CMS6100

Quick Start Guide

Thank you for purchasing the CMS6100 centralized monitoring system (*Monitor*). This Quick Start walks you through installation, configuration and local operation. For more details please refer to the *User Manual* on the CDROM.

Step1 Check kit contents

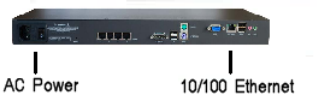
CMS6100 Monitor

This Quick Start & CD-ROM

Power cable

Step 2 Connect the CMS6100 hardware

- Plug the CMS6100 into the AC mains
- Connect the CMS6100 to your management network



Step 3 Set up the CMS6100 Monitor

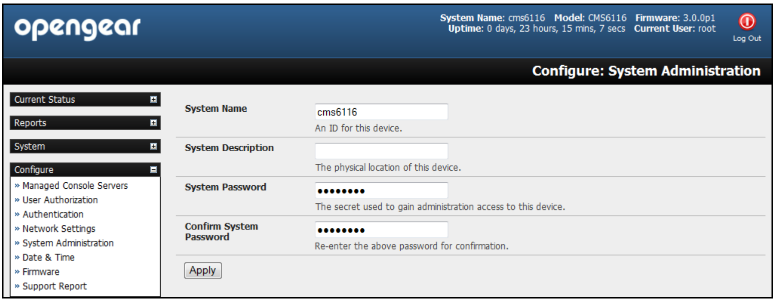
The default Monitor IP Address is *192.168.0.1* (subnet mask *255.255.255.0*). With a web browser on any computer that is LAN connected to the Monitor:

- Enter **https://192.168.0.1** into the address bar

Note: The LAN connected computer must have an IP address in the same network range (192.168.0.xxx) as the Monitor. If this is not convenient, you can use the *ARP Ping* command to set the IP address (refer *User Manual* or online FAQ for details). The Monitor also has its DHCP client enabled by default, so it will automatically accept any network IP address assigned by any DHCP server on your network – and will then respond at both 192.168.0.1 and its DHCP address.

- Log in using the default system user name *root* and the default password *default.* An Opengear **Welcome** screen listing the basic configuration steps is displayed

- Select **Configure: System Administration** and enter and confirm a new **System Password**
- You may also wish to enter a **System Name** and **System Description** to give the CMS6100 a unique ID and make it simple to identify. Click **Apply**



System Name: cms6116 **Model:** CMS6116 **Firmware:** 3.0.0p1
Uptime: 0 days, 23 hours, 15 mins, 7 secs **Current User:** root

Configure: System Administration

System Name cms6116
An ID for this device.

System Description
The physical location of this device.

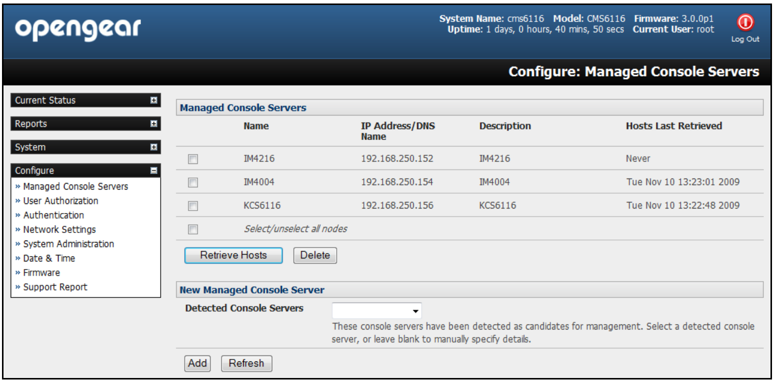
System Password ••••••••
The secret used to gain administration access to this device.

Confirm System Password ••••••••
Re-enter the above password for confirmation.

- To assign the CMS6100 Monitor a new static IP address or to permanently enable DHCP, select **Configure: Network Settings** then **Network Interface** and check **DHCP** or **Static** for **Configuration Method**

Step 4 Configure managed console servers

- Select **Configure: Managed Console Servers**. The *Managed Console Server* list shows all the console servers currently being monitored. The *Detected Managed Console Servers* drop down list also shows all the detected console servers not currently being monitored



System Name: cms6116 **Model:** CMS6116 **Firmware:** 3.0.0p1
Uptime: 1 days, 0 hours, 40 mins, 50 secs **Current User:** root

Configure: Managed Console Servers

Managed Console Servers

	Name	IP Address/DNS Name	Description	Hosts Last Retrieved
□	IM4216	192.168.250.152	IM4216	Never
□	IM4004	192.168.250.154	IM4004	Tue Nov 10 13:23:01 2009
□	KCS6116	192.168.250.156	KCS6116	Tue Nov 10 13:22:48 2009
□	*Select/unselect all nodes*			

New Managed Console Server

Detected Console Servers
These console servers have been detected as candidates for management. Select a detected console server, or leave blank to manually specify details.

- To add a console server to either select one from the drop down list or add the new console server's IP Addresses and click **Add**
- Enter **IP Address, Description** and **Name** for the *Managed Console Server* you are adding
- Enter the **Remote *Root* Password** (i.e. the System Password that has been set on this remote *Managed Console Server)*

Note: This password is used to propagate auto generated SSH keys and then forgotten. This password will not be stored. The CMS6100 *Monitor* communicates with the local and remote *Managed Console Servers* with secure SSH connections. This is done using public key authentication and the *Opengear Monitor* automatically generates SSH key pairs for these communications - rather than using passwords -ensuring secure authenticated communications

- Click **Apply** and the Monitor will set up a secure tunnel to the remote *Managed Console Server* and upload all its configuration settings (managed device details, user accounts, PDU and UPS settings, serial console and environmental alerts etc)

Step 5 Authorize added new users

Monitor retrieves all the user accounts from each *Managed Console Server* but does not automatically give any of them any access privileges to the Monitor itself (only the *root* user has access by default).

- Select **Configure: User Authorization**. This will display a list of all the user which have been set up on all the *Managed Console Servers* currently being monitored by the *Opengear Monitor*
- For any user then select **Edit** and enter a new password that will be used by that user when accessing the Monitor. You may also wish to modify the *Group* membership and *Description* associated with the authorized user. Users in the **user** group can access the all the monitoring screens/menus whereas users in the **admin** group have this access plus the ability to reconfigure using the *Configure* menu
- Click **Apply**

Step 6 Configure date and time

It is recommended that you set the local Date and Time as logging entries are time-stamped (and certificate generation needs to check the validity period)

- Select **Configure: Date & Time** and set manually or select synchronizing with a remote time server using the Network Time Protocol (NTP)

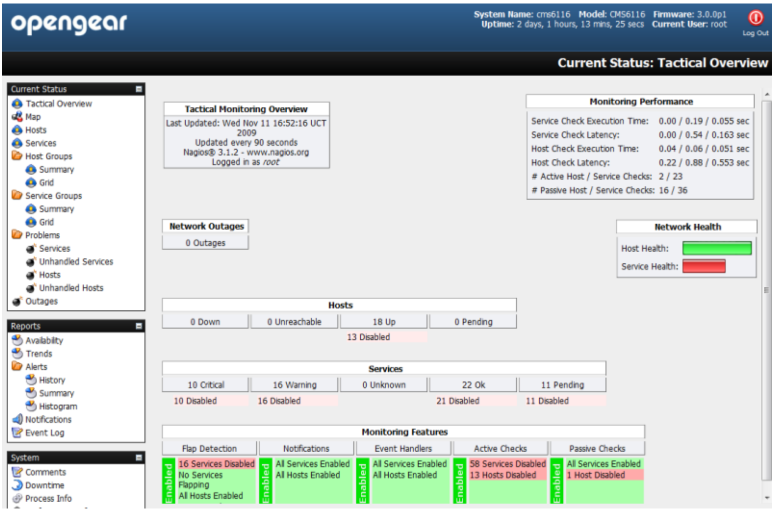
Step 7 Certificate update

The default SSL certificate that comes with Monitor device is for initial set up purpose and should not be relied on for secured global access (and when you initially https:// accessed the Monitor your browser may have responded with a message that verified the security certificates validity but noted that it is not necessarily verified by a certifying authority. So it is recommended you generate and install a new base64 X.509 certificate that is unique for you.

- Select **System: SSL Certificate**, fill out the fields and click on **Generate CSR** for the Certificate Signing Request (CSR)
- **Download** the CSR string and send it to a Certification Authority (CA) for certification. They will return you a new certificate which you can then **Upload** to Monitor

Step 8 Commence monitoring

Monitor runs Nagios (www.nagios.org) and the *Current Status*, *Reports* and *System* menu show the status and history of all the applications, computers and devices in your distributed networks - highlights problems and giving warnings



System Name: cms6116 **Model:** CMS6116 **Firmware:** 3.0.0p1
Uptime: 2 days, 1 hours, 13 mins, 25 secs **Current User:** root

Current Status: Tactical Overview

Tactical Monitoring Overview
Last Updated: Wed Nov 11 16:52:16 UCT 2009
Updated every 90 seconds
Nagios® 3.1.2 - www.nagios.org
Logged in as *root*

Monitoring Performance

Service Check Execution Time:	0.00 / 0.19 / 0.055 sec
Service Check Latency:	0.00 / 0.54 / 0.163 sec
Host Check Execution Time:	0.04 / 0.06 / 0.051 sec
Host Check Latency:	0.22 / 0.88 / 0.553 sec
# Active Host / Service Checks:	2 / 23
# Passive Host / Service Checks:	16 / 36

Network Outages
0 Outages

Network Health
Host Health: 🟩
Service Health: 🟥

Hosts

0 Down	0 Unreachable	18 Up	0 Pending
		13 Disabled	

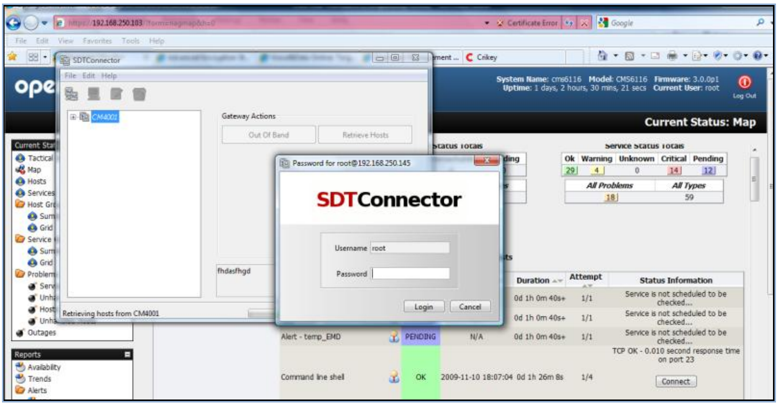
Services

10 Critical	16 Warning	0 Unknown	22 Ok	11 Pending
10 Disabled	16 Disabled		21 Disabled	11 Disabled

Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled 16 Services Disabled No Services Flapping All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled 58 Services Disabled 13 Hosts Disabled	Enabled All Services Enabled 1 Host Disabled

- ➢ To remedy identified problems simply click on the **Connect** or **Manage Power** or **View Status/Logs** button. Your browser will download a configured *SDT Connector* Java application from the CMS6100 Monitor which will run on your computer and securely connect you to the relevant screen on the *Managed Device* or *Managed Console Server*



Username root
Password

System Name: cms6116 **Model:** CMS6116 **Firmware:** 3.0.0p1
Uptime: 1 days, 2 hours, 30 mins, 21 secs **Current User:** root

Current Status: Map

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
29	4	0	14	12

All Problems	All Types
18	59

				Duration	Attempt	Status Information
				0d 1h 0m 40s+	1/1	Service is not scheduled to be checked...
				0d 1h 0m 40s+	1/1	Service is not scheduled to be checked...
Alert - temp_EMD		PENDING	N/A	0d 1h 0m 40s+	1/1	Service is not scheduled to be checked...
Command line shell		OK	2009-11-10 18:07:04	0d 1h 26m 8s	1/4	TCP OK - 0.010 second response time on port 23 Connect