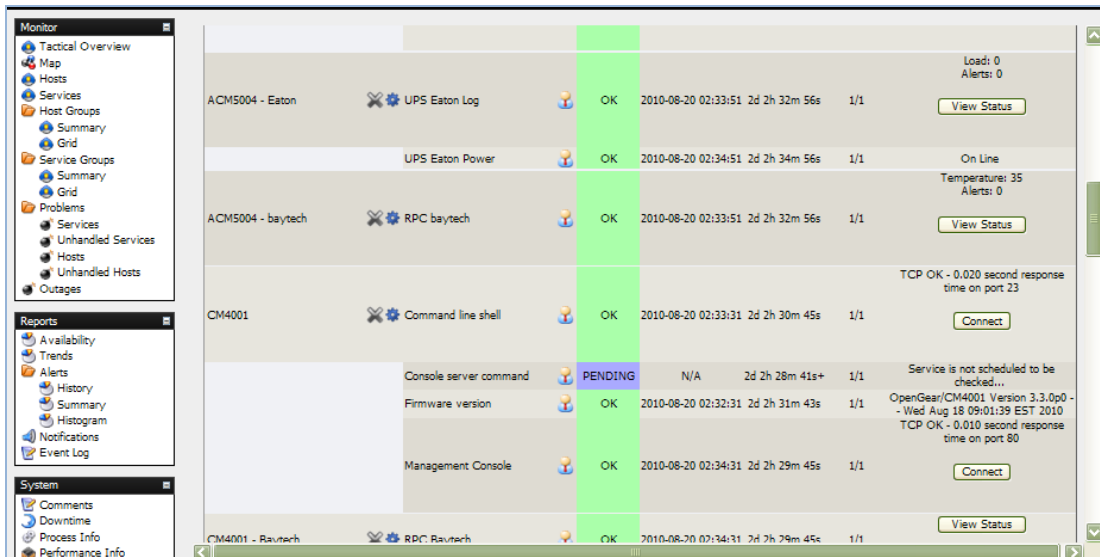


- *SDT Connector* will then log you into the SSH server embedded in the *Managed Console Server*, using the credentials of the user currently logged in to the *CMS*. Then, if appropriate, it will SSH tunnel connect you through to the target *Managed Device*

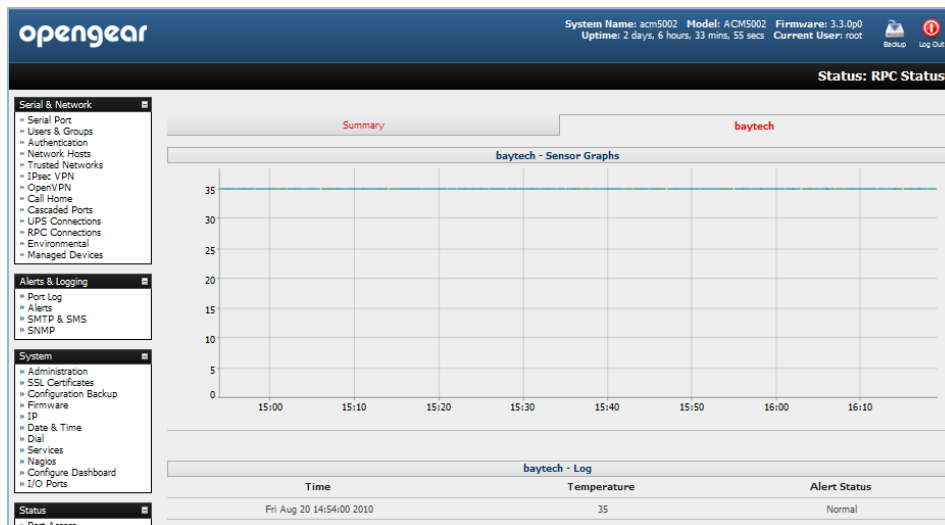


- Lastly *SDT Connector* will automatically load and run the appropriate application (*service*) on your computer that is needed to connect to the appropriate *Managed Device* or *Managed Console Server* screen.

This *service* could be a text-based console tool (such as SSH, telnet, SoL) or a browser/graphical/network tools (such as VNC, RDP, HTTPS, HTTP, X11, VMware, DRAC, iLO).



For example, if you clicked on the **View Status** button of the Monitor:ServiceScreen, shown above, to get an update on the status of the BayTech RPC that is managed by a remote *Managed Console Server* named acm5002), the *SDT Connector* would launch and connect you the acm5002 *Managed Console Server*, and be presented with the *RPC: Status* display for the BayTech power device (shown below)

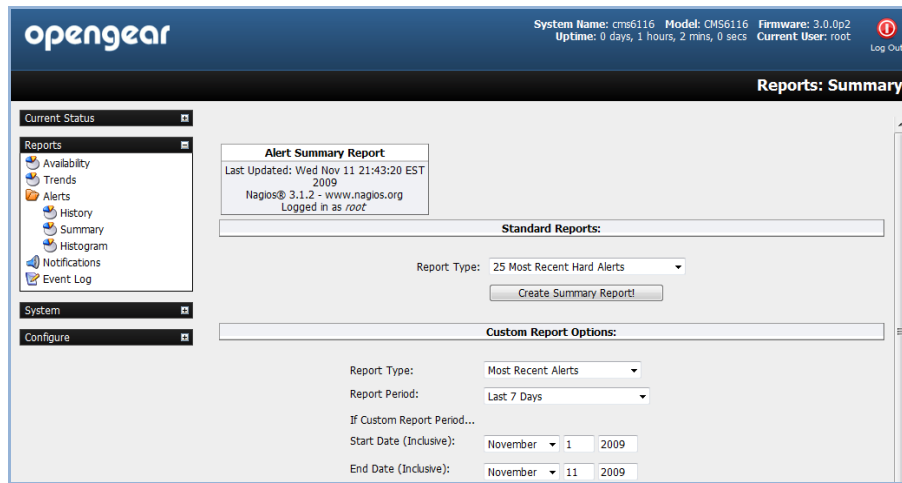


- So this connection is fully *point 'n click*

Note The location of the application which needs to be loaded and the appropriate commands to invoke it (e.g. which browser or SSH client software service will run) will vary from computer to computer. So you may need to configure the *SDT Connector* Java application with this information as detailed in Chapter 5. Alternatively, if you have a permanent *SDT Connector* client already installed on your computer, then when your browser downloads the preconfigured *SDT Connector* Java application it will, by default, use the *service* configurations already set up on your installed client.

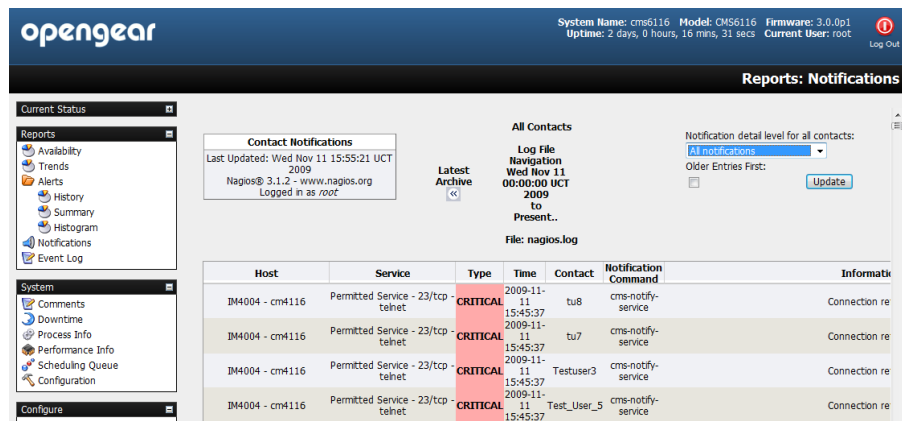
5.2 Reports and system

The *CMS* provides all the standard Nagios customizable reports and logs:



5.2.1 Notifications

All Opengear *console servers* can be configured to send email and SMS alert notifications in event of an alert trigger event (pattern match on serial port, elevated temperature, door open etc). However, the Nagios features in *CMS* allow more sophisticated notification.



Basically, host and service *notifications* occur when a hard state change occurs, or when a host or service remains in a non-OK state for a specified period of time specified (since the last notification was sent out). *CMS* also allows for escalation of these notifications. For details on configuring notifications and escalations refer to the next section.

5.3 Extended Nagios

At the core of *CMS's* monitoring is Nagios (<http://www.nagios.org>) - the leading open source host, service and network monitoring tool. Nagios lets you manage different types of services and hosts running on different operating systems like Linux, Windows, and Solaris. It's flexible in configuration and can be extended. It's configured within text files and managed with a web browser.

When you do a basic *CMS* installation, you get a set of Nagios check programs which are automatically configured to let you start monitoring all the hosts and services on your *Managed Console Servers* and all their *Managed Devices*.

However, you can also extend the Nagios configuration to your special needs:

- You can add more check programs (refer to <http://www.nagiosexchange.org> where other developers have available their check programs for download)
- You can write your own in the supported programming languages (Bash, Perl)
- You can even have these new checks (NRPE and NCSA) running on your remote *Managed Console Servers* (to take load off the *CMS* and reduce network traffic)
- If you want, you can setup notifications with elevations
- You can extend the graphical web views of your managed hosts using NagVis

5.3.1 Adding custom checks + scripting/config set up

To submit additional check results to the *CMS*, make an NSCA connection to the loopback interface using *send_nasca* on the *Managed Console Server*:

```
send_nasca -H 127.0.0.1 -c /etc/config/node-send_nasca.cfg
```

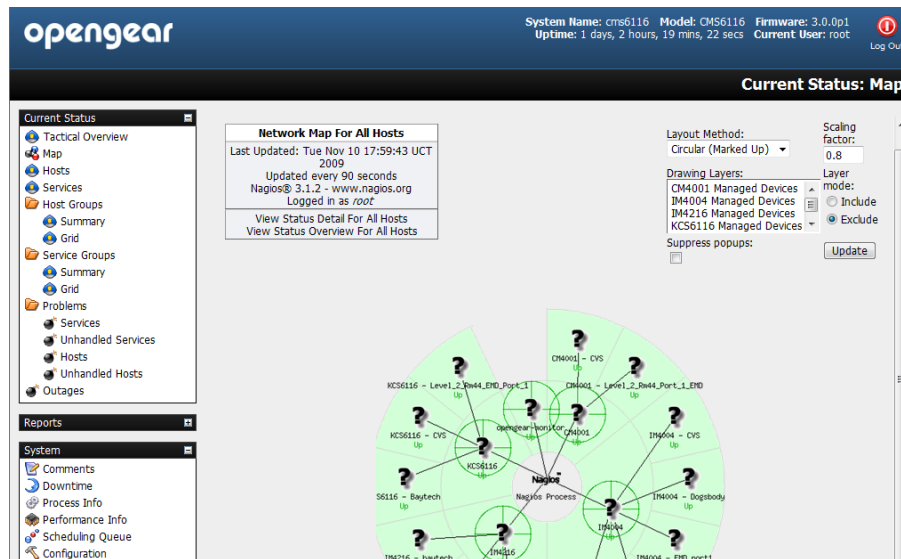
This port is securely tunneled back to the *CMS* NSCA server e.g. on the *Managed Console Server*, run:

```
printf "My Managed Host\tService Description\t0\tOK\n" | send_nasca -H  
127.0.0.1 -c /etc/config/node-send_nasca.cfg
```

The Nagios server on the *CMS* must have a service configured to receive the check result. Place custom Nagios configuration files in */etc/config/nagios/user/* on the *CMS*, then verify and (if successful) reload Nagios configuration with:

```
nagios -v /etc/config/nagios/nagios.cfg && pkill -HUP nagios
```

5.3.2 Introducing NagVis



The standard Monitor: Map display in Nagios presents a basic image of the monitored host and service states. However, the NagVis1 add-on gives you a powerful flexible visualization tool for customizing the status display against any background image you choose.

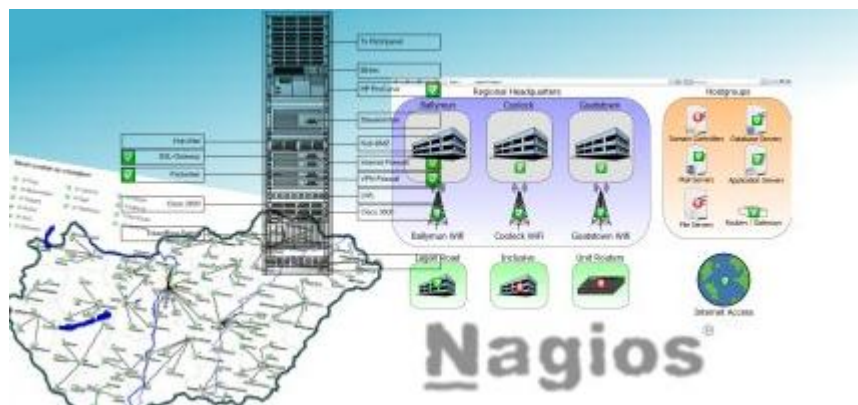
NagVis can display different icons, depending on the state of the object (red for the CRITICAL state, yellow for WARNING, green for OK, and a question mark on a gray background for UNKNOWN). If an acknowledgment was set, this is indicated by a green button with a picture of a worker on it.

There are different icons for hosts and services. In the default template, host icons are rectangular and service icons are round. A finished NagVis *map* might present using a geographical map, or a photo of the server room as a background. In addition to hosts and services, host and service groups can also be integrated into a NagVis display, as well as additional maps. Thus a geographical overview map could be used for the start page, which has an icon for each location monitored that links to a detailed NagVis map specifically for that location.

If an icon contains several states, as is the case for host and service groups, for instance, NagVis displays the state with the highest priority. CRITICAL has a higher priority than WARNING, WARNING trumps UNKNOWN, UNKNOWN gets more attention than an acknowledgment, and OK has the lowest priority of all. If any host in a host group assumes the CRITICAL state, this is shown accordingly for the entire host group.

For hosts and host groups, NagVis offers you the choice of having only host states considered in determining the state that is displayed, or having the services dependent on these hosts are included as well (see page 394). In the latter case, a red stop light is displayed if even a single service of a host is in the critical state

For details on using NagVis refer www.nagvis.org



5.3.3 Notifications

All Opengear *console servers* can be configured to send email and SMS alert notifications in event of an alert trigger event (e.g. a pattern match on serial port, elevated temperature or door open event). However the Nagios features in *CMS* allow more sophisticated notification.

The screenshot shows the Nagios web interface. At the top, it displays system information: 'System Name: cms6116', 'Model: CMS6116', 'Firmware: 3.0.0p1', and 'Uptime: 2 days, 0 hours, 16 mins, 31 secs'. The current user is 'root'. The main content area is titled 'Reports: Notifications' and shows a table of notifications. The table has columns for Host, Service, Type, Time, Contact, Notification Command, and Information. The notifications listed are all 'CRITICAL' and relate to 'Permitted Service - 23/tcp - telnet' on host 'IM4004 - cm4116'. The contacts involved are 'tu8', 'tu7', 'Testuser3', and 'Test_User_5'. The notification command for all is 'cms-notify-service'.

With Nagios, host and service notifications occur when a hard state change occurs, or when a host or service remains in a hard non-OK state and the time specified (by the `<notification_interval>` option in the host or service definition) has passed since the last notification was sent out.

Each host and service definition has a `<contact_groups>` option that specifies what contact groups receive notifications for that particular host or service. Contact groups can contain one or more individual contacts.

When Nagios sends out a host or service notification, it will notify each contact that is a member of any contact groups specified in the `<contactgroups>` option of the service definition. Nagios realizes that a contact may be a member of more than one contact group, so it removes duplicate contact notifications before it does anything.

Just because there is a need to send out a host or service notification doesn't mean that any contacts are going to get notified. There are several filters that potential notifications must pass before they are deemed worthy enough to be sent out. Even then, specific contacts may not be notified if their notification filters do not allow for the notification to be sent to them. For example if the host or service is in a period of scheduled downtime. If it is in a scheduled downtime, no one gets notified.

The Nagios software can be configured to notify you of problems and recoveries pretty much anyway you want: pager, cell phone, email, instant message, audio alert, electric shocker, etc. How notifications are sent depend on the notification commands that are defined in your object definition files:

`/etc/config/scripts/cms-notify-service`

`/etc/config/scripts/cms-notify-host`

For more details refer http://nagios.sourceforge.net/docs/3_0/notifications.html

5.3.4 Notification Elevation

The Nagios software in CMS also supports optional escalation of contact notifications for hosts and services. Escalation of host and service notifications is accomplished by defining host escalations and service escalations in your object configuration file(s).

Notifications are escalated *if and only if* one or more escalation definitions match the current notification that is being sent out. If a host or service notification *does not* have any valid escalation definitions that apply to it, the contact group(s) specified in either the host group or service definition will be used for the notification.

Users can define service and host escalations in */etc/config/nagios/user directory*

For more details refer http://nagios.sourceforge.net/docs/3_0/escalations.html

5.3.5 An example showing you how to add new check programs

This example adds a simple bash script that checks if the file */tmp/nagios.chk* is available. If it is there and it's executable the service goes to critical, if it is there and not executable it's going to warning and if it doesn't exist the service is ok.

1. Create the executable check file

```
# vi /usr/local/nagios/libexec/check_file_exist.sh
```

Add the following to that file:

```
#!/bin/bash
#
# Check if a local file exist
#
while getopts F: VAR
do
case "$VAR" in
F ) LOGFILE=$OPTARG ;;
* ) echo "wrong syntax: use $o -F <file to check>"
exit 3 ;;
esac
done

if test "$LOGFILE" = ""
then
echo "wrong syntax: use $0 -F <file to check>"
# Nagios exit code 3 = status UNKNOWN = orange
exit 3
fi
if test -e "$LOGFILE"
then
if test -x "$LOGFILE"
then
echo "Critical $LOGFILE is executable !"
# Nagios exit code 2 = status CRITICAL = red
exit 2
else
echo "Warning $LOGFILE exists !"
# Nagios exit code 1 = status WARNING = yellow
exit 1
fi
else
echo "OK: $LOGFILE does not exist !"
```

```
# Nagios exit code 0 = status OK = green
exit 0
fi
```

Now set the file attributes:

```
# chown nagios.nagios /usr/local/nagios/libexec/check_file_exist.sh
# chmod +x /usr/local/nagios/libexec/check_file_exist.sh
```

Add the check program to the nagios configuration

Each new check command has to be defined once in the global Nagios configuration:

```
# vi /usr/local/nagios/etc/minimal.cfg
```

Add the following block at the end of the file:

```
define command{
command_name check_file_exist
command_line $USER1$/check_file_exist.sh -F /tmp/nagios.chk
}
```

Add a new service to the localhost. Each new service has to be defined once in the Nagios configuration and can be assigned to a single host, multiple hosts or even a host group. We assign it only to the localhost that is already defined in this base configuration:

```
# vi /usr/local/nagios/etc/minimal.cfg
```

Add the following block at the end of the file:

```
define service{
use generic-service
host_name localhost
service_description File check
is_volatile 0
check_period 24x7
max_check_attempts 4
normal_check_interval 5
retry_check_interval 1
contact_groups admins
notification_options w,u,c,r
notification_interval 960
notification_period 24x7
check_command check_file_exist
}
```

Verify Nagios configuration and restart it. After all changes of the config files you should check the Nagios configuration and you have to restart Nagios after that:

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

The Total Warnings and Total Errors should be 0 if you have done everything correct.
So restart it with:

```
# /etc/init.d/nagios restart
```

Check if the new program is working. First take a look at the tactical screen and you should see that one service is in status pending. That means no check was done before for this service. Wait a view minutes and it should disappear as pending and the number of OKs should increment from 5 to 6.

Now create the file and watch the tactical screen, the service detail screen or the service problems screen.

```
# touch /tmp/nagios.chk
```

As we set the *normal_check_interval* to 5 minutes in the service definition, you should get the warning message during that time. Now add the executable attribute and watch:

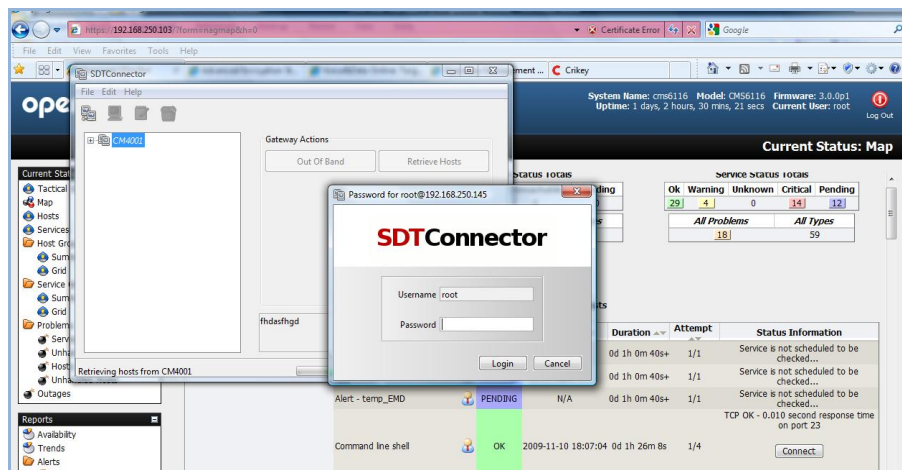
```
# chmod +x /tmp/nagios.chk
```

The status should change during the check interval to critical. When you delete the file the service should return to status ok.

This chapter describes using *SDT Connector* to securely communicate with *Managed Console Servers* and their attached *Managed Devices*.

SDT Connector is a simple Java application that sets up secure SSH tunnels and then runs a local application.

As covered earlier, when you are browser connected to the *CMS* you can click on the **Connect** or **Manage Power** or **View Status** or **View Logs** button in the *Status Information* field of any monitored *Host* and browser will download a pre-configured *SDT Connector* Java application from the *CMS* and you will be connected to the *Host* (proxied via the *CMS*).



This pre-configured *SDT Connector* is preconfigured with the *gateway* details (that being the *Managed Console Server*) and the host details (which will be one of the *Managed Devices* attached to the *Managed Console Server*, or the *Managed Console Server* itself) and it will log you into the SSH server embedded in the *Managed Console Server* (you will need to enter a Username Password) and then automatically load and run the appropriate application (*service*) on your computer that is needed to connect to the appropriate *Managed Device* or *Managed Console Server* screen.

The *service* details (location of the application itself and commands to run) may need to be configured in the *SDT Connector* (refer Chapter 6.1). Alternatively if you have a permanent *SDT Connector* installed on your computer it will use the *service* configuration already set up there.

There are many advantages to having such a permanent installation and the balance of this chapter then covers such installation and configuration options:

- Configuring the *console server* for SSH tunneled access to network attached hosts and setting up permitted Services and user access (*Section 6.1*)

- Setting up the *SDT Connector* client with gateway, host, service and client application details and making connections between the Client PC and hosts connected to the *console server* (Section 6.2)
- Using *SDT Connector* to browser access the Management Console (Section 6.3)
- Using *SDT Connector* to Telnet or SSH connect to devices that are serially attached to the *console server* (Section 6.4)

The chapter then covers more advanced *SDT Connector* and SSH tunneling topics:

- Using *SDT Connector* for out of band access(Section 6.5)
- Automatic importing and exporting of configurations (Section 6.6)
- Configuring Public Key Authentication (Section 6.7)
- Setting up a SDT Secure Tunnel for Remote Desktop (Section 6.8)
- Setting up a SDT Secure Tunnel for VNC (Section 6.9)
- Using SDT to IP connect to hosts that are serially attached to the *console server* (Section 6.10)

6.1 Configuring for SSH Tunneling to Hosts

To set up the *console server* for SSH tunneled access a network attached *host*:

- Add the new *host* and the *permitted services* using the **Serial & Network: Network Hosts** menu as detailed in *Network Hosts* (Chapter 4.4). Only these *permitted services* will be forwarded through by SSH to the *host*. All other services (TCP/UDP ports) will be blocked.

Note Following are some of the TCP Ports used by SDT in the *console server*.

22	SSH (All SDT Tunneled connections)
23	Telnet on local LAN (forwarded inside tunnel)
80	HTTP on local LAN (forwarded inside tunnel)
3389	RDP on local LAN (forwarded inside tunnel)
5900	VNC on local LAN (forwarded inside tunnel)
73XX	RDP over serial from local LAN – where XX is the serial port number (i.e. 7301to 7348 on a 48 port <i>console server</i>)
79XX	VNC over serial from local LAN – where XX is the serial port number

- Add the new *Users* using **Serial & Network: Users & Groups** menu as detailed in *Network Hosts* (Chapter 4.4). *Users* can be authorized to access the *console server* ports and specified network-attached hosts. To simplify configuration, the *Administrator* can first set up *Groups* with group access permissions, then *Users* can be classified as members of particular *Groups*.

6.2 SDT Connector client installation and configuration

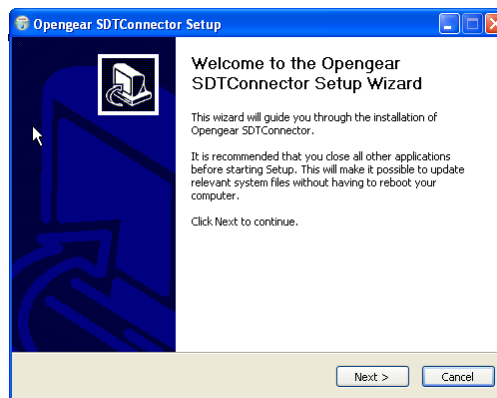
The *SDT Connector* client works with all Opengear *console servers*. Each of these remote *console servers* have an embedded OpenSSH based server which can be configured to *port forward* connections from the *SDT Connector* client to hosts on their local network as detailed in the previous chapter. The *SDT*

Connector can also be pre-configured with the access tools and applications that will be available to be run when access to a particular host has been established.

SDT Connector can connect to the *console server* using an alternate OoB access. It can also access the *console server* itself and access devices connected to serial ports on the *console server*.

6.2.1 SDT Connector client installation

- The *SDT Connector* set up program (*SDTConnectorSetup-1.n.exe* or *sdtcon-1.n.tar.gz*) is included on the CD supplied with your Opengear *console server* product (or a copy can be freely download from Opengear’s website)
- Run the set-up program:



Note For Windows clients, the *SDTConnectorSetup-1.n.exe* application will install the *SDT Connector 1.n.exe* and the config file *defaults.xml*. If there is already a config file on the Windows PC then it will not be overwritten. To remove earlier config file run the *regedit* command and search for “*SDT Connector*” then remove the directory with this name.

For Linux and other Unix clients, *SDTConnector.tar.gz* application will install the *sdtcon-1.n.jar* and the config file *defaults.xml*

Once the installer completes you will have a working *SDT Connector* client installed on your machine and an icon on your desktop:



- Click the *SDT Connector* icon on your desktop to start the client


Note *SDT Connector* is a Java application so it must have a Java Runtime Environment (JRE) installed. This can be freely downloaded from <http://java.sun.com/j2se/>. It will install on Windows 2000, XP, 2003, Vista PCs and on most Linux platforms. Solaris platforms are also supported however they must have Firefox installed. *SDT Connector* can run on any system with Java 1.4.2 and above installed, but it assumes the web browser is Firefox, and that *xterm -e telnet* opens a telnet window

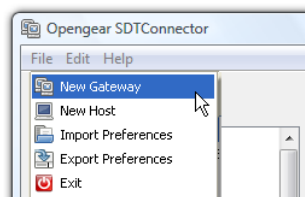
To operate *SDT Connector*, you first need to add new gateways to the client software by entering the access details for each *console server* (refer *Section 6.2.2*) then let the client auto-configure with all host and serial port connections from each *console server* (refer *Section 6.2.3*) then point-and-click to connect to the Hosts and serial devices(refer *Section 6.2.4*)

Alternately you can manually add network connected hosts (refer *Section 6.2.5*) and manually configure new services to be used in accessing the *console server* and the hosts (refer *Section 6.2.6*) then manually configuring clients to run on the PC that will use the service to connect to the hosts and serial port devices (refer *Section 6.2.7 and 6.2.9*). *SDT Connector* can also be set up to make an out-of-band connection to the *console server* (refer *Section 6.2.9*)

6.2.2 Configuring a new gateway in the SDT Connector client

To create a secure SSH tunnel to a new *console server*:

- Click the *New Gateway*  icon or select the **File: New Gateway** menu option

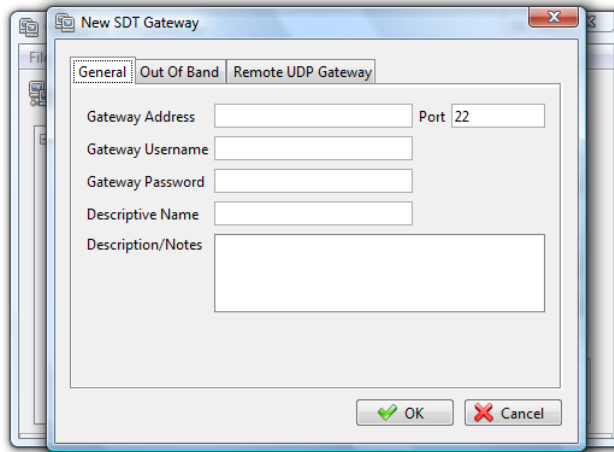


- Enter the IP or DNS **Address** of the *console server* and the SSH port that will be used (typically 22)

Note If *SDT Connector* is connecting to a remote *console server* through the public Internet or routed network you will need to:

- Determine *the public IP address* of the *console server* (or of the router/ firewall that connects the *console server* to the Internet) as assigned by the ISP. One way to find the public IP address is to access <http://checkip.dyndns.org/> or <http://www.whatismyip.com/> from a computer on the same network as the *console server* and note the reported IP address
- Set port forwarding for TCP port 22 through any firewall/NAT/router that is located between *SDT Connector* and the *console server* so it points to the *console server*. <http://www.portforward.com> has port forwarding instructions for a range of routers. Also you can use the Open Port Check tool from <http://www.canyouseeme.org> to check if port forwarding through local firewall/NAT/router devices has been properly configured

-
- Enter the **Username** and **Password** of a user on the gateway that has been enabled to connect via SSH and/or create SSH port redirections

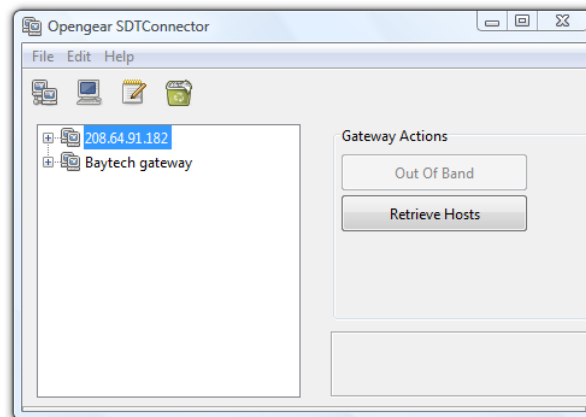


- Optionally, enter a **Descriptive Name** to display instead of the IP or DNS address, and any **Notes** or a **Description** of this gateway (such as its firmware version, site location or anything special about its network configuration).
- Click **OK** and an icon for the new gateway will now appear in the *SDT Connector* home page

Note For an *SDT Connector* user to access a *console server* (and then access specific hosts or serial devices connected to that *console server*), that user must first be setup on the *console server*, and must be authorized to access the specific ports / hosts (refer Chapter 5) and only these *permitted services* will be forwarded through by SSH to the Host. All other services (TCP/UDP ports) will be blocked.

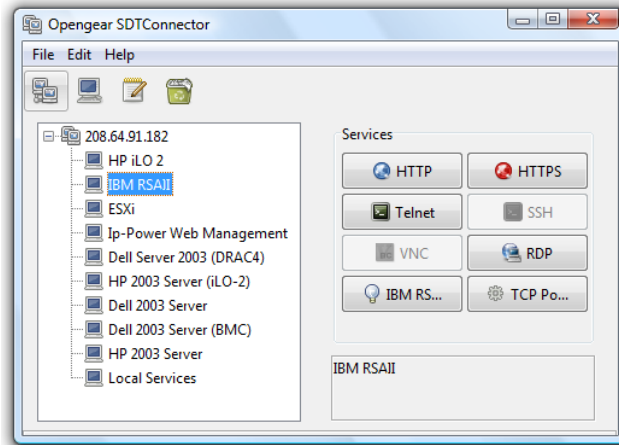
6.2.3 Auto-configure SDT Connector client with the user's access privileges

Each user on the *console server* has an access profile which has been configured with those specific connected hosts and serial port devices the user has authority to access, and a specific set of the enabled services for each of these. This configuration can be auto-uploaded into the *SDT Connector* client:



- Click on the new gateway icon and select **Retrieve Hosts**. This will:

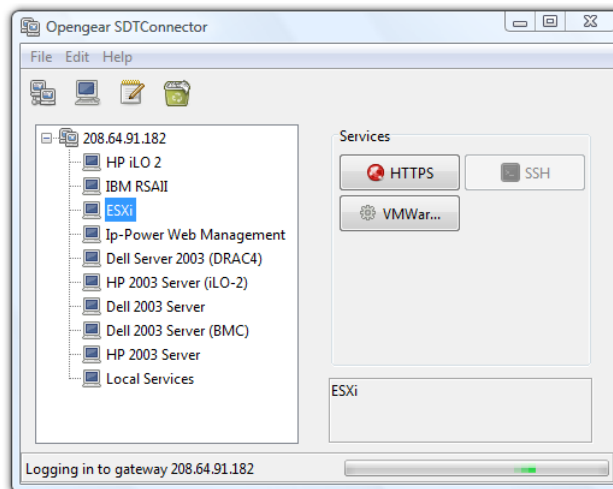
- configure access to network connected Hosts that the user is authorized to access and set up (for each of these Hosts) the services (e.g. HTTPS, IPMI2.0) and the related IP ports being redirected
- configure access to the *console server* itself (this is shown as a *Local Services* host)
- configure access with the enabled services for the serial port devices connected to the *console server*



Note The Retrieve Hosts function will auto-configure all classes of user (i.e. they can be members of *user* or *admin* or some other group or no group) however *SDT Connector* will not auto-configure the *root* (and it recommended that this account is only used for initial config and for adding an initial *admin* account to the *console server*)

6.2.4 Make an SDT connection through the gateway to a host

- Simply **point** at the host to be accessed **and click** on the service to be used in accessing that host. The SSH tunnel to the gateway is then automatically established, the appropriate ports redirected through to the host, and the appropriate local client application is launched pointing at the local endpoint of the redirection:




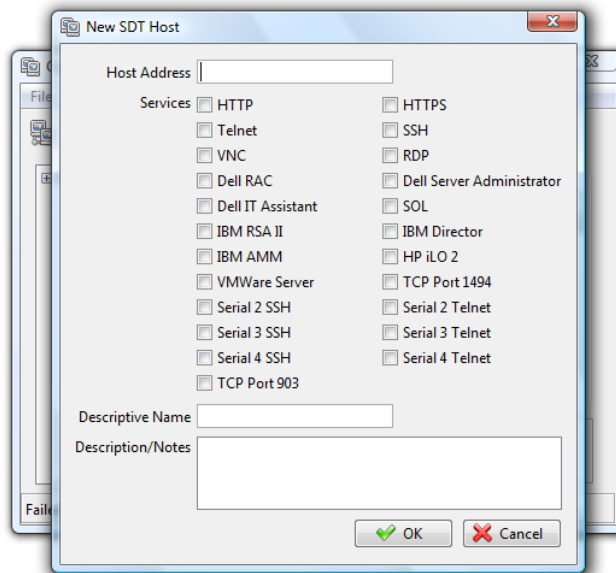
Note The *SDT Connector* client can be configured with unlimited number of Gateways. Each Gateway can be configured to port forward to an unlimited number of locally networked Hosts. Similarly there is no limit on the number of *SDT Connector* clients who can be configured to access the one Gateway. Nor are there limits on the number of Host connections that an *SDT Connector* client can concurrently have open through the one Gateway tunnel.

However there is a limit on the number of *SDT Connector* SSH tunnels that can be open at the one time on a particular Gateway. SD4002/4008 and CM4001/4008 devices support at least 10 simultaneous client tunnels; IM4216/4248 and CM4116/4148 each support at least 50 such concurrent connections. So for a site with a CM4116 gateway you can have, at any time up to 50 users securely controlling an unlimited number of network attached computers and appliances (servers, routers etc) at that site.

6.2.5 Manually adding hosts to the SDT Connector gateway

For each gateway, you can manually specify the network connected hosts that will be accessed through that *console server*; and for each host, specify the services that will be used in communicating with the host

- Select the newly added gateway and click the *Host* icon  to create a host that will be accessible via this gateway. (Alternatively select **File: New Host**)

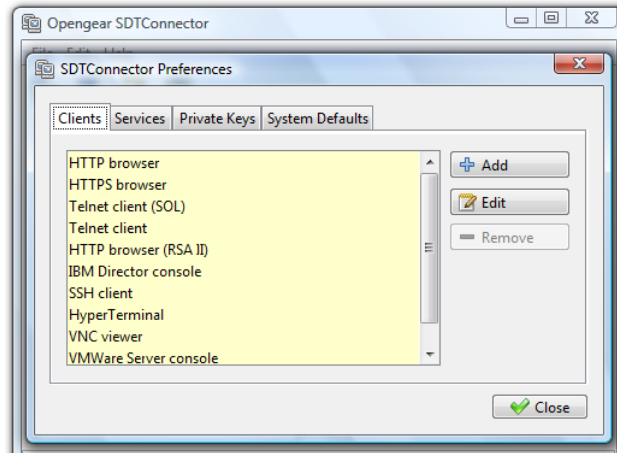


- Enter the IP or DNS **Host Address** of the host (if this is a DNS address, it must be resolvable by the gateway)
- Select which **Services** are to be used in accessing the new host. A range of service options are pre-configured in the default *SDT Connector* client (RDP, VNC, HTTP, HTTPS, Dell RAC, VMware etc). However if you wish to add new services the range then proceed to the next section (**Adding a new service**) then return here
- Optionally, enter a **Descriptive Name** for the host, to display instead of the IP or DNS address, and any **Notes** or a **Description** of this host (such as its operating system/release, or anything special about its configuration)
- Click **OK**

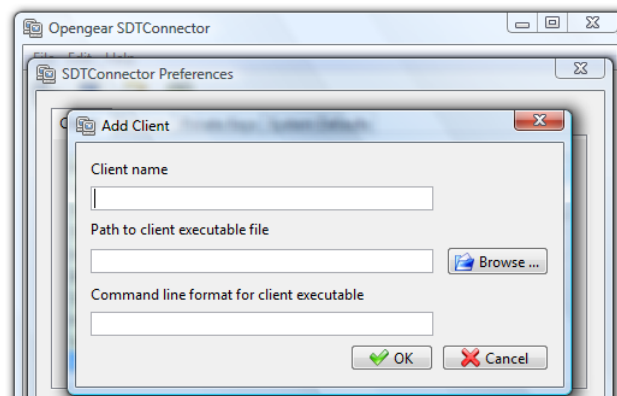
6.2.6 Manually adding new services to the new hosts

To extend the range of services that can be used when accessing hosts with *SDT Connector*:

- Select **Edit: Preferences** and click the **Services** tab. Click **Add**
- Enter a **Service Name** and click **Add**
- Under the **General** tab, enter the TCP Port that this service runs on (e.g. 80 for HTTP). Optionally, select the client to use to access the local endpoint of the redirection



- Select which **Client** application is associated with the new service. A range of client application options are pre-configured in the default *SDT Connector* (RDP client, VNC client, HTTP browser, HTTPS browser, Telnet client etc). However if you wish to add new client applications to this range then proceed to the next section (**Adding a new client**) then return here

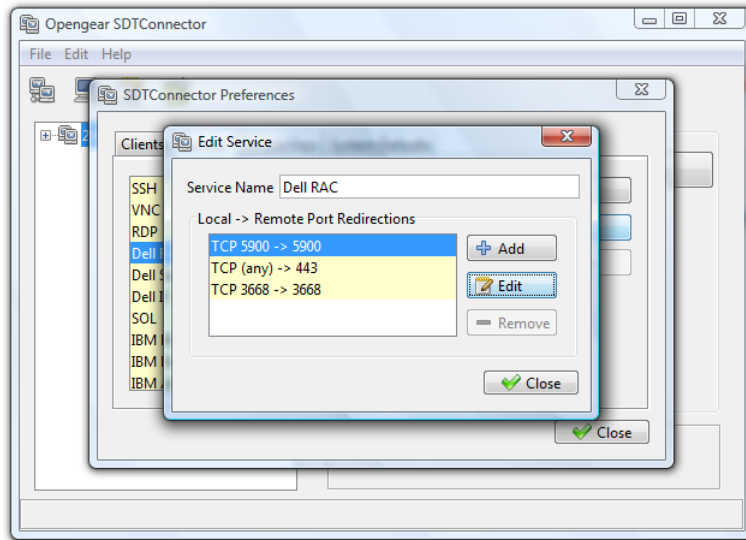


- Click **OK**, then **Close**

A service typically consists of a single SSH port redirection and a local client to access it. However it may consist of several redirections; some or all of which may have clients associated with them.

An example is the Dell RAC service. The first redirection is for the HTTPS connection to the RAC server - it has a client associated with it (web browser) that is launched immediately upon clicking the button for this service.

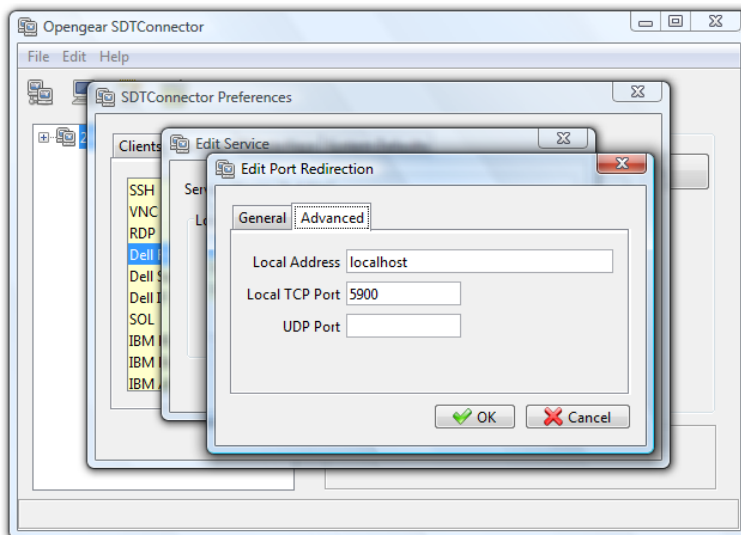
The second redirection is for the VNC service that the user may choose to later launch from the RAC web console. It is automatically loads in a Java client served through the web browser, so it does not need a local client associated with it.



- On the Add Service screen you can click **Add** as many times as needed to add multiple new port redirections and associated clients

You may also specify **Advanced** port redirection options:

- Enter the local address to bind to when creating the local endpoint of the redirection. It is not usually necessary to change this from "localhost".
- Enter a local TCP port to bind to when creating the local endpoint of the redirection. If this is left blank, a random port will be selected.



Note *SDT Connector* can also tunnel UDP services. *SDT Connector* tunnels the UDP traffic through the TCP SSH redirection, so in effect it is a tunnel within a tunnel.

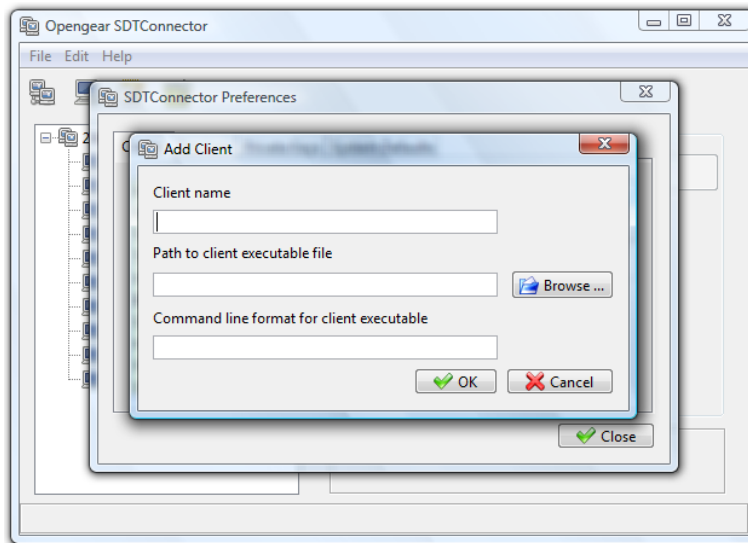
Enter the UDP port on which the service is running on the host. This will also be the local UDP port that *SDT Connector* binds as the local endpoint of the tunnel.

Note that for UDP services, you still need to specify a TCP port under General. This will be an arbitrary TCP port that is not in use on the gateway. An example of this is the SOL Proxy service. It redirects local UDP port 623 to remote UDP port 623 over the arbitrary TCP port 6667

6.2.7 Adding a client program to be started for the new service

Clients are local applications that may be launched when a related service is clicked. To add to the pool of client programs:

- Select **Edit: Preferences** and click the **Client** tab. Click **Add**



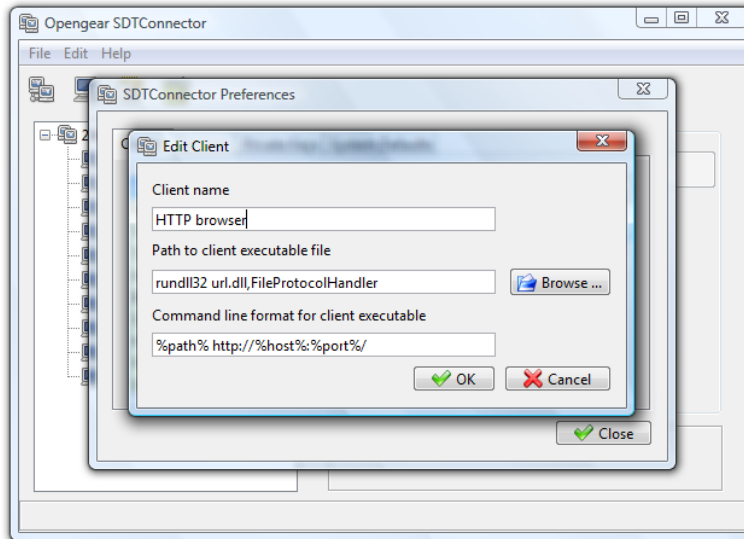
- Enter a **Name** for the client. Enter the **Path** to the executable file for the client (or click **Browse** to locate the executable)
- Enter a **Command Line** associated with launching the client application. *SDT Connector* typically launches a client using command line arguments to point it at the local endpoint of the redirection. There are three special keywords for specifying the command line format. When launching the client, *SDT Connector* substitutes these keywords with the appropriate values:

%path% is path to the executable file, i.e. the previous field.

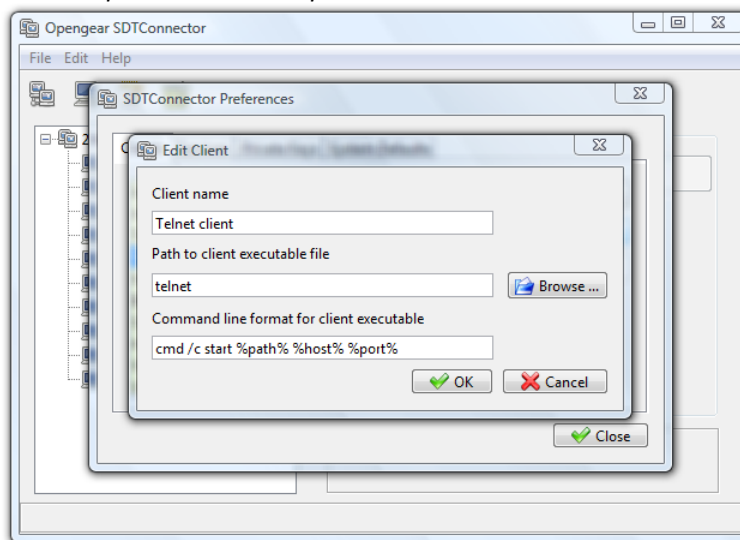
%host% is the local address to which the local endpoint of the redirection is bound, i.e. the Local Address field for the Service redirection Advanced options.

%port% is the local port to which the local endpoint of the redirection is bound, i.e. the Local TCP Port field for the Service redirection Advanced options. If this port is unspecified (i.e. "Any"), the appropriate randomly selected port will be substituted.

For example *SDT Connector* is preconfigured for Windows installations with a HTTP service client that will connect with whichever local browser the local Windows user has configured as the default. Otherwise the default browser used is Firefox:



Also some clients are launched in a command line or terminal window. The Telnet client is an example of this so the “Path to client executable file” is *telnet* and the “Command line format for client executable” is *cmd /c start %path% %host% %port%* :



- Click OK

6.2.8 Dial in configuration

If the client PC is dialing into *Local/Console* port on the *console server* you will need to set up a dial-in PPP link:

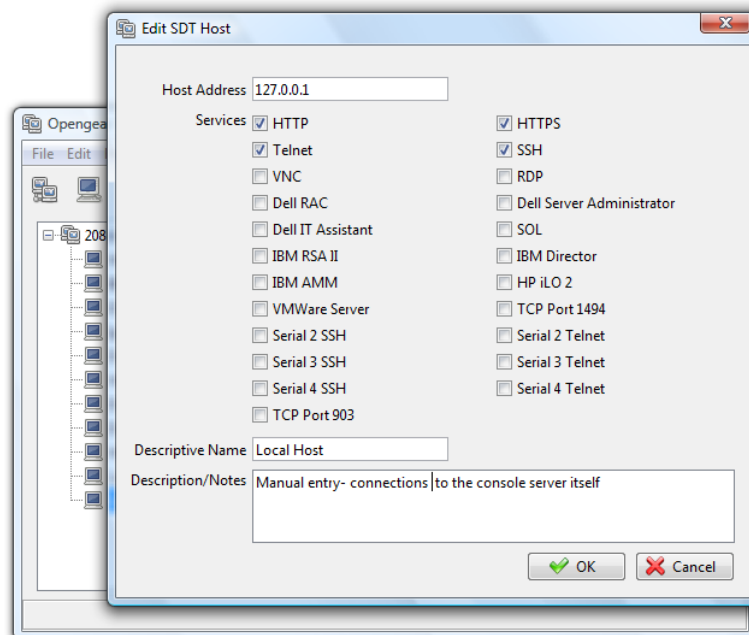
- Configure the *console server* for dial-in access (following the steps in the **Configuring for Dial-In PPP Access** section in *Chapter 5, Configuring Dial In Access*)
- Set up the PPP client software at the remote *User PC* (following the **Set up the remote Client** section in *Chapter 5*)

Once you have a dial-in PPP connection established, you then can set up the secure SSH tunnel from the remote Client PC to the *console server*.

6.3 SDT Connector to Management Console

SDT Connector can also be configured for browser access the gateway's Management Console – and for Telnet or SSH access to the gateway command line. For these connections to the gateway itself, you must configure *SDT Connector* to access the gateway (itself) by setting the *Console server* up as a *host*, and then configuring the appropriate services:

- Launch *SDT Connector* on your PC. Assuming you have already set up the *console server* as a *Gateway* in your *SDT Connector* client (with *username/ password* etc) select this newly added *Gateway* and click the Host icon to create a host. Alternatively, select **File -> New Host**
- Enter 127.0.0.1 as the **Host Address** and give some details in **Descriptive Name/Notes**. Click OK



- Click the **HTTP** or **HTTPS** Services icon to access the gateway's Management Console, and/or click **SSH** or **Telnet** to access the gateway command line console

Note: To enable SDT access to the gateway console, you must now configure the *console server* to allow port forwarded network access to itself:

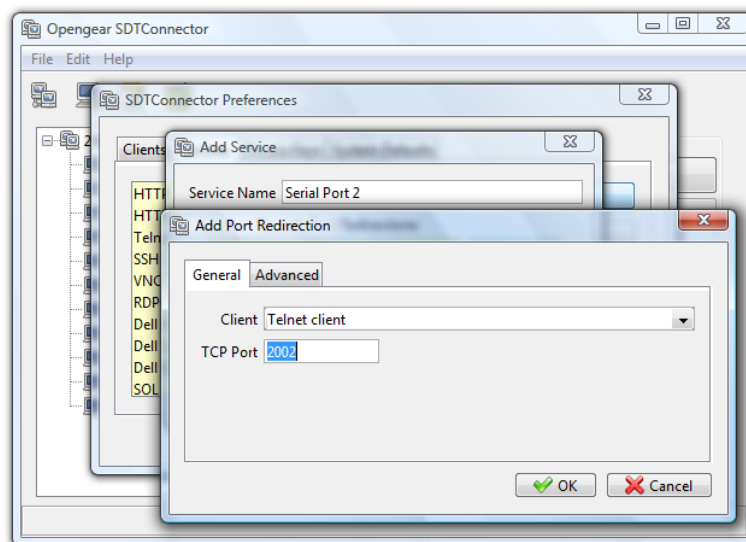
- Browse to the *console server* and select **Network Hosts** from **Serial & Network**, click **Add Host** and in the **IP Address/DNS Name** field enter 127.0.0.1 (this is the Opengear's network loopback address) and enter *Loopback* in **Description**
- Remove all entries under **Permitted Services** except for those that will be used in accessing the Management Console (80/http or 443/https) or the command line (22/ssh or 23/telnet) then scroll to the bottom and click **Apply**
- *Administrators* by default have gateway access privileges, however for *Users* to access the gateway Management Console you will need to give those *Users* the required access privileges. Select **Users & Groups** from **Serial & Network**. Click **Add User**. Enter a

Username, Description and Password/Confirm. Select 127.0.0.1 from **Accessible Host(s)** and click **Apply**

6.4 SDT Connector - telnet or SSH connect to serially attached devices

SDT Connector can also be used to access text consoles on devices that are attached to the *console server* serial ports. For these connections, you must configure the *SDT Connector* client software with a Service that will access the target gateway serial port, and then set the gateway up as a host:

- Launch *SDT Connector* on your PC. Select **Edit -> Preferences** and click the **Services** tab. Click **Add**
- Enter "*Serial Port 2*" in **Service Name** and click **Add**
- Select **Telnet** client as the Client. Enter 2002 in **TCP Port**. Click **OK**, then **Close** and **Close** again



- Assuming you have already set up the target *console server* as a *gateway* in your *SDT Connector* client (with *username/ password* etc), select this *gateway* and click the **Host** icon to create a host. Alternatively, select **File -> New Host**.
- Enter 127.0.0.1 as the **Host Address** and select **Serial Port 2** for Service. In **Descriptive Name**, enter something along the lines of Loopback ports, or Local serial ports. Click **OK**.
- Click *Serial Port 2* icon for Telnet access to the serial console on the device attached to serial port #2 on the gateway

To enable *SDT Connector* to access to devices connected to the gateway's serial ports, you must also configure the *Console server* itself to allow port forwarded network access to itself, and enable access to the nominated serial port:

- Browse to the *Console server* and select **Serial Port** from **Serial & Network**
- Click **Edit** next to selected Port # (e.g. Port 2 if the target device is attached to the second serial port). Ensure the port's serial configuration is appropriate for the attached device

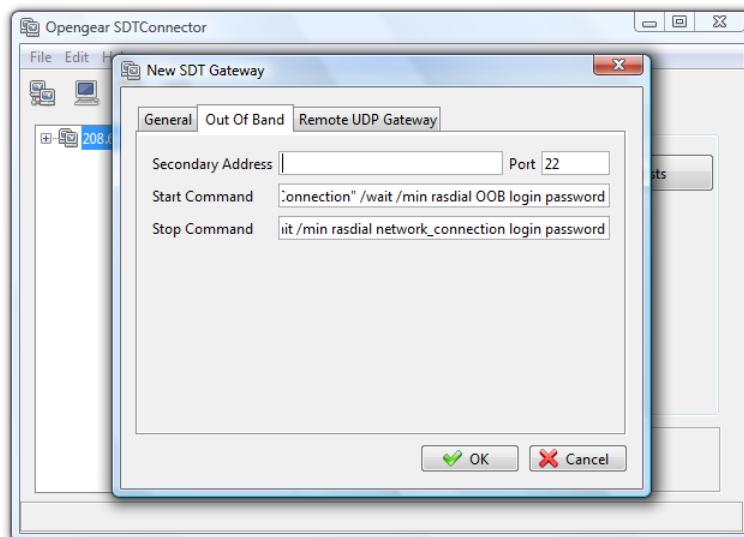
- Scroll down to *Console Server Setting* and select **Console server Mode**. Check **Telnet** (or SSH) and scroll to the bottom and click **Apply**
- Select **Network Hosts** from **Serial & Network** and click **Add Host**
- In the **IP Address/DNS Name** field enter *127.0.0.1* (this is the Opendgear's network loopback address) and enter *Loopback* in **Description**
- Remove all entries under **Permitted Services** and select **TCP** and enter *200n* in **Port**. (This configures the Telnet port enabled in the previous step, so for Port 2 you would enter *2002*)
- Click **Add** then scroll to the bottom and click **Apply**
- *Administrators* by default have gateway and serial port access privileges; however for *Users* to access the gateway and the serial port, you will need to give those *Users* the required access privileges. Select **Users & Groups** from **Serial & Network**. Click **Add User**. Enter a **Username**, **Description** and **Password/Confirm**. Select *127.0.0.1* from **Accessible Host(s)** and select Port 2 from **Accessible Port(s)**. Click **Apply**.

6.5 Using SDT Connector for out-of-band connection to the gateway

SDT Connector can also be set up to connect to the *console server* (gateway) out-of-band (OoB). OoB access uses an alternate path for connecting to the gateway to that used for regular data traffic. OoB access is useful for when the primary link into the gateway is unavailable or unreliable.

Typically a gateway's primary link is a broadband Internet connection or Internet connection via a LAN or VPN, and the secondary out-of-band connectivity is provided by a dial-up or wireless modem directly attached to the gateway. So out-of-band access enables you to access the hosts and serial devices on the network, diagnose any connectivity issues, and restore the gateway's primary link.

In *SDT Connector*, OoB access is configured by providing the secondary IP address of the gateway, and telling *SDT Connector* how to start and stop the OoB connection. Starting an OoB connection may be achieved by initiating a dial up connection, or adding an alternate route to the gateway. *SDT Connector* allows for maximum flexibility in this regard, by allowing you to provide your own scripts or commands for starting and stopping the OoB connection.



To configure *SDT Connector* for OoB access:

- When adding a new gateway or editing an existing gateway select the **Out Of Band** tab
- Enter the secondary, OoB IP address of the gateway (e.g. the IP address it is accessible using when dialed in directly). You also may modify the gateway's SSH port if it's not using the default of 22
- Enter the command or path to a script to start the OoB connection in **Start Command**
 - To initiate a pre-configured dial-up connection under Windows, use the following Start Command:

```
cmd /c start "Starting Out of Band Connection" /wait /min rasdial network_connection login password
```

Where *network_connection* is the name of the network connection as displayed in *Control Panel -> Network Connections*, *login* is the dial-in username, and *password* is the dial-in password for the connection.
 - To initiate a pre-configured dial-up connection under Linux, use the following Start Command:

```
pon network_connection
```

where *network_connection* is the name of the connection.
- Enter the command or path to a script to stop the OoB connection in **Stop Command**
 - To stop a pre-configured dial-up connection under Windows, use the following Stop Command:

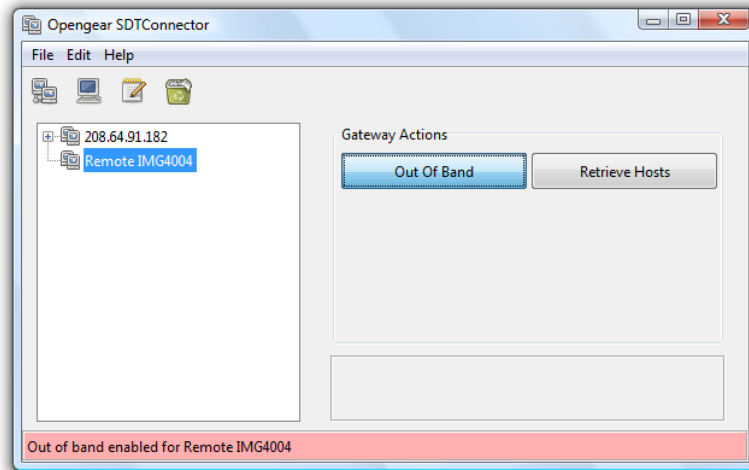
```
cmd /c start "Stopping Out of Band Connection" /wait /min rasdial network_connection /disconnect
```

where *network connection* is the name of the network connection as displayed in *Control Panel -> Network Connections*.
 - To stop a pre-configured dial-up connection under Linux, use the following Stop Command:

```
poff network_connection
```

To make the OoB connection using *SDT Connector*:

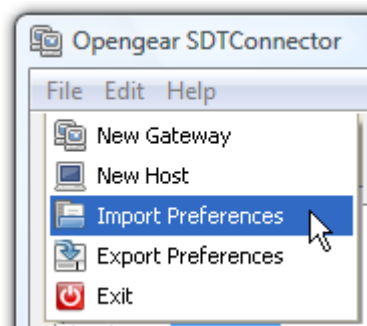
- Select the gateway and click Out Of Band. The status bar will change color to indicate this gateway is now being access using the OoB link rather than the primary link



When you connect to a service on a host behind the gateway, or to the *console server* gateway itself, *SDT Connector* will initiate the OoB connection using the provided Start Command. The OoB connection isn't stopped (using the provided Stop Command) until Out Of Band under Gateway Actions is clicked off, at which point the status bar will return to its normal color.

6.6 Importing (and exporting) preferences

To enable the distribution of pre-configured client config files, *SDT Connector* has an *Export/Import* facility:



- To save a configuration .xml file (for backup or for importing into other *SDT Connector* clients) select **File -> Export Preferences** and select the location to save the configuration file
- To import a configuration select **File -> Import Preferences** and select the .xml configuration file to be installed

6.7 SDT Connector Public Key Authentication

SDT Connector can authenticate against an SSH gateway using your SSH key pair rather than requiring you to enter your password. This is known as public key authentication.

To use public key authentication with *SDT Connector*, first you must add the public part of your SSH key pair to your SSH gateway:

- Ensure the SSH gateway allows public key authentication, this is typically the default behavior
- If you do not already have a public/private key pair for your client PC (the one running *SDT Connector* on) generate them now using *ssh-keygen*, *PuTTYgen* or a similar tool. You may use RSA or DSA, however it is important that you leave the passphrase field blank:
 - PuTTYgen: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
 - OpenSSH: <http://www.openssh.org/>
 - OpenSSH (Windows): <http://sshhwindows.sourceforge.net/download/>
- Upload the public part of your SSH key pair (this file is typically named *id_rsa.pub* or *id_dsa.pub*) to the SSH gateway, or otherwise add to *.ssh/authorized keys* in your home directory on the SSH gateway
- Next, add the private part of your SSH key pair (this file is typically named *id_rsa* or *id_dsa*) to *SDT Connector*. Click **Edit -> Preferences -> Private Keys -> Add**, locate the private key file and click **OK**

You do not have to add the public part of your SSH key pair, it is calculated using the private key.

SDT Connector will now use public key authentication when connecting through the SSH gateway (*console server*). You may have to restart *SDT Connector* to shut down any existing tunnels that were established using password authentication.

Also if you have a host behind the *console server* that you connect to by clicking the SSH button in *SDT Connector* you may also wish to configure access to it for public key authentication as well. This configuration is entirely independent of *SDT Connector* and the SSH gateway. You must configure the SSH client that *SDT Connector* launches (e.g. Putty, OpenSSH) and the host's SSH server for public key authentication. Essentially what you are using is SSH over SSH, and the two SSH connections are entirely separate.

6.8 Setting up SDT for Remote Desktop access

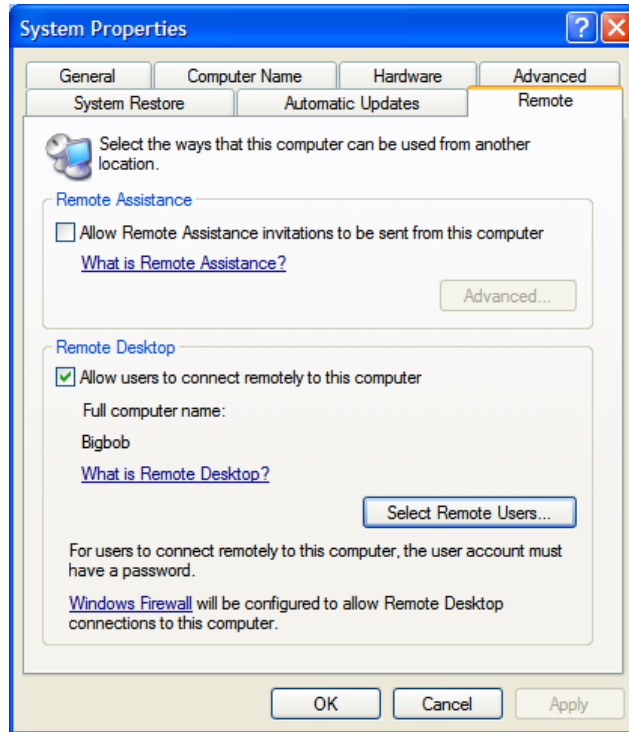
Microsoft's Remote Desktop Protocol (RDP) enables the system manager to securely access and manage remote Windows computers – to reconfigure applications and user profiles, upgrade the server's operating system, reboot the machine etc. Opengear's Secure Tunneling uses SSH tunneling, so this RDP traffic is securely transferred through an authenticated and encrypted tunnel.

SDT with RDP also allows remote *Users* to connect to Windows XP, Vista, Server2003, Server 2008 computers and to Windows 2000 Terminal Servers; and to have access to all of the applications, files, and network resources (with full graphical interface just as though they were in front of the computer screen at work). To set up a secure Remote Desktop connection you must enable Remote Desktop on the target Windows computer that is to be accessed and configure the RPD client software on the client PC.

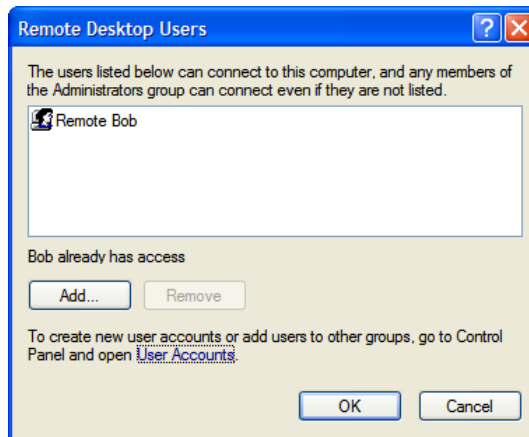
6.8.1 Enable Remote Desktop on the target Windows computer to be accessed

To enable **Remote Desktop** on the Windows computer being accessed:

- Open **System** in the Control Panel and click the **Remote** tab



- Check **Allow users to connect remotely to this computer**
- Click **Select Remote Users**



- To set the user(s) who can remotely access the system with RDP click **Add** on the **Remote Desktop Users** dialog box

Note If you need to set up new users for Remote Desktop access, open **User Accounts** in the Control Panel and proceed through the steps to nominate the new user's name, password and account type (*Administrator* or *Limited*)

Note With Windows XP Professional and Vista, you have only one Remote Desktop session and it connects directly to the Windows root console. With Windows Server 2008 you can have

multiple sessions (and with Server 2003 you have three sessions - the console session and two other general sessions). So more than one user can have active sessions on a single computer.

When the remote user connects to the accessed computer on the console session, Remote Desktop automatically locks that computer (so no other user can access the applications and files). When you come back to your computer at work, you can unlock it by typing CTRL+ALT+DEL.

6.8.2 Configure the Remote Desktop Connection client

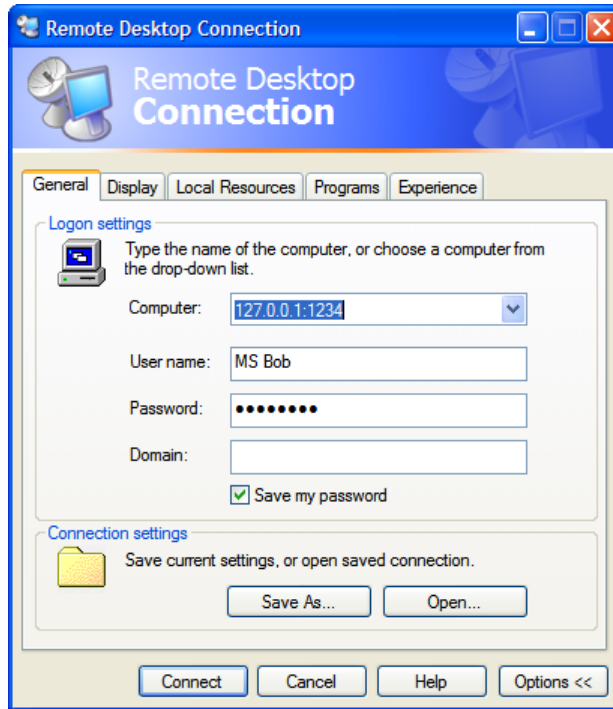
Now you have the Client PC securely connected to the *console server* (either locally, or remotely - thru the enterprise VPN, or a secure SSH internet tunnel or a dial-in SSH tunnel) you can establish the Remote Desktop connection from the Client. To do this you simply enable the **Remote Desktop Connection** on the remote client PC then point it to the SDT Secure Tunnel port in the *console server*:

A. On a Windows client PC

- Click **Start**. Point to **Programs**, then to **Accessories**, then **Communications**, and click **Remote Desktop Connection**



- In **Computer**, enter the appropriate IP Address and Port Number:
 - Where there is a direct local or enterprise VPN connection, enter the IP Address of the *console server*, and the Port Number of the SDT Secure Tunnel for the *console server* serial port that is attached to the Windows computer to be controlled e.g. if the Windows computer is connected to serial Port 3 on a *console server* located at 192.168.0.50 then you would enter *192.168.0.50:7303*
 - Where there is an SSH tunnel (over a dial up PPP connection or over a public internet connection or private network connection) simply enter the *localhost* as the IP address i.e. *127.0.0.1* For Port Number, enter the *source port* you created when setting SSH tunneling /port forwarding (in Section 6.1.6) e.g. *:1234*
- Click **Option**. In the **Display** section specify an appropriate color depth (e.g. for a modem connection it is recommended you not use over 256 colors). In **Local Resources** specify the peripherals on the remote Windows computer that are to be controlled (printer, serial port etc)



➤ Click **Connect**

Note The Remote Desktop Connection software is pre-installed with Windows XP, Vista and Server 2003/2008, however for earlier Windows PCs you will need to download the RDP client:

- Go to the Microsoft Download Center site <http://www.microsoft.com/downloads/details.aspx?familyid=80111F21-D48D-426E-96C2-08AA2BD23A49&displaylang=en> and click the **Download** button

This software package will install the client portion of Remote Desktop on Windows 95, Windows 98 and 98 Second Edition, Windows Me, Windows NT 4.0 and Windows 2000. When run, this software allows these older Windows platforms to remotely connect to a computer running current Windows.

B. On a Linux or UNIX client PC:

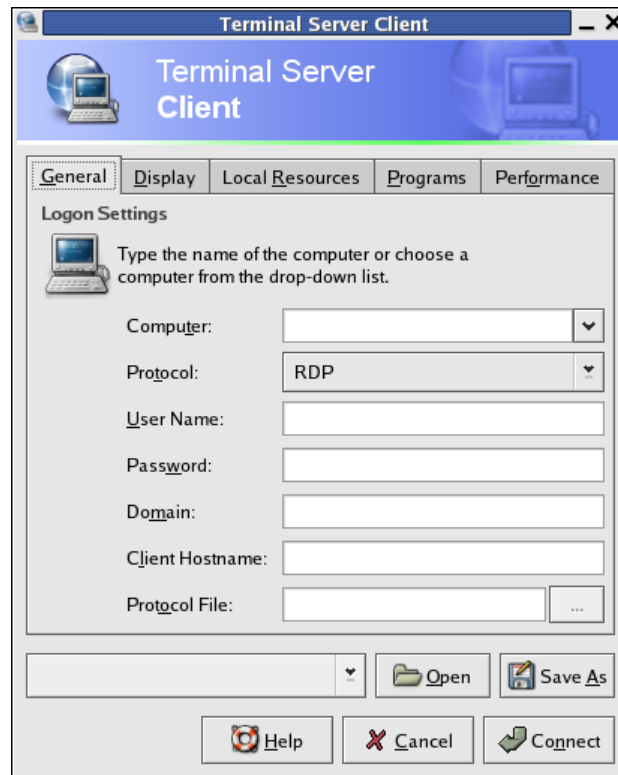
➤ Launch the open source *rdesktop* client:

rdesktop -u windows-user-id -p windows-password -g 1200x950 ms-windows-terminal-server-host-name

option	description
-a	Color depth: 8, 16, 24
-r	Device redirection. i.e. Redirect sound on remote machine to local device i.e. -0 -r sound (MS/Windows 2003)
-g	Geometry: <i>widthxheight</i> or 70% screen percentage.

-p Use -p - to receive password prompt.

- You can use GUI front end tools like the GNOME Terminal Services Client *tsclient* to configure and launch the *rdesktop* client. (Using *tsclient* also enables you to store multiple configurations of *rdesktop* for connection to many servers)



Note The *rdesktop* client is supplied with Red Hat 9.0:

- `rpm -ivh rdesktop-1.2.0-1.i386.rpm`

For Red Hat 8.0 or other distributions of Linux; download source, untar, configure, make, make then install.

rdesktop currently runs on most UNIX based platforms with the X Window System and can be downloaded from <http://www.rdesktop.org/>

C. On a Macintosh client:

- Download Microsoft's free Remote Desktop Connection client for Mac OS X <http://www.microsoft.com/mac/otherproducts/otherproducts.aspx?pid=remotedesktopclient>

6.9 SDT SSH Tunnel for VNC

Alternately, with SDT and Virtual Network Computing (VNC), *Users* and *Administrators* can securely access and control Windows 98/NT/2000/XP/2003, Linux, Macintosh, Solaris and UNIX computers. There's a range of popular VNC software available (UltraVNC, RealVNC, TightVNC) - freely and commercially. To set up a secure VNC connection you must install and configure the VNC Server software on the computer to be accessed, then install and configure the VNC Viewer software on the Viewer PC.

6.9.1 Install and configure the VNC Server on the computer to be accessed

Virtual Network Computing (VNC) software enables users to remotely access computers running Linux, Macintosh, Solaris, UNIX, all versions of Windows and most other operating systems.

A. For Microsoft Windows servers (and clients):

Windows does not include VNC software, so you will need to download, install and activate a third party VNC Server software package:



RealVNC <http://www.realvnc.com> is fully cross-platform, so a desktop running on a Linux machine may be displayed on a Windows PC, on a Solaris machine, or on any number of other architectures. There is a Windows server, allowing you to view the desktop of a remote Windows machine on any of these platforms using exactly the same viewer. RealVNC was founded by members of the AT&T team who originally developed VNC.



TightVNC <http://www.tightvnc.com> is an enhanced version of VNC. It has added features such as file transfer, performance improvements, and read-only password support. They have just recently included a video drive much like UltraVNC. TightVNC is still free, cross-platform (Windows Unix and Linux) and compatible with the standard (Real) VNC.



UltraVNC <http://ultravnc.com> is easy to use, fast and free VNC software that has pioneered and perfected features that the other flavors have consistently refused or been very slow to implement for cross platform and minimalist reasons. UltraVNC runs under Windows operating systems (95, 98, Me, NT4, 2000, XP, 2003) Download UltraVNC from Sourceforge's [UltraVNC file list](#)

B. For Linux servers (and clients):

Most Linux distributions now include VNC Servers and Viewers and they are generally can be launched from the (Gnome/KDE etc) front end e.g. with Red Hat Enterprise Linux 4 there's VNC Server software and a choice of Viewer client software, and to launch:

- Select the **Remote Desktop** entry in the **Main Menu -> Preferences** menu
- Click the **Allow other users...** checkbox to allow remote users to view and control your desktop



➤ To set up a persistent VNC server on Red Hat Enterprise Linux 4:

- Set a password using **vncpasswd**
- Edit **/etc/sysconfig/vncservers**
- Enable the service with **chkconfig vncserver on**
- Start the service with **service vncserver start**
- Edit **/home/username/.vnc/xstartup** if you want a more advanced session than just *twm* and an *xterm*

C. For Macintosh servers (and clients):

OSXvnc <http://www.redstonesoftware.com/vnc.html> is a robust, full-featured VNC server for Mac OS X that allows any VNC client to remotely view and/or control the Mac OS X machine. OSXvnc is supported by Redstone Software

D. Most other operating systems (Solaris, HP/UX, PalmOS etc) either come with VNC bundled, or have third party VNC software that you can download

6.9.2 Install, configure and connect the VNC Viewer

VNC is truly *platform-independent* so a VNC Viewer on any operating system can connect to a VNC Server on any other operating system. There are Viewers (and Servers) from a wide selection of sources (e.g. UltraVNC TightVNC or RealVNC) for most operating systems. There are also a wealth of Java viewers available so that any desktop can be viewed with any Java-capable browser (<http://en.wikipedia.org/wiki/VNC> lists many of the VNC Viewers sources).

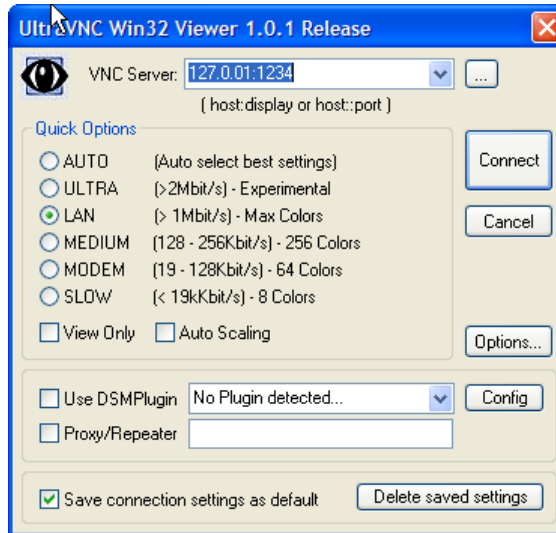
➤ Install the VNC Viewer software and set it up for the appropriate speed connection

Note To make VNC faster, when you set up the Viewer:

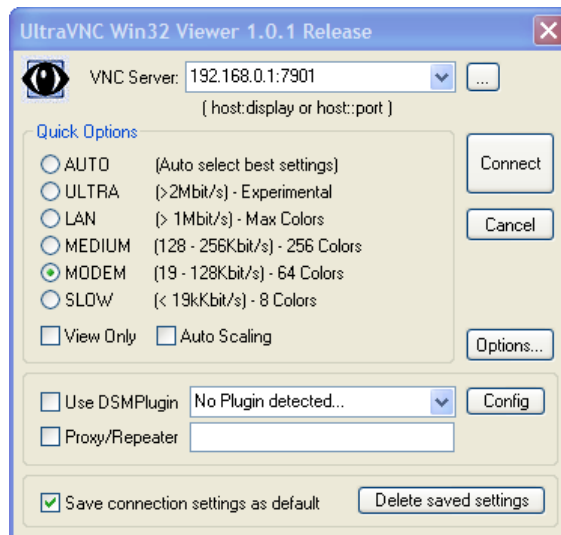
- Set encoding to ZRLE (if you have a fast enough CPU)
 - Decrease color level (e.g. 64 bit)
 - Disable the background transmission on the Server or use a plain wallpaper
- (Refer to <http://doc.uvnc.com> for detailed configuration instructions)
-

- To establish the VNC connection, first configure the VNC Viewer, entering the VNC Server IP address

- A. When the Viewer PC is connected to the *console server* thru a SSH tunnel (over the public Internet, or a dial-in connection, or private network connection), enter *localhost* (or 127.0.0.1) as the IP VNC Server IP address; and *the source port* you entered when setting SSH tunneling /port forwarding (in Section 6.2.6) e.g. :1234



- B. When the Viewer PC is connected directly to the *console server* (i.e. locally or remotely through a VPN or dial in connection); and the VNC Host computer is serially connected to the *console server*; enter the IP address of the *console server* unit with the TCP port that the SDT tunnel will use. The TCP port will be 7900 plus the physical serial port number (i.e. 7901 to 7948, so all traffic directed to port 79xx on the *console server* is tunneled thru to port 5900 on the PPP connection on serial Port xx) e.g. for a Windows Viewer PC using UltraVNC connecting to a VNC Server which is attached to Port 1 on a *console server* located 192.168.0.1



- You can then establish the VNC connection by simply activating the VNC Viewer software on the Viewer PC and entering the password



Note For general background reading on Remote Desktop and VNC access we recommend the following:

- *The Microsoft Remote Desktop How-To*
<http://www.microsoft.com/windowsxp/using/mobility/getstarted/remotaintro.mspx>
 - *The Illustrated Network Remote Desktop help page*
<http://theillustratednetwork.mvps.org/RemoteDesktop/RemoteDesktopSetupandTroubleshooting.html>
 - *What is Remote Desktop in Windows XP and Windows Server 2003?* by Daniel Petri
http://www.petri.co.il/what's_remote_desktop.htm
 - *Frequently Asked Questions about Remote Desktop*
<http://www.microsoft.com/windowsxp/using/mobility/rdfaq.mspx>
 - *Secure remote access of a home network using SSH, Remote Desktop and VNC for the home user*
<http://theillustratednetwork.mvps.org/RemoteDesktop/SSH-RDP-VNC/RemoteDesktopVNCandSSH.html>
 - *Taking your desktop virtual with VNC*, Red Hat magazine
<http://www.redhat.com/magazine/006apr05/features/vnc/> and
<http://www.redhat.com/magazine/007may05/features/vnc/>
 - *Wikipedia* general background on VNC <http://en.wikipedia.org/wiki/VNC>
-

6.10 Using SDT to IP connect to hosts that are serially attached to the gateway

Network (IP) protocols like RDP, VNC and HTTP can also be used for connecting to host devices that are serially connected through their COM port to the *console server*. To do this you must:

- establish a PPP connection (Section 6.7.1) between the host and the gateway, then
- set up Secure Tunneling - Ports on the *console server* (Section 6.7.2), then
- configure *SDT Connector* to use the appropriate network protocol to access IP consoles on the host devices that are attached to the *Console server* serial ports (Section 6.7.3)

6.10.1 Establish a PPP connection between the host COM port and *console server*

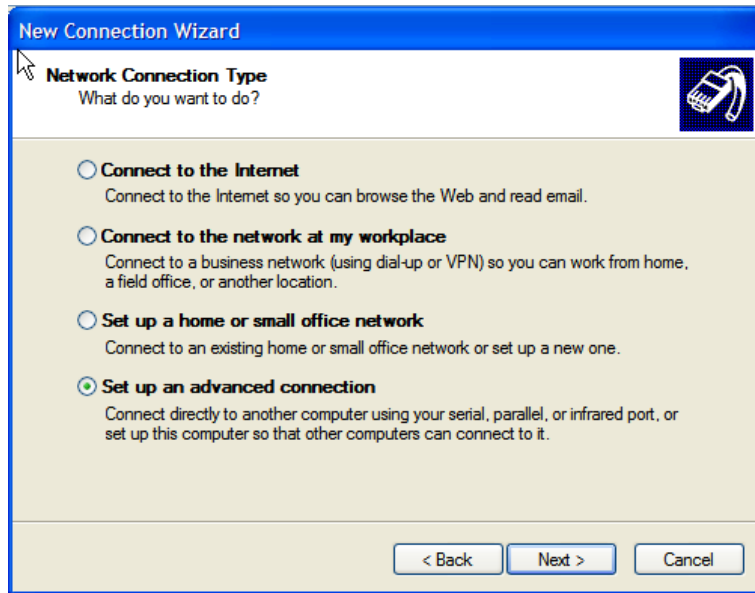
(This step is only necessary for serially connected computers)

Firstly, physically connect the COM port on the host computer that is to be accessed, to the serial port on the *console server* then:

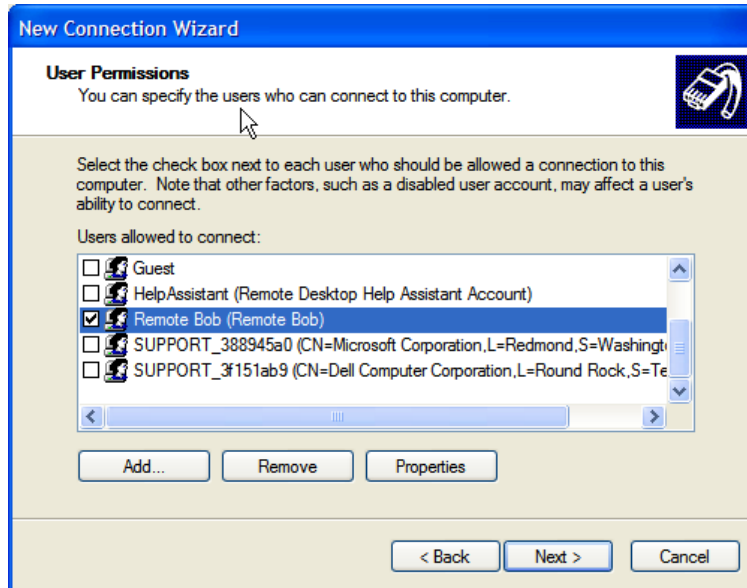
- A. For non Windows (Linux, UNIX, Solaris etc) computers establish a PPP connection over the serial port. The online tutorial <http://www.yolinux.com/TUTORIALS/LinuxTutorialPPP.html> presents a selection of methods for establishing a PPP connection for Linux

B. For Windows XP and 2003 computers follow the steps below to set up an advanced network connection between the Windows computer, through its COM port to the *console server*. Both Windows 2003 and Windows XP Professional allow you to create a *simple dial in service* which can be used for the Remote Desktop/VNC/HTTP/X connection to the *console server*:

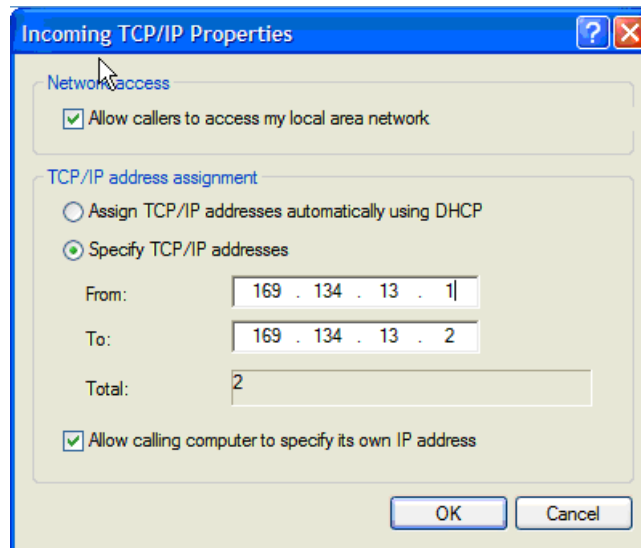
- Open **Network Connections** in Control Panel and click the **New Connection Wizard**



- Select **Set up an advanced connection** and click **Next**
- On the **Advanced Connection Options** screen select **Accept Incoming Connections** and click **Next**
- Select the **Connection Device** (i.e. the serial COM port on the Windows computer that you cabled through to the *console server*). By default select **COM1**. The COM port on the Windows computer should be configured to its maximum baud rate. Click **Next**
- On the **Incoming VPN Connection Options** screen select **Do not allow virtual private connections** and click **Next**



- Specify which *Users* will be allowed to use this connection. This should be the same *Users* who were given Remote Desktop access privileges in the earlier step. Click **Next**
- On the **Network Connection** screen select **TCP/IP** and click **Properties**



- Select **Specify TCP/IP addresses** on the **Incoming TCP/IP Properties** screen select **TCP/IP**. Nominate a *From:* and a *To:* TCP/IP address and click **Next**

Note You can choose any TCP/IP addresses so long as they are addresses which are not used anywhere else on your network. The *From:* address will be assigned to the Windows XP/2003 computer and the *To:* address will be used by the *console server*. For simplicity use the IP address as shown in the illustration above:

From: 169.134.13.1

To: 169.134.13.2

Alternately you can set the advanced connection and access on the Windows computer to use the *console server* defaults:

- Specify 10.233.111.254 as the *From:* address
- Select *Allow calling computer to specify its own address*

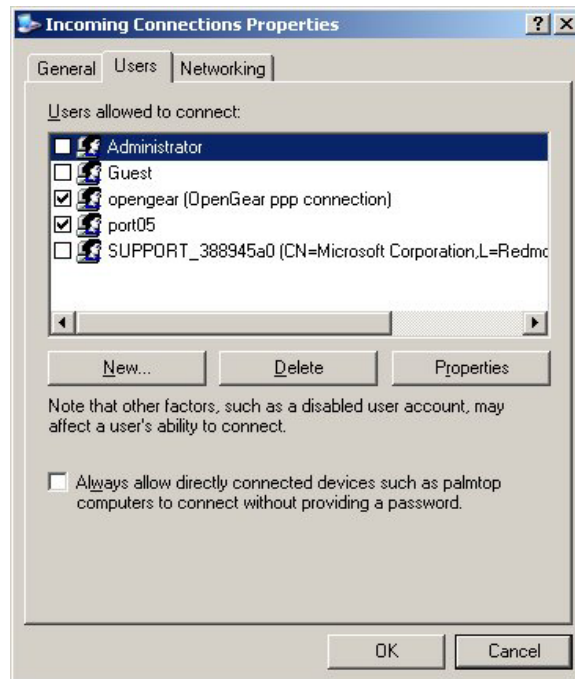
Also you could use the *console server* default username and password when you set up the new Remote Desktop *User* and gave this *User* permission to use the advance connection to access the Windows computer:

- The *console server* default *Username* is *portXX* where *XX* is the serial port number on the *console server*.
- The default *Password* is *portXX*

So to use the defaults for a RDP connection to the serial port 2 on the *console server*, you would have set up a Windows user named *port02*

-
- When the PPP connection has been set up, a network icon will appear in the Windows task bar

Note The above notes describe setting up an incoming connection for Windows XP. The steps are similar for Vista and Windows Server 2003/2008 however the set up screens present slightly differently:



You need to put a check in the box for *Always allow directly connected devices such as palmtop.....*

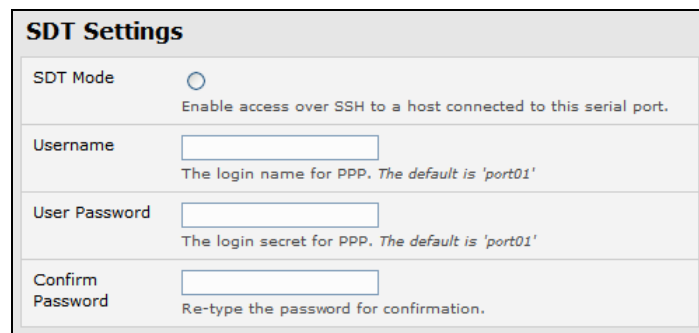
Also the option for to **Set up an advanced connection** is not available in Windows 2003 if RRAS is configured. If RRAS has been configured it is a simply task to enable the null modem connection for the dial-in configuration.

- C. For earlier version Windows computers again follow the steps in Section B. above, however to get to the **Make New Connection** button:
- For Windows 2000, click **Start** and select **Settings** then at the **Dial-Up Networking Folder** click **Network and Dial-up Connections** and click **Make New Connection**. Note you may need to first set up connection over the COM port using **Connect directly to another computer** before proceeding to **Set up an advanced connection**
 - For Windows 98 you double click **My Computer** on the Desktop, then open **Dial-Up Networking** and double click

6.10.2 Set up SDT Serial Ports on *console server*

To set up *RDP (and VNC) forwarding* on the *console server* Serial Port that is connected to the Windows computer COM port:

- Select the **Serial & Network: Serial Port** menu option and click **Edit** (for the particular Serial Port that is connected to the Windows computer COM port)
- On the SDT Settings menu select **SDT Mode** (which will enable port forwarding and SSH tunneling) and enter a **Username** and **User Password**.



Note When you enable SDT, this will override all other Configuration protocols on that port

Note If you leave the *Username* and *User Password* fields blank, they default to *portXX* and *portXX* where *XX* is the serial port number. So the default username and password for Secure RDP over Port 2 is *port02*

- Ensure the *console server* **Common Settings** (Baud Rate, Flow Control) are the same as were set up on the Windows computer COM port and click **Apply**
- RDP and VNC forwarding over serial ports is enabled on a Port basis. You can add *Users* who can have access to these ports (or reconfigure *User* profiles) by selecting **Serial & Network :User & Groups** menu tag - as described earlier in Chapter 4 *Configuring Serial Ports*

6.10.3 Set up SDT Connector to ssh port forward over the *console server* Serial Port

In the *SDT Connector* software running on your remote computer specify the gateway IP address of your *console server* and a username/password for a user you have setup on the *console server* that has access to the desired port.

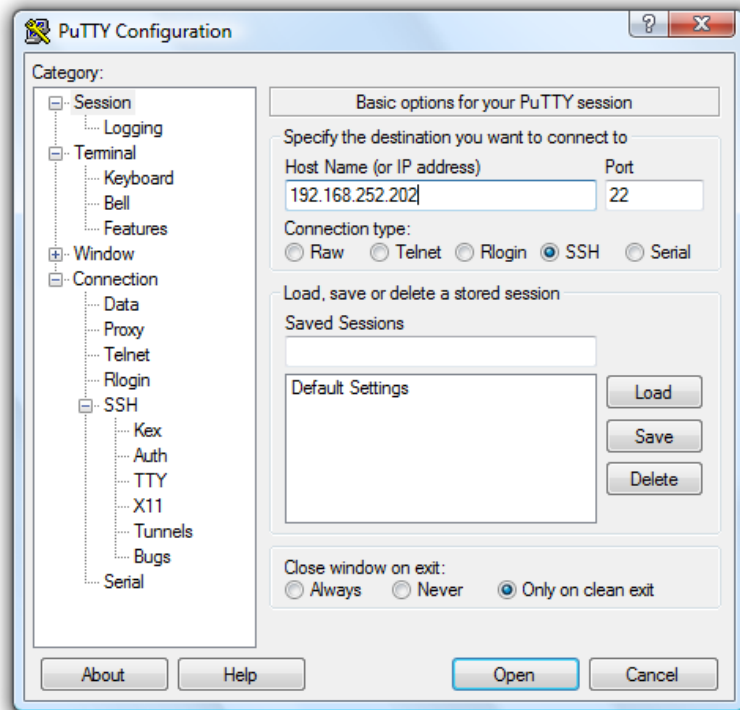
Next you need to add a New SDT Host. In the Host address you need to put portxx where xx = the port you are connecting to. Example for port 3 you would have a Host Address of: port03 and then select the RDP Service check box.

6.11 SSH Tunneling using other SSH clients (e.g. PuTTY)

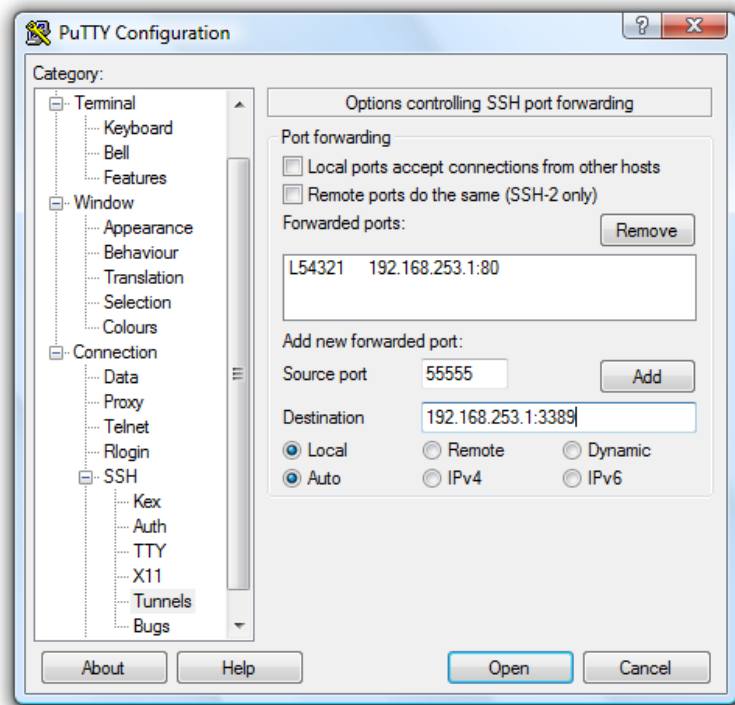
As covered in the previous sections of this chapter we recommend you use the *SDT Connector* client software that is supplied with the *console server*. However there's also a wide selection of commercial and free SSH client programs that can also provide the secure SSH connections to the *console servers* and secure tunnels to connected devices:

- PuTTY is a complete (though not very user friendly:) freeware implementation of SSH for Win32 and UNIX platforms
- SSHTerm is a useful open source SSH communications package
- SSH Tectia is leading end-to-end commercial communications security solution for the enterprise
- Reflection for Secure IT (formerly F-Secure SSH) is another good commercial SSH-based security solution

By way of example the steps below show the establishment of an SSH tunneled connection to a network connected device using the PuTTY client software.



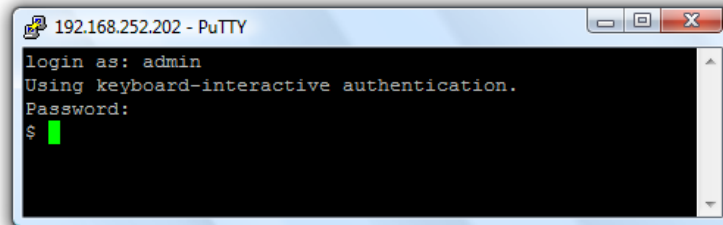
- In the **Session** menu enter the IP address of the *console server* in the **Host Name or IP address** field
 - For dial-in connections, this IP address will be the **Local** Address that you assigned to the *console server* when you set it up as the Dial-In PPP Server
 - For Internet (or local/VPN connections) connections this will be the public IP address of the *console server*
- Select the **SSH Protocol**, and the **Port** will be set as 22
- Go to the **SSH -> Tunnels** menu and in *Add new forwarded port* enter any high unused port number for the **Source port** e.g 54321
- Set the **Destination:** IP details
 - If your destination device is network connected to the *console server* and you are connecting using RDP, set the Destination as *<Managed Device IP address/DNS Name>:3389* e.g. if when setting up the *Managed Device* as *Network Host* on the *console server* you specified its IP address to be 192.168.253.1 (or its DNS Name was *accounts.myco.intranet.com*) then specify the Destination as *192.168.253.1:3389* (or *accounts.myco.intranet.com:3389*). Only devices which have been configured as networked Hosts can be accessed using SSH tunneling (except by the “root” user who can tunnel to any IP address the *console server* can route to.



- If your destination computer is serially connected to the *console server*, set the *Destination* as *<port label>:3389* e.g. if the **Label** you specified on the serial port on the *console server* is *win2k3*, then specify the remote host as *win2k3:3389* . Alternative you can set the *Destination* as *portXX:3389* where XX is the SDT enabled serial port number e.g. if port 4 is on the *console server* is to carry the RDP traffic then specify *port04:3389*

Note http://www.jfitz.com/tips/putty_config.html has useful examples on configuring PuTTY for SSH tunneling

- Select **Local** and click the **Add** button
- Click **Open** to SSH connect the Client PC to the *console server*. You will now be prompted for the Username/Password for the *console server* user



- If you are connecting as a *User* in the “users” group then you can only SSH tunnel to Hosts and Serial Ports where you have specific access permissions
- If you are connecting as an *Administrator* (in the “admin” group) then you can connect to any configured Host or Serial Ports (which has SDT enabled)

To set up the secure SSH tunnel for a HTTP browser connection to the *Managed Device* specify port 80 (rather than port 3389 as was used for RDP) in the Destination IP address.

To set up the secure SSH tunnel from the Client (Viewer) PC to the *console server* for VNC follow the steps above, however when configuring the VNC port redirection specify port 5900 in the Destination IP address.

Note How secure is VNC? VNC access generally allows access to your whole computer, so security is very important. VNC uses a random challenge-response system to provide the basic authentication that allows you to connect to a VNC server. This is reasonably secure and the password is not sent over the network.

However, once connected, all subsequent VNC traffic is unencrypted. So a malicious user could snoop your VNC session. Also there are VNC scanning programs available, which will scan a subnet looking for PCs which are listening on one of the ports which VNC uses.

Tunneling VNC over a SSH connection ensures all traffic is strongly encrypted. Also no VNC port is ever open to the internet, so anyone scanning for open VNC ports will not be able to find your computers. When tunneling VNC over a SSH connection, the only port which you're opening on your *console server* the SDT port 22.

So sometimes it may be prudent to tunnel VNC through SSH even when the Viewer PC and the *console server* are both on the same local network.

The CMS platform is a dedicated Linux computer, optimized to provide monitoring and secure access to serial and network consoles of critical server systems and their supporting power and networking infrastructure.

The CMS is built on the 2.6 uCLinux kernel as developed by the uCLinux project. This is GPL code and source can be found at <http://cvs.uclinux.org>. Some uCLinux commands have config files that can be altered (e.g. *portmanager*, *inetd*, *init*, *ssh/sshd/scp/sshkeygen*, *ucd-snmpd*, *samba*, *fnord*, *sslwrap*). Other commands you can run and do neat stuff with (e.g. *loopback*, *bash* (shell), *ftp*, *hwclock*, *iproute*, *iptables*, *netcat*, *ifconfig*, *mii-tool*, *netstat*, *route*, *ping*, *portmap*, *pppd*, *routed*, *setserial*, *smtplib*, *stty*, *stunnel*, *tcpdump*, *ftpp*, *tip*, *traceroute*)

Below are most of the standard uCLinux and BusyBox commands (and some custom Opendgear commands) that are in the default build tree. The *Administrator* can use these to configure the CMS, and monitor and manage attached serial console and host devices:

addgroup *	Add a group or add an user to a group
adduser *	Add an user
agetty	alternative Linux getty
arp	Manipulate the system ARP cache
arping	Send ARP requests/replies
bash	GNU Bourne-Again Shell
busybox	Swiss army knife of embedded Linux commands
cat *	Concatenate FILE(s) and print them to stdout
chat	Useful for interacting with a modem connected to stdin/stdout
chgrp *	Change file access permissions
chmod *	Change file access permissions
chown *	Change file owner and group
config	Opendgear tool to manipulate and query the system configuration from the command line
cp *	Copy files and directories
date *	Print or set the system date and time
dd *	Convert and copy a file
deluser *	Delete USER from the system
df *	Report filesystem disk space usage
dhcpcd	Dynamic Host Configuration Protocol server
discard	Network utility that listens on the discard port
dmesg *	Print or control the kernel ring buffer
echo *	Print the specified ARGs to stdout
erase	Tool for erasing MTD partitions
eraseall	Tool for erasing entire MTD partitions
false *	Do nothing, unsuccessful
find	Search for files
flashw	Write data to individual flash devices
flatfsd	Daemon to save RAM file systems back to FLASH
ftp	Internet file transfer program
gen-keys	SSH key generation program
getopt *	Parses command options
gettyd	Getty daemon
grep *	Print lines matching a pattern

gunzip *	Compress or expand files
gzip *	Compress or expand files
hd	ASCII, decimal, hexadecimal, octal dump
hostname *	Get or set hostname or DNS domain name
httpd	Listen for incoming HTTP requests
hwclock	Query and set hardware clock (RTC)
inetd	Network super-server daemon
inetd-echo	Network echo utility
init	Process control initialization
ip	Show or manipulate routing, devices, policy routing and tunnels
ipmitool	Linux IPMI manager
iptables	Administration tool for IPv4 packet filtering and NAT
ip6tables	Administration tool for IPv6 packet filtering
iptables-restore	Restore IP Tables
iptables-save	Save IP Tables
kill *	Send a signal to a process to end gracefully
ln *	Make links between files
login	Begin session on the system
loopback	Opengear loopback diagnostic command
loopback1	Opengear loopback diagnostic command
loopback2	Opengear loopback diagnostic command
loopback8	Opengear loopback diagnostic command
loopback16	Opengear loopback diagnostic command
loopback48	Opengear loopback diagnostic command
ls *	List directory contents
mail	Send and receive mail
mkdir *	Make directories
mkfs.jffs2	Create an MS-DOS file system under Linux
mknod *	Make block or character special files
more *	File perusal filter for crt viewing
mount *	Mount a file system
msmtp	SMTP mail client
mv *	Move (rename) files
nc	TCP/IP Swiss army knife
netflash	Upgrade firmware on ucLinux platforms using the blkmem interface
netstat	Print network connections, routing tables, interface statistics etc
ntpd	Network Time Protocol (NTP) daemon
pgrep	Display process(es) selected by regex pattern
pidof	Find the process ID of a running program
ping	Send ICMP ECHO_REQUEST packets to network hosts
ping6	IPv6 ping
pkill	Sends a signal to process(es) selected by regex pattern
pmchat	Opengear command similar to the standard chat command (via portmanager)
pmdeny	
pminetd	
pmloggerd	
pmshell	Opengear command similar to the standard <i>tip</i> or <i>cu</i> but all serial port access is directed via

	the portmanager.
pmusers	Opengear command to query portmanager for active user sessions
portmanager	Opengear command that handles all serial port access
portmap	DARPA port to RPC program number mapper
pppd	Point-to-Point protocol daemon
ps *	Report a snapshot of the current processes
pwd *	Print name of current/working directory
reboot *	<i>Soft</i> reboot
rm *	Remove files or directories
rmdir *	Remove empty directories
routed	Show or manipulate the IP routing table
routed	Show or manipulate the IP routing table
route	IP Route tool to flush IPv4 routes
route	IP Route tool to list routes
rtacct	Applet printing /proc/net/rt_acct
rtmon	RTnetlink listener
scp	Secure copy (remote file copy program)
sed *	Text stream editor
setmac	Sets the MAC address
setserial	Sets and reports serial port configuration
sh	Shell
showmac	Shows MAC address
sleep *	Delay for a specified amount of time
smbmnt	Helper utility for mounting SMB file systems
smbmount	Mount an SMBFS file system
smbumount	SMBFS umount for normal users
snmpd	SNMP daemon
snmptrap	Sends an SNMP notification to a manager
sredird	RFC 2217 compliant serial port redirector
ssh	OpenSSH SSH client (remote login program)
ssh-keygen	Authentication key generation, management, and conversion
sshd	OpenSSH SSH daemon
sslwrap	Program that allows plain services to be accessed via SSL
stty	Change and print terminal line settings
stunnel	Universal SSL tunnel
sync *	Flush file system buffers
sysctl	Configure kernel parameters at runtime
syslogd	System logging utility
tar *	The tar archiving utility
tc	Show traffic control settings
tcpdump	Dump traffic on a network
telnetd	Telnet protocol server
tftp	Client to transfer a file from/to tftp server
tftpd	Trivial file Transfer Protocol (tftp) server
tip	Simple terminal emulator/cu program for connecting to modems and serial devices
top	Provide a view of process activity in real time
touch *	Change file timestamps
traceroute	Print the route packets take to network host

tracert6	Tracert for IPv6
true *	Returns an exit code of TRUE (0)
umount *	Unmount file systems
uname *	Print system information
usleep *	Delay for a specified amount of time
vconfig *	Create and remove virtual ethernet devices
vi *	Busybox clone of the VI text editor
w	Show who is logged on and what they are doing
zcat *	Identical to gunzip -c

Commands above which are appended with '*' come from BusyBox (the Swiss Army Knife of embedded Linux) <http://www.busybox.net/downloads/BusyBox.html>. Others are generic Linux commands and most commands the **-h** or **--help** argument to provide a terse runtime description of their behavior. More details on the generic Linux commands can be found online at <http://en.tldp.org/HOWTO/HOWTO-INDEX/howtos.html> and <http://www.faqs.org/docs/Linux-HOWTO/Remote-Serial-Console-HOWTO.html>

An updated list of the commands in the latest CMS build can be found at <http://www.opengear.com/faq233.html>. However it may be worth using **ls** command to view all the commands actually available in the `/bin` directory in your CMS.

There were a number of Opengear tools listed above that make it simple to configure the CMS and ensure the changes are stored in the CMS's flash memory etc. These commands are covered in the previous chapters and include:

- **config** which allows manipulation and querying of the system configuration from the command line. With *config* a new configuration can be activated by running the relevant configurator, which performs the action necessary to make the configuration changes live
- **SDT Connector** is a java client application that provides point-and-click SSH tunneled connections to the CMS and *Managed Devices*
- **Nagios** is a popular enterprise-class management tool that provides central monitoring of the hosts and services in distributed networks. For CLI details refer <http://www.nagios.org>

Many components of the CMS software are licensed under the GNU General Public License (version 2), which Opengear supports. You may obtain a copy of the GNU General Public License at <http://www.fsf.org/copyleft/gpl.html>. Opengear will provide source code for any of the components of the software licensed under the GNU General Public License upon request.

The CMS BIOS (boot loader code) is a port of *uboot* which is also a GPL package with source openly available.

The CMS CGIs (the html code, xml code and web config tools for the Management Console) are proprietary to Opengear, however the code will be provided to customers, under NDA.

Also inbuilt in the CMS is a Port Manager application and Configuration tools as described in *Chapters 14* and *15*. These both are proprietary to Opengear, but open to customers (as above).

The CMS also supports GNU *bash* shell script enabling the *Administrator* to run custom scripts. GNU *bash*, version 2.05.0(1)-release (arm-OpenGear-linux-gnu) offers the following shell commands:

alias [-p] [name[=value] ...]	local name[=value] ...
bg [job_spec]	logout
bind [-lpsPVS] [-m keymap] [-f fi break [n]]	popd [+N -N] [-n]
builtin [shell-builtin [arg ...]]	printf format [arguments]
case WORD in [PATTERN [PATTERN]]	pushd [dir +N -N] [-n]
cd [-PL] [dir]	pwd [-PL]
command [-pVv]	read [-ers] [-t timeout] [-p prompt]
command [arg ...]	readonly [-anf] [name ...] or read return [n]

<p> compngen [-abcdefjkvu] [-o option] complete [-abcdefjkvu] [-pr] [-o o] continue [n] declare [-afRxi] [-p] name[=value] dirs [-clpv] [+N] [-N] disown [-h] [-ar] [jobspec ...] echo [-neE] [arg ...] enable [-pnds] [-a] [-f filename] eval [arg ...] exec [-cl] [-a name] file [redirec] exit [n] export [-nf] [name ...] or export false fc [-e ename] [-nlr] [first] [last] fg [job_spec] for NAME [in WORDS ... ;] do COMMA function NAME { COMMANDS ; } or NA getopts optstring name [arg] hash [-r] [-p pathname] [name ...] help [-s] [pattern ...] history [-c] [-d offset] [n] or hi if COMMANDS; then COMMANDS; [elif jobs [-lnprs] [jobspec ...] or <i>job kill</i> [-s <i>sigspec</i> <i>-n signum</i> <i>-si let arg</i> [arg ...] </p>	<p> select NAME [in WORDS ... ;] do COMMANDS set [--abefhkmnptuvxBCHP] [-o opti] shift [n] shopt [-pqsu] [-o long-option] opt source filename suspend [-f] test [expr] time [-p] PIPELINE times trap [arg] [signal_spec ...] true type [-apt] name [name ...] typeset [-afRxi] [-p] name[=value ulimit [- SHacdfImnpstuv] [limit] umask [-p] [-S] [mode] unalias [-a] [name ...] unset [-f] [-v] [name ...] until COMMANDS; do COMMANDS; done variables - Some variable names an wait [n] while COMMANDS; do COMMANDS; done { COMMANDS ; } </p>
---	---

FEATURE	VALUE
Dimensions	17 x 6.7 x 1.75 in (44 x 17 x 4.5 cm)
Weight	8.5 lb (3.9 kg)
Ambient operating temperature	5°C to 50°C (41°F to 122°F)
Non operating storage temp	-30°C to +60°C (-20°F to +140°F)
Humidity	5% to 90%
Power Consumption	Less than 30W
CPU	AMD Geode LX800 500MHz
Memory	256MB DDR, 4GB Compact Flash, 4MB Award BIOS
Ethernet Connectors	One RJ-45 10/100Base-T Ethernet ports

Please take care to follow the safety precautions below when installing and operating the *CMS*:

- Do not remove the metal covers. There are no operator serviceable components inside. Opening or removing the cover may expose you to dangerous voltage which may cause fire or electric shock. Refer all service to Opendgear qualified personnel
- To avoid electric shock the power cord protective grounding conductor must be connected through to ground.
- Always pull on the plug, not the cable, when disconnecting the power cord from the socket.

Do not connect or disconnect the *CMS* during an electrical storm. Also it is recommended you use a surge suppressor or UPS to protect the equipment from transients.

FCC Warning Statement

This device complies with Part 15 of the FCC rules. Operation of this device is subject to the following conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.

TERM	MEANING
Authentication	Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Authentication confirms that data is sent to the intended recipient and assures the recipient that the data originated from the expected sender and has not been altered on route
BIOS	Basic Input/Output System is the built-in software in a computer that are executed on start up (boot) and that determine what the computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions
Bonding	Ethernet Bonding or Failover is the ability to detect communication failure transparently, and switch from one LAN connection to another.
BOOTP	Bootstrap Protocol. A protocol that allows a network user to automatically receive an IP address and have an operating system boot without user interaction. BOOTP is the basis for the more advanced DHCP
Certificates	A digitally signed statement that contains information about an entity and the entity's public key, thus binding these two pieces of information together. A certificate is issued by a trusted organization (or entity) called a Certification Authority (CA) after the CA has verified that the entity is who it says it is.
Certificate Authority	A Certificate Authority is a trusted third party, which certifies public key's to truly belong to their claimed owners. It is a key part of any Public Key Infrastructure, since it allows users to trust that a given public key is the one they wish to use, either to send a private message to its owner or to verify the signature on a message sent by that owner.
Certificate Revocation List	A list of certificates that have been revoked by the CA before they expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a connection to the CMS.
CHAP	Challenge-Handshake Authentication Protocol (CHAP) is used to verify a user's name and password for PPP Internet connections. It is more secure than PAP, the other main authentication protocol.
DHCP	Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses to computers when they are connected to the network.
DNS	Domain Name System that allocates Internet domain names and translates them into IP addresses. A domain name is a meaningful and easy to remember name for an IP address.
DUN	Dial Up Networking
Encryption	The technique for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. The proper decryption key is required to read the message.

Ethernet	A physical layer protocol based upon IEEE standards
Firewall	A network gateway device that protects a private network from users on other networks. A firewall is usually installed to allow users on an intranet access to the public Internet without allowing public Internet users access to the intranet.
Gateway	A machine that provides a route (or pathway) to the outside world.
Hub	A network device that allows more than one computer to be connected as a LAN, usually using UTP cabling.
Internet	A worldwide system of computer networks - a public, cooperative, and self-sustaining network of networks accessible to hundreds of millions of people worldwide. The Internet is technically distinguished because it uses the TCP/IP set of protocols.
Intranet	A private TCP/IP network within an enterprise.
IPMI	Intelligent Platform Management Interface (IPMI) is a remote hardware health monitoring and management system that defines interfaces for use in monitoring the physical health of servers, such as temperature, voltage, fans, power supplies and chassis. It was developed by Dell, HP, Intel and NEC, but has now been adopted by more than 150 server technology and ships with over 70% of servers. Servers with IPMI functionality let network managers access and monitor server hardware, and diagnose and restore a frozen server to normal operation. IPMI defines the protocols for interfacing with a service processor embedded into a server platform.
Key lifetimes	The length of time before keys are renegotiated
LAN	Local Area Network
LDAP	The Lightweight Directory Access Protocol (LDAP) is based on the X.500 standard, but significantly simpler and more readily adapted to meet custom needs. The core LDAP specifications are all defined in RFCs. LDAP is a protocol used to access information stored in an LDAP server.
LED	Light-Emitting Diode
MAC address	Every piece of Ethernet hardware has a unique number assigned to it called it's MAC address. Ethernet is used locally to connect the CMS to the Internet, and it may share the local network with many other appliances. The MAC address is used by the local Internet router in order to direct CMS traffic to it rather than somebody else in the local area. It is a 48-bit number usually written as a series of 6 hexadecimal octets, e.g. 00:d0:cf:00:5b:da. A CMS has a MAC address listed on a label underneath the device.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server. It is more secure than PAP or CHAP, and is the only option that also supports data encryption.
NAT	Network Address Translation. The translation of an IP address used on one network to an IP address on another network. Masquerading is one particular form of NAT.
Net mask	The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range.
NFS	Network File System is a protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer.

NTP	Network Time Protocol (NTP) used to synchronize clock times in a network of computers
OUT OF BAND	Out-of-Band (OoB) management is any management done over channels and interfaces that are separate from those used for user/customer data. Examples would include a serial console interface or a network interface connected to a dedicated management network that is not used to carry customer traffic, or to a BMC/service processor. Any management done over the same channels and interfaces used for user/customer data is In Band.
PAP	Password Authentication Protocol (PAP) is the usual method of user authentication used on the internet: sending a username and password to a server where they are compared with a table of authorized users. Whilst most common, PAP is the least secure of the authentication options.
PPP	Point-to-Point Protocol. A networking protocol for establishing simple links between two peers.
RADIUS	The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises as an access server authentication and accounting protocol. The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms.
Router	A network device that moves packets of data. A router differs from hubs and switches because it is "intelligent" and can route packets to their final destination.
SMASH	Systems Management Architecture for Server Hardware is a standards-based protocols aimed at increasing productivity of the management of a data center. The SMASH Command Line Protocol (SMASH CLP) specification provides an intuitive interface to heterogeneous servers independent of machine state, operating system or OS state, system topology or access method. It is a standard method for local and remote management of server hardware using out-of-band communication
SMTP	Simple Mail Transfer Protocol. CMS includes, SMTPclient, a minimal SMTP client that takes an email message body and passes it on to a SMTP server (default is the MTA on the local host).
SOL	Serial Over LAN (SOL) enables servers to transparently redirect the serial character stream from the baseboard universal asynchronous receiver/transmitter (UART) to and from the remote-client system over a LAN. With SOL support and BIOS redirection (to serial) remote managers can view the BIOS/POST output during power on, and reconfigured.
SSH	Secure Shell is secure transport protocol based on public-key cryptography.
SSL	Secure Sockets Layer is a protocol that provides authentication and encryption services between a web server and a web browser.
TACACS+	The Terminal Access Controller Access Control System (TACACS+) security protocol is a more recent protocol developed by Cisco. It provides detailed accounting information and flexible administrative control over the authentication and authorization processes. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting services independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. There is a draft RFC detailing this protocol.
TCP/IP	Transmission Control Protocol/Internet Protocol. The basic protocol for Internet communication.

TCP/IP address	Fundamental Internet addressing method that uses the form nnn.nnn.nnn.nnn.
Telnet	Telnet is a terminal protocol that provides an easy-to-use method of creating terminal connections to a network.
UTC	Coordinated Universal Time.
UTP	Unshielded Twisted Pair cabling. A type of Ethernet cable that can operate up to 100Mb/s. Also known as Category 5 or CAT 5.
VNC	Virtual Network Computing (VNC) is a desktop protocol to remotely control another computer. It transmits the keyboard presses and mouse clicks from one computer to another relaying the screen updates back in the other direction, over a network.
WAN	Wide Area Network
WINS	Windows Internet Naming Service that manages the association of workstation names and locations with IP addresses

For further technology definitions refer:

<http://linux-documentation.com/en/documentation/linux-dictionary/index.html> or

<http://en.wikipedia.org/>

READ BEFORE USING THE ACCOMPANYING SOFTWARE

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE ACCOMPANYING SOFTWARE, THE USE OF WHICH IS LICENSED FOR USE ONLY AS SET FORTH BELOW. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE. IF YOU USE ANY PART OF THE SOFTWARE, SUCH USE WILL INDICATE THAT YOU ACCEPT THESE TERMS.

You have acquired a product that includes Opengear (“Opengear”) proprietary software and/or proprietary software licensed to Opengear. This Opengear End User License Agreement (“EULA”) is a legal agreement between you (either an individual or a single entity) and Opengear for the installed software product of Opengear origin, as well as associated media, printed materials, and “online” or electronic documentation (“Software”). By installing, copying, downloading, accessing, or otherwise using the Software, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, Opengear is not willing to license the Software to you. In such event, do not use or install the Software. If you have purchased the Software, promptly return the Software and all accompanying materials with proof of purchase for a refund.

Products with separate end user license agreements that may be provided along with the Software are licensed to you under the terms of those separate end user license agreements.

LICENSE GRANT. Subject to the terms and conditions of this EULA, Opengear grants you a nonexclusive right and license to install and use the Software on a single CPU, provided that, (1) you may not rent, lease, sell, sublicense or lend the Software; (2) you may not reverse engineer, decompile, disassemble or modify the Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation; and (3) you may not transfer rights under this EULA unless such transfer is part of a permanent sale or transfer of the Product, you transfer at the same time all copies of the Software to the same party or destroy such materials not transferred, and the recipient agrees to this EULA.

No license is granted in any of the Software’s proprietary source code. This license does not grant you any rights to patents, copyright, trade secrets, trademarks or any other rights with respect to the Software.

You may make a reasonable number of copies of the electronic documentation accompanying the Software for each Software license you acquire, provided that, you must reproduce and include all copyright notices and any other proprietary rights notices appearing on the electronic documentation. Opengear reserves all rights not expressly granted herein.

INTELLECTUAL PROPERTY RIGHTS. The Software is protected by copyright laws, international copyright treaties, and other intellectual property laws and treaties. Opengear and its suppliers retain all ownership of, and intellectual property rights in (including copyright), the Software components and all copies thereof, provided however, that (1) certain components of the Software, including *SDT Connector*, are components licensed under the GNU General Public License Version 2, which Opengear supports, and (2) the *SDT Connector* includes code from JSch, a pure Java implementation of SSH2 which is licensed under BSD style license. Copies of these licenses are detailed below and Opengear will provide source code for any of the components of the Software licensed under the GNU General Public License upon request.

EXPORT RESTRICTIONS. You agree that you will not export or re-export the Software, any part thereof, or any process or service that is the direct product of the Software in violation of any applicable laws or regulations of the United States or the country in which you obtained them.

U.S. GOVERNMENT RESTRICTED RIGHTS. The Software and related documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights at 48 C.F.R. 52.227-19, as applicable, or any successor regulations.

TERM AND TERMINATION. This EULA is effective until terminated. The EULA terminates immediately if you fail to comply with any term or condition. In such an event, you must destroy all copies of the Software. You may also terminate this EULA at any time by destroying the Software.

GOVERNING LAW AND ATTORNEY’S FEES. This EULA is governed by the laws of the State of Utah, USA, excluding its conflict of law rules. You agree that the United Nations Convention on Contracts for the International

Sale of Goods is hereby excluded in its entirety and does not apply to this EULA. If you acquired this Software in a country outside of the United States, that country's laws may apply. In any action or suit to enforce any right or remedy under this EULA or to interpret any provision of this EULA, the prevailing party will be entitled to recover its costs, including reasonable attorneys' fees.

ENTIRE AGREEMENT. This EULA constitutes the entire agreement between you and Opengear with respect to the Software, and supersedes all other agreements or representations, whether written or oral. The terms of this EULA can only be modified by express written consent of both parties. If any part of this EULA is held to be unenforceable as written, it will be enforced to the maximum extent allowed by applicable law, and will not affect the enforceability of any other part.

Should you have any questions concerning this EULA, or if you desire to contact Opengear for any reason, please contact the Opengear representative serving your company.

THE FOLLOWING DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY IS INCORPORATED INTO THIS EULA BY REFERENCE. THE SOFTWARE IS NOT FAULT TOLERANT. YOU HAVE INDEPENDENTLY DETERMINED HOW TO USE THE SOFTWARE IN THE DEVICE, AND OPENGEAR HAS RELIED UPON YOU TO CONDUCT SUFFICIENT TESTING TO DETERMINE THAT THE SOFTWARE IS SUITABLE FOR SUCH USE.

LIMITED WARRANTY Opengear warrants the media containing the Software for a period of ninety (90) days from the date of original purchase from Opengear or its authorized retailer. Proof of date of purchase will be required. Any updates to the Software provided by Opengear (which may be provided by Opengear at its sole discretion) shall be governed by the terms of this EULA. In the event the product fails to perform as warranted, Opengear's sole obligation shall be, at Opengear's discretion, to refund the purchase price paid by you for the Software on the defective media, or to replace the Software on new media. Opengear makes no warranty or representation that its Software will meet your requirements, will work in combination with any hardware or application software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the Software will be corrected.

OPENGEAR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OTHER THAN AS STATED HEREIN, THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT IS WITH YOU. ALSO, THERE IS NO WARRANTY AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE OR AGAINST INFRINGEMENT. IF YOU HAVE RECEIVED ANY WARRANTIES REGARDING THE DEVICE OR THE SOFTWARE, THOSE WARRANTIES DO NOT ORIGINATE FROM, AND ARE NOT BINDING ON, OPENGEAR.

NO LIABILITY FOR CERTAIN DAMAGES. EXCEPT AS PROHIBITED BY LAW, OPENGEAR SHALL HAVE NO LIABILITY FOR COSTS, LOSS, DAMAGES OR LOST OPPORTUNITY OF ANY TYPE WHATSOEVER, INCLUDING BUT NOT LIMITED TO, LOST OR ANTICIPATED PROFITS, LOSS OF USE, LOSS OF DATA, OR ANY INCIDENTAL, EXEMPLARY SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER UNDER CONTRACT, TORT, WARRANTY OR OTHERWISE ARISING FROM OR IN CONNECTION WITH THIS EULA OR THE USE OR PERFORMANCE OF THE SOFTWARE. IN NO EVENT SHALL OPENGEAR BE LIABLE FOR ANY AMOUNT IN EXCESS OF THE LICENSE FEE PAID TO OPENGEAR UNDER THIS EULA. SOME STATES AND COUNTRIES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

JSch License

SDT Connector includes code from JSch, a pure Java implementation of SSH2. JSch is licensed under BSD style license and it is:

Copyright (c) 2002, 2003, 2004 Atsuhiko Yamanaka, JCraft, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JCRAFT, INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SDT Connector License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING

OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

SUN Java License

1. **Java Technology Restrictions.** Licensee shall not create, modify, change the behavior of, or authorize licensees of Licensee to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation. In the event that Licensee creates an additional API(s) which: (a) extends the functionality of a Java Environment; and (b) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, Licensee must promptly publish broadly an accurate specification for such API for free use by all developers.

2. **Trademarks and Logos.** This License does not authorize an end user licensee to use any Sun Microsystems, Inc. name, trademark, service mark, logo or icon. The end user licensee acknowledges that Sun owns the Java trademark and all Java-related trademarks, logos and icons including the Coffee Cup and Duke ("Java Marks") and agrees to: (a) comply with the Java Trademark Guidelines at <http://java.sun.com/trademarks.html>; (b) not do anything harmful to or inconsistent with Sun's rights in the Java Marks; and (c) assist Sun in protecting those rights, including assigning to Sun any rights acquired by Licensee in any Java Mark.

3. **Source Code.** Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of your license. Source code may not be redistributed unless expressly provided for in the terms of your license.

4. **Third Party Code.** Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file.

STANDARD WARRANTY

Opengear, Inc., its parent, affiliates and subsidiaries, (collectively, "Opengear") warrant your Opengear product to be in good working order and to be free from defects in workmanship and material (except in those cases where the materials are supplied by the Purchaser) under normal and proper use and service for the period of four (4) years from the date of original purchase from an Authorized Opengear reseller (for CMS6100, CMS6000, KCS61xx, CM4116, CM4148 and all IM/IMG42xx products) and one (1) year from the date of original purchase from an Authorized Opengear reseller for all other product. In the event that this product fails to meet this warranty within the applicable warranty period, and provided that Opengear confirms the specified defects, Purchaser's sole remedy is to have Opengear, in Opengear's sole discretion, repair or replace such product at the place of manufacture, at no additional charge other than the cost of freight of the defective product to and from the Purchaser. Repair parts and replacement products will be provided on an exchange basis and will be either new or reconditioned. Opengear will retain, as its property, all replaced parts and products. Notwithstanding the foregoing, this hardware warranty does not include service to replace or repair damage to the product resulting from accident, disaster, abuse, misuse, electrical stress, negligence, any non- Opengear modification of the product except as provided or explicitly recommended by Opengear, or other cause not arising out of defects in material or workmanship. This hardware warranty also does not include service to replace or repair damage to the product if the serial number or seal or any part thereof has been altered, defaced or removed. If Opengear does not find the product to be defective, the Purchaser will be invoiced for said inspection and testing at Opengear's then current rates, regardless of whether the product is under warranty.

RMA RETURN PROCEDURE

If this product requires service during the applicable warranty period, a Return Materials Authorization (RMA) number must first be obtained from Opengear. Product that is returned to Opengear for service or repair without an RMA number will be returned to the sender unexamined. Product should be returned, freight prepaid, in its original or equivalent packaging, to:

Opengear Service Center
Suite A, 630 West 9560 South
Sandy, Utah 84070

Proof of purchase date must accompany the returned product and the Purchaser shall agree to insure the product or assume the risk of loss of damage in transit. Contact Opengear by emailing support@opengear.com for further information.

TECHNICAL SUPPORT

Purchaser is entitled to thirty (30) days free telephone support (USA ONLY) and twelve (12) months free e-mail support (world wide) from date of purchase provided that the Purchaser first register their product(s) with Opengear by filling in the on-line form <http://www.opengear.com/registration.html>. Telephone and e-mail support is available from 9:00 AM to 5:00 PM, Mountain Time.

Opengear's standard warranty includes free access to Opengear's Knowledge Base as well as any application notes, white papers and other on-line resources that may become available from time to time.

Opengear reserves the right to discontinue all support for products that are no longer covered by warranty.

LIMITATION OF LIABILITY

No action, regardless of form, arising from this warranty may be brought by either party more than two (2) years after the cause of action has occurred. Purchaser expressly agrees that Opengear's liability, if any, shall be limited solely to the replacement or repair of the product in accordance with the warranties specifically and expressly set forth herein. The remedies of the Purchaser are the exclusive and sole remedies available, and, in the event of a breach or repudiation of any provision of this agreement by Opengear, the Purchaser shall not be entitled to receive any incidental damages as that term is defined in Section 2-715 of the Uniform Commercial Code. Opengear waives the benefit of any rule that disclaimer of warranty shall be construed against Opengear and agrees that such disclaimers herein shall be construed liberally in favor of Opengear.

THE FOREGOING WARRANTIES ARE THE SOLE ANDEXCLUSIVE WARRANTIES GIVEN IN CONNECTION WITH THE PRODUCT AND THE HARDWARE. OPENGear DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES AS TO THE SUITABILITY OR MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. OPENGear DOES NOT PROMISE THAT THE PRODUCT IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION. IN NO EVENT SHALL OPENGear BE LIABLE FOR ANY LOST OR ANTICIPATED PROFITS, OR ANY INCIDENTAL, EXEMPLARY, SPECIAL OR CONSEQUENTIAL DAMAGES, REGARDLESS OF WHETHER OPENGear WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.