

# KCS6104 & KCS6116

## Quick Start Guide

Thank you for purchasing the KCS6104/6116 console server. This Quick Start walks you through installation, configuration and local operation. For more details please refer to the *User Manual* on the CDROM.

### Step 1 Check kit contents



KCS6104/6116  
KVM console server



UTP cable(s) and DB9F-RJ45S  
straight and cross-over



This Quick Start  
& CD-ROM



Power cable

### Step 2 Connect the hardware

- Plug the console server into the AC mains
- Attach any serial or USB devices and connect the KCS6104/6116 to your management network
- Attach any local screen/ keyboard/ mouse (LCD drawer or KVM switch)



AC or DC Power | RJ Serial Console Ports | USB Ports | VGA | USB Ports  
Modem Port | Video Keyboard | 10/100 Ethernet

**Note:** If you plan to use out-of-band (OoB) dial-in access the LOCAL serial port can be connected to an external modem

### Step 3 Set up the console server

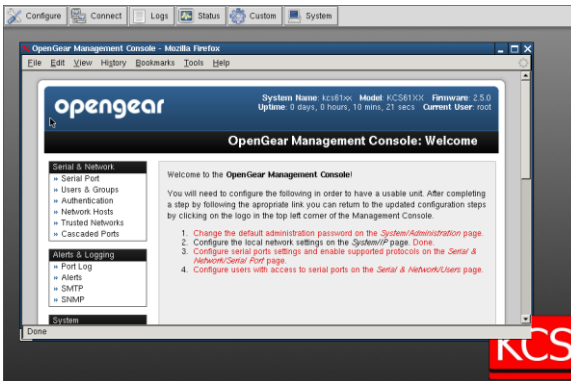
The default console server IP address is *192.168.0.1* (subnet mask *255.255.255.0*). With a web browser on any computer that is LAN connected to the console server:

- Enter **https://192.168.0.1** and log in using the default system user name *root* and the default password *default*. A **Welcome** screen listing the basic configuration steps is displayed

**Note:** The LAN connected computer must have an IP address in the same network range (192.168.0.xxx) as the console server. 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 console server 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.

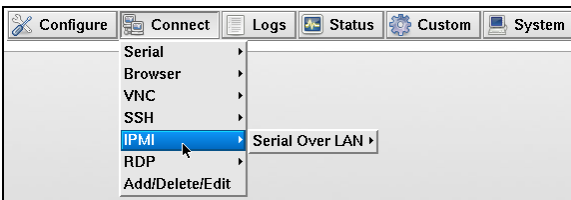
- Select **System: Administration**, enter and confirm a new **System Password** and click **Apply**
- To assign your KCS6104/6116 a static IP address or to permanently enable DHCP, select **System: IP** then **Network Interface** and check **DHCP** or **Static** for **Configuration Method**

**Note:** Alternately you can configure the KCS6104/6116 *console server* using the directly connected video console. Power-on and login from the local screen/ keyboard using *root default*. Then click **Configure** on the control panel to load *Firefox* and the Management Console and log in again using *root default*



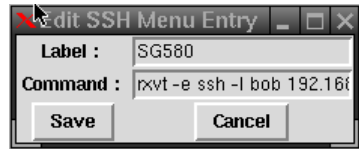
## Step 4 Configure local thin client access

Configure any of the KCS6104/6116 thin clients you will be using (e.g. Terminal, HTTP, HTTPS, VNC, RDP, IPMI) with details of the networked devices they will be accessing:



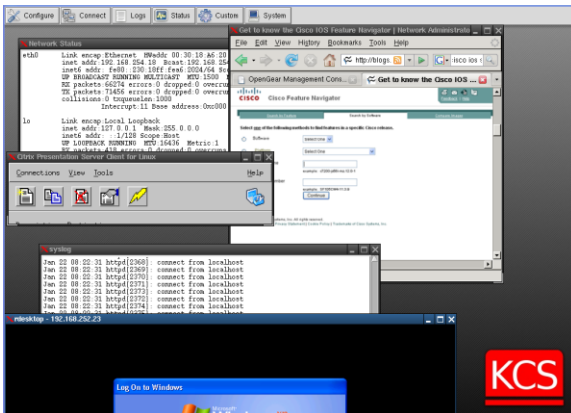
- Select **Connect: Add/Delete/Edit** on the control panel and for each selected client enter the **IP Address** or **DNS Name** of the Host to be accessed and possibly a **Username**)

- Once a Host has been added you can update the commands that will be executed in connecting the service to the existing Host



The four (KCS6104) or sixteen (KCS6116) serial ports are all pre-configured by default in Console Server Mode with RS232 settings of 9600 baud, no parity, 8 data bits and 1 stop bit. If you wish to change these settings:

- Click **Configure** to load the Management Console, the select **Serial& Network: Serial Port** and click **Edit** for the relevant *Port #*. Then configure the **Common Settings** (Baud Rate, Parity, Data Bits, Stop Bits and Flow Control) to match those of the device being controlled.
- At this stage you can also select the Console Server protocols (Telnet, SSH, TCP, Unauthenticated telnet or RFC2217) that are to be used for the remote data connection to this serial port. A **Logging Level** may also be set to specify the level of information to be logged and monitored for each that port. Click **Apply**



## Step 5 Remote control

The KCS6104/6116 has two advanced remote control options. One is to use VNC to remotely control the thin client software (RDP, SSH etc) that is running in the KCS6104/6116 itself, and have these clients control the devices. To do this:

- Select **System: Services** on the Management Console and enable the VNC server. At this point you may also want to enable other services that you may wish to use in remotely accessing and configuring the console server (and connected devices). The factory default enables HTTPS and SSH access to the console server and disables HTTP and Telnet. Click **Apply**
- Click **Manage: KCS: Connect** and your browser will automatically download and run a Java VNC applet client. Or you can run the VNC client of your choice (RealVNC, TightVNC, UltraVNC) on your remote management computer and configure it with the KCS6104/6116 IP address to connect to

A second option is run the management client software (RDP, SSH etc) remotely and then securely SSH tunnel these clients through the KCS6104/6116 to the serially or network attached devices. This is particularly useful when you have proprietary

applications (such as Dell Open Manage or VMware VDI client) on your remote computer that you want to use to manage a DRAC service processor or VMware virtual device on one of your servers:

- Select **Serial & Network: Network Hosts** and click **Add Host**
- Enter local **IP address/ DNS Name** of the Host and edit the **Permitted Services** (or TCP/UDP port numbers) to be used for accessing this Host e.g. HTTPS (port 443) or VNC (port 5990). Only these *permitted services* will be SSH forwarded through the KCS6104/6116 to the Host. All other services will be blocked. At this stage you may also specify the level of information to be logged and monitored for each Host access. Click **Apply**
- Install the **SDT Connector** java application on your remote management computer and set up the KCS6104/6116 as a gateway (entering the IP or DNS **Address**, the SSH port and **Username** and **Password**)
- Click **Retrieve Hosts** and SDT Connector will auto load any limitations you may have configured on the ports/host/services the remote user can access
- Then simply *point* at the host to be accessed and *click* on the service to be used in accessing that host - and an SDT connection will be setup from the remote PC through the KCS6104/6116 to a connected host

## Step 6 Advanced configurations



**Please register your product** to activate the warranty and to automatically receive advice of future firmware updates. Go to: <http://opengear.com/product-registration.html>

---

The KCS6104/6116 also offers many more advanced functions including:

- ❖ The **Alerts & Logging: Alerts** facility monitors serial ports, hosts, user logins, power etc. External EMDs can be connected to the serial ports and a broad selection of trigger can be specified. When triggered, a warning email, SMS, Nagios or SNMP alert is sent
- ❖ Management of third party UPSes and PDUs using open source *NUT* and *Powerman* tools. The **Manage: Power** facility enables both administrators and regular users to manage attached power strips, and servers with embedded IPMI.
- ❖ Historical logs of all communications with serial and network attached devices, system activity, UPS and PDU power status, environmental status, etc. The level of logging is set as ports and devices are configured, **Alerts & Logging: Port Log** allows this history to be saved locally or remotely
- ❖ Other advanced features, such as *Serial Port Cascading*, remote *Authentication*, *Trusted Networks*, *Secure Tunneling*, *Nagios Distributed Monitoring*, the *Command Line* interface – these are covered in detail in the *User Manual* on the CDROM.

---

**Note:** On the CDROM you will find the *PortShare* and *SDT Connector* software tools. *SDT Connector* provides you with secure, point and click access to the console server and all the attached devices *PortShare* connects the COM/tty port applications on your Windows PC, Linux server or virtual machine to the serial devices attached to the KCS6104/6116 **Refer to the provided Quick Starts**

---