

Enterprise Grade Central Management

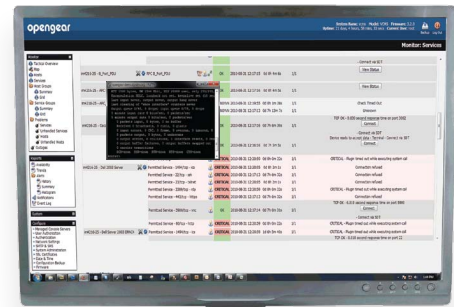
Opengear VCMS is a powerful system that centrally manages your network of distributed console servers and their managed devices. This enables you to actively monitor and resolve IT infrastructure problems before they affect critical business processes. Alerts are raised in the event of a disconnect or problem being identified at the remote site so the sysadmin / network manager can quickly respond. To remedy identified problems, the manager simply clicks on their browser on the VCMS web UI to be securely connected to the downstream console server or managed device for maintenance, reconfiguration or power cycling.

Simply install the VCMS appliance and point it to all the console servers. Secure SSH tunnels are automatically set up and the configuration for each console server's managed devices, users and alerts is downloaded. Or, use the Call Home feature and have remote sites restricted by firewall rules and VPN's call outbound to the VCMS using a secure SSH tunnel.

Like all Opengear solutions, the VCMS is open and extensible. The core Nagios software is familiar to many sys admins, so it can be custom configured and extended with the thousands of Nagios add-ons.

Reduce on-site service calls and truck rolls for remote site management. Monitor, diagnose and resolve infrastructure problems from anywhere at anytime.

Simply point and click from a browser to securely connect to any device on your network

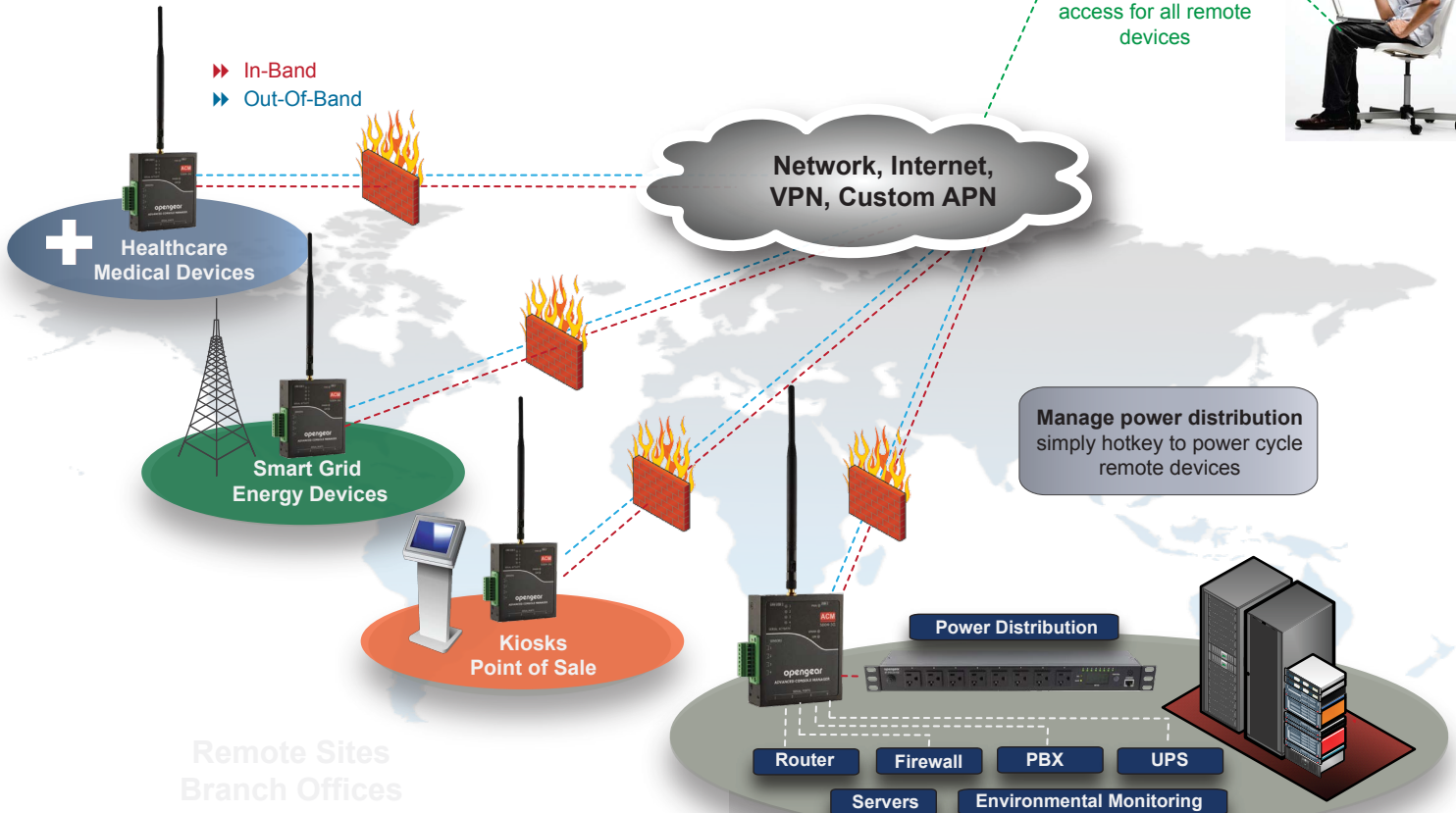


Single point of authentication and access for all remote devices



Opengear VCMS Centralized Monitoring Solution

- Single pane of glass view of your distributed infrastructure
- Manage up to thousands of Opengear Appliances
- Securely access and manage devices behind firewalls
- Point and click connection from anywhere anytime
- Plug and play deployment with automatic configuration



Who can most benefit from VCMS?

Managed service providers (MSPs)

Infrastructure management with complete monitoring, single point of authentication and access to equipment behind firewalls. Maintain customer firewall integrity and enhance service level.

Enterprise help desks

Technical and product support teams, account control for specialists divisions. Secure access to routers, switches, PBX, UPS & PDU, firewall, and servers all using industry leading corporate security policies.

Remote device maintenance and warranty providers

Access devices through customer firewalls in locations where inbound access is nearly impossible such as hospitals. Perform maintenance, access logs and support equipment without having a truck roll.

Operations support providers

Centralized access to environmental monitoring, digital I/O's, serial and network hosts. High temperature end points available for harsh environments such as pipeline, grid, transportation and public utilities.

Installation Requirements

Opengear's VCMS virtual central management appliance can be run as a guest under Linux Kernel-based Virtual Machine, VMware ESX, VMware ESXi, VMware Server.

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

Hardware Requirements

500MHz CPU core

256MB RAM

4GB disk space

. In addition, the following virtual devices are required:

* Disk device SATA (VMware) or IDE (Linux KVM)

* E1000 compatible Ethernet NIC, bridged

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

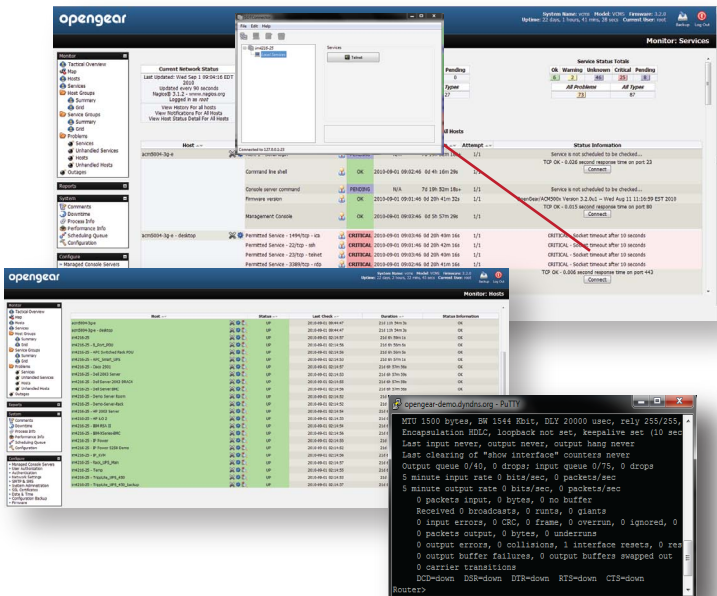
Compatible Console Servers

Opengear IM, IMG, CM, SD, ACM, KCS

Manage up to 255 Opengear Appliances

Central Access and to and control of over 10,000 distributed managed devices

One view of the entire enterprise



Part Number: **VCMS**
License Key (VMware and Linux KVM)

Click to Connect with SDT

The SDT Connector java client is built into Opengear's VCMS Central Monitoring System provides a 'Connect' button in the Status Information field of the monitored Host. When clicked, SDT Connector establishes a secure SSH tunnel to the downstream console servers. Once the tunnel is established the SDT Connector client will forward local services through the secure tunnel to the managed device. Securely forward telnet, RDP, VNC, X, HTTP, HTTPS and much more over one secure link

USA Head Office

630 West 9560 South
Suite A
Sandy, UT 84070
+1 888 346 6853 (Sales)
+1 801 606 2798 (Fax)
sales@opengear.com

Australian Office

Benson House Suite 44
2 Benson Street
Toowong QLD 4066
+61 7 3871 1800 (Sales & Admin)
+61 7 3720 8289 (Fax)
sales@opengear.com.au