BLACK BOX®

Virtual Central Management System (VCMS)

Works with LES1200, LES1300, LES1400, and LES1500 Series Console Servers.

Contact Information

Order toll-free in the U.S. or for FREE technical support: Call 877-877-BBOX
(outside U.S. call 724-746-5500)
www.blackbox.com • info@blackbox.com

Trademarks Used in this Manual

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Instrucciones de Seguridad
(Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    - A: El cable de poder o el contacto ha sido dañado; u
    - B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    - C: El aparato ha sido expuesto a la lluvia; o
    - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    - E: El aparato ha sido tirado o su cubierta ha sido dañada.

Safety Information

Follow the safety precautions below when installing and operating the Value-Line and Advanced Console Servers:

- Do not remove the metal covers. There are no operator serviceable components inside. Opening or removing the cover may expose you to dangerous voltage that may cause fire or electric shock. Refer all service to Black Box 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 Console Server during an electrical storm. We recommend that you use a surge suppressor or UPS to protect the equipment from transients.

Table of Contents

1. Introduction

This User Manual describes the Black Box Virtual Central Management System (LES-VCMS) that works with the LES Series Console Servers and provides instructions for using the VCMS together with the console server.

- These centralized management appliances include the VCMS software appliance and the LES Series Console Servers. These are referred to generically in this manual as console servers.
- The Console Servers all run the same centralized management software (referred to in this manual as VCMS). VCMS enables network engineers and system administrators to centrally manage Black Box appliances and attached IT networking gear.
- Black Box console servers include the LES1202A, LES1203A-M, LES1203A-11G, LES1204A, LES1204A-R2, LES1204A-3G-DEMO, LES1204A-3G, LES1508A, LES1208A, LES1208A-R2, LES1216A, LES1216A-R2, LES1232A, LES1248A, LES1248A-R2, LES1308A, LES1316A, LES1332A, LES1348A, LES1408A, LES1416A, LES1432A, LES1448A, LES1108A, LES1116A, LES1132A, LES1148A, LES1101A,and LES1102A product lines. They are referred to generically in this manual as console servers, or as Managed Console Servers when they are being managed by VCMS.

1.1 Who should read this guide?

You should read this manual if you are responsible for evaluating, installing, operation, or managing an LES Series Console Server with the Virtual Central Management Software (VCMS). This manual assumes you are familiar with the internal network of your organization, and are familiar with the Internet and IP networks, HTTP, FTP, and basic security operations.

1.2 Manual Organization

This manual contains the following chapters:

1. Introduction: The chapter you are reading now.
2. Installation: Console server and VCMS software installation.
3. Configuration: Initial VCMS configuration and connection to the Managed Console Servers.
4. Operation: Details the status displays and reports, and connecting with hosts.
5. Nagios: Customization of the Nagios monitoring.
6. Accessing the Console Servers with an SSH Client

To download this user manual, visit the Black Box Web site (www.blackbox.com) and enter LES-VCMS in the search bar.

This documentation describes using your browser to configure and operate the console servers with VCMS and monitor all the connected hosts. However, these console servers all run a Linux® operating system, so experienced Linux/Nagios® users may prefer to operate at the command line.

2. Initial Deployment

Black Box VCMS software runs on VCMS virtual software appliance platforms, and on Value-Line and Advanced Console Server physical hardware platforms.

This chapter describes the initial deployment and configuration of these console servers using VCMS.

2.1 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 or
- VMware Server, VMware Workstation

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

2.1.1 System Requirements

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

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

The appropriate level of reserved virtual server resources will depend on the number of console servers—and connected managed devices—being managed by the VCMS. For installations supporting 1000 or more appliances, the recommended resource would be:

- 2 GHz CPU core
- 16 GB RAM
- 600 GB disk space

In addition, you will need the following virtual devices:

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

2.1.2 Distributed Files

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

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

- For Linux KVM, use the raw HDD image: vcms-x.y.z-kvm.hdd.gz
- For VMware ESX/ESXi, use the deployment OVF: vcms-x.y.z-vmware-ovf.zip
- For VMware server, use: vcms-x.y.z-vmware.tar.gz

Uncompress the full image using gunzip, Winzip, or similar software before deployment. Follow the instructions provided by your virtualization management suite to deploy the ovf, vmx, or hdd file as appropriate.

See the examples on the next pages for VMware ESXi 4, VMware Workstation 7, and ElasticHosts cloud hosting provider.

2.1.3 Software deployment

Follow the instructions provided by your virtualization management suite to deploy the ovf, vmx or hdd file as appropriate.

Examples are given on the next pages for VMware ESXi 4, VMware Workstation 7, and ElasticHosts cloud hosting provider.

Example deployment: VMware ESXi 4

To complete this deployment you must have VMware ESXi 4 installed and running on a bare metal machine, and the VMware vSphere Client installed on a PC running Microsoft Windows.

Before proceeding, download and extract the full disk image for VMware ESXi, as described in the "Distributed Files" section.

1. Launch the vSphere Client and log into the ESXi with a user who has administrator privileges.
2. In the vSphere Client, select File: Deploy OVF Template. The Deploy OVF Template wizard is displayed.
3. Specify the source location and click Next.
4. Select Deploy from File and Browse the file system for the location where you extracted the contents of:

   vcms-x.y.z-vm-ovf.zip

   Select the OVF template file, e.g.: vcms-vm.ovf
5. Check the OVF Template Details page and click Next.
6. If required, edit the OVF Template name.
7. Review the Ready to Complete details. To re-edit Source, OVF Template Details and Name and Location, click on the respective link on the left hand side of the window. Click Finish when complete.
8. The OVF Template is now displayed in the left-hand vSphere Client Status panel under the relevant host.
9. To start the virtual machine, select the Virtual Machine tab from the right-hand panel. Select the Virtual Machine by name and click the Play button from the top menu.
10. Deployment is now complete. You can monitor the VCMS boot progress using the vSphere Client console, or proceed to "Configuring VCMS" to begin configuration.

Example deployment: VMware Workstation 7

To complete this deployment you must have VMware Workstation 7 installed and running on a PC running Microsoft Windows®. Before proceeding, download and extract the full disk image for VMware Workstation, as described in the "Distributed Files" section.

1. Launch VMware Workstation.
2. Click the Launch Existing VM or Team icon in the right-hand side of the window. Browse the file system for the location where you extracted the contents.
3. Select Deploy from File and Browse the file system for where you extracted the contents: vcms-x.y.z-vm.tar.gz

   Select and Open the VMX file, e.g.: VCMS.vmx

   The Black Box VCMS tab is displayed.
4. Click the "Power on this virtual machine" link located in the Commands box.
5. Deployment is now complete. You can monitor the VCMS boot progress using the VMware Workstation console, or proceed to "Configuring VCMS" to begin configuration.

Example Cloud Deployment: ElasticHosts

(These instructions are current as of 04 April 2013.)

1. Browse to http://www.elastichosts.com and create an account at your preferred peer location.
2. 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 "Commited data transfer" to 10 GB or higher and/or have 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 that you purchase a static IP address; otherwise, you must also configure VCMS to use a dynamic DNS service.

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

http://www.elastichosts.com/question/how-can-upload-my-own-iso-cd-mages/

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

Full documentation for the API and usage examples can be found here:

http://www.elastichosts.com/support/api/

Your user UUID and secret API key is available on your Profile page. You should combine them into the EHAUTH environment variable:

export EHAUTH=<user uuid>:<secret API key>

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-vm.hdd

4. 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-vm.hdd". Click Add.
5. Click Edit on the Server you just added. Select the static IP address to use if available, and set the VNC password. Click Start.
6. Deployment is now complete. You can now monitor the VCMS boot progress using VNC, or proceed to "Configuring VCMS" to begin configuration.

Configuring VCMS

After initial installation, you cannot log in to the VCMS until a root password is set.

Connect to the virtual VGA console to set the root password.

After the root password is set, on first login, configuration information is displayed. Further VCMS configuration can be

performed by browsing to the IP address listed. (By default, the VCMS will have both an address obtained via DHCP, and a static address of 192.168.0.1).

The default credentials:

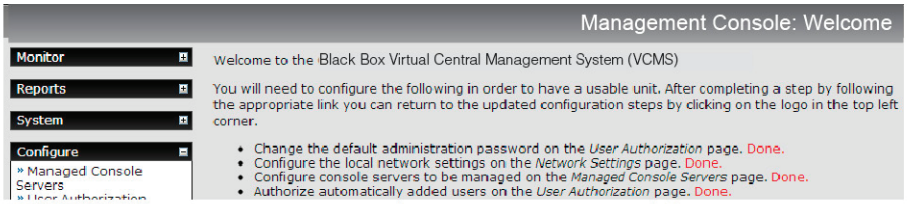
root/<set via console on first start up>

2.1.4 Initial Login

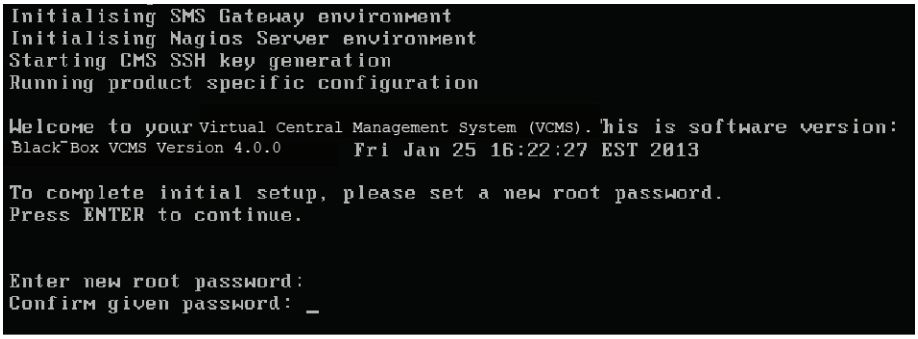
Once VCMS has been deployed and the virtual appliance has booted, you can configure the system by browsing to the IP address of the virtual NIC. The virtual NIC obtains an address using DHCP and has a static IP address of 192.168.0.1

You will be presented with the login screen on your browser.

- Login as root with the root password
- You will then arrive at the Welcome to the Black Box Virtual Central Management System (VCMS) screen.



NOTE: The default username/password is root/default. However, on the initial deployment during the load process, you will be prompted to enter and confirm a new root password. If you simply have upgraded to a new version, you won't be prompted for a new root password, the device will just boot normally with the password it already has.



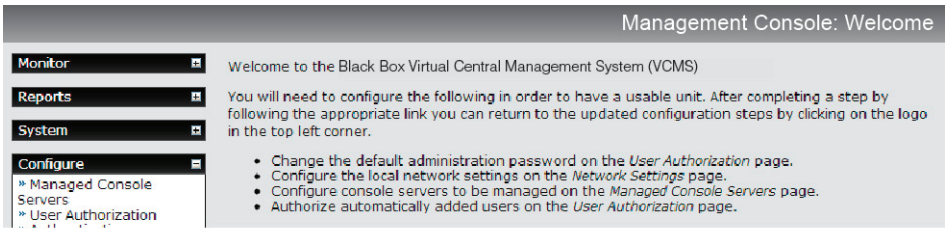
3. Configuration

This chapter covers the initial configuration for a usable Virtual Central Management System appliance.

It also discusses the other Configure and Status menu items that the administrator may use in managing VCMS, such as connecting to the Managed Console Servers, setting time/date and upgrading the firmware.

3.1 Welcome

Login as root. Initially, only the administration user named root can log into VCMS. The default password is default, However, you will have changed this on initial deployment.



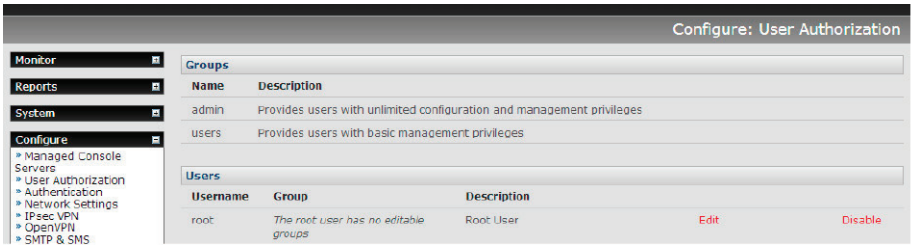
You will arrive at the Welcome to the Black Box Virtual Central Management System (VCMS) screen. Follow the initial configuration steps:

- Enter new passwords (Chapter 3.2).
- Configure the local network settings (Chapter 3.3).
- Configure console servers to be managed (Chapter 3.4).
- Authorize automatically added users (Chapter 3.6).

After completing a step (by following the appropriate link), you can return to the updated configuration steps by clicking on the logo in the top left corner.

3.2 Passwords

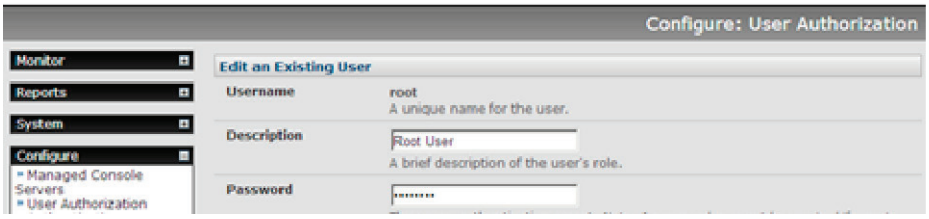
The first step "Change the default administration password" takes you to Configure: User Authorization, where you can again reset the password for root.



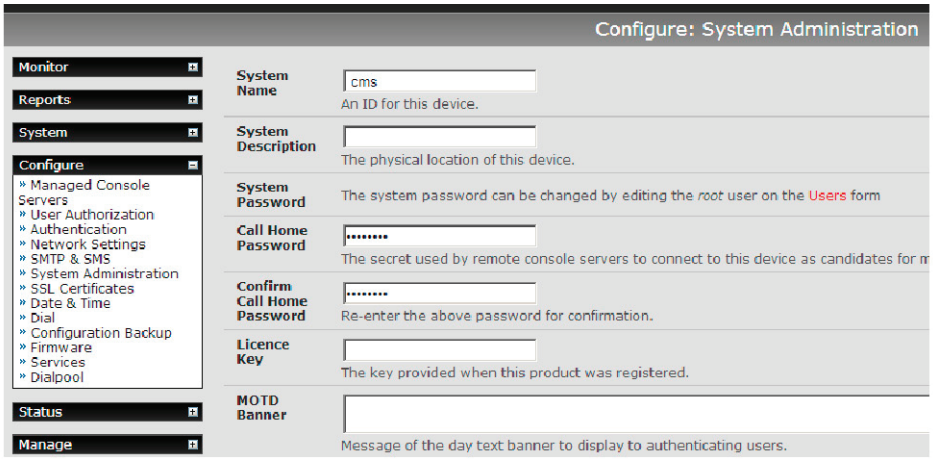
NOTE: With VCMS, you will have already been prompted to change the root password during initial deployment, so this step may already be Done. Since this is the main administrative user account, choose a complex password and keep it safe.

- Enter a new System Password then re-enter it in Confirm System Password.

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



• Select Configure: System Administration to now enter other passwords.



• At this stage you may also wish to enter a System Name and System Description to give your VCMS appliance 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.

3.2.1 Enter Call Home Password

If you wish to monitor Managed 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.

• 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.

NOTE: If you use remote authentication without any fallback to local authentication checks, the "VCMS" user authentication will fail if you don't have a "VCMS" user in the remote authentication. This authentication failure will cause the set-up of a new Call Home console server to fail.

3.2.2 Enter License Key (VM only)

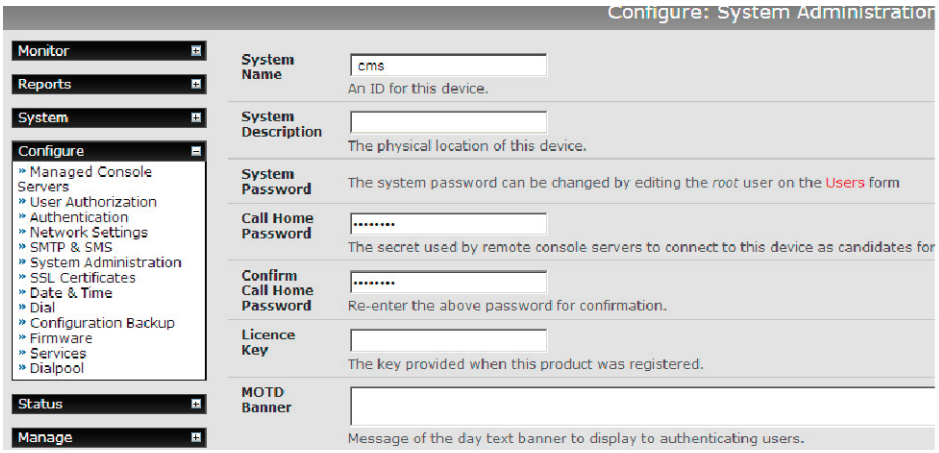
When you ordered your VCMS license you will have been emailed a License Key. Install this key now—before proceeding with the configuration steps (described in the next chapter).

To install the Key:

• Copy the Key from the email that you received into the License Key field.

• Click Apply.

This step is required for VCMS only. With the Advanced or Value-Line Console Server the Key is pre-installed.



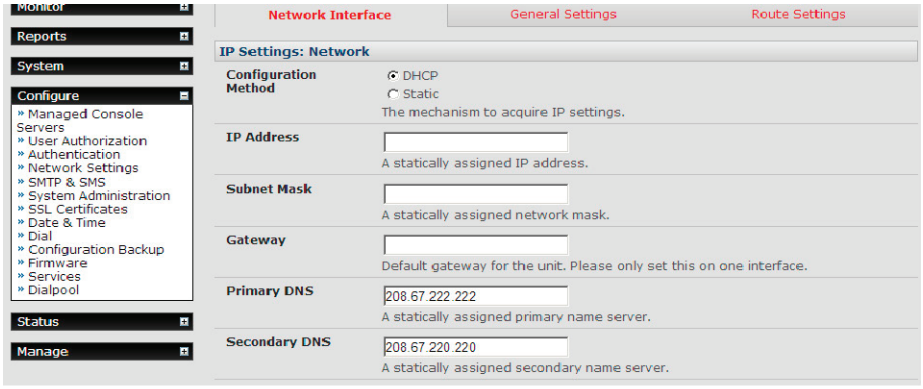
NOTE: This License Key provides you with a commercial license to use the VCMS software appliance to manage up to the designated number of appliances for the defined period. For example, ordering an LES-VCMS-100-3Y license enables you to use your VCMS appliance to manage a distributed network with up to 100 Black Box console servers with support and feature upgrades for 3 years. You can then renew your License Key annually to receive ongoing support and upgrades. If you have to contact Black Box Technical support at 877-877-2269 or info@blackbox.com, they will ask you to quote the License Key number.

3.3 Configure Local Network Settings

The next step is to enter an IP address and network settings for the Network port on the VCMS, or to enable its DHCP client so that it automatically obtains an IP address from a DHCP server on the network it will connect 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 VCMS will look for configuration details from a DHCP server on your management LAN. This selection automatically disables any static address.

NOTE: In its factory default state (with no Configuration Method selected) the VCMS 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 VCMS will then respond to both its Static address (192.168.0.1) and its newly assigned DHCP address.

• By default the VCMS Network port auto-detects the Ethernet connection speed. 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 VCMS 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.

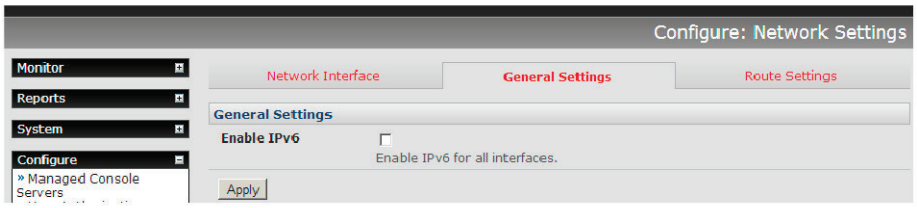
- Click Apply.
- You will need to reconnect the browser on the PC/workstation that is connected to the VCMS by entering https://new IP address.

NOTE: If you selected the DHCP configuration method, and plan to use Call Home, we strongly recommend 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 VCMS 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.

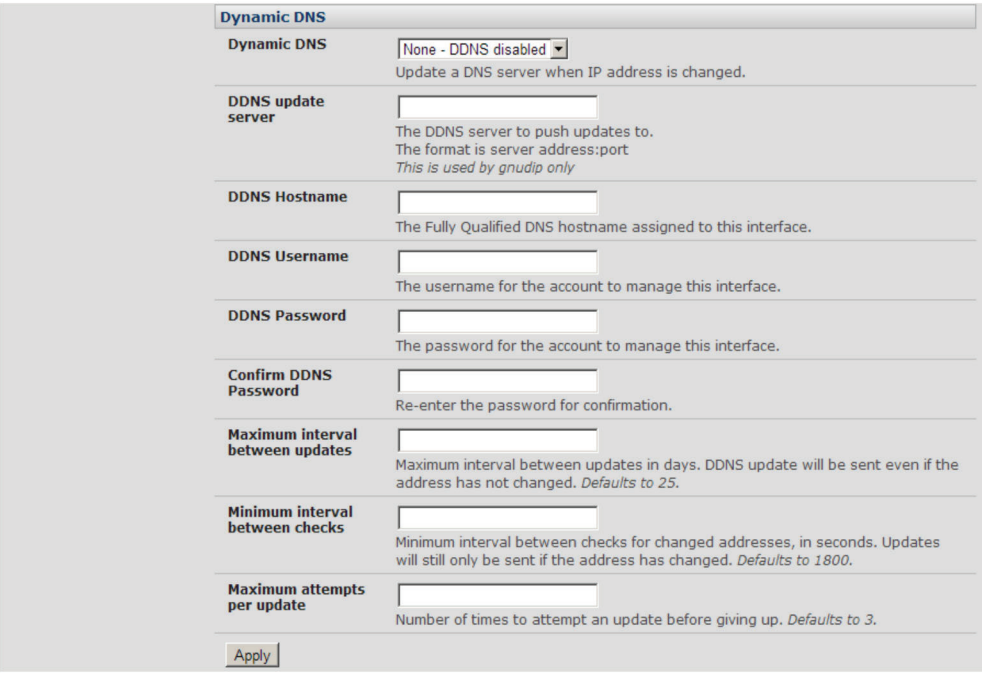
- The first step in enabling DDNS is to create an account with the supported DDNS service provider of your choice. Supported DDNS providers include:

- 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. With a paid plan, any URL hostname (including your own registered domain name) can be used. By default, DDNS is disabled. To enable:

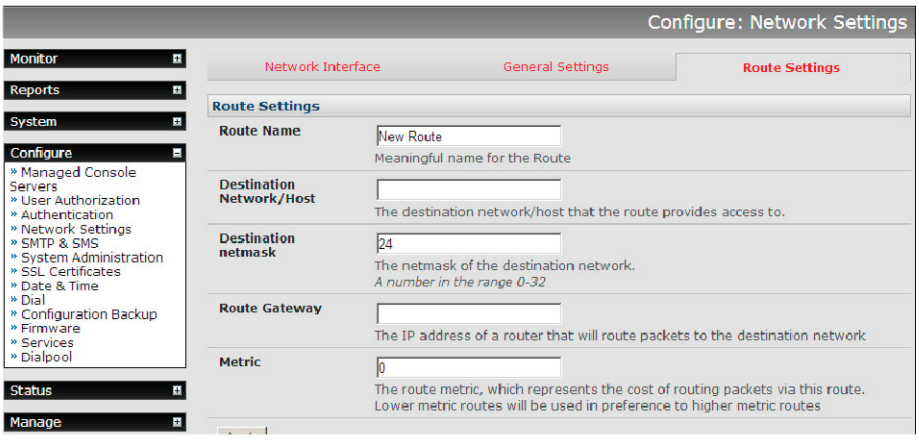
- On the Configure: Network Settings menu, select the Network Interface page, then select the DDNS service provider from the drop-down Dynamic DNS list.



- 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).

3.3.3 Static routes

Route Settings enables you to set up static routes which provide a very quick way to route data from one subnet to a different subnet. So, you can hard-code a path that specifies to the VCMS/router to get to a certain subnet by using a certain path. This may be useful for remotely accessing various subnets at a remote site when using the cellular OOB connection.



To add to the static route to the route table of the system:

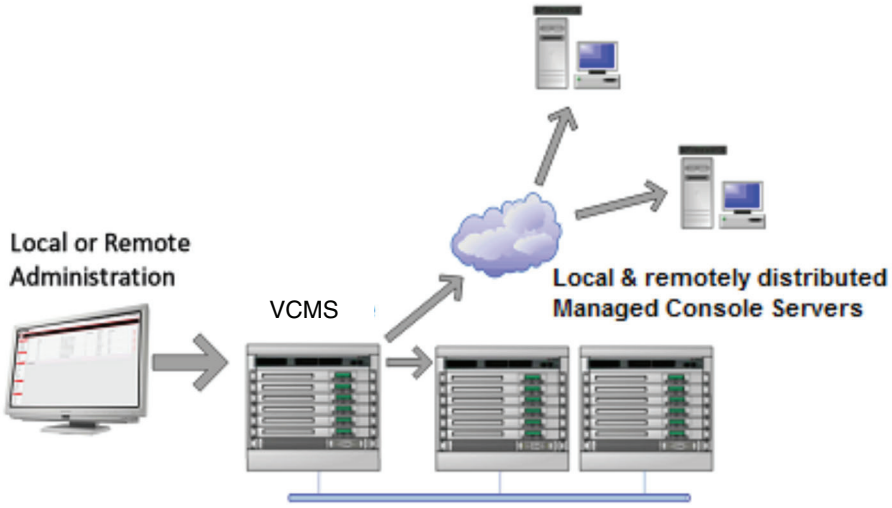
- Select the Route Settings tab on the System: IP General Settings menu.
- Enter a meaningful Route Name for the route.

- In the Destination Network/Host field, enter the IP address of the destination network/host that the route provides access to.
- Enter a value in the Destination netmask field that identifies the destination network or host. It can be any number between 0 and 32. A subnet mask of 32 identifies a host route.
- Enter Route Gateway with the IP address of a router that will route packets to the destination network.
- Enter a value in the Metric field that represents the metric of this connection. This generally only has to be set if two or more routes conflict or have overlapping targets. It can be any number equal to or greater than 0.
- Click Apply.

3.4 Configure Managed Console Servers

VCMS 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 connected Managed Devices.

To manage Local Console Servers, or console servers that are reachable from the VCMS, the SSH connections are initiated by VCMS. To manage Remote Console Servers, or console servers that are firewalled, not routable, or otherwise unreachable from the VCMS, 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 VCMS:

- The Managed Device 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 VCMS. 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 VCMS is accessing this Managed Console Server:

- For a Local Console Server, it shows the network address and SSH server port that VCMS 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.

3.4.1 Adding a Console Server

The Detected Console Servers list displays all the console servers that are currently not being monitored by the VCMS:

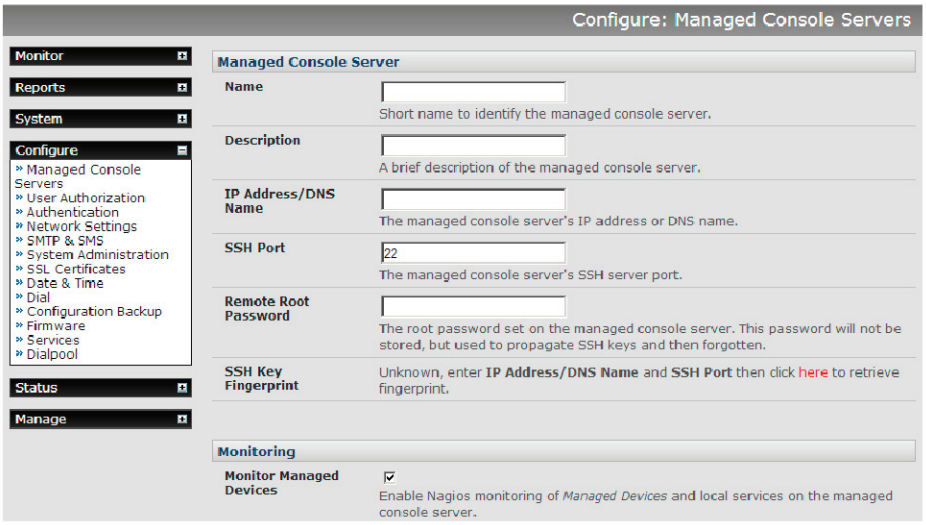
- The Local Console Servers drop-down list shows all the console servers that are on the same subnet as the VCMS, and are not currently being monitored. Click Refresh to update.
- The Remote Console Servers drop-down list shows all the console servers that have established a Call Home connection (so 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, 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 VCMS—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 /DNS Name 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").



- 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 VCMS to propagate auto-generated SSH keys and then forgotten. This password will not be stored.

- Check Monitor Managed Devices to enable Nagios monitoring of Managed Devices and local services on the managed console server.
- Check Monitor Auto-Responses to enable Nagios monitoring of auto-response status on the managed console server.
- The Serial Port Proxy sets the number of ports on the Managed Console Server the VCMS has proxy access to.
- Add the RFC2217 Proxy Port Base when you want VCMS to act as a single point for virtual com port access (e.g., as a Portshare gateway). Setting the number of ports also determines how many Ajax Webterms are accessible from the Access Console Server page.

• For details on Remote Dialin Setup refer to the subsequent Dialpool section.

• Click Apply.

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

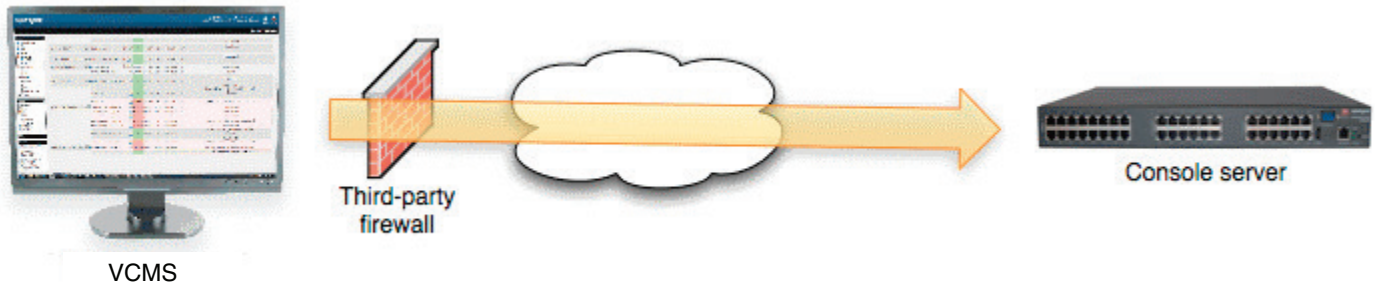
3.4.2 Connecting to sites on separate private or firewalled networks

Often, the remote console servers—or the VCMS appliance itself—will be on private firewalled networks. So they are unable to directly connect to each other.

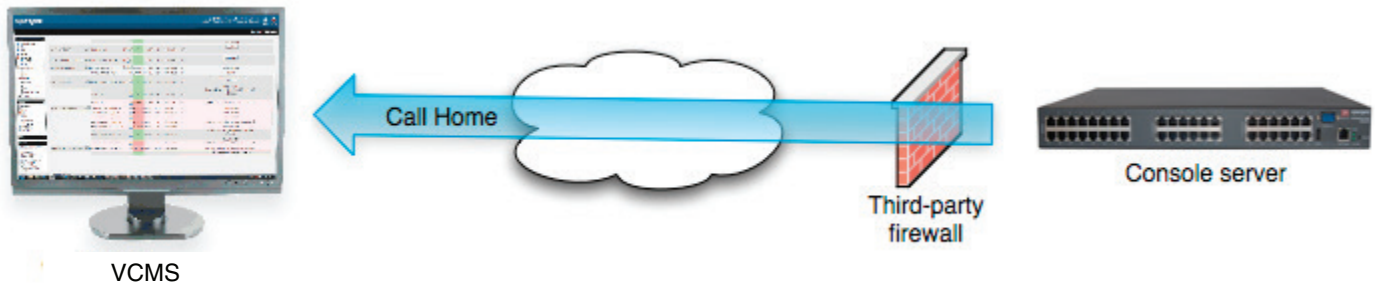
Whatever the topology, as long as either VCMS can SSH to the console server or the console server can SSH to VCMS, then the VCMS can manage the console server.

There are three common scenarios:

I. The console server has a public address and the VCMS has a private or firewalled address.



In this case, ensure that the third-party firewall allows outbound connections to 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 VCMS, but can be added manually at the VCMS using Configure -> Managed Console Servers -> New Console Server -> Add as described above.



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

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

There are two options in this scenario:

(a) Make VCMS 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 VCMS on a central private operations network.

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

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

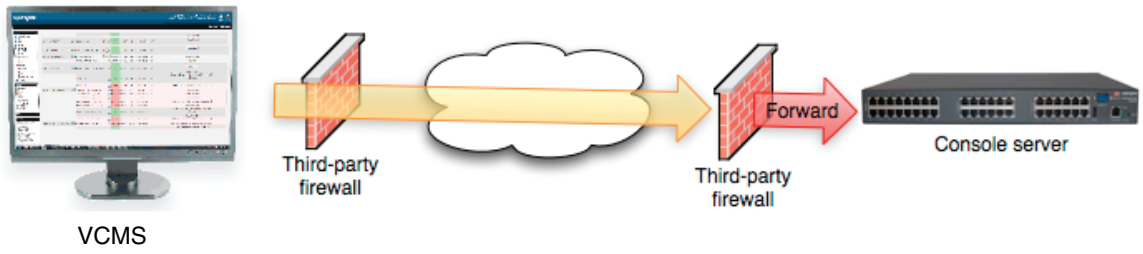
config -s config.VCMS.address=4.3.2.1 config -s config.VCMS.sshport=2222

... 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 VCMS using the forwarded port as per scenario 2 above.

(b) Make the console server accessible by VCMS.

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 VCMS as described in the earlier section.

3.5 Call Home

To manage a console server, the VCMS 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 can be initiated from the console server to the VCMS. This creates an SSH listening port on the VCMS, that is redirected back across the Call Home connection to the console server. This allows the VCMS to connect to the console server using SSH, and thereby manage it.

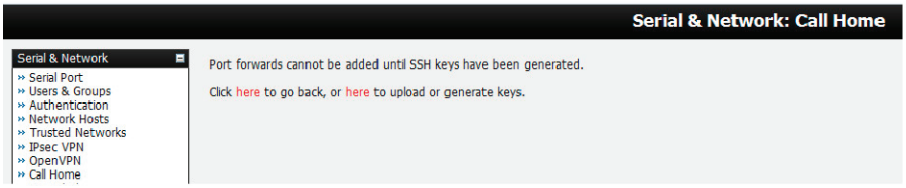
Any console server with Firmware V3.2 or later has Call Home support.

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

3.5.1 Setting up console server as a management candidate on VCMS

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

- 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 Value-Line and Advanced Console Servers' 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 VCMS.
- Enter the Password that you configured on the VCMS as the Call Home Password.
- Click Apply.

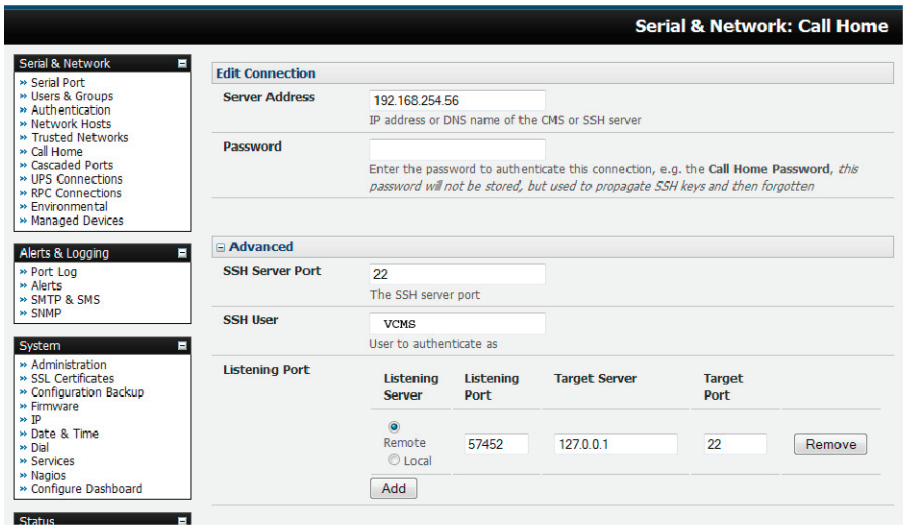
These steps initiate the Call Home connection from the console server to the VCMS. An SSH listening port is created on the VCMS, and the console server is set up as a candidate to be accepted as a Managed Console Server.

Once the candidate has been accepted on the VCMS (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 VCMS 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 VCMS), 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:

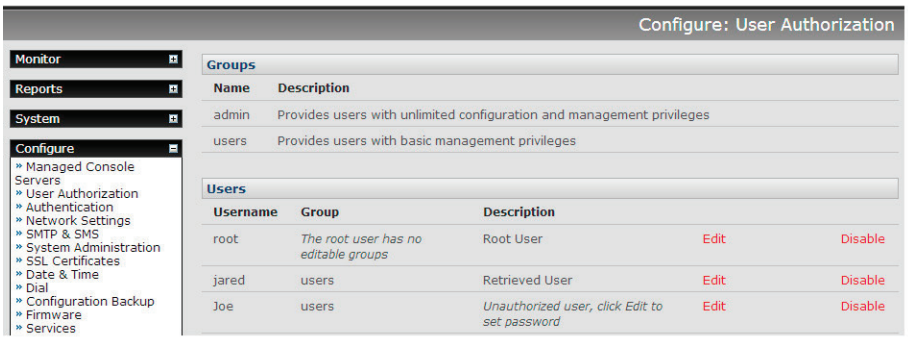
- Specify a Listening Port to forward from, leave this field blank to allocate an unused port.
- Enter the Target Server and Target Port that will be the recipient of forwarded connections.

3.6 Authorize Automatically Added Users

VCMS 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 VCMS before that user can log in to the VCMS.

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



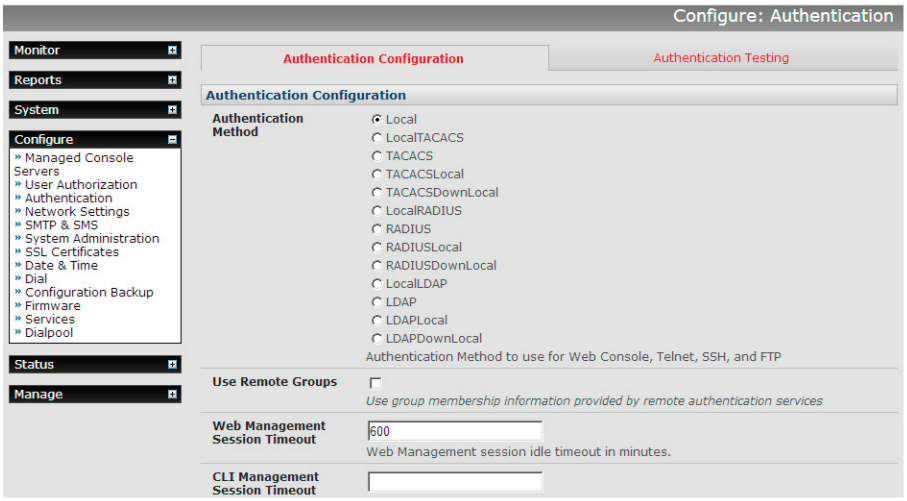
- For any user, select Edit and enter a new password that will be used by that user when accessing VCMS.
- At this stage, you can also modify the Group membership and Description associated with that particular user. Users in the user group can access the Current Status menus, the Reports menus, and the System menu (basically all the monitoring screens), whereas users in the admin group have this access plus the ability to reconfigure the VCMS using the Configure menu.
- Enter the user's Email Address to be used for sending notifications.
- An SMS alert can also be sent via an SMTP (email) gateway. You will need to specify the SMTP SMS Email Address in the format specified by the gateway provider.

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

• Click Apply.

3.7 Authentication Configuration

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

The VCMS 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).

3.7.1 Local authentication

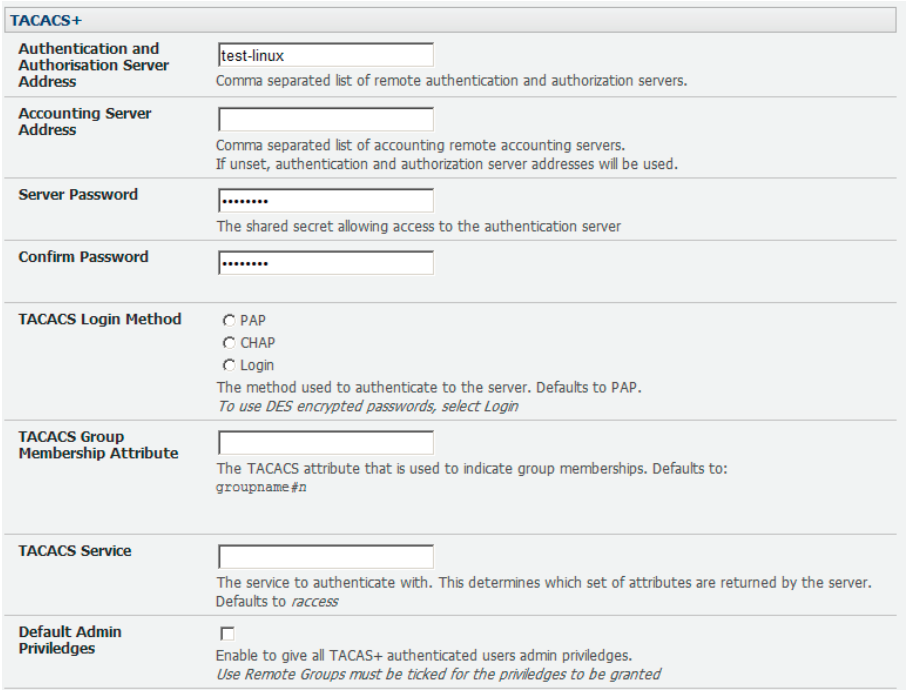
• Select Configure: Authentication and check Local.

• Click Apply.

3.7.2 TACACS authentication

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

• Select Configure: Authentication and check TACAS or LocalTACACS or TACACSLocal or TACACSDownLocal.



- 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 for separate lists of Authentication/Authorization servers and Accounting servers. If no Accounting servers are specified, the Authentication/Authorization servers are used instead.
- Enter and confirm the Server Password. Then select the method to be used to authenticate to the server (defaults to PAP). To use DES encrypted passwords, select Login.
- If required enter the TACACS Group Membership Attribute that is to be used to indicate group memberships (defaults to groupname#n).
- If required, specify TACACS Service to authenticate with. This determines which set of attributes are returned by the server (defaults to raccess).
- If required, check Default Admin Privileges to give all TACAS+ authenticated users admin privileges. Use Remote Groups must also be ticked for these privileges to be granted.
- Click Apply. TACACS+ remote authentication will now be used for all user access to console server and serially or network attached devices.

TACACS+: The Terminal Access Controller Access Control System (TACACS+) security protocol is a 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

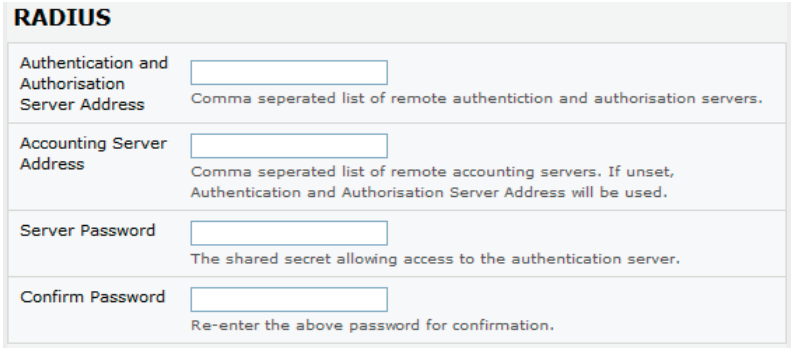
http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a00800eb6d6.html

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

3.7.3 RADIUS authentication

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

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



- 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 VCMS 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-eecd-49e4-88f6-9e304f97fefc.mspx

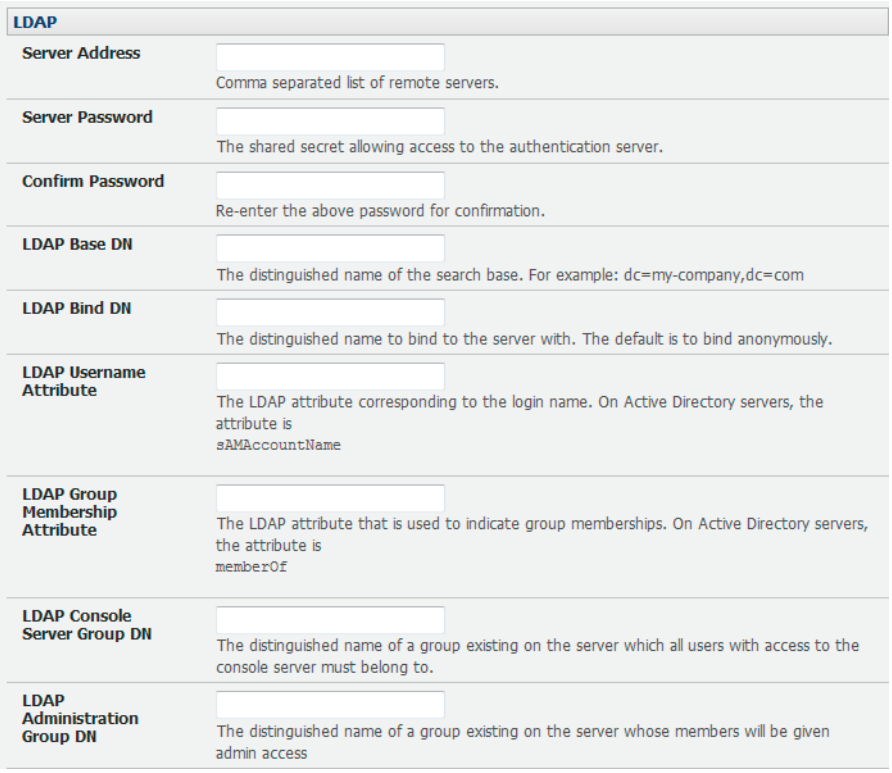
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml

http://www.freeradius.org/

3.7.4 LDAP authentication

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

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



- 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 the user account that exists on our VCMS to work with the remote server; i.e. you can't just create the user on your LDAP server and not tell the VCMS about it. You need to add the user account.

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

LDAP: The Lightweight Directory Access Protocol (LDAP) is based on the X.500 standard, but is 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/

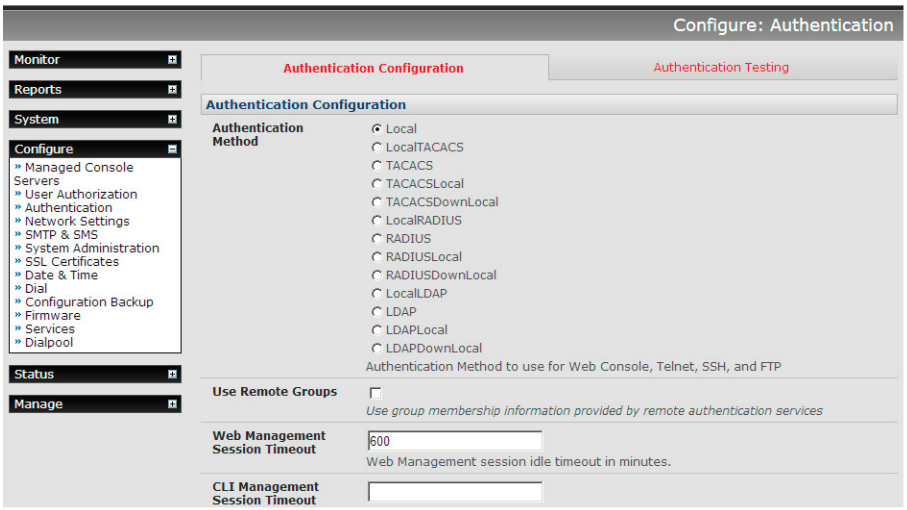
3.7.5 Group support with remote authentication

VCMS allows remote authentication via RADIUS, LDAP, and TACACS+. RADIUS and LDAP can provide additional restrictions on user access based on group information or membership. For example, with remote group support, users can belong to a local group that has been set up to have restricted access to serial ports, network hosts, and managed devices.

Remote authentication with group support works by matching a local group name with a remote group name provided by the authentication service. If the list of remote group names returned by the authentication service matches any local group names, the user is given permissions as configured in the local groups.

To enable group support to be used by remote authentication services:

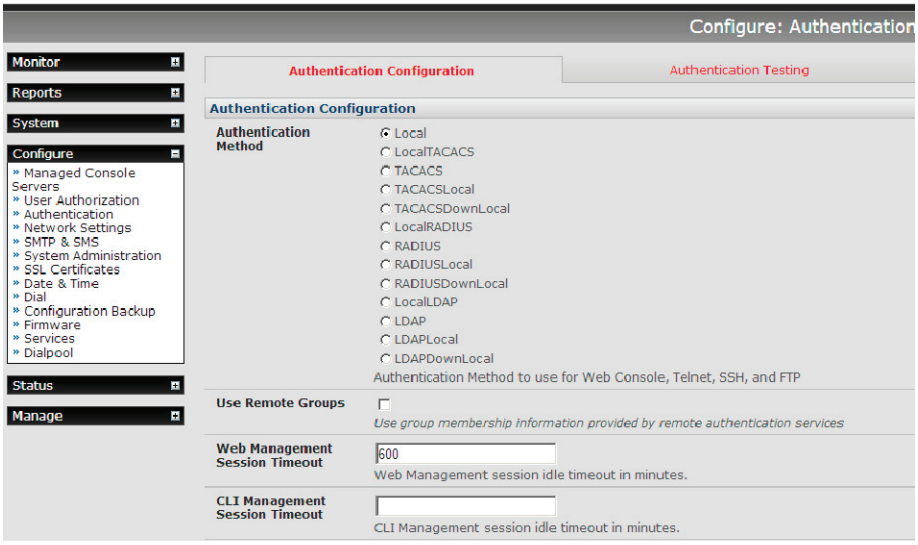
- Select Configure: Authentication.
- Select the relevant Authentication Method.
- Check the Use Remote Groups button.



- Refer to your console server User Guide for remote group configuration details.

3.7.6 Idle timeout

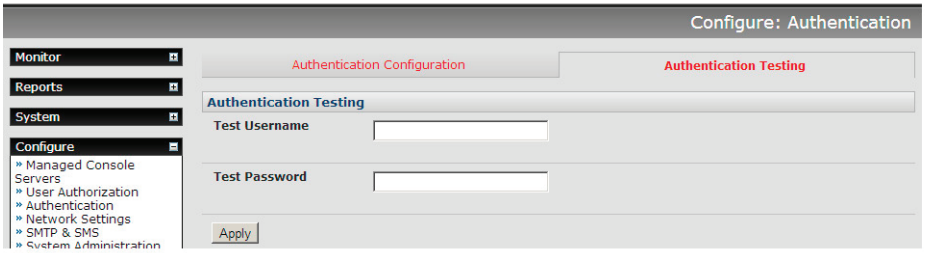
You can specify the amount of time in minutes that the VCMS waits before it terminates an idle ssh or web connection.



- Select Configure: Authentication.
- Web Management Session Timeout specifies the browser console session idle timeout in minutes. The default setting is 20 minutes.
- CLI Management Session Timeout specifies the ssh console session idle timeout in minutes. The default setting is to never expire.

3.7.7 Authentication testing

The Authentication Testing enables the connection to the remote authentication server to be tested.



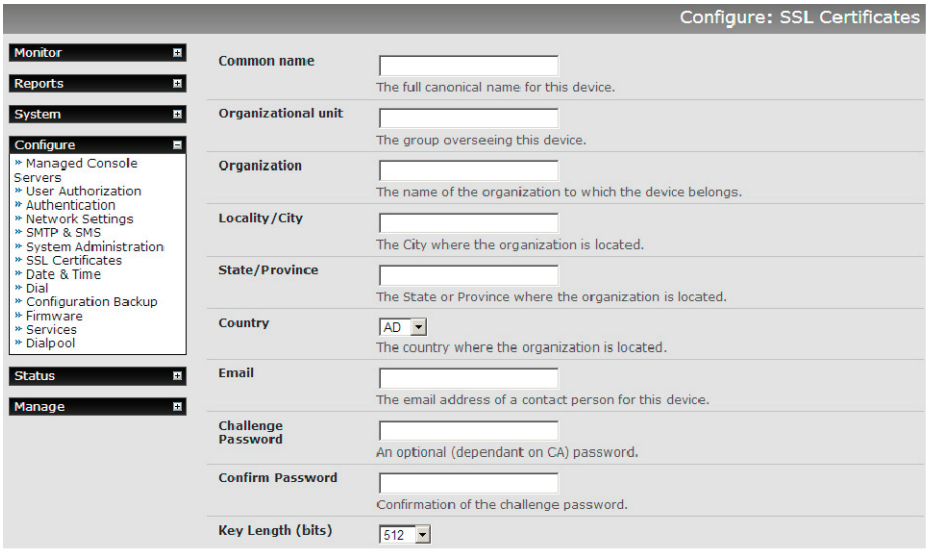
3.8 SSL Certificate

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

NOTE: 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, we recommended that you generate and install a new base64 X.509 certificate that is unique for a particular VCMS.



To do this, the VCMS 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 VCMS:

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

- Common name This is the network name of the VCMS 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 VCMS 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 VCMS is accessed using HTTPS.

- Organizational Unit: This field is used for specifying to which department within an organization the VCMS belongs.
- Organization: The name of the organization to which the VCMS 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. This country code has to be entered in CAPITAL LETTERS.
- Email: The email address of a contact person who is responsible for the VCMS 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 VCMS 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 VCMS using the Upload button.

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

3.9 IPsec VPN

Each VCMS includes Openswan, a Linux implementation of the IPsec (IP Security) protocols, which can be used to configure a Virtual Private Network (VPN). The VPN allows multiple sites or remote administrators to access the VCMS securely over the Internet.

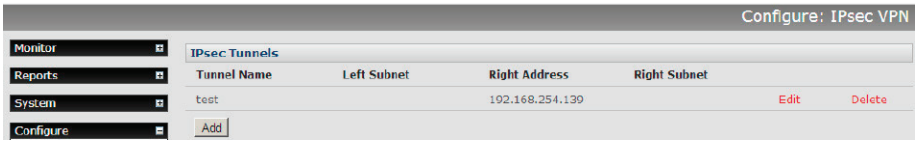
The administrator can establish an encrypted authenticated VPN connection between a virtual VCMS or hardware VCMS appliance on their central office network and a VPN gateway (such as Cisco router running IOS IPsec or an LES Series server) at a remote site.

The road warrior administrator can use a VPN IPsec software client such as TheGreenBow (www.thegreenbow.com/vpn_gateway.html) or Shrew Soft (www.shrew.net/support) to remotely access their VCMS (and its Managed Console Servers and their connected and managed devices).

Configuration of IPsec is quite complex, so Black Box provides a simple GUI interface for basic setup. For more detailed information on configuring Openswan IPsec at the command line and interconnecting with other IPsec VPN gateways and road warrior IPsec software, refer to http://wiki.openswan.org.

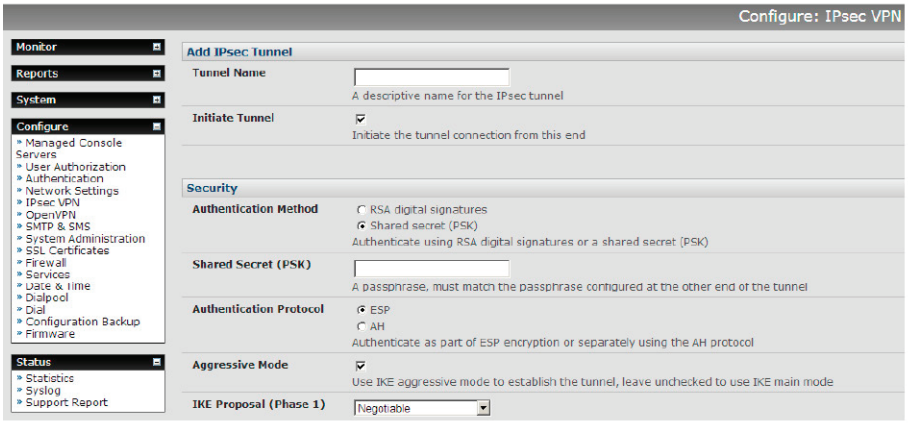
3.9.1 Enable the VPN gateway

• Select IPsec VPN on the Serial & Networks menu.



• Click Add and complete the Add IPsec Tunnel screen.

• Enter any descriptive name you wish to identify the IPsec Tunnel you are adding such as WestStOutlet-VPN.



- Select the Authentication Method to be used, either RSA digital signatures or a Shared secret (PSK).

- If you select RSA, you will asked to click here to generate keys. This will generate an RSA public key for the VCMS (the Left Public Key). You will need to find out the key to be used on the remote gateway, then cut and paste it into the Right Public Key.

- If you select Shared secret, you will need to enter a Pre-shared secret (PSK): The PSK must match the PSK configured at the other end of the tunnel.

- In Authentication Protocol, select the authentication protocol to be used. Either authenticate as part of ESP (Encapsulating Security Payload) encryption or separately using the AH (Authentication Header) protocol.

- Enter a Left ID and Right ID. This is the identifier that the Local host/gateway and remote host/gateway use for IPsec negotiation and authentication. Each ID must include an '@' and can include a fully qualified domain name preceded by '@' (e.g. left@example.com).

- Enter the public IP or DNS address of this Black Box VPN gateway (or if not an LES1204A-G, enter the address of the gateway device connecting it to the Internet) as the Left Address. You can leave this blank to use the interface of the default route.

- In Right Address enter the public IP or DNS address of the remote end of the tunnel (only if the remote end has a static or dyndns address). Otherwise, leave this blank.

- If the Black Box VPN gateway is serving as a VPN gateway to a local subnet (e.g. the VCMS has a Management LAN configured), enter the private subnet details in Left Subnet. Use the CIDR notation (where the IP address number is followed by a slash and the number of "one" bits in the binary notation of the netmask). For example 192.168.0.0/24 indicates an IP address where the first 24 bits are used as the network address. This is the same as 255.255.255.0. If the VPN access is only to the VCMS itself and to its attached serial console devices, then leave Left Subnet blank.

- If there is a VPN gateway at the remote end, enter the private subnet details in Right Subnet. Again, use the CIDR notation and leave it blank if there is only a remote host.

- Select Initiate Tunnel if the tunnel connection is to be initiated from the Left VCMS end. This can only be initiated from the VPN gateway (Left) if the remote end was configured with a static (or dyndns) IP address.

- Click Apply to save changes.

NOTE: The configuration details set up on the VCMS (referred to as the Left or Local host) must exactly match the set up entered when configuring the Remote (Right) host/gateway or software client.

3.10 OpenVPN

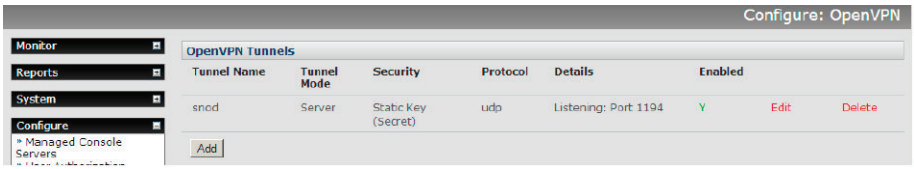
Each VCMS includes OpenVPN which is based on TSL (Transport Layer Security) and SSL (Secure Socket Layer). With OpenVPN, it is easy to build cross-platform, point-to-point VPNs using x509 PKI (Public Key Infrastructure) or custom configuration files. The VPN allows multiple sites or remote administrators to access the VCMS securely over the Internet.

OpenVPN also allows the use of Dynamic IP addresses by both the server and client to provide client mobility. For example, an OpenVPN tunnel may be established between a roaming windows client and a Black Box advanced console server within a data center.

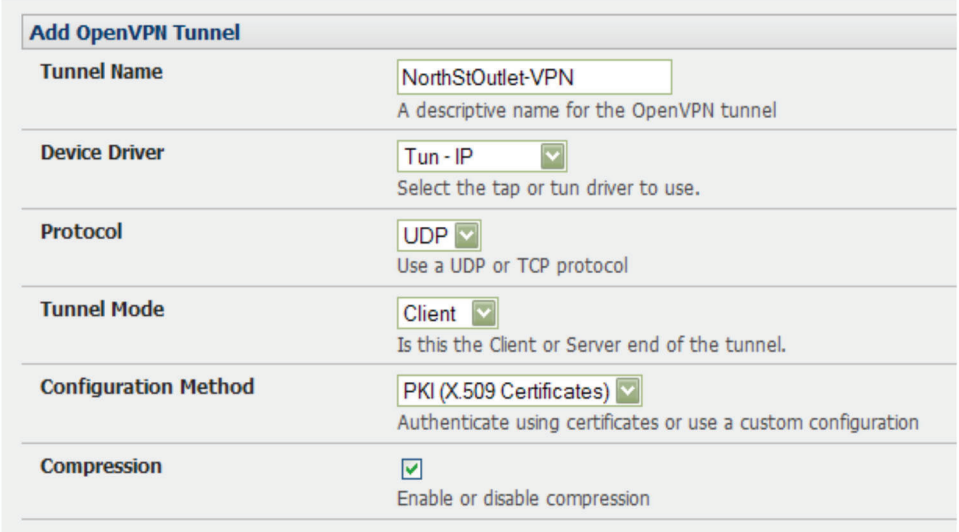
Configuration of OpenVPN can be complex, so Black Box provides a simple GUI interface for basic setup as described below. For more detailed information on configuring OpenVPN Access server or client refer, to the HOW TO and FAQs at http://www.open-vpn.net.

3.10.1 Enable the OpenVPN

- Select OpenVPN on the Serial & Networks menu.
- Click Add and complete the Add OpenVPN Tunnel screen.



- Enter any descriptive name you wish to identify the OpenVPN Tunnel you are adding, for example NorthStOutlet-VPN.



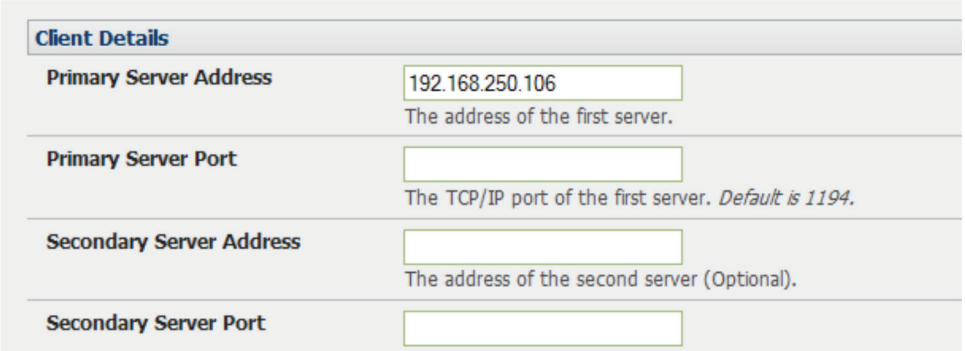
- Select the Device Driver to be used, either Tun-IP or Tap-Ethernet. The TUN (network tunnel) and TAP (network tap) drivers are virtual network drivers that support IP tunneling and Ethernet tunneling, respectively. TUN and TAP are part of the Linux kernel.
- Select either UDP or TCP as the Protocol. UDP is the default and preferred protocol for OpenVPN.
- In Tunnel Mode, nominate whether this is the Client or Server end of the tunnel. When running as a server, the advanced VCMS supports multiple clients connecting to the VPN server over the same port.
- In Configuration Method, select the authentication method to be used. To authenticate using certificates, select PKI (X.509 Certificates) or select Custom Configuration to upload custom configuration files. Custom configurations must be stored in /etc/config.

NOTE: If you select PKI (public key infrastructure) you will need to establish:

- *Separate certificate (also known as a public key). This Certificate File will be a *.crt file type.*
- *Private Key for the server and each client. This Private Key File will be a *.key file type.*
- *Master Certificate Authority (CA) certificate and key which is used to sign each of the server and client certificates. This Root CA Certificate will be a *.crt file type.*

For a server, you may also need dh1024.pem (Diffie Hellman parameters). Refer to http://openvpn.net/easyrsa.html for a guide to basic RSA key management. For alternative authentication methods, see http://openvpn.net/index.php/documentation/howto.html#auth. For more information, also see http://openvpn.net/howto.html

- Check or uncheck the Compression button to enable or disable compression, respectively.



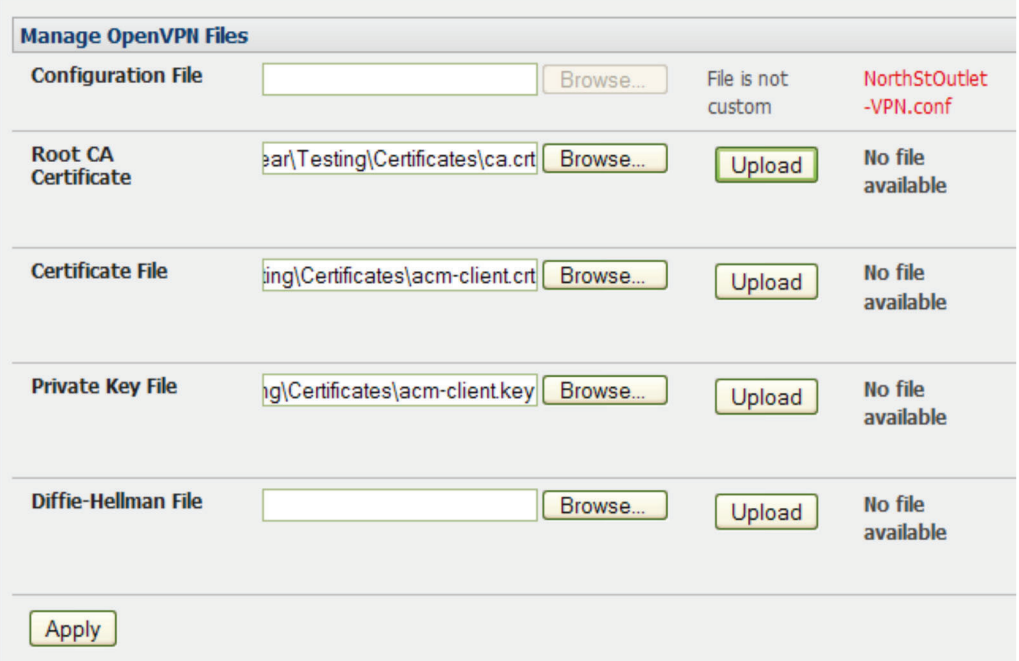
3.10.2 Configure as Server or Client

- Complete the Client Details or Server Details depending on the Tunnel Mode selected.

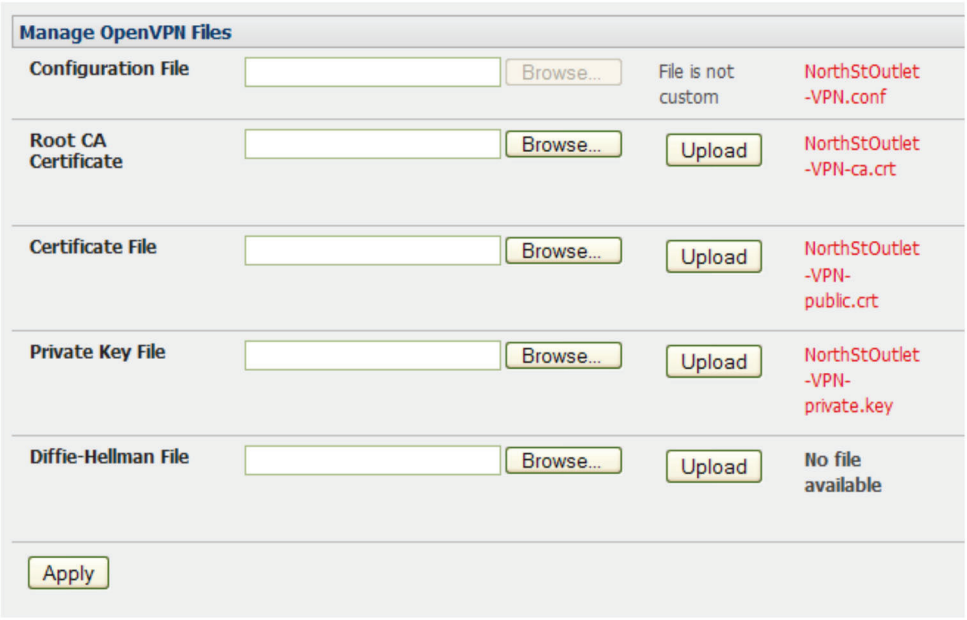
- If Client has been selected, the Primary Server Address will be the address of the OpenVPN Server.
- If Server has been selected, enter the IP Pool Network address and the IP Pool Network mask for the IP Pool. The network defined by the IP Pool Network address/mask is used to provide the addresses for connecting clients.

- Click Apply to save changes.

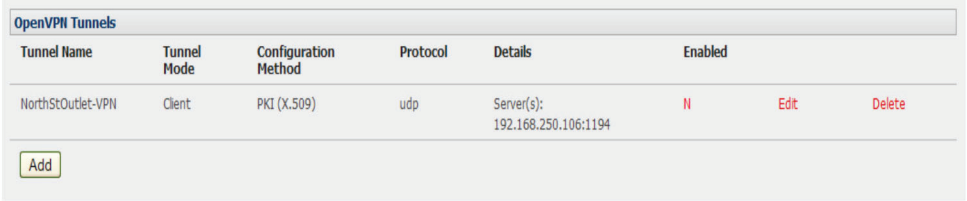
- To enter authentication certificates and files, Edit the OpenVPN tunnel.
- Select the Manage OpenVPN Files tab. Upload or browse to relevant authentication certificates and files.



- Apply to save changes. Saved files will be displayed in red on the right-hand side of the Upload button.

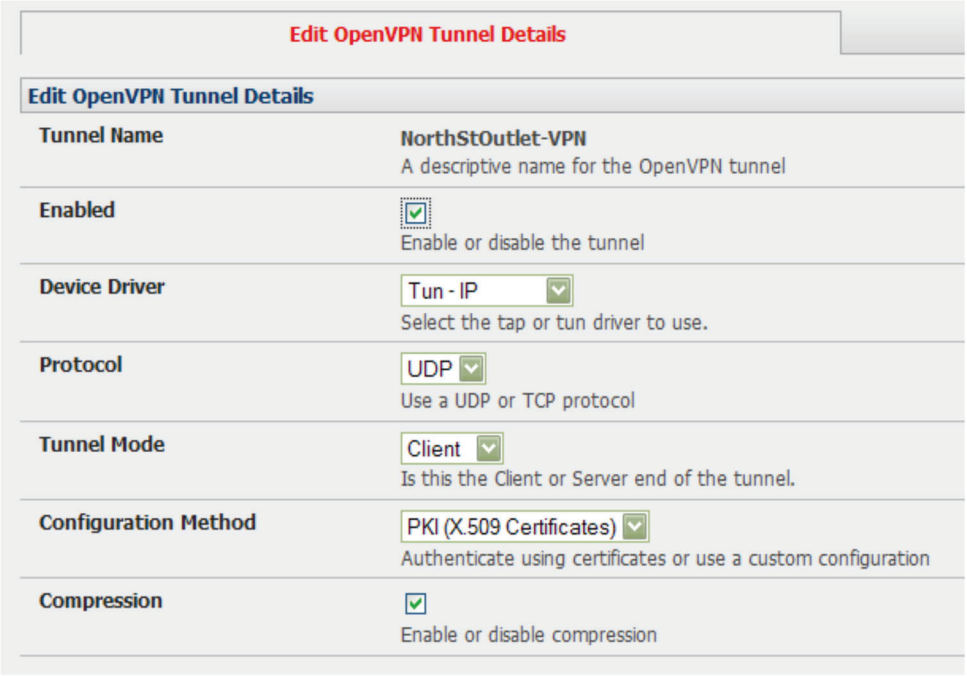


- To enable OpenVPN, Edit the OpenVPN tunnel.

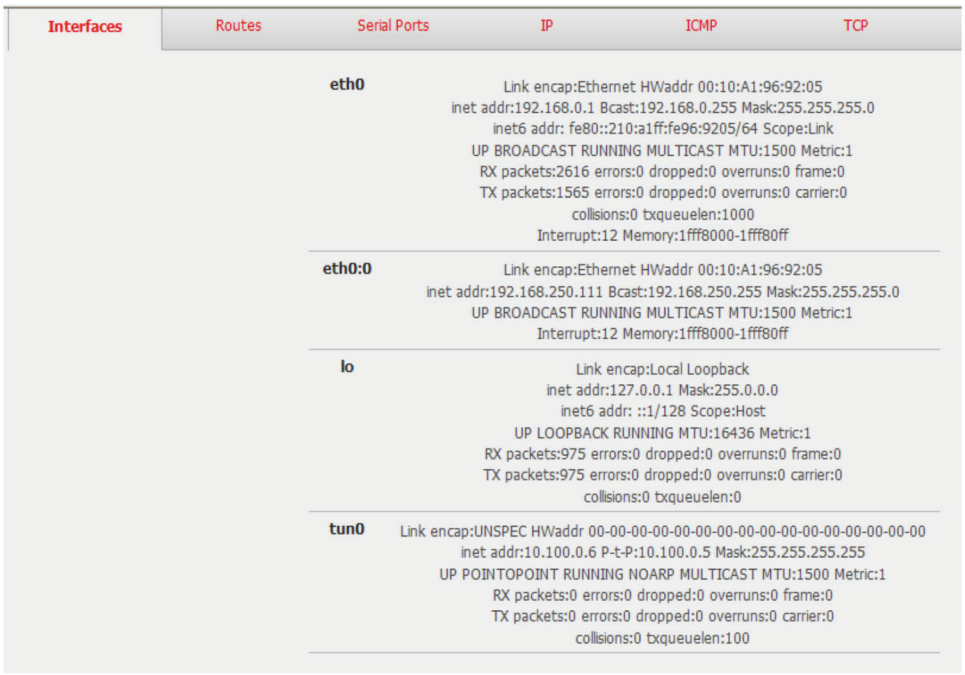


- Check the Enabled button.
- Apply to save changes.

NOTE: Make sure that the VCMS system time is correct when working with OpenVPN. Otherwise, authentication issues may arise.



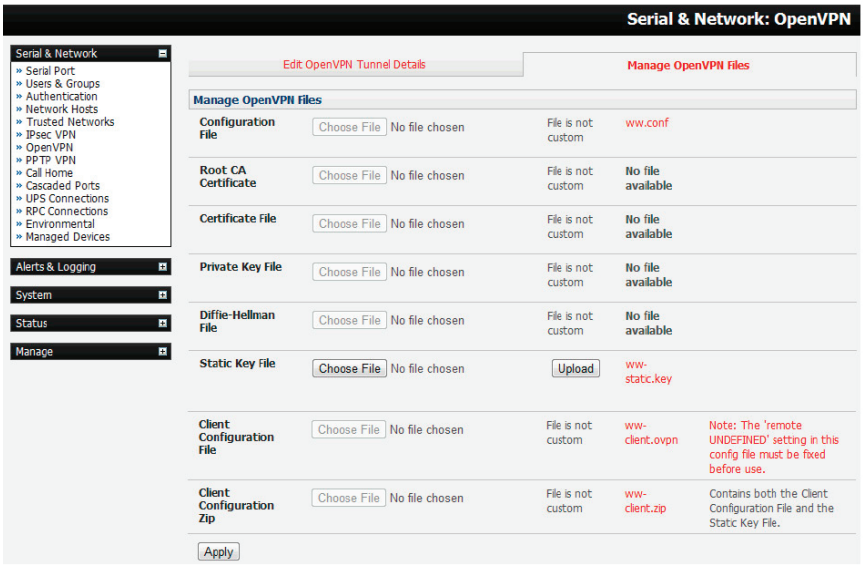
- Select Statistics on the Status menu to verify that the tunnel is operational.



3.10.3 Windows OpenVPN Client and Server set up

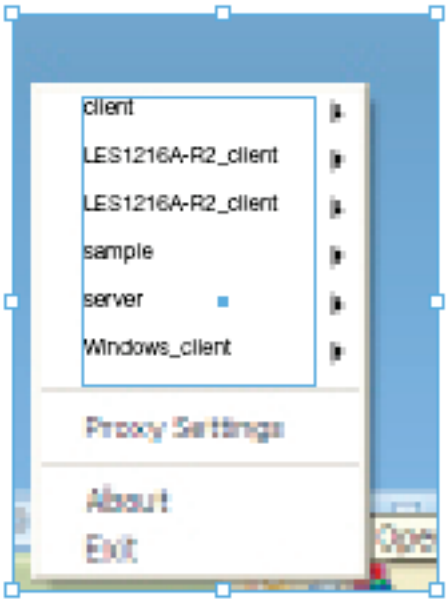
Windows does not come standard with any OpenVPN server or client. This section outlines the installation and configuration of a Windows OpenVPN client or a Windows OpenVPN server and setting up a VPN connection to a VCMS.

VCMS appliances will generate Windows client config automatically from the GUI—for Pre-shared Secret (Static Key File) configurations.



OpenVPN GUI for Windows software (which includes the standard OpenVPN package plus a Windows GUI) can be downloaded from http://openvpn.se/download.html.

- Once installed on the Windows machine, an OpenVPN icon will have been created in the Notification Area located in the right side of the taskbar. Right-click on this icon to start (and stop) VPN connections, and to edit configurations and view logs.



When the OpenVPN software is started, the C:\Program Files\OpenVPN\config folder will be scanned for ".opvn" files. This folder will be rechecked for new configuration files whenever the OpenVPN GUI icon is right-clicked. So once OpenVPN is installed, a configuration file will need to be created:

- Using a text editor, create an xxxx.ovpn file and save in C:\Program Files\OpenVPN\config. For example, C:\Program Files\OpenVPN\config\client.ovpn

An example of an OpenVPN Windows client configuration file is shown below:

```
# description: LES1216A-R2_client
client
proto udp
verb 3
dev tun
remote 192.168.250.152
port 1194
ca c:\\openvpnkeys\\ca.crt
cert c:\\openvpnkeys\\client.crt
key c:\\openvpnkeys\\client.key
nobind
persist-key
persist-tun
comp-lzo
```

An example of an OpenVPN Windows Server configuration file is shown below:

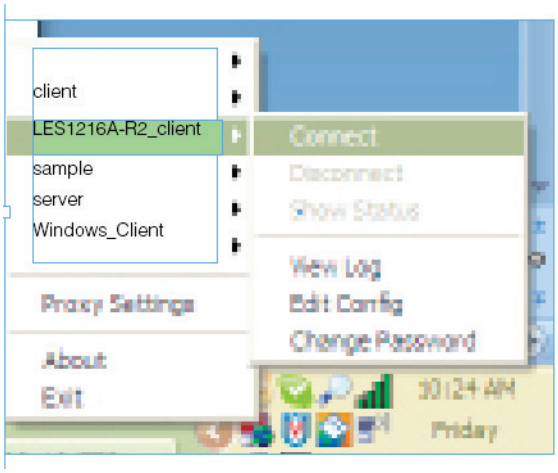
```
server 10.100.10.0 255.255.255.0
port 1194
keepalive 10 120
proto udp
mssfix 1400
persist-key
persist-tun
dev tun
ca c:\\openvpnkeys\\ca.crt
cert c:\\openvpnkeys\\server.crt
key c:\\openvpnkeys\\server.key
dh c:\\openvpnkeys\\dh.pem
comp-lzo
verb 1
syslog LES1216A-R2_OpenVPN_Server
```

The Windows client/server configuration file options are:

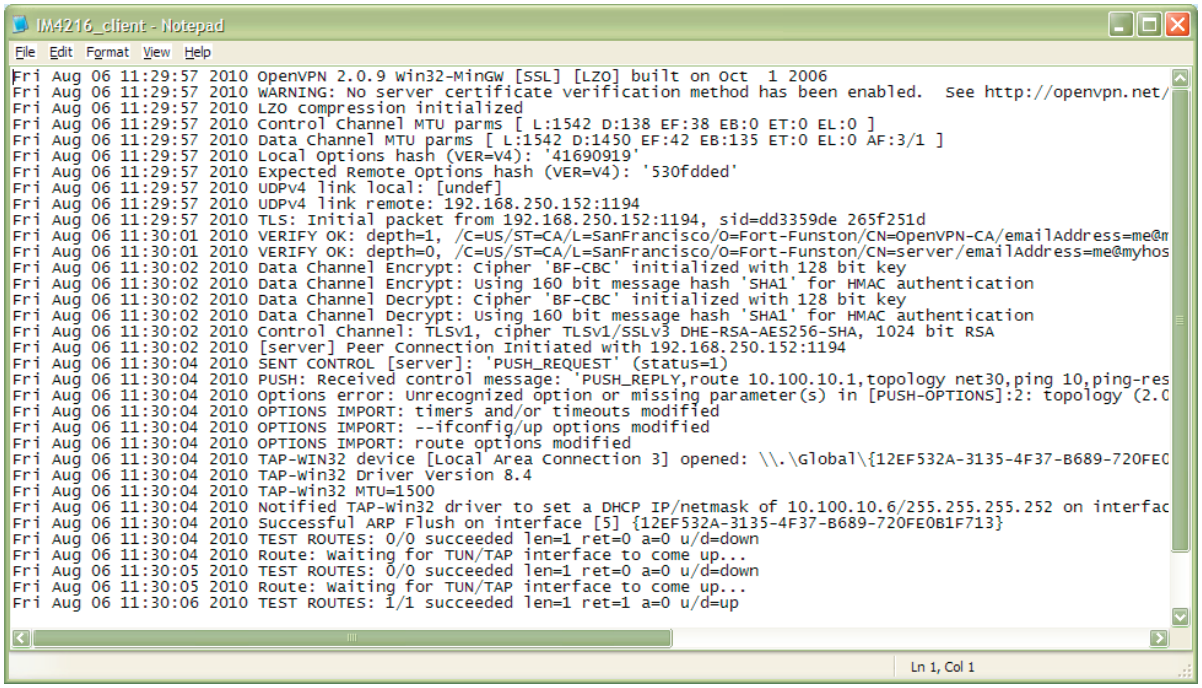
Options	Description
#description:	This is a comment describing the configuration. Comment lines start with '#' and are ignored by OpenVPN.
Client server	Specify whether this will be a client or server configuration file. In the server configuration file, define the IP address pool and netmask. For example, server 10.100.10.0 255.255.255.0
proto udp proto tcp	Set the protocol to UDP or TCP. The client and server must use the same settings.
mssfix <max. size>	Mssfix sets the maximum size of the packet. This is only useful for UDP if problems occur.
verb <level>	Set log file verbosity level. Log verbosity level can be set from 0 (minimum) to 15 (maximum). For example: 0 = silent except for fatal errors 3 = medium output, good for general usage 5 = helps with debugging connection problems 9 = extremely verbose, excellent for troubleshooting
dev tun dev tap	Select "dev tun" to create a routed IP tunnel or "dev tap" to create an Ethernet tunnel. The client and server must use the same settings.
remote <host>	The hostname/IP of OpenVPN server when operating as a client. Enter either the DNS hostname or the static IP address of the server.
Port	The UDP/TCP port of the server.
Keepalive	Keepalive uses ping to keep the OpenVPN session alive. 'Keepalive 10 120' pings every 10 seconds and assumes the remote peer is down if no ping has been received over a 120-second time period.
http-proxy <proxy server> <proxy port #>	If a proxy is required to access the server, enter the proxy server DNS name or IP and port number.
ca <file name>	Enter the CA certificate file name and location. The same CA certificate file can be used by the server and all clients. *NOTE: Ensure each "\" in the directory path is replaced with ""\\". For example, c:\openvpnkeys\ca.crt will become c:\\openvpnkeys\\ca.crt*
key <file name>	Enter the file name and location of the client's or server's key. Each client should have its own certificate and key files. *NOTE: Ensure each "\" in the directory path is replaced with "\\".*
dh <file name>	This is used by the server only. Enter the path to the key with the Diffie-Hellman parameters.
Nobind	"Nobind" is used when clients do not need to bind to a local address or specific local port number. This is the case in most client configurations.
persist-key	This option prevents the reloading of keys across restarts.
persist-tun	This option prevents the close and reopen of TUN/TAP devices across restarts.
cipher BF-CBC Blowfish (default) cipher AES-128-CBC AES cipher DES-EDE3-CBC Triple-DES	Select a cryptographic cipher. The client and server must use the same settings.
comp-lzo	Enable compression on the OpenVPN link. This must be enabled on both the client and the server.
syslog	By default, logs are located in syslog or, if running as a service on Window, in \ Program Files\OpenVPN\log directory.

To initiate the OpenVPN tunnel following the creation of the client/server configuration files:

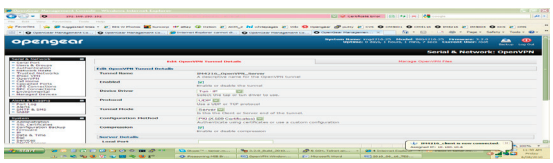
- Right click on the OpenVPN icon in the Notification Area.
- Select the newly created client or server configuration. For example, LES1216A-R2_client.
- Click "Connect" as shown below.



- The log file will be displayed as the connection is established.



- Once established, the OpenVPN icon will display a message notifying of the successful connection and assigned IP. This information, as well as the time the connection was established, is available anytime by scrolling over the OpenVPN icon.



NOTE: An alternate OpenVPN Windows client can be downloaded from http://www.openvpn.net/index.php/openvpn-client/downloads.html. Refer to http://www.openvpn.net/index.php/openvpn-client/howto-openvpn-client.html for help.

3.11 Firewall and Forwarding

VCMS appliances have basic routing, NAT (Network Address Translation), packet filtering, and port forwarding support on all network interfaces.

- Network Forwarding allows the network packets on one network interface to be forwarded to another network interface. So, locally networked devices can IP connect through the VCMS to devices on remote networks.
- IP Masquerading is used to allow all the devices on your local private network to hide behind and share the one public IP address when connecting to a public network. This type of translation is only used for connections originating within the private network destined for the outside public network, and each outbound connection is maintained by using a different source IP port number.
- When using IP Masquerading, devices on the external network cannot initiate connections to devices on the internal network. Port Forwards allows external users to connect to a specific port on the external interface of the VCMS and be redirected to a specified internal address for a device on the internal network.
- With Firewall Rules, packet filtering inspects each packet passing through the firewall and accepts or rejects it based on user-defined rules.
- Then Service Access Rules can be set for connecting to the VCMS itself.

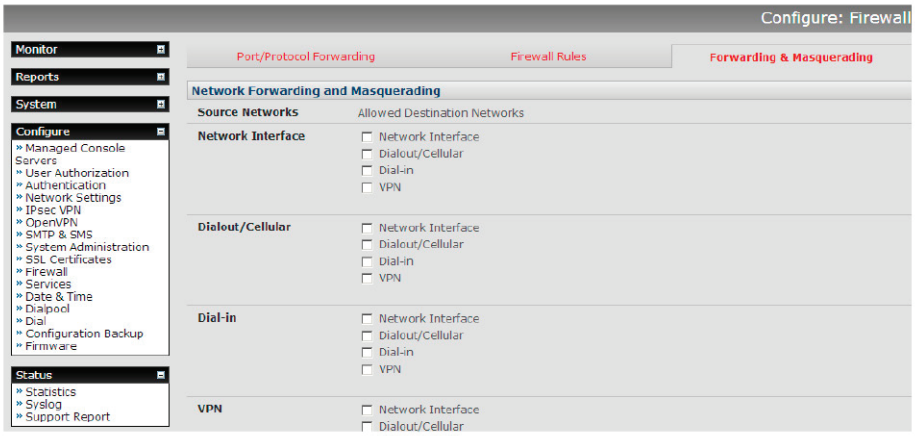
3.11.1 Configuring network forwarding and IP masquerading

To use a VCMS as an Internet or external network gateway requires establishing an external network connection and then setting up forwarding and masquerading.

NOTE: Network forwarding allows the network packets on one network interface to be forwarded to another network interface. So, locally networked devices can IP connect through the VCMS to devices on remote networks. IP masquerading is used to allow all the devices on your local private network to hide behind and share the one public IP address when connecting to a public network. This type of translation is only used for connections originating within the private network destined for the outside public network, and each outbound connection is maintained by using a different source IP port number.

By default, all VCMS models are configured so that they will not route traffic between networks. To use the VCMS as an Internet or external network gateway, forwarding must be enabled so that traffic can be routed from the internal network to the Internet/external network:

- Navigate to the System: Firewall page, and then click on the Forwarding & Masquerading tab.



• Find the Source Network to be routed, and then tick the relevant Destination Network to enable Forwarding.

IP Masquerading is generally required if the VCMS will be routing to the Internet, or if the external network being routed to does not have routing information about the internal network behind the VCMS.

IP Masquerading performs Source Network Address Translation (SNAT) on outgoing packets, to make them appear like they've come from the VCMS (rather than devices on the internal network). When response packets come back to devices on the external network, the VCMS will translate the packet address back to the internal IP, so that it is routed correctly. This allows the VCMS to provide full outgoing connectivity for internal devices using a single IP Address on the external network.

By default, IP Masquerading is disabled for all networks. To enable masquerading:

• Select Forwarding & Masquerading panel on the System: Firewall menu.

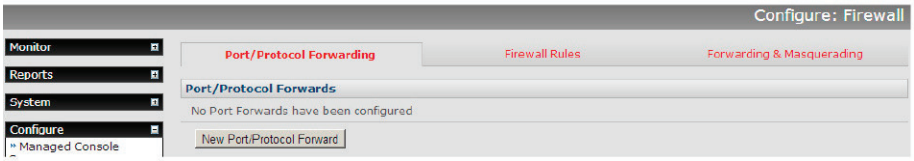
• Check Enable IP Masquerading (SNAT) on the network interfaces where masquerading is be enabled.

Generally, this masquerading would be applied to any interface that is connecting with a public network such as the Internet, e.g. for the VCMS with an external modem, the IP masquerading would be enabled on Dialout/Cellular.

3.11.2 Port/Protocol forwarding

When using IP Masquerading, devices on the external network cannot initiate connections to devices on the internal network.

To work around this, Port Forwards can be set up to allow external users to connect to a specific port, or range of ports on the external interface of the VCMS, and have the VCMS redirect the data to a specified internal address and port range.



To setup a port/protocol forward:

• Navigate to the System: Firewall page, and click on the Port Forwarding tab.

• Click Add New Port Forward.

• Fill in the following fields:

- Name: Name for the port forward. This should describe the target and the service that the port forward is used to access.

- Input Interface: This allows the user to only forward the port from a specific interface. In most cases, this should be left as "Any."

- Source Address/Address Range: This allows the user to restrict access to a port forward to a specific source IP address or IP address range of the data. This may be left blank. IP address ranges use the format ip/netmask (where netmask is in bits 1–32).

- Destination Address/Address Range: The destination IP address/address range to match. This may be left blank.

- IP address ranges use the format ip/netmask (where netmask is in bits 1–32).

- Input Port Range: The range of ports to forward to the destination IP. These will be the port(s) specified when accessing the port forward. These ports need not be the same as the output port range.

- Protocol: The protocol of the data being forwarded. The options are TCP or UDP or "TCP and UDP" or ICMP or ESP or GRE or Any.

- Output Address: The target of the port forward. This is an address on the internal network where packets sent to the Input Interface on the input port range are sent.

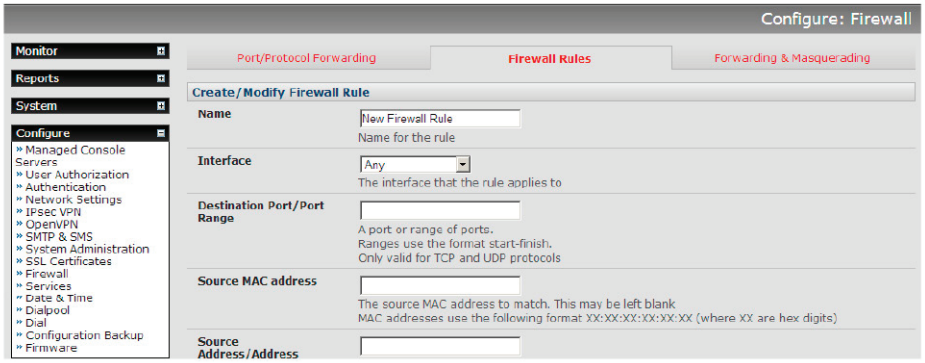
- Output Port Range: The port or range of ports that the packets will be redirected to on the Output Address. Ranges use the format start-finish. Only valid for TCP and UDP protocols.

3.11.3 Firewall rules

Firewall rules can be used to block or allow traffic through an interface based on port number, the source and/or destination IP address (range), the direction (ingress or egress), and the protocol. This can be used to allow custom on-box services, or to block traffic based on policy.

To setup a firewall rule:

• Navigate to the System: Firewall page, and click on the Firewall Rules tab.



• Click New Firewall Rule

• Fill in the following fields:

- Name: Name the rule. This name should describe the policy the firewall rule is being used to implement (e.g. block ftp, Allow Tony).

- Interface: Select the interface that the firewall rule will be applied to (i.e. Any, Dialout/Cellular, VPN, Network Interface, Dial-in, etc).

- Port Range: Specify the Port or range of Ports (e.g. 1000–1500) that the rule will apply to. This may be left blank for Any.

- Source MAC address: Specify the source MAC address to be matched. This may be left blank for any. MAC addresses use the format XX:XX:XX:XX:XX:XX, where XX are hex digits.

- Source Address Range: Specify the source IP address (or address range) to match. IP address ranges use the format ip/netmask (where netmask is in bits 1–32). This may be left blank for Any.

- Destination Range: Specify the destination IP address/address range to match. IP address ranges use the format ip/netmask (where netmask is in bits 1–32). This may be left blank.

- Protocol: Select if the firewall rule will apply to TCP or UDP or "TCP and UDP" or ICMP or ESP or GRE or Any.

- Direction: Select the traffic direction that the firewall rule will apply to (Ingress = incoming or Egress = outgoing).

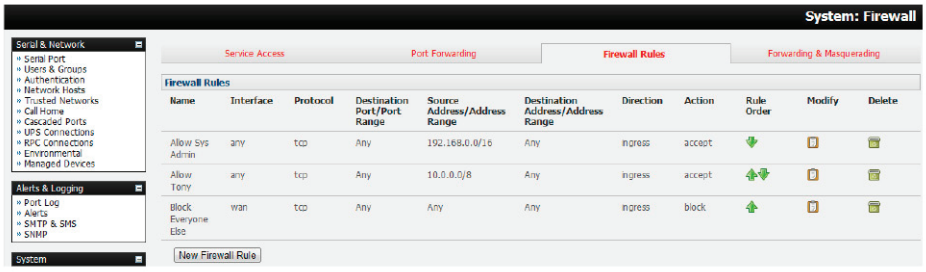
- Action: Select the action (Accept or Block) that will be applied to the packets detected that match the Interface+ Port Range+ Source/destination Address Range+ Protocol+ Direction.

For example, to block all SSH traffic from leaving Dialout Interface, the following settings can be used:

- Interface: Dialout/Cellular
- Port Range: 22
- Protocol: TCP
- Direction: Egress
- Action: Block

The firewall rules are processed in a set order: from top to bottom. Rule placement is important. For example, with the following rules, all traffic coming in over the Network Interface is blocked except when it comes from two nominated IP addresses (SysAdmin and Fred):

	To allow all incoming traffic on all interfaces from the SysAdmin:	To allow all incoming traffic from Fred:	To block all incoming traffic from the Network Interface:
Interface	Any	Any	Network Interface
Port Range	Any	Any	Any
Source MAC	Any	Any	Any
Source IP	IP address of SysAdmin	IP address of Fred	Any
Destination IP	Any	Any	Any
Protocol	TCP	TCP	TCP
Direction	Ingress	Ingress	Ingress
Action	Accept	Accept	Block



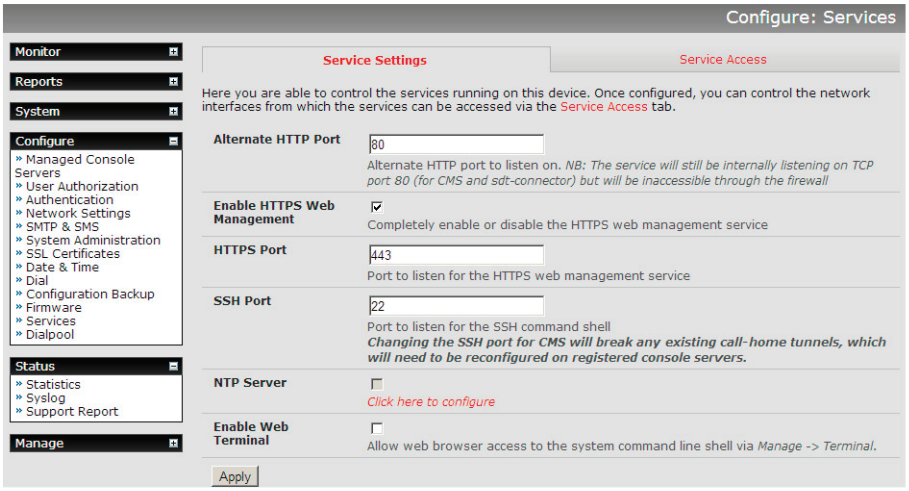
If the Rule Order above was to be changed so the "Block Everyone Else" rule was second on the list, then the traffic coming in over the Network Interface from Fred would be blocked.

3.12 Services and Service Access

The Administrator can access the VCMS (and its Managed Console Servers and their connected and managed devices), using a range of access protocols/services. You can control the services running on the VCMS and the network interfaces from which the services can be accessed.

To enable and/or configure a service:

- Select the Service Settings tab on the Configure: Services page.



- Enable and configure basic services:

- HTTP: By default, the HTTP service is running and it cannot be fully disabled. By default, HTTP access is disabled on all interfaces and we recommend that this access remain disabled if the VCMS is to be remotely accessed over the Internet.

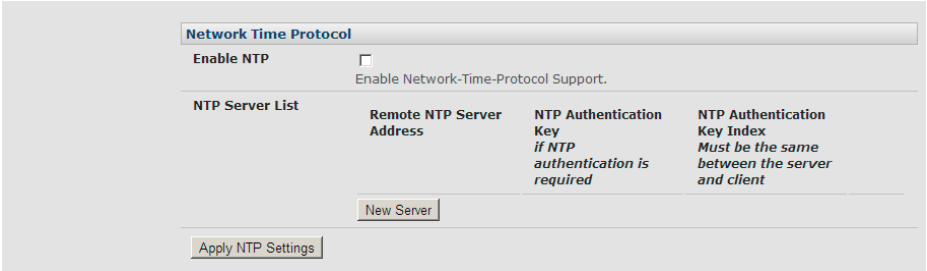
  Alternate HTTP also enables you to configure an alternate HTTP port to listen on. But, the HTTP service will continue listening internally on TCP port 80 (for VCMS and sdt-connector communications), but will be inaccessible through the firewall.

- HTTPS: By default, the HTTPS service is running and this service is enabled on all network interfaces. We recommend that you only use HTTPS access if the VCMS is to be managed over any public network (e.g. the Internet). This ensures the Administrator has secure browser access to all the menus on the VCMS. The HTTPS service can be completely disabled (or re-enabled) by checking HTTPS Web Management and specifying an alternate port (default port is 443).

- SSH: This service provides secure SSH access to the VCMS. The SSH service is always running and, by default, is enabled on all interfaces. An alternate SSH port to listen on can be specified in SSH command shell port (default port is 22). But changing the SSH port for VCMS will break any existing call-home tunnels, which will need to be reconfigured on registered VCMSs.

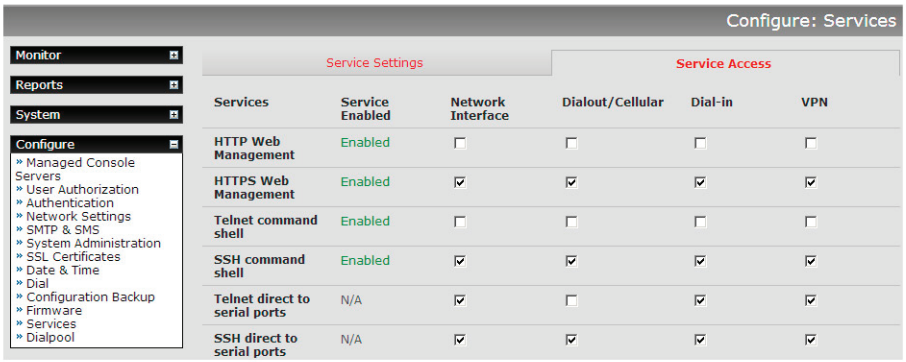
- Web Terminal: Checking Enable Web Terminal will allow Web browser access to the system command line shell via Manage: Terminal.

- NTP: Configuring NTP ensures the VCMS clock is kept extremely accurate (once Internet connection has been established). Select the Enable NTP checkbox, and enter the IP address of the remote NTP Server. If your external NTP server requires authentication, you need to specify the NTP Authentication Key and the Key Index to use when authenticating with the NTP server. Click Apply NTP Settings.



To control the network interfaces from which the services can be accessed:

- Select the Service Access tab on the System: Services page. This will display the services currently enabled for the VCMS appliance's network interfaces.

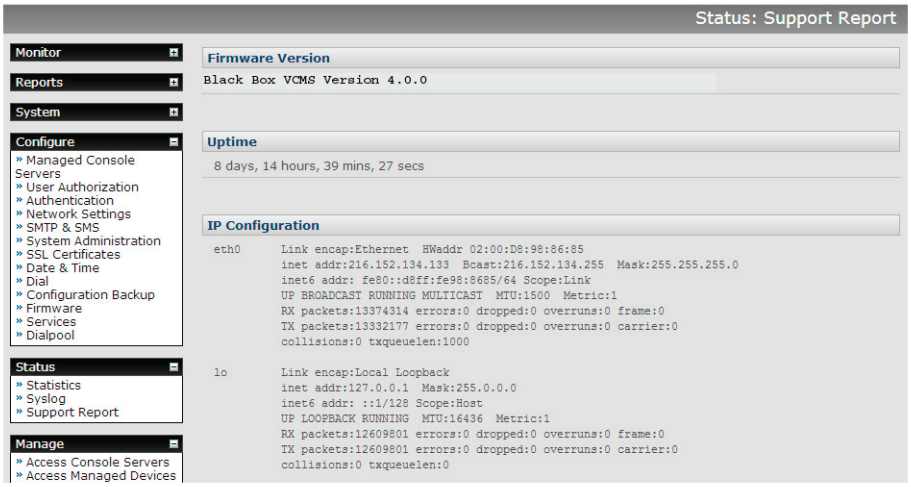


- Check/uncheck for each network that you want to enable/disable service access for.
- Click Apply to apply your services access selections.

3.13 Support Report

The Support Report provides useful status information that will assist the Black Box technical support team to solve any problems you may experience with your VCMS. Contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

If you do experience a problem and have to contact tech 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.



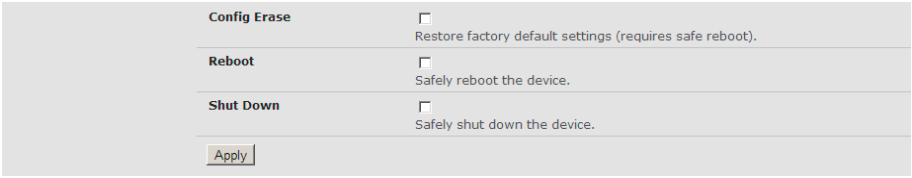
- Select Status: Support Report and you will be presented with a status snapshot.
- Save the file as a text file and attach it to your support email.

3.14 System Reset

The Administrator can reboot or reset the VCMS to default settings.

For a soft reset:

- Select Reboot in the Configure: System Administration menu to safely reboot your VCMS appliance. The VCMS reboots with all settings (e.g. the assigned network IP address) preserved. This soft reset does disconnect all users and ends any SSH sessions that had been established.
- Select Config Erase to erase all configurations and restore factory default settings. This setting requires a safe reboot. On reboot you will be prompted to enter and confirm a new root password before the device (UI and ssh) can be accessed.
- Click Apply.



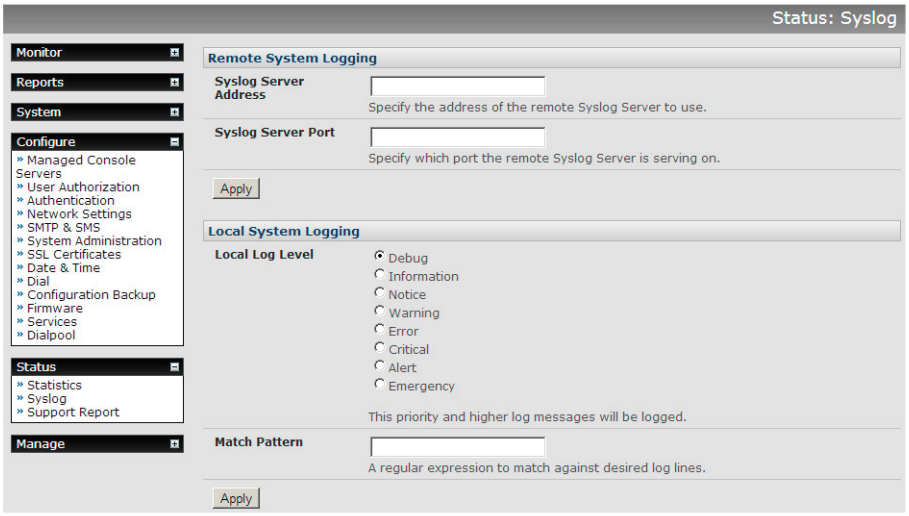
3.15 Syslog

The Linux System Logger in VCMS maintains a record of all system messages and errors. The syslog record can be redirected to a remote Syslog Server:

- Select Status: Syslog and enter the remote Syslog Server Address and Syslog Server Port details and click Apply.

The console maintains a local Syslog. To view the local Syslog file:

- Select Status: Syslog



- Local Log Level enables you to limit the amount of Syslog information logged by specifying event types to be logged.
- To make it easier to find information in the local Syslog file, a pattern matching filter tool is provided. Specify the Match Pattern that is to be searched for.
- Click Apply. The Syslog will then be represented with only those entries of the nominated event type and that actually include any specified pattern.

3.16 Dialpool — centralized dial-out

VCMS enables you to build modems into a simple virtual modem pool that can be browser-accessed by field engineers for out-of-band connection to remote sites.

The modems in the out-dial pool are serially connected to downstream Managed Console Servers—which themselves may be distributed regionally (or internationally).

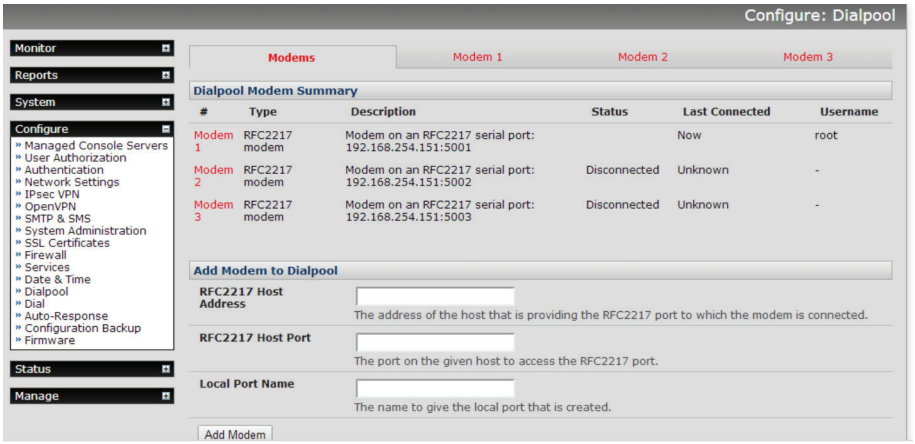
So dialpool provides a centralized dial-out capability. Admins from anywhere use their browser to trigger a dial-out session and connect to managed console servers at remote sites out-of-band via an analog modem connection—without the need to carry their own modem. Also, by distributing the downstream console servers (that host the dialpool modem[s] within the remote countries and regions, they can overcome international line quality issues from trying to use compressed PSTN lines and dialing globally.

Establishing the dialpool and initiating a dial-out connection is a simple process of:

- Establishing RFC2217 connections to the modem port(s) on downstream console servers that are IP connected to the VCMS.
- Adding each modem to the VCMS dialpool and adding the connection details for the Managed Console Server that is to be dialed (e.g., dial-out phone number).
- Configuring the Managed Console Server for in-dial access.
- Clicking Dial.

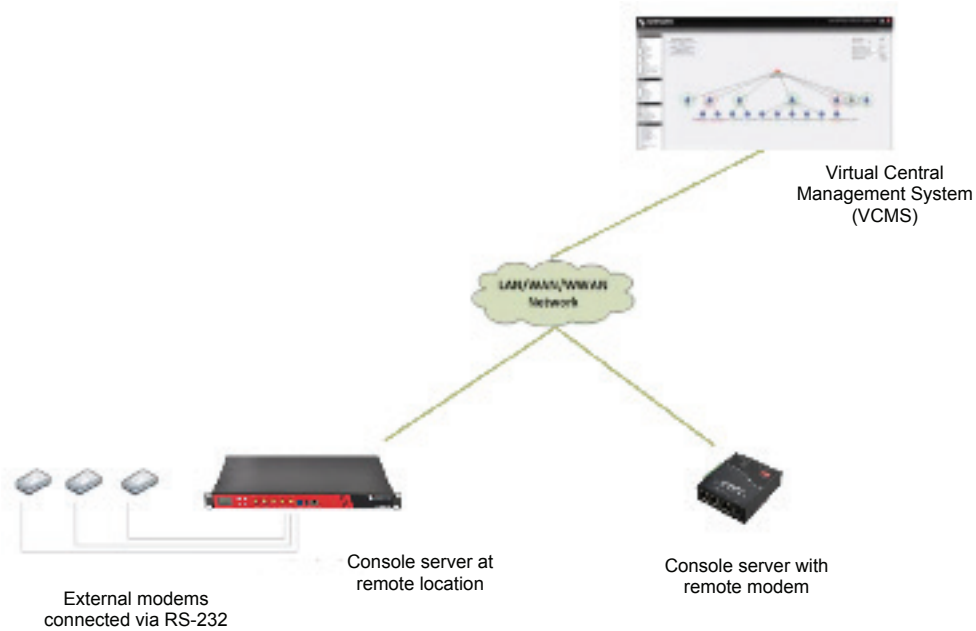
3.16.1 Dialpool setup

The Configure: Dialpool shows the modems in the dialpool. The Modems tab (v4.3 and later) presents a summary view with details about modem setup, type, current status information (disconnected, dialing, or connected) as well as the connection time and the user that initiated dialing. More details are provided within each of the individual modem tabs.



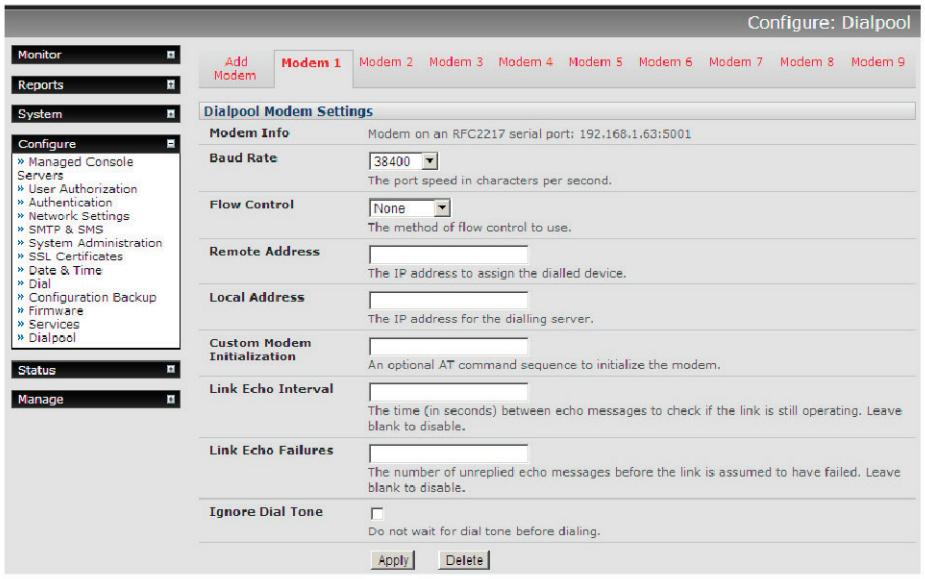
3.16.2 Add modems to the dialpool

To add a modem to the pool, select Configure: Dialpool and go to the Add Modem to Dialpool section. Enter the Host Address (i.e. the IP address or Domain Name of the downstream Managed Console Server) and the RFC2217 Host Port address (i.e. the tcp port # of the modem serial port, e.g. 5011).

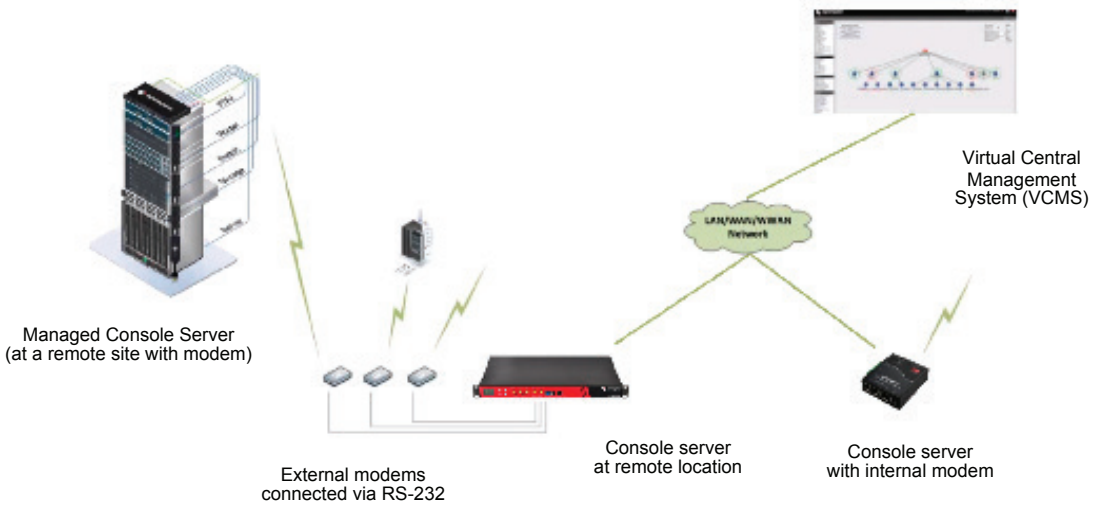


NOTE: RFC2217 provides for virtual serial port connections, and the serial port with the modem must have this enabled. To enable this on the downstream console server, simply tick RFC2217 as the Console Server Setting for the specific serial port in the Serial & Network: Serial Ports menu.

- Provide the modem a Local Port Name and click Add Modem.
- A new tab will have been created on the Configure: Dialpool page for the modem you added. Select this tab and set up for your out-dial settings.

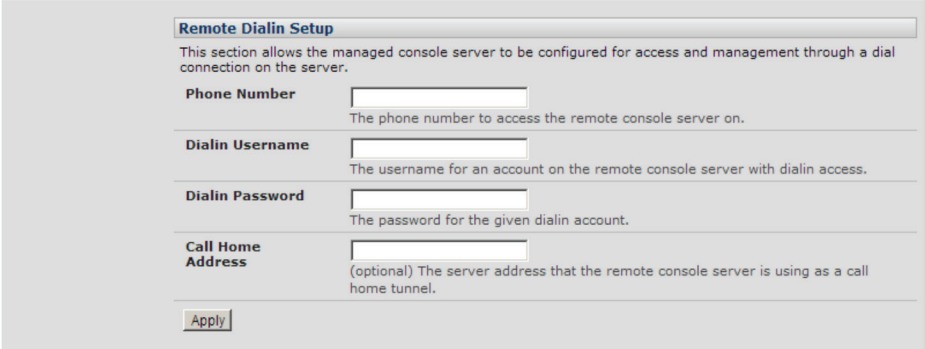


Once you have the modem pool set up for your dial out, you will need to set up the phone numbers etc. of the modems you may wish to dial into for out of band management.



As you add new Managed Console Servers, or edit existing ones:

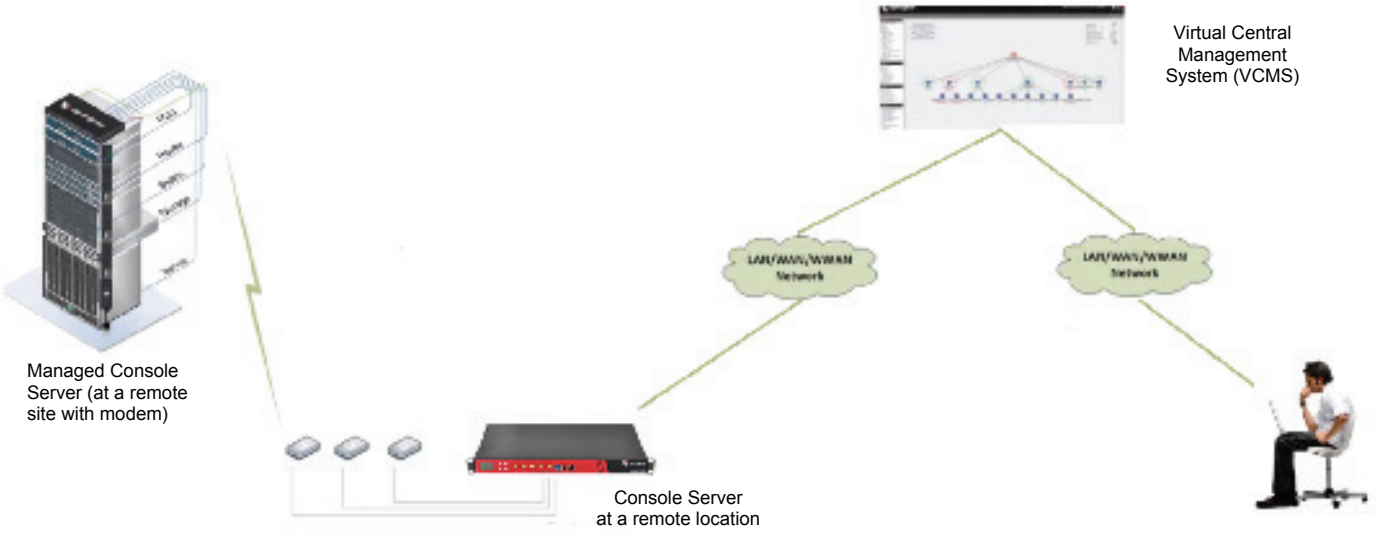
- In Configure: Managed Console Servers configure Remote Dialin Setup to allow it to be accessed and managed through a dial in connection.



- Enter the Phone Number to access the remote Managed Console Server on.
- Enter the Dialin Username and Password for a user account on the Managed Console Server with dialin access.

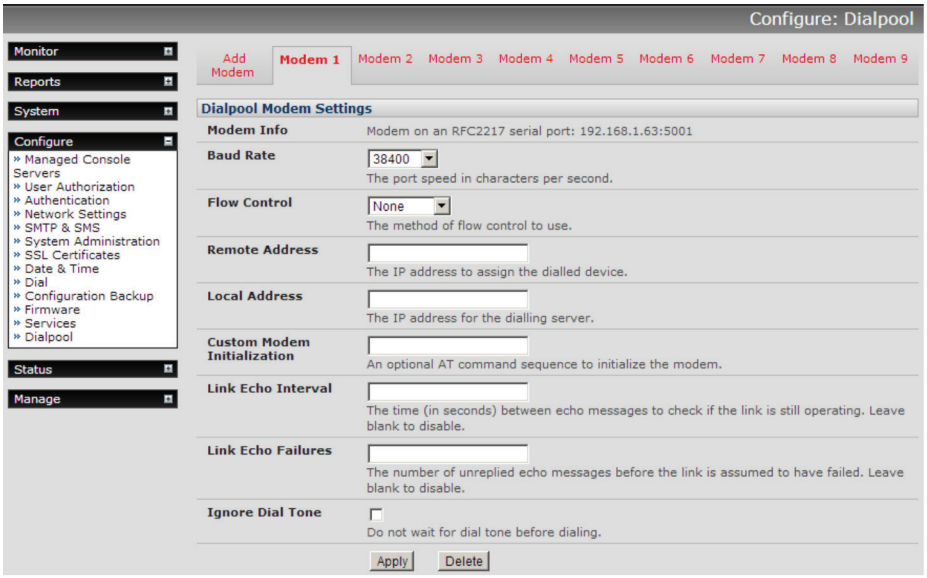
3.16.3 Dialing Managed Console Servers

There are two paths for accessing any of these configured console servers through the virtual datapool.

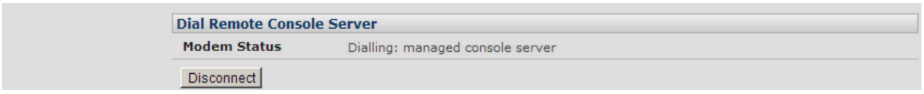


The Configure: Dialpool page allows you to manually select any modem from the pool and dial:

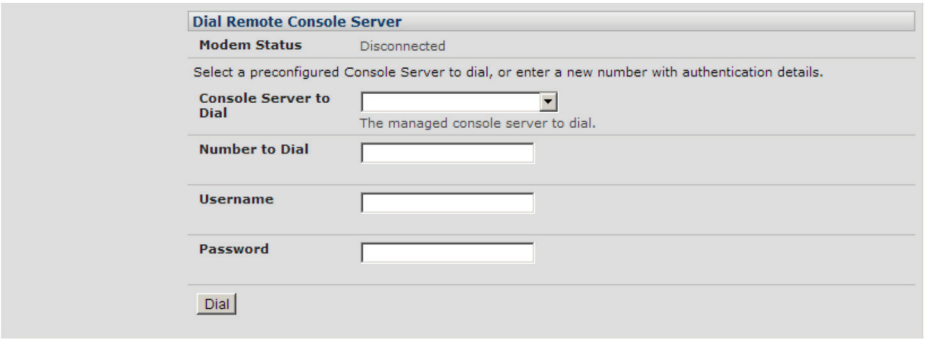
- Select Configure: Dialpool and select any modem in the virtual pool.



- If the modem is already in use (Dial Remote Console Server reports Modem Status: Dialling), then simply browse for a free modem in the pool.



- Select a preconfigured Console Server to Dial from the drop down list, or enter a new Number to Dial with authentication details.
- Press Dial.



- You will now be dial connected to the Managed Console Server and can access it and its Managed Devices through the Manage: Access Console Servers page.

Alternately, with software V4.3 and later, the Manage: Access Console Servers page includes an extra column for dial access that will automatically select a free modem from the pool and dial.

- Select Manage: Access Console Servers. This will show, for each managed console server, if it has been set up for dial access, and if so, the current status.
- Buttons are provided to either dial the console server (if disconnected), or disconnect a currently dialed connection.

3.16.4 Dialpool health monitoring

The dialpool health test (V4.3 and later) is configured through the Auto-Response interface. A new test type, "Dialpool Health," is available, which gives the following options to test connectivity to managed console servers and/or dialpool modems.

- Test Managed Console Servers: if managed console servers (with dial acess configured) should be regularly tested, as per the specified parameters.
- Threshold: the number of hours/days/weeks/months that a managed console server must not have been accessed for, before the health test will attempt to dial it.
- Max Modem Count: the maximum number of modems to use in parallel to test dial managed console servers. This can be used to ensure that some modems are always available for use.
- Test Dialpool Modems: if dialpool modems should be tested if they have not been used within the specified timeframe.
- Threshold: the number of hours/days/weeks/months that a modem must not have been used before it will be tested by the health check.

Once configured, the health can be used with the standard Auto Response actions (e.g., it could send a notification email whena modem or console server fails to connect.

When using an action for the dial health test Auto-Response, there are some extra custom variables that can be used:

- DIAL_DEVICE: the type of device that has failed, either "modem" or "device."
- DIAL_NAME: the name of the device that has failed, or the modem number if a modem.
- DIAL_LASTTIME: The last time the device was successfully connected.
- DIAL_FAILURES: The number of repeated failures the device has had since last connect.

An example alert message could be:

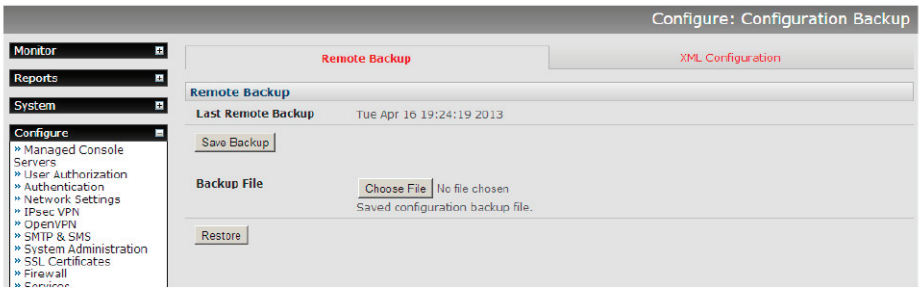
$TIMESTAMP: Dial health test failed connection to $DIAL_DEVICE $DIAL_NAME: Last connected time was $DIAL_LASTTIME. Has failed $DIAL_FAILURES times.

3.17 Configuration Backup

We recommend that you back up the VCMS configuration whenever you make significant changes (such as adding new Users or Managed Devices) or before performing a firmware upgrade.

- Select the System: Configuration Backup menu option or click the Backup icon.

NOTE: The configuration files can also be backed up from the command line.



You can save the backup file remotely on your PC, and you can restore configurations from remote locations:

- Click Save Backup in the Remote Configuration Backup menu.
- The config backup file (System Name_date_config.opg) will be downloaded to your PC and saved in the location you nominate.

To restore a remote backup:

- Click Browse in the Remote Configuration Backup menu and select the Backup File you wish to restore.

• Click Restore and click OK. This will overwrite all the current configuration settings in your console server.

3.18 Upgrade Firmware

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

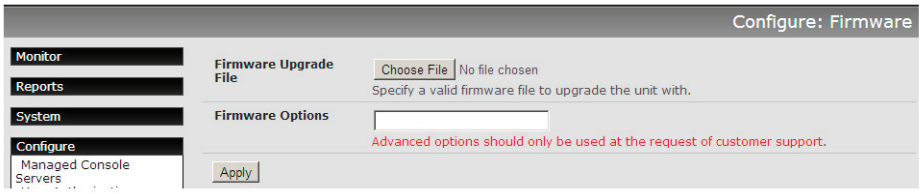
• The Firmware version is displayed in the header of each page, or you can select Configure: Support Report and note the Firmware Version listed there.

• The VCMS upgrade files (*.bin) are available from http://www.Black Box.com/firmware/. Which upgrade file you use also depends on your solution.

- For VCMS (VMware and Linux KVM) use vcms-x.y.z-vm.bin (e.g., vcms-4.1.0u1-vm.bin)

- For Advanced and Value-Line Console Servers, use vcms-x.y.z-hw.bin

• Save this downloaded firmware image file on to a system on the same subnet as the VCMS.



• Also download and read the release_notes.txt for the latest information.

• To upload the firmware image file to your VCMS, select Configure: Firmware.

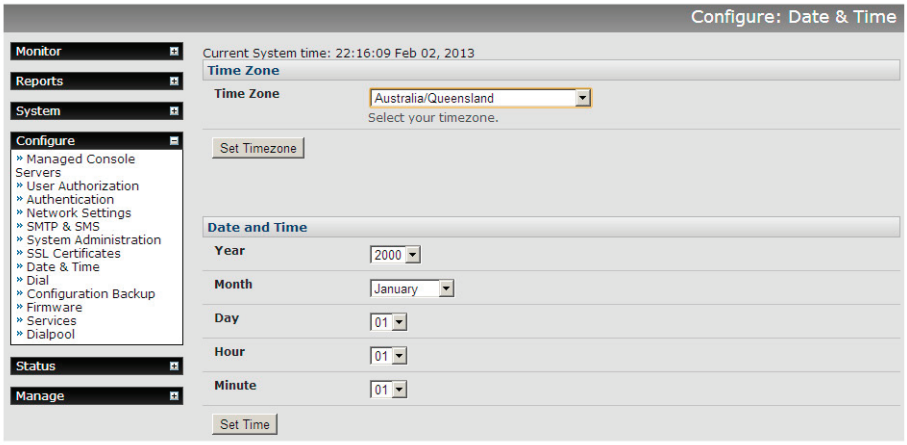
- Browse the local PC and locate the downloaded file.

- Click Apply and the VCMS appliance will perform 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 VCMS will have retained all its pre-upgrade configuration information.

3.19 Configure Date and Time

We recommend that you set the local Date and Time in the VCMS as soon as it is configured. Many of the VCMS 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.

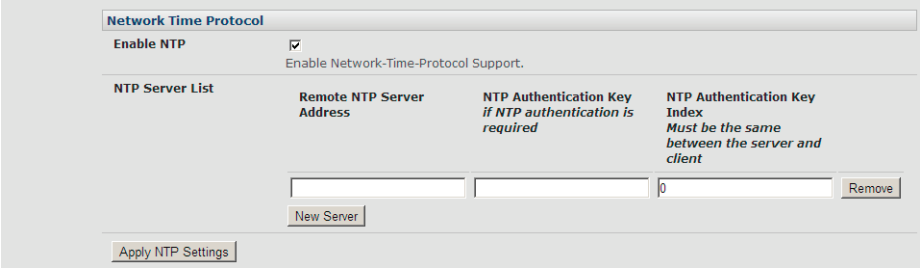
Alternately, the VCMS can synchronize its system time with a remote time server using the Network Time Protocol (NTP). Configuring the NTP time server ensures that the VCMS clock will be accurate soon after the Internet connection is established. To set the system time using NTP:

• Select the Enable NTP checkbox in the Network Time Protocol section.

• Enter the IP address of the remote NTP Server.

• If your external NTP server requires authentication, you need to specify the NTP Authentication Key and the Key Index to use when authenticating with the NTP server.

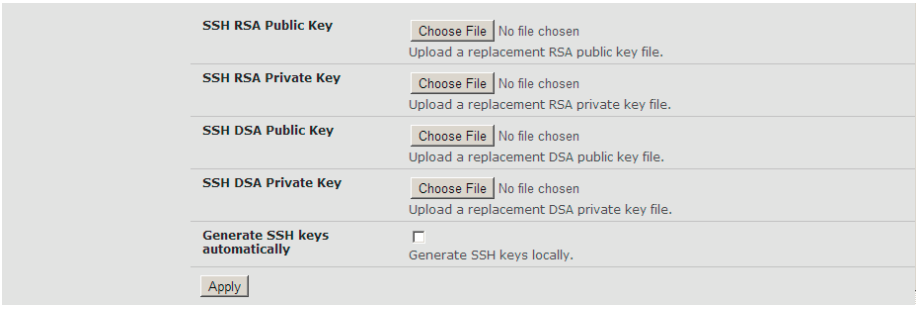
• Click Apply NTP Settings.



3.20 Key Exchange

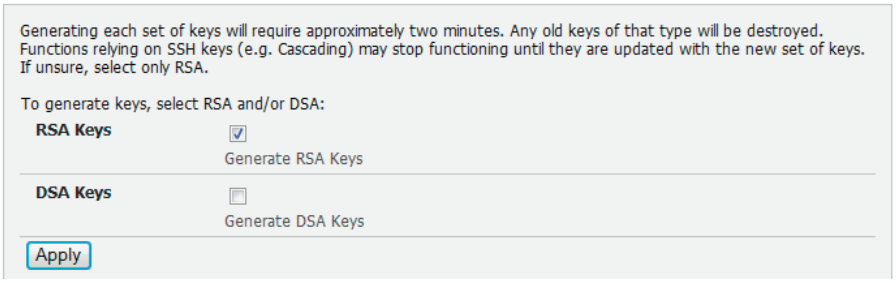
The VCMS automatically generates the SSH keys used to communicate with each of its Managed Console Servers.

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 VCMS.



• 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 VCMS:

• Select Configure: System Administration on the VCMS.

• 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.

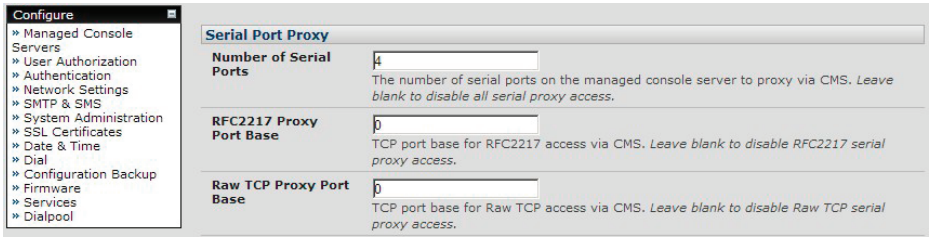
3.21 Console Gateway

VCMS provides a single point of access for multiple console servers, and the Console Gateway feature allows command line access to any of the devices serially connected to the console servers through a single IP address. This feature requires VCMS software V4.4 (and later) and console server firmware V3.9.0u3 (and later).

3.21.1 Configuring the Console Gateway

To enable the Console Gateway functionality on a Managed Console Server, the number of serial ports it has must be specified.

• This is either done at the time of adding new Managed Console Servers or by editing existing Managed Console Servers. As described in Section 3.4.1 this involves specifying the number of serial ports to be proxied (which generally would be all the serial ports on the console server).



• With the Console Gateway, the menu generation and authorization decisions take place on VCMS, so it is important to keep the console servers synchronized with VCMS after configuration changes. This can be done by going to the Managed Console Servers page, selecting the console server, and clicking Retrieve Managed Devices. Failure to do so may mean that port labels and user authorization become inconsistent.

  When the VCMS retrieves the config from the device, it gets a list of all of the serial ports, their labels, and the users and groups that have access to them. This is what is used to generate the menus, and to do the authorization.

3.21.2 Console Gateway access

To use this functionality, use SSH to connect to the Lighthouse appliance, with the username format username:serial This will connect to the Lighthouse, and present a list of console servers that the user has access to.

Once the user selects a console server, they are presented with a list of console ports the user has access to. When one is selected, the user is connected to that port.

For faster access, there are some shortcuts that can be used in the username format that can give more specific lists of serial ports, or direct access without a menu:

username:console_server_name

When a valid console server name is specified, a list of console ports that the user has access to on that console server will be presented. If they do not have access to that console server, the connection will fail.

username:console_server_name:port_name

When a valid console server name and port name are specified, and the user has access to that console server and port, the user will be directly connected to that port. If they do not have access to that port, the connection will fail.

username:port_name

When a valid port name is specified, the user will be connected to the first console server port with that port name found. If the user does not have access to that port, the connection will fail.

NOTE: The console server names and port names are not case-sensitive.

3.21.3 Authentication and Authorization

VCMS supports both local and remote authentication including Radius,TACACS,LDAP (Active Directory), and Kerberos

Local Authentication

When local authentication is used, users are retrieved from the managed console servers and are given authorization and passwords via the User Authorization page on the VCMS. The user will have access to console servers that the users were retrieved from. For example, if the user "joe" exists on three console servers, then he will have access to those three console servers, and any ports on those console servers than he has been given access to (via the console server's User page).

Remote Authentication

Remote authentication can be used in two ways: Authentication only or Authentication and Authorization.

When the remote authentication service is used for authentication only, the users must exist on the console servers that they have access to, and be configured in the manner described above in the "Local Authentication" section. Kerberos can only be used in this mode.

When the remote authentication service is being used for authentication and authorization, minimal configuration of the console servers is needed to provide many users access to the ports. This is enabled by ticking the "Use Remote Groups" box on the Authentication page.

Radius, LDAP and TACACS can be configured to pass a list of groups back as part of an authentication operation. If any of these groups exist on the managed console servers, then the remote users will have access to those console servers, and the ports specified in the group definition on the console server.

For example, if on each console server, there is a NetworkGroup group configured that has access to a number of ports on each server (e.g. switches and routers), then any remote user that has NetworkGroup as a group will get access to those ports.

TACACS can also be further configured to provide a list of console servers and ports that the user has access to. Below is a snippet from a tac_plus configuration:

```
user = tu1 {
        service = raccess {
                port2 = acm5003/port02
                port3 = acm5003/port03
                port4 = kcs6104/port02
                port5 = kcs6104/port03
                port6 = cm4116/port01
                port7 = cm4116/port02
                port8 = cm4116/port03
                port9 = cm4116/port04
                port10 = kcs6104/port04
                port11 = acm5003/port01
                port12 = img4216-25/port01
                port13 = img4216-25/port02
                port14 = img4004-5/port01
                port15 = img4004-5/port02
                port16 = cm4001/port01
                port17 = imx4216/port01
                port18 = imx4216/port03
                port19 = im4248-34/port01
                port20 = acm550x/port04 priv-lvl = 4
        }
}
```

This snippet shows a number of console servers and ports that the user tu1 has access to. The important parts of a config line are as follows:

port2 = acm5003/port02

port2 <- this is an access list index, it is not related to a specific port number on the console server
LES1516A <- this is the name of the console server in VCMS
port02 <- this is the number of the port on the console server (port numbers start at port01)

This configuration syntax allows full access configuration to be done at the central point, rather than requiring extra groups to be configured on the console server. Please note that this only works for the Serial port concentrator functionality - the WebUI access console server page does not support

4. Accessing Managed Console Servers and Devices

The VCMS provides a simple way to monitor and access Managed Console Servers and Devices using a single sign-on. It also provides a selection of paths through which network engineers and system administrators can access and manage their Managed Console Servers and attached Managed Devices and serial ports.

These include browser, web terminal, and SSH connection facilities. This chapter covers these access paths, and covers some batch command facilities reconfiguring Managed Console Servers.

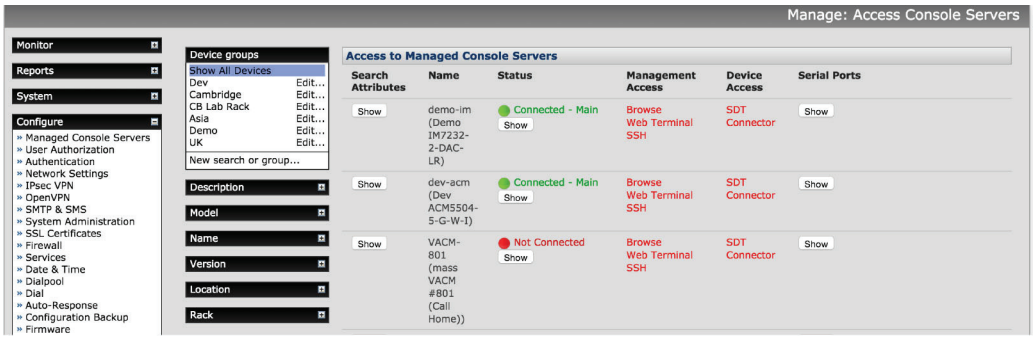
4.1 Viewing Managed Console Servers and Devices

4.1.1 Viewing Managed Console Servers

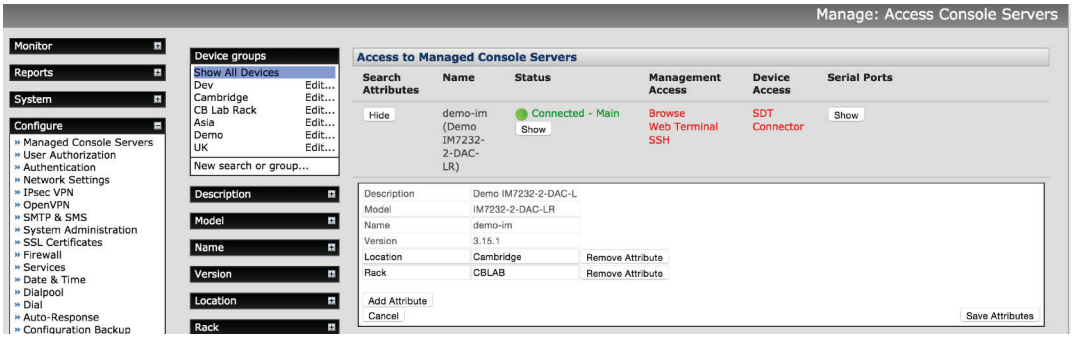
The Manage: Access Console Server screen provides a search and filter-by-attribute tool for accessing and managing groups of Managed Console Servers.

- Click Manage: Access Console Servers. The console servers (and the Managed Devices and serial ports) that the current user has access to are listed under Access to Managed Console Servers.

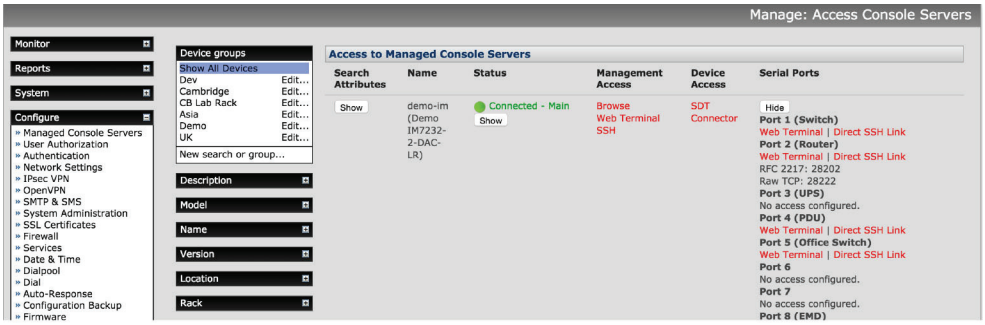
NOTE: If the current VCMS user has "user" or "admin" group access on a console server, they are deemed to have access to that console server.



- The Managed Console Servers displayed can be filtered by attribute (Description, Location, Model, Names, etc.).
- Click Show in the Search Attributes column of any particular Managed Console Server to view and edit the attributes.



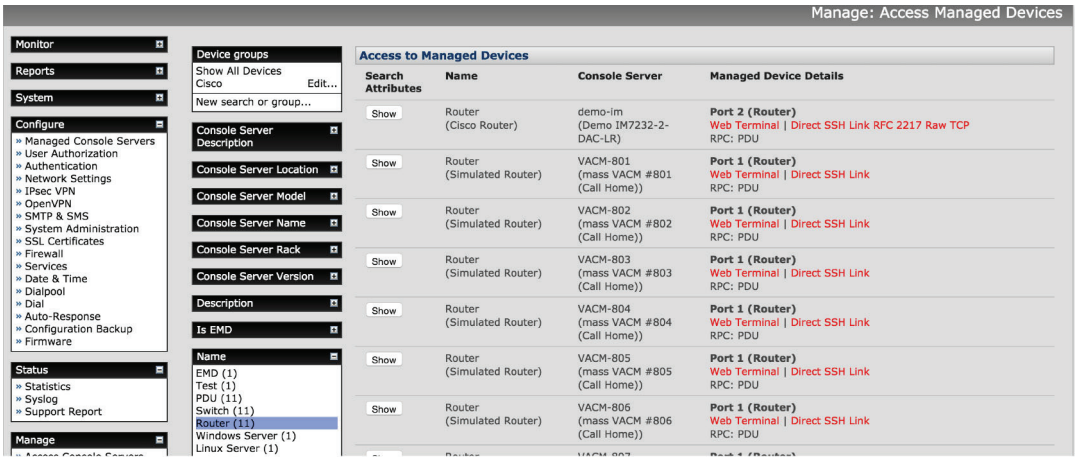
- Click Show in the Serial Ports column of any particular Managed Console Server to view all devices attached to the serial ports of that Managed Console Server.



4.1.2 Viewing Managed Devices

Managed Devices can also be viewed on the Manage: Access Managed Devices screen—which also provides a filtering-by-attribute tool.

- Click Manage: Access Managed Devices and the Managed Devices displayed can be filtered by attribute (e.g., Console Server Description/Location/Model/Names, etc., or if is it a UPS or EMD device, etc.). For example in the following screen, only devices attached to Managed Console Servers running V3.6.0b firmware are displayed.



4.2 Accessing Managed Console Servers and Devices

4.2.1 Accessing Managed Console Servers

The Management Access column on the Manage: Access Console Server screen presents a selection of access paths to the Managed Console Servers:

- Click Browse to connect to the Managed Console Server's web UI. This connection is proxied via VCMS, 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 displays in the Web UI header:

"This Console Server is being accessed via VCMS. Click here to return to VCMS."

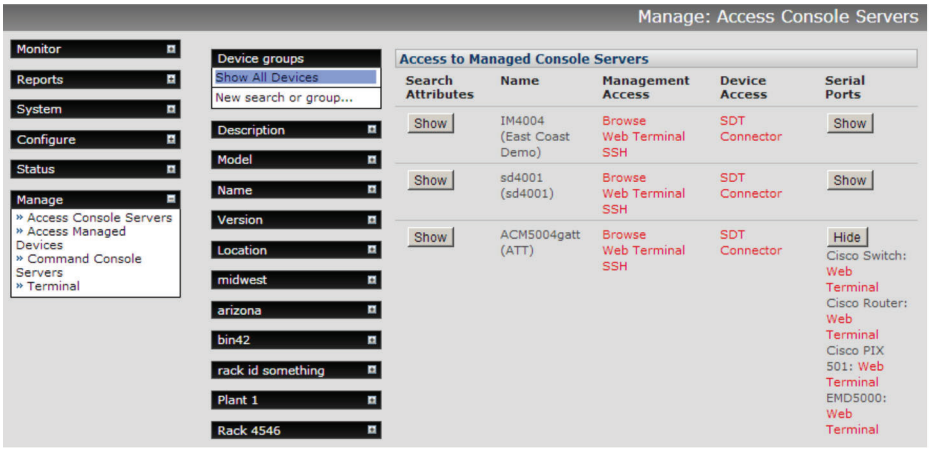
- Click Web Terminal to connect to the Managed Console Server's command line. The Web Terminal service uses AJAX to enable the web browser to connect through the VCMS to the Managed Console Server using HTTPS as a terminal.
- Click SSH to establish an SSH link to the Managed Console Server. You will need to set up URL handlers for the ssh:// links. The procedure here depends on the SSH client software and on the operating system you're using (Windows, Ubuntu, etc.).

4.2.2 Accessing Managed Devices

The Device Access column on the Manage: Access Console Server screen presents a selection of access paths to the Managed Devices. These paths are also accessible from Manage: Access Managed Devices screen.

Similarly, the Serial Ports column of any particular Managed Console Server on the Manage: Access Console Server screen presents a selection of access paths to serially attached devices.

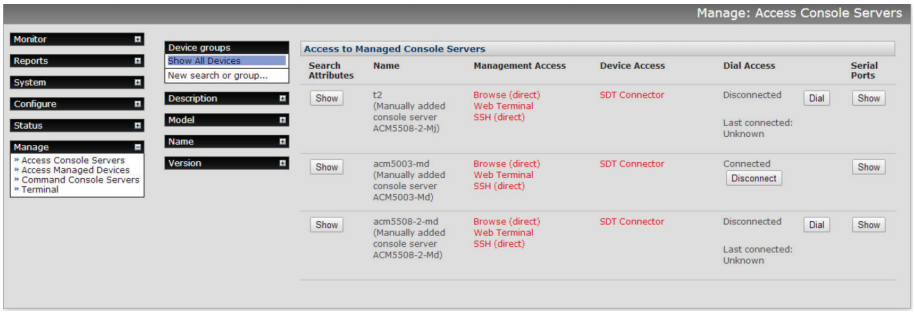
- Click Show to view all devices attached to the serial ports of that Managed Console Server.



- Where configured, you can then click Web Terminal to connect to the device on the remote Managed Console Server's serial port—as a terminal.

4.2.3 Dialing Managed Console Servers

With firmware V4.3 and later, the Access Managed Console Server page includes an extra column for dial access. For details, refer to the dialpool section in Chapter 3.



4.3 Batch or Bulk Control of Managed Console Servers

VCMS can schedule commands to run on one or more Managed Console Servers. Network engineers can automate remote firmware upgrades, and system administrators can lock out nominated user access to specified sets of sites.

There are two systems to send commands to managed console servers en masse. The node-* CLI commands execute commands directly via SSH and offers maximum flexibility and functionality for advanced users. The Command Console Servers UI offers simplified ease of use but limited functionality, scheduling and executing commands via the Nagios subsystem.

4.3.1 node-command Bulk CLI Command

The node-command CLI tool is used to run commands on managed console servers, allowing administrators to easily run a single CLI command in bulk, on all or on a range of their console server deployment.

NOTE: To run node- commands, you must be authorized as an admin group user.

Getting Started

To get started with any of the node- tools, you can get quick information on how to use it from the command line:

```
node-command --help
```

To see a list of all the registered console servers that the tool can operate on:

```
node-command --list-nodes
```

Selecting Console Servers

There are a number of ways to select console servers (aka "nodes") as targets on which to run a command, listed below. These can be used multiple times, or together, to select a range of console servers.

Select individually by name, address, Call Home address or numeric config index (as per --list-nodes output):

```
node-command --node-name BNE-R01-IM4248
node-command --node-address 192.168.0.33:22
node-command --node-address localhost:40121
node-command --node-index 17
```

Select all:

```
node-command --all
```

Select multiple using regular expression pattern matches or inverse pattern match, against console server attributes defined under Manage: Access Console Servers UI:

```
node-command --select-match 'Model=LES.*'
node-command --deselect-match 'Version=3.11.1'
```

Running Commands

Once console servers have been selected, the commands to be run for each can be given. These are run on each managed console server, in parallel. This command can be any command you can run from the console server CLI, commands are run as root.

For example to check the version on the first three configured console servers:

```
node-command --node-index 1 --node-index 2 --node-index 3 cat /etc/version
```

NOTE: When using non-trivial selection arguments, you can check which target console servers have been selected for an initial pass specifying --list-nodes rather than the final command.

Copying Files

node-copy is a variation of node-command that can be used to copy a file to selected managed console servers, by specifying a source and destination, e.g. to copy a Cisco IOS system image that has been pre-copied onto the Lighthouse CMS's /var/nvlog directory, to all managed IM family console servers' TFTP server:

```
node-copy --select-match 'Model=LES.*' --source-file /var/nvlog/ios.img \
/var/tmp/usbdisk/tftpboot/
```

Output Format: CLI

The command outputs the result of each command run on each remote console server. For example, the example node- command from the Running Commands section gives the following result:

```
node-command --node-index 1 --node-index 2 --node-index 3 cat /etc/version
== node-command ID 2014-03-12T05:10:29.360164_29534 ==
15:10:29 [SUCCESS] BNE-R01-IM4248 10.10.0.1:22
BlackBox/LESxxxx Version 3.11.0 --    Tue Jun 24 03:23:59 EST 2014

15:10:29 [SUCCESS] BNE-R01-IM4248 10.10.0.2:22
Black Box/LExxxx Version 3.11.0 --    Tue Jun 24 03:23:59 EST 2014

15:10:29 [SUCCESS] BNE-R01-IM4248 10.10.0.3:22
Black Box/LExxxx Version 3.11.0 -- Tue Jun 24 03:23:59 EST 2014
```

There are a number of components to this output:

1. The first line displays the run ID. This is the unique ID for this command including a timestamp of when the command was run, used to locate historical logs (discussed below).
2. Each node command result has a result header line. This contains the time the command completed, if the command succeeded or failed, the node name, and the node address.
3. The output (stdout) of the command being run is listed for each node on which the command was run. If there is no output, only the header line is listed.

There are a few ways to modify the output of the command, useful for batch operation or noisy commands. To hide the command output results, use the --quiet argument and only the headers will be shown. To suppress headers and display command output only, use the --batch argument. Combine both arguments to hide all output.

Output Format: Logs

Information about each run is logged to the filesystem, by default. Filesystem logging can be disabled by using the `--disable-fslog` argument. The logs are stored in /var/nvlog/node-command/, and are indexed using the run ID of each command (as detailed in the Output Format: CLI section).

A new directory is created for each run, and contains 3 things:

1. A targets.txt file, listing the addresses on which the command was run.
2. a stdout directory, containing the output to stdout for the command printed by each console server.
3. a stderr directory, containing the output to stderr for the command printed by each console server.

By default, a history of the last 30 commands are kept logged to the file system before being removed.

Syslog Information

In addition to the output and file logging, the running of commands is also recorded in syslog (Status: Syslog in the UI or /var/log/messages from the CLI).

```
<11>Mar 12 15:10:29 node-command[29534]: User 'root' ran command 'cat /etc/version' on node
'10.10.0.1:22'

<11>Mar 12 15:10:29 node-command[29534]: User 'root' ran command 'cat /etc/version' on node
'10.10.0.2:22'

<11>Mar 12 15:10:29 node-command[29534]: User 'root' ran command 'cat /etc/version' on node
'10.10.0.3:22'
```

4.3.2 node-upgrade Bulk Firmware Upgrade

The node-upgrade tool is used to upgrade the firmware of managed console servers, allowing administrators to easily perform firmware upgrades on all or on a range of their console server deployment.

Similar to the other node- commands, node-upgrade uses the SSH tunnel to transfer the firmware image from VCMS and initiate the upgrade. So unlike the Command Console Servers upgrade command, access to an external HTTP server is not required, making it ideal for firewalled environments.

NOTE: The node-upgrade command requires the remote console server to have USB local storage available on the selected console server to store the firmware image prior to upgrade.

Getting Started

The node-upgrade tool is based on the node-command tool, and many basic arguments such as displaying help and selecting console servers are the same. Please refer to the node-command Getting Started and Selecting Console Servers sections before continuing.

Staging Firmware on VCMS

First, node-upgrade needs the firmware file to be available on the Lighthouse CMS's filesystem.

For temporary storage of the files, they can be placed at /tmp, otherwise, the non-volatile storage at /var/nvlog is a good place to store firmware images.

The appropriate firmware image can be copied on to the Lighthouse CMS's filesystem with using a program like WinScp from Windows PCs or scp CLI from OS X, Linux and other Unix-like systems, e.g.:

Scp lesxxxx-3.11.1.flash root@vcms:/var/nvlog/

Upgrading Firmware

Run node-upgrade with the --firmware-file parameter, specifying the full path to the firmware file staged in the previous step, and the appropriate arguments selecting the console servers to upgrade.

e.g. to upgrade all LESxxxxs to 3.11.1 that have not been upgraded already:

```
node-upgrade ---select-match 'Model=LESxxxx.*' --deselect-match 'Version=3.11.1' \
--firmware-file  /var/nvlog/lesxxxx-3.11.1.flash
```

4.3.3 node-user Suite Bulk User Management

The node-user suite of tools are used to modify the user database on managed console servers, allowing administrators to easily add, remove and modify local users in bulk, on all or on a range of their console server deployment.

The individual command names are:

node-user-add node-user-del node-user-mod

Getting Started

The node-user tools are based on the node-command tool, and many basic arguments such as displaying help and selecting console servers are the same. Please refer to the node-command Getting Started and Selecting Console Servers sections before continuing.

Adding a User

Run node-user-add --help to display the arguments and syntax for adding a user:

usage: node-user-add [options] username

username Username to add

-G --group-list list List of groups to give membership to for this user

-C --port-list list List of ports numbers to give access for this user

-T --description desc User viewable description for this user

-X --no-prompt password Set the users password

-P --password Prompt for a password

e.g. to a user on all console servers with a username of myadmin, a description of My Administrator and membership of the admin group:

node-user-add --all --group-list admin --description “My Administrator” myadmin

Deleting a User

Run node-user-del --help to display the arguments and syntax for deleting a user:

usage: node-user-del [options] username [username...]

username [username ...] List of users to delete

e.g. to delete the user myadmin and myuser from all console servers:

```
node-user-del --all myadmin myuser
```

Modifying a User

Run node-user-mod --help to display the arguments and syntax for modifying a user:

usage: node-user-mod [options] username username Username to modify

-G --group-list list List of groups to add membership to for this user

-C --port-list list List of ports numbers to grant access for this user

-T --description desc User viewable description for this user

-L --lock-user Lock this user from accessing the device

-U --unlock-user Unlock this user from accessing the device

-X --no-prompt password Set the user's password

-P --password Prompt for a password

Lock and unlock temporarily disables and re-enables a user's ability to login to console server (establish sessions are not affected).

Port list is a list of serial ports a user account is explicitly permitted to access. Each port number can be preceded by a + or a - character. If a port number is preceded by a + the port is added to the user's explicit permissions list. If a port number is preceded by -, the port is removed from the user's explicit permissions list. Note that removed a port may not revoke access to a port, if the user has inherited permissions to access it by some other means (e.g. group permissions or admin group membership).

Similarly, the + and - syntax can be used when specifying the group list to add and remove group membership. If neither + nor - precedes a port or group, + is assumed.

e.g. to add myuser to the users group and grant permission to access serial port 1 on all console servers:

```
node-user-mod --all --port-list 1 --group-list users myuser
```

Passwords

For operations that require a password, such as node-user-add or node-user-mod with a -P or -X option, there are two ways that that password can be obtained. By default, when a password is required, it interactively prompts the administrator running the command for the password.

Alternatively, specify the password on the command line with the -X option, but be aware this means that the user's password will appear in plaintext in any ps process listings. The password is then encrypted before being sent across to the remote console server so that it does not appear in any logs in plaintext.

Synchronizing Console Servers

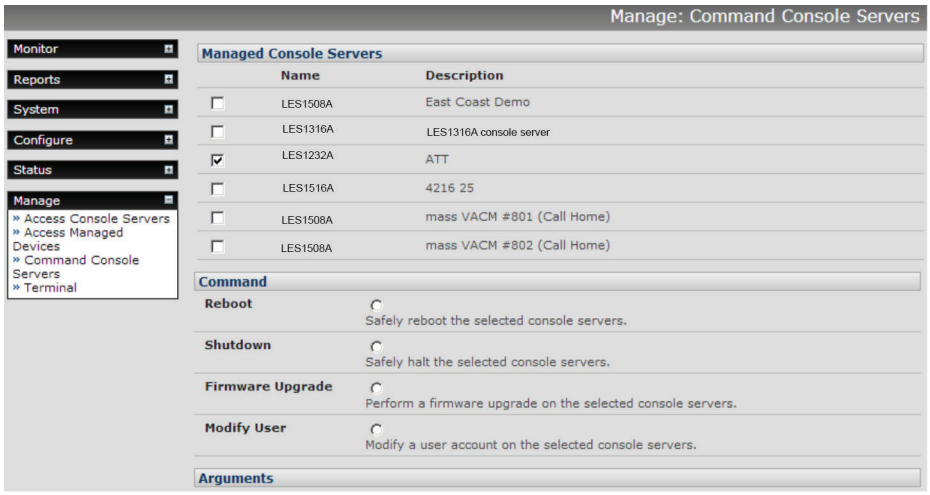
As users are added and deleted on the remote console servers, the user database on the Lighthouse CMS needs to be keep in synchronicity with the remote user databases. At the end of each node-user-add, node-user-mod and node- user-del, the administrator is prompted to resynchronize the affected remote console servers.

The synchronization is equivalent to the administrator had navigating to the Configure: Managed Console Servers UI and performing a Retrieve Managed Devices step. Alternatively, the behavior can be forced with either a -R (to always retrieve) or a -N (to not retrieve) option.

4.3.4 Command Console Servers UI

- 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.

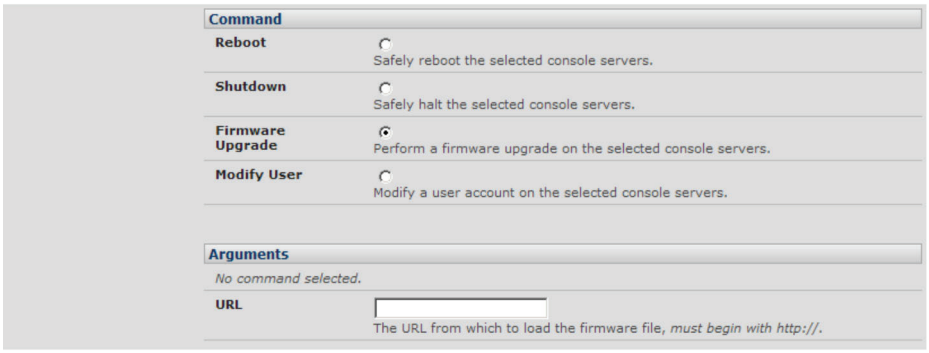


- Check to select the Managed Console Server(s) to command.
- Select the Command to schedule:

- Reboot: Soft reboot the selected console servers

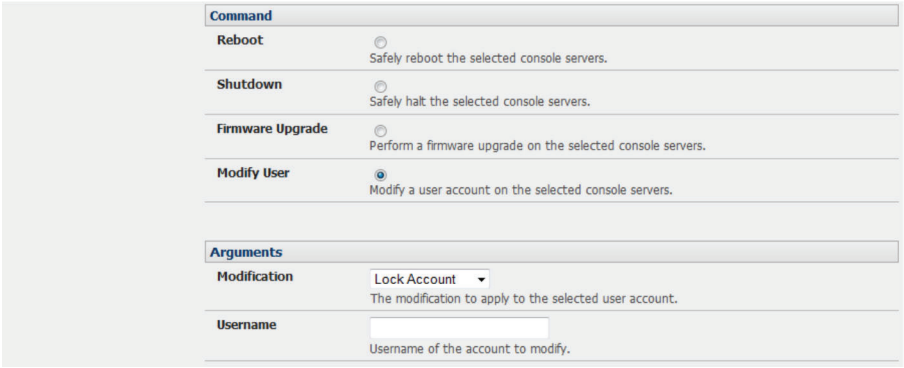
- Shutdown: Halt the selected console servers. After being shut down, manual intervention in the form of a physical power cycle is required before the console server becomes available again

- Firmware Upgrade: Perform a firmware upgrade. Call Black Box technical support at 877-877-2269 for details.

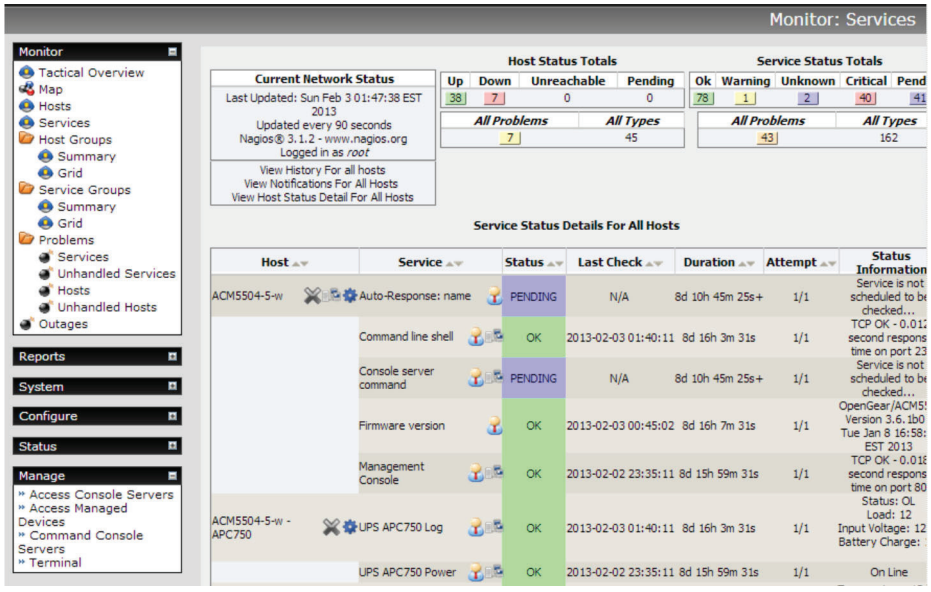


NOTE: Be sure to upload the correct firmware file (i.e. one that matches the particular device type of the Managed Console Server). This is especially important when uploading firmware on multiple devices. Failure to do so could result in the need to net boot the device to recover, which in turn requires physically visiting the device.

- 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.



- 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.



4.4 Manage Terminal

You can access the VCMS command line directly from a Web browser:

- Select Manage: Terminal.
- Click here in Terminal to activate the Web Terminal service. This uses AJAX to enable the Web browser to connect to the VCMS appliance using HTTP or HTTPS, as a terminal—without the need for additional client installation on the user's PC.

5. Monitoring with Nagios

5.1 Monitor

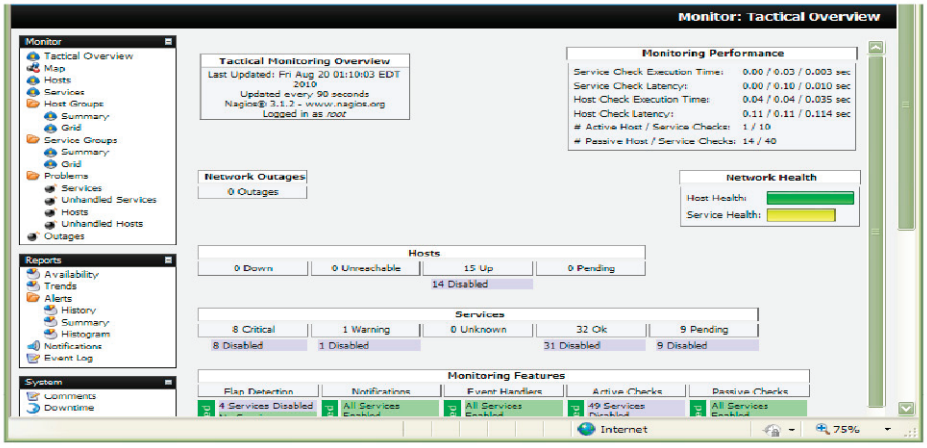
This section covers the Monitor menu options. The VCMS monitoring software in your VCMS appliance is built on a Nagios Core. All status screens under Monitor automatically refresh every 30 seconds, so there is no need to reload them (and this refresh time can be changed to even lower values in the VCMS Nagios configuration files).

5.1.1 Tactical Overview

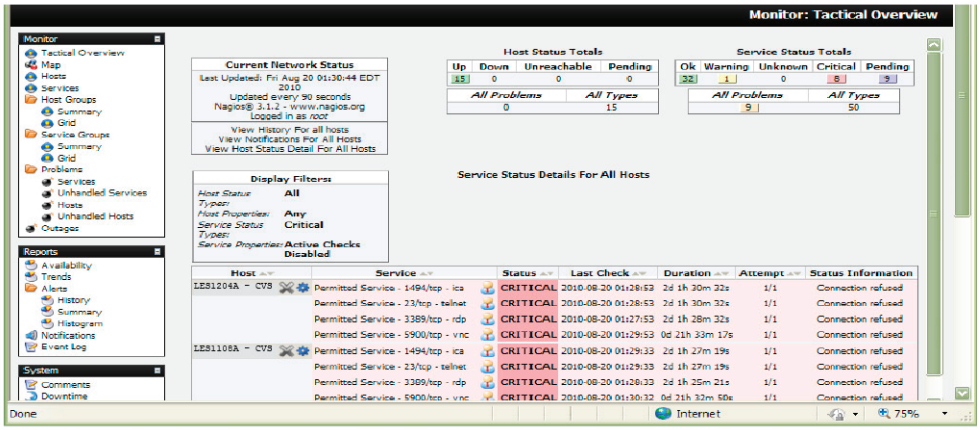
This screen gives you an overview of the current status of the monitored services and hosts.

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.

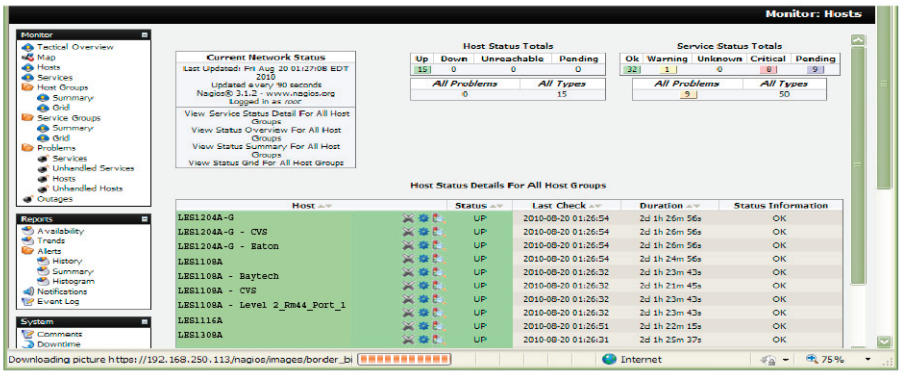


Most fields on this page are links to more specific views, e.g., if you wanted to see more details about your monitored services you can either click on the 8 Critical field within the Services table (as shown below) or select Problems: Services from the Monitor menu:



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.



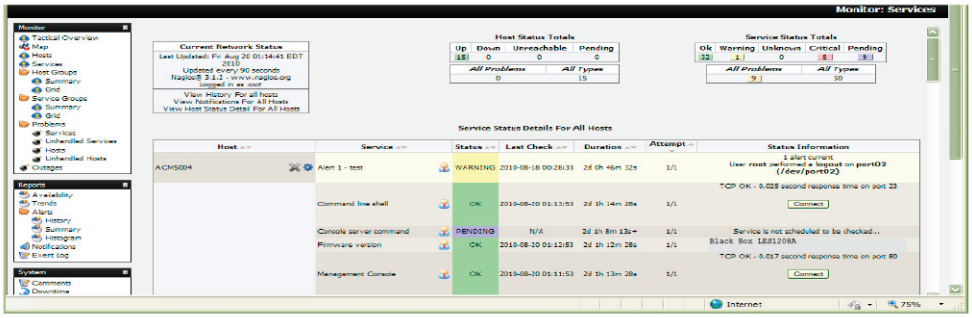
As we saw in the Tactical screen, here are the fifteen hosts we monitor right now. You can see basic information about each host on this page:

- Host shows all the hosts that 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 is 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 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.

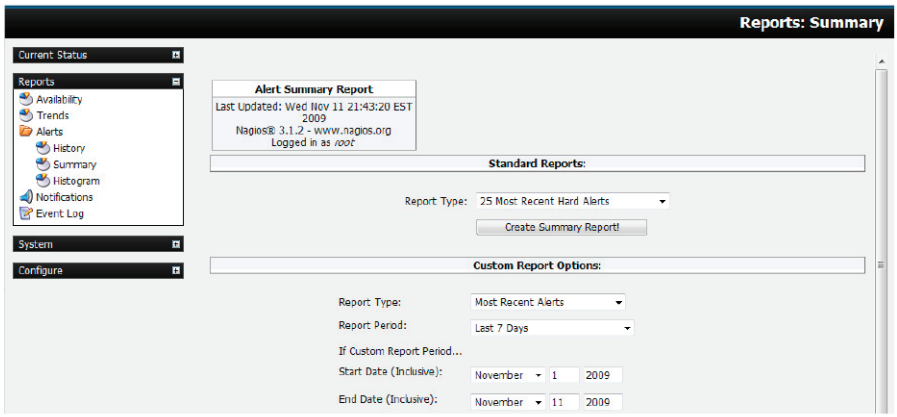
5.1.4 Problems

The problem screen shows 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 browser refreshes every 30 seconds so you get the current list of failed services. Also, VCMS 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, VCMS 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.

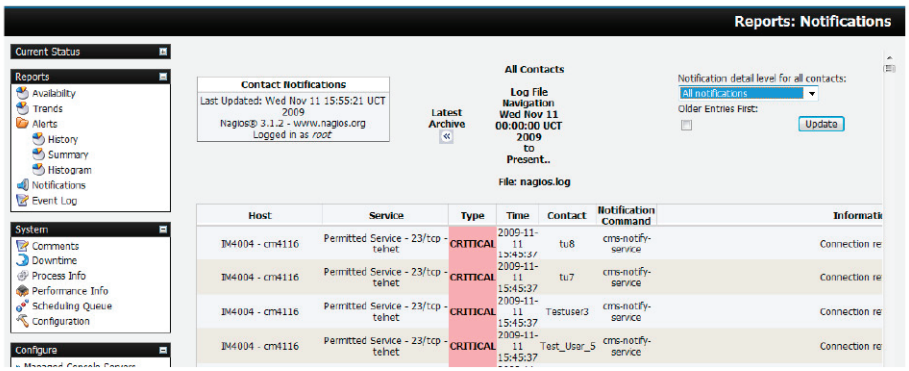
5.2 Reports and system

The VCMS provides all the standard Nagios customizable reports and logs:



5.2.1 Notifications

All Black Box console servers can be configured to send email and SMS alert notifications in case of an alert trigger event (pattern match on serial port, elevated temperature, door open etc). The Nagios features in VCMS 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 (since the last notification was sent out). VCMS 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 the VCMS 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 VCMS installation, you get a set of Nagios check programs that are automatically configured to let you start monitoring all the hosts and services on your Managed Console Servers and all their Managed Devices.

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 VCMS 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 VCMS, make an NSCA connection to the loopback interface using send_nsca on the Managed Console Server:

send_nsca -H 127.0.0.1 -c /etc/config/node-send_nsca.cfg

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

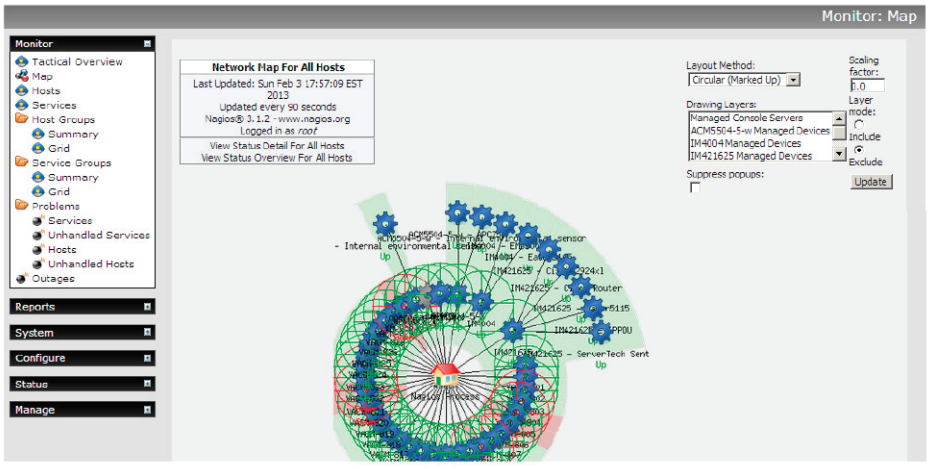
printf "My Managed Host\tService Description\t0\tOK\n" | send_nsca -H

127.0.0.1 -c /etc/config/node-send_nsca.cfg

The Nagios server on the VCMS must have a service configured to receive the check result. Place custom Nagios configuration files in /etc/config/nagios/user/ on the VCMS, 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.

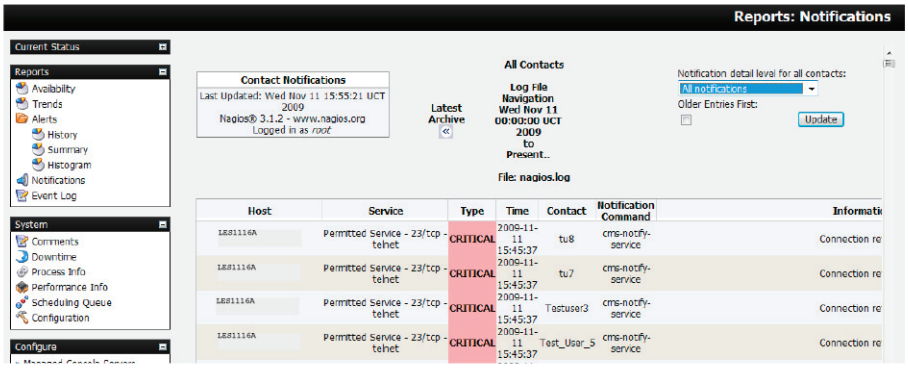
There are different icons for hosts and services. In the default template, host icons are rectangular and service icons are round. A finished NagVis map might present using a geographical map, or a photo of the server room as a background. In addition to hosts and services, host and service groups can 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 included as well. 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 Black Box console servers can be configured to send email and SMS alert notifications if an alert is triggered (e.g., a pattern match on serial port, elevated temperature, or door open). The Nagios features in VCMS allow more sophisticated notification.



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, when the host or service is in a period of scheduled downtime, no one is 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/VCMS-notify-service

/etc/config/scripts/VCMS-notify-host

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

5.3.4 Notification Elevation

The Nagios software in VCMS 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 exists
#
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 been 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, check the Nagios configuration and then restart Nagios:

 # /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.

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.

6. Accessing with an SSH Client

This chapter briefly describes configuring the console server with an SSH client to access a network attached host.

6.1 Configuring for SSH Tunneling to Hosts

To set up the console server for SSH tunneled access to 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 that can be used 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. 7301 to 7348 on a 48-port console server)*

79XX *VNC over serial from local LAN – where XX is the serial port number.*

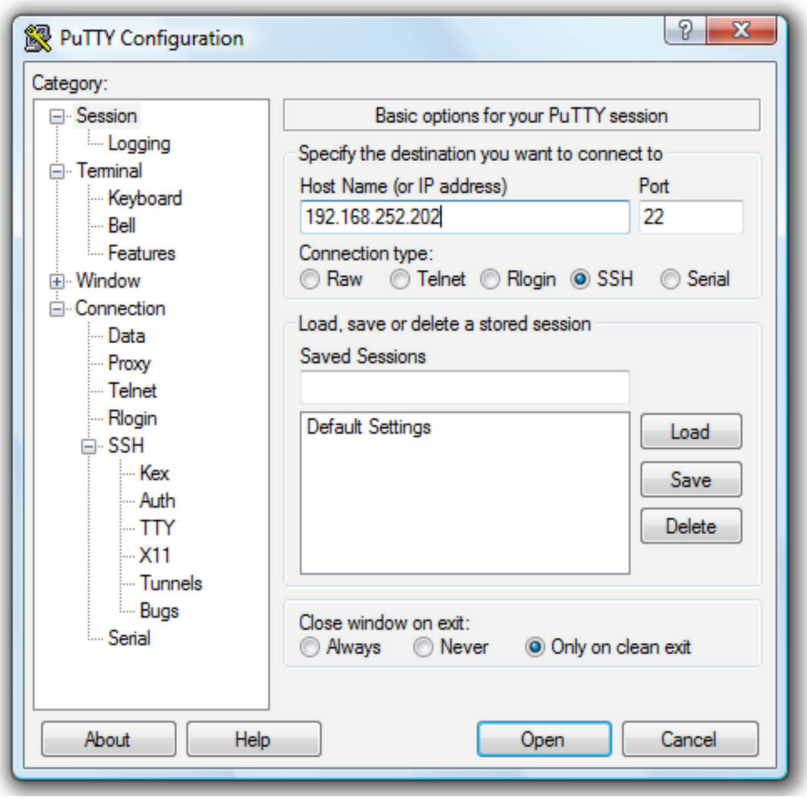
- Add the new Users using the Serial & Network: Users & Groups menu as detailed in Network Hosts (Chapter 4.4). Users can be authorized to access the console server ports and specified network-attached hosts. To simplify configuration, the Administrator can first set up Groups with group access permissions,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

6.2 SSH Tunneling using SSH clients (e.g. PuTTY)

A wide selection of commercial and free SSH client programs 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.

As an example, the following steps 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.

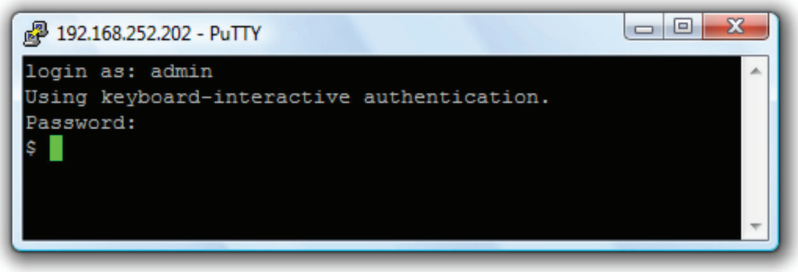
- If your destination device is network connected to the console server and you are connecting using RDP, set the Destination as <Managed Device IP address/DNS Name>:3389. For example, if when setting up the Managed Device as Network Host on the console server, you specified its IP address to be 192.168.253.1 (or its DNS Name was accounts.myco.intranet.com), then specify the Destination as 192.168.523.1:3389 (or accounts.myco.intranet.com:3389). Only devices that 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. Alternatively, 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.

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 previous steps; 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.

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 that are listening on one of the ports that 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 is 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.

Appendix A. Linux Commands and Source Code

The console server 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.

Black Box console servers are built on the 2.6 uCLinux kernel as developed by the uCLinux project (except for LES1101A, which has less flash and uses 2.4 uCLinux kernel). 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, smtpclient, stty, stunel, tcpdump, tftp, tip, traceroute).

Below are most of the standard uCLinux and Busybox commands (and some custom Black Box commands) that are in the default build tree. The Administrator can use these to configure the console server, 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	Black Box 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 file system disk space usage.
dhcpd	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	Black Box loopback diagnostic command
loopback1	Black Box loopback diagnostic command
loopback2	Black Box loopback diagnostic command
loopback8	Black Box loopback diagnostic command
loopback16	Black Box loopback diagnostic command
loopback48	Black Box 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	Black Box command similar to the standard chat command (via portmanager)
pmdeny	
pminetd	
pmloggerd	
pmshell	Black Box command similar to the standard tip or cu but all serial port access is directed via the portmanager.
pmusers	Black Box command to query portmanager for active user sessions
portmanager	Black Box 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 *	Soft 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
routef	IP Route tool to flush IPv4 routes
routel	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
traceroute6	Traceroute for IPv6
true *	Returns an exit code of TRUE (0)
umount *	Unmounts 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 * I	dentical to gunzip -c

Commands above that 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 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 console server build can be found at http://www.Black Box.com/faq233.html. It may be worth using ls command to view all the commands actually available in the /bin directory in your console server.

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

- config 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.
- portmanager provides a buffered interface to each serial port. It is supported by the pmchat and pmshell commands which ensure all serial port access is directed via the portmanager.
- pmpower is a configurable tool for manipulating remote power devices that are serially or network connected to the console server.

There are also a number of other CLI commands related to other open source tools embedded in the console server including:

- PowerMan provides power management for many preconfigured remote power controller (RPC) devices. For CLI details refer http://linux.die.net/man/1/powerman
- Network UPS Tools (NUT) provides reliable monitoring of UPS and PDU hardware and ensure safe shutdowns of the systems that are connected—with a goal to monitor every kind of UPS and PDU. For CLI details refer http://www.networkupstools.org
- 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 console server software are licensed under the GNU General Public License (version 2), which Black Box supports. You may obtain a copy of the GNU General Public License at http://www.fsf.org/copyleft/gpl.html. Black Box will provide source code for any of the components of the software licensed under the GNU General Public License upon request.

NOTE: The software included in each Black Box console server contains copyrighted software that is licensed under the GPL.

To download the complete source code, contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

The console server also embodies the okvm console management software. This is GPL code and the full source is available from http://okvm.sourceforge.net.

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

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

Also built in the console server is a Port Manager application and Configuration tools as described in Chapters 14 and 15. These both are proprietary to Black Box, but open to customers (as above).

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

alias [-p] [name[=value] ...]

bg [job_spec]

bind [-lpvsPVS] [-m keymap] [-f fi break [n]

builtin [shell-builtin [arg ...]]

case WORD in [PATTERN [| PATTERN]

cd [-PL] [dir]

command [-pVv]

command [arg ...]

compgen [-abcdefjkvu] [-o option]

complete [-abcdefjkvu] [-pr] [-o o]

continue [n]

declare [-afFrxi] [-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 job kill [-s sigspec | -n signum | -si let arg [arg ...] local name[=value] ...

logout

popd [+N | -N] [-n]

printf format [arguments]

pushd [dir | +N | -N] [-n]

pwd [-PL]

read [-ers] [-t timeout] [-p promp]

readonly [-anf] [name ...] or read return [n]

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 [-afFrxi] [-p] name[=value ulimit [-SHacdflmnpstuv] [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 ; }

Appendix B. Terminology

3G: Third-generation cellular technology. The standards that determine 3G call for greater bandwidth and higher speeds for cellular networks.

AES: The Advanced Encryption Standard (AES) is a new block cipher standard to replace DES, developed by NIST, the US National Institute of Standards and Technology. AES ciphers use a 128-bit block and 128-, 192-, or 256-bit keys. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks.

APN: Access Point Name (APN) is used by carriers to identify an IP packet data network that a mobile data user wants to communicate with and the type of wireless service.

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 en route.

BIOS: Basic Input/Output System is the built-in software in a computer that is executed on startup (boot) and that determines 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 keys 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 console server.

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.

VCMS: The term VCMS refers to the Virtual Central Management Software running in the console servers.

Console server: The term console server refers generically to the Black Box datacenter and remote management appliances, including the ACM5000, ACM5500, IM4200, CM41000 and SD4000 product lines.

DES: The Data Encryption Standard is a block cipher with 64-bit blocks and a 56-bit key.

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 set of common interfaces to a computer system which system administrators can use to monitor system health and manage the system. The IPMI standard 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 its MAC address. Ethernet is used locally to connect the console server 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 console server 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 console server has a MAC address listed on a label underneath the device.

Managed Console Server: Managed Console Server refers generically to any console server that is being centrally managed by VCMS.

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.

SIM: Subscriber Identity Module (SIM) card stores unique serial numbers and security authentication used to identify a subscriber on mobile telephony devices.

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. console server 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.

UDP: User Datagram Protocol.

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.

VPN: Virtual Private Network (VPN) a network that uses a public telecommunication infrastructure and Internet, to provide remote offices or individual users with secure access to their organization's network.

WAN: Wide Area Network

WINS: Windows Internet Naming Service (WINS) that manages the association of workstation names and locations with IP addresses.

Appendix C: Virtual Central Management System (VCMS) software EULA

Read before using the VCMS software.

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE VCMS 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 Black Box ("Black Box") proprietary software and/or proprietary software licensed to Black Box. This Black Box End User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Black Box for the installed software product of Black Box 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, Black Box 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, Black Box grants you a nonexclusive right and license to install and use the Software on a single physical or virtual CPU, and to install and use the Software on a second physical or virtual CPU to serve as an idle standby, 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;

(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;

(4) if you have not obtained and installed a Software License Key from Black Box (or its authorized reseller) you are permitted to use the Software solely for evaluation or demonstration purposes however your right to use the Software shall terminate thirty (30) days after your installation of the Software, at which time you must return or destroy the Software; and

(5) if you have installed a Software License Key you may not use the Software to concurrently manage more than the number of appliances specified in that Software License Key

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. Black Box 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. Black Box and its suppliers retain all ownership of, and intellectual property rights in (including copyright), the Software components and all copies thereof, provided however, that certain components of the Software are components licensed under the GNU General Public License Version 2, which Black Box supports. Black Box 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. Each unique VCMS Software license has an associated active term. Black Box reserves the right to terminate product support and product updates if the active license term has expired. However this term expiration does not affect the EULA validity. 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 Black Box 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 Black Box for any reason, please contact the Black Box 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, AND Black Box HAS RELIED UPON YOU TO CONDUCT SUFFICIENT TESTING TO DETERMINE THAT THE SOFTWARE IS SUITABLE FOR SUCH USE.

LIMITED WARRANTY

Black Box warrants the media containing the Software for a period of ninety (90) days from the date of original purchase from Black Box or its authorized retailer. Proof of date of purchase will be required. Any updates to the Software provided by Black Box (which may be provided by Black Box at its sole discretion) shall be governed by the terms of this EULA. In the event the product fails to perform as warranted, Black Box's sole obligation shall be, at Black Box'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. Black Box 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.

Black Box 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, Black Box. NO LIABILITY FOR CERTAIN DAMAGES. EXCEPT AS PROHIBITED BY LAW, Black Box 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 Black Box BE LIABLE FOR ANY AMOUNT IN EXCESS OF THE LICENSE FEE PAID TO Black Box UNDER THIS EULA. SOME STATES AND COUNTRIES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTI DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

Black Box Tech Support: FREE! Live. 24/7.

Great tech support is just 60 seconds away at 877-877-2269 or blackbox.com.

BLACK BOX®

About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 60 seconds or less.

LES-VCMS User Manual, version 2