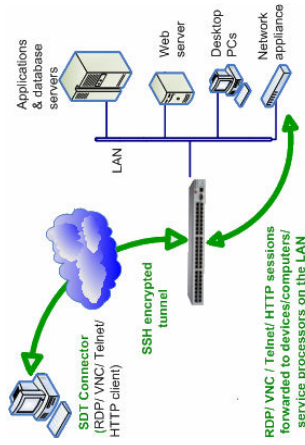


SDTConnector Quick Start Guide

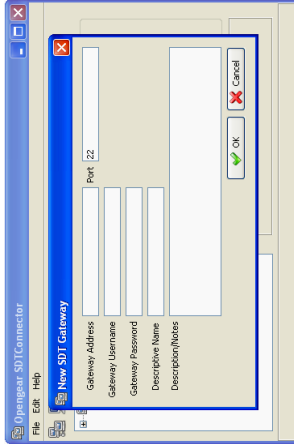


1

Install SDTConnector client software

The *SDTConnector* client software runs on your local or remote PCs to provide secure encrypted access to systems and devices attached to your IM/CM4000

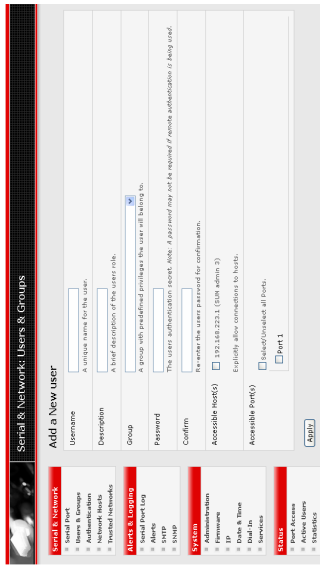
- Load and run the set-up program *SDTConnector Setup-1.n.exe* (or *sdctcon-1.n.tar.gz*) from the CD to install the SDT Connector client
- Run *SDTConnector* from the new icon and select **File: New Gateway**. Enter public IP address of the IM/CM4000 gateway to be accessed, or of the router/firewall that connects it to the Internet. Tools like <http://www.whatismyip.com/> or <http://checkip.dvndns.org/> may help here
- Enter the SSH port to be used (22 by default) and a Username Password fro accessing the gateway



2

Configure the IM/CM4000 gateway for SDT access

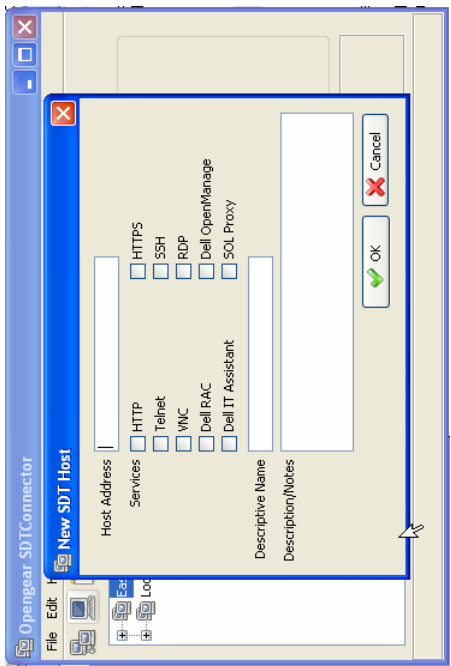
- On the gateway's **Serial & Network: Users and Groups** menu nominate which **Accessible Hosts and Ports** the User will have access to
- Select **Serial & Network: Network Hosts** and ensure the appropriate **Permitted Services** have been enabled (HTTP, VNC etc). Only nominated Host and serial consoles, and the permitted services will be forwarded. All other services (TCP/UDP ports) will be blocked



3

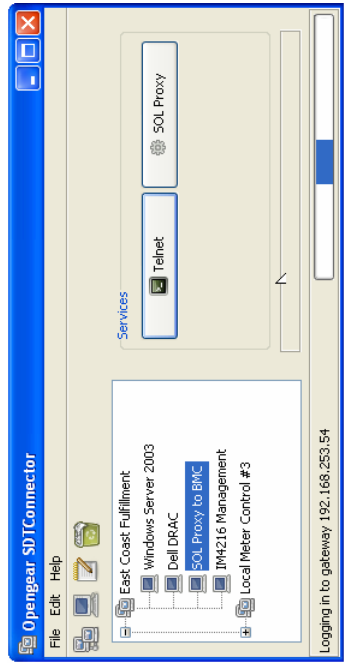
Access a connected Host using SDTConnector

- Select **File: New Host** on the *SDTConnector* client and enter the IP of the LAN connected host, and select which **Services** are to be used in accessing the new host. A range of service options are pre-configured in the *SDTConnector* client (RDP, VNC, HTTP, HTTPS, Dell RAC etc). However if you wish to add new services the range then proceed to the next section refer the *SDTConnector User Manual*. Click **OK**



- Now simply **point** at the host to be accessed **and click** on the service to be used in accessing that host. The SSH tunnel to the gateway is then automatically established, the appropriate ports redirected through to the host, and the appropriate local client (e.g. your Firefox browser for a HTTP service) is launched pointing at the local endpoint of the redirection

The *SDTConnector* client can be configured to access multiple *Gateways* and each *Gateway* can be configured to port forward to hundreds of locally networked *Hosts*. Similarly hundreds of *SDTConnector* clients can be configured to access the one *Gateway*, and there is no limit on the number of *Host* connections that an *SDTConnector* client can concurrently have open through the one *Gateway* tunnel. However there is a limit on the number of *SDTConnector* SSH tunnels that can be open at the one time on a particular *Gateway*. SD4002/4008 and CM4001/4008 devices support at least 10 simultaneous client tunnels; IM4216/4248 and CM4116/4148 each support at least 50 such concurrent connections



Browser access the gateway Management Console

SDTConnector can also be used for secure browser access the IM/CM4000 gateway's Management Console, or for Telnet/SSH access to the gateway command line.



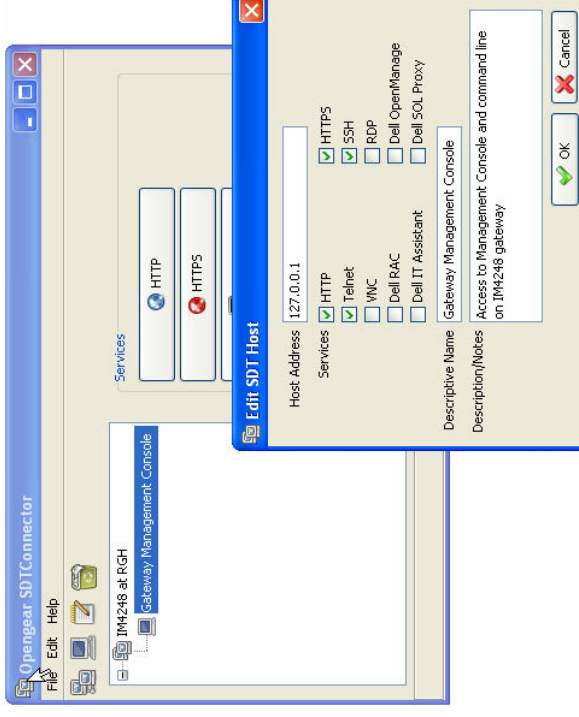
Remote or local
User/Administrator

For this connection, you must configure port forwarding on the gateway so the SSH tunnelled traffic is forwarded to itself.

- On the IM/CM4000 gateway Management Console select **Serial & Network: Network Hosts** and **Add Host**. In the **IP Address/DNS Name** field enter 127.0.0.1 and enter **Loopback** in **Description**
- Remove all entries under **Permitted Services** except for those that will be used in accessing the Management Console (80/http or 443/https) or the command line (22/ssh or 23/telnet) and click **Apply**
- Administrators by default have gateway access privileges, however for Users to access the gateway Management Console you will need to give those Users the required access privileges. Select **Users & Groups** from **Serial & Network**. Click **Add User**. Enter a **Username**, **Description** and **Password/Confirm**. Select 127.0.0.1 from **Accessible Host(s)** and click **Apply**

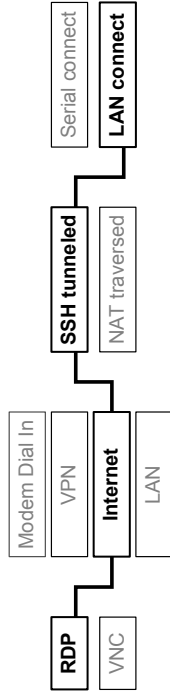
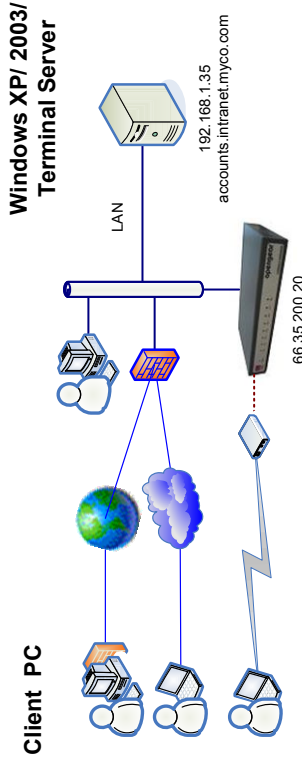
Next you must configure the SDTConnector client to access the gateway (itself) by setting the IM/CM4000 gateway up as a *Host*, and then configuring the appropriate services:

- Launch SDTConnector on your PC. Assuming you have already set up the IM/CM4000 as a Gateway in your SDTConnector client with *username/password*, select this Gateway and select **File -> New Host** to create a host
- Enter 127.0.0.1 as the **Host Address** and give some details in **Descriptive Name/Notes**. Select the appropriate **HTTP, HTTPS, SSH** or **Telnet** services you will use to access the gateway and click **OK**



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

Windows Remote Desktop Connection



For an Internet connected Client PC to remotely control (using Remote Desktop) a Windows XP/2003 computer (thru a secure SSH tunnel to a locally networked IM/CM4000 gateway):

- 1) Enable Remote Desktop on the Windows computer being accessed
 - Click **Control Panel** -> **System** -> **Remote**. Check **Allow users to connect remotely to this computer** and select the **Remote Users** you will enable to Remote Desktop access
- 2) Set up **RDP forwarding** on IM/CM4000 gateway
 - Select **Serial & Network: Network Hosts** and enter local **IP address/ DNS Name** of the Windows computer and select **3389/tcp (rdp)** as the permitted service
 - On the gateway's **Serial & Network: Users** menu nominate the Windows computer as an **Accessible Hosts** that the User can access
- 3) Ensure there is a known path to the IM/CM4000
 - Determine the **public IP address** of the IM/CM4000 (or of the router/firewall that connects the IM/CM4000 to the Internet) as assigned by the ISP. (You can easily find public IP addresses with tools from <http://checkip.dyndns.org/> or <http://www.whatismyip.com/>)
 - Set port forwarding for TCP port 22 through any firewall/NAT/router that is located between the remote Client PC and the IM/CM4000
- 4) Establish a secure SSH tunnel from the Client PC to the IM/CM4000
 - Install and launch an SSH client on the Client PC ([PuTTY](#), [SSHTerm](#), [SSH Lectia](#))
 - Set up an SSH connection eg. If running PuTTY on a Windows Client PC: Click **Session** tab, enter the public IP address of the IM/CM4000 in the **Host Name or IP address** field. Select the **SSH Protocol**, and the **Port** will be set as 22

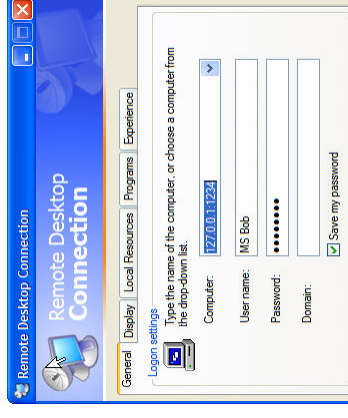


- Set up the SSH port forwarding e.g. If using PuTTY: Click **SSH** -> **Tunnels** tab and under **Add new forwarded port**, enter any number for **Source port** (eg 1234) Set **Destination** as the < SDT Host's IP address/DNS Name>:3389 Select **Local**. Click **Add** then click **Open** and (when prompted) enter Username/Password for the CM400 Permitted User



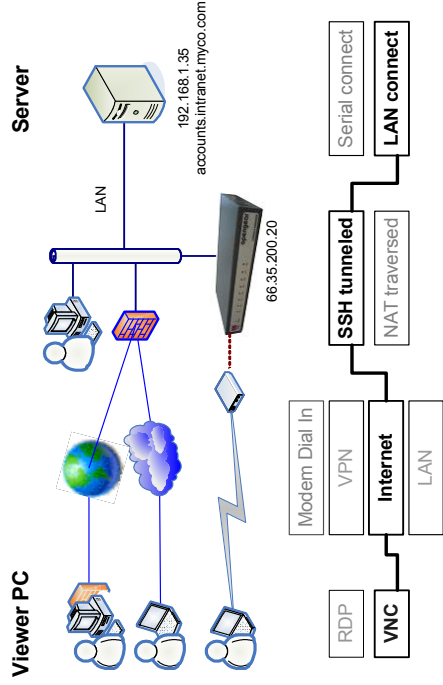
5) Configure the RPD client software on the client PC

- On a Windows Client PC: Click **Start** and select **Programs** -> **Accessories** -> **Communications** -> **Remote Desktop Connection**. Enter the **localhost** as the IP address (i.e. 127.0.0.1) and the SSH **Source port** you created when setting SSH tunneling e.g. :1234
- Click **Connect** and (when connected) enter the Username/ Password for the Remote Desktop Users Windows computer being accessed
- On a Linux or UNIX Client PC, launch the open source **rdesktop** client:
 - rdesktop -u windows-user-id -p windows-password -g 1024x768 localhost:1234**



As an alternate to steps 4) and 5) you could use the **SDTConnector Java** client. **SDTConnector** is preconfigured with a support for SSH tunneled RDP access. Refer **SDTConnector Quick Start**

VNC Connection

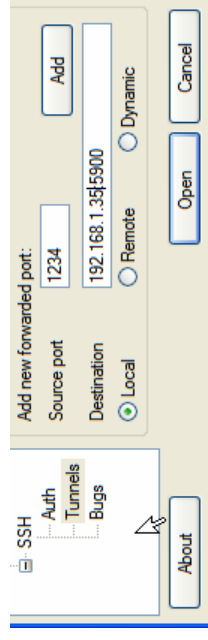


For an Internet connected Viewer PC to remotely VNC access a Linux or Windows Server computer (thru a secure SSH tunnel to a locally networked IM/CM4000):

- A.** Enable Remote Desktop on Windows computer being accessed
 - Most Linux distributions include VNC Servers e.g. To launch VNC for Red Hat Enterprise Linux: Select in the **Main Menu** -> **Preferences** -> **Remote Desktop**. Tick **Allow other users** and enter **Password**
 - For Windows, you will need to download, install third party VNC Server software e.g. UltraVNC <http://ultravnc.com> is easy to use
- B.** Set up *VNC forwarding* on the IM/CM4000 gateway
 - Select **Serial & Network**: **Network Hosts** and enter local **IP address/ DNS Name** of the Windows computer and select **5900/tcp (vnc)** as the permitted service
 - On the gateway's **Serial & Network**: **Users** menu nominate the Windows computer as an **Accessible Hosts** that the User can access
- C.** Ensure there is a known path to the IM/CM4000 :
 - Determine the *public IP address* of the IM/CM4000 (or of the router/firewall that connects the IM/CM4000 to the Internet) as assigned by the ISP. (You can easily find IP addresses with tools from <http://checkip.dyndns.org/> or <http://www.whatismyip.com/>)
 - Set port forwarding for TCP port 22 through any firewall/NAT/router that is located between the remote Viewer PC and the IM/CM4000
- D.** Establish a secure SSH tunnel from Viewer PC to the IM/CM4000:
 - Install and launch SSH client software on the Viewer ([PuTTY](#) , [SSHTerm](#) , [SSH Tectia](#))
 - Set up an SSH connection eg. If using PuTTY on a Windows Viewer PC: Click **Session** tab, enter the public IP address of the IM/CM4000 in the **Host Name or IP address** field. Select the **SSH Protocol**, and the **Port** will be set as 22



- Set up the SSH port forwarding eg. If using PuTTY: Click **SSH** -> **Tunnels** tab and under **Add new forwarded port**, enter any number for **Source port** (eg 1234). Set **Destination** as the < SDT Host's IP address/DNS Name>:3389 Select **Local**. Click **Add** then click **Open** and (when prompted) enter Username/Password for the CM400 Permitted User



E. Configure the VNC Viewer software on the Viewer PC

- On a Windows PC you need to download VNC Viewer software e.g. UltraVNC Enter the *localhost* as the host IP address (i.e. 127.0.0.1) and the SSH *Source port* you created when setting SSH tunnel (eg :1234) Click **Connect** and enter the **Password** for the VNC Server being accessed
- Most Linux and UNIX PC will have installed VNC Viewers and to connect simply configure the Server address as *localhost:1234* and enter **Password**.
- VNC Viewers are freely available for most other operating systems (Solaris, Macintosh) and platforms (PDAs) - and they are truly platform independent. So a VNC Viewer on any operating system can connect to a VNC Server on any other operating system.



As an alternate to steps D) and E) you could use the SDTConnector Java client. SDTConnector is preconfigured with a support for SSH tunneled VNC access. Refer SDTConnector Quick Start