APPLICATION NOTE

Using SDTConnector

with IBM xSeries/System x Servers

Rev: 1.0

May 25, 2007

1. *Introduction*

IBM's eServer, xSeries and BladeCenter families include a range of system management hardware components and software support functions including IBM Director software, IBM baseboard management controllers (BMC) and Remote Supervisor Adapters (RSA, RSA II and RSA SlimLine). Opengear's IM4200 gateways are preconfigured with support for these components and this Application Note explores how Opengear's SDTConnector client enables you to securely access and control the IBM embedded service processors and interface with the Director and higher level management applications.

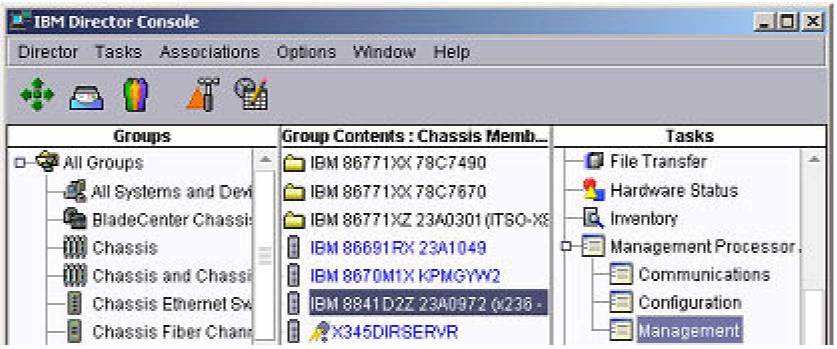
IBM's server families all offer management hardware for around-the-clock remote management. A BMC is a built-in system component in xSeries and BladeCenter servers and it provides basic monitoring and troubleshooting facilities, such as sending alerts and remote power control. However it is IBM's Remote Supervisor Adapter (in particular the popular RSA II) that represents the next generation of comprehensive server management.

The IBM RSA II is a PCI card service processor and it is standard in some servers and an option in others. It manages the BMC located on the server motherboard, and augments the BMC capability so you can perform systems management functions whether your server is operational or not. The RSA II provides an extensive range of remote server management features including Virtual KVM which provides full graphic console redirection. So you can use a local desktop to access and control a remote server, run applications and receive system alerts in whatever form you choose (and no longer is there a need for any external KVMoIP appliances at the remote site). Virtual KVM also maintains a log of the last screen before a system failure. The RSA has both command line and a Web interface and other features include virtual media access; UDP/TCP Ethernet connection; remote power control; local logs & alerts; and secure SSH, SSL & LDAP access.

Another RSA model is the SlimLine which is an internal card that includes the BMC and uses a dedicated Ethernet connector on the server for communication. The BladeCenter's management module also uses a modified version of the RSA with an integrated KVM switch to provide access to individual server blades.

More details can be found in the IBM Redbook (http://www.redbooks.ibm.com/redbooks/SG246495/wwhelp/wwhimpl/js/html/wwhelp.htm) which describes the integrated BMC, the RSA II family of adapters and the BladeCenter management module.

IBM's service processors can securely accessed with the IM4200 then managed using IBM Director, an integrated suite of system management tools that enables administrators to locally or remotely track the usage and performance of their server's processors, disks, and memory. IBM Director extends the basic RSA II software by providing a central platform for monitoring and managing all the IBM hardware resources.



2. *Connecting to BMC services*

All xSeries/System x servers contain a baseboard management controller (BMC). It is a service processor integrated into the motherboard, designed to provides access to the xSeries/System x server independently of the operating system. The BMC typically does not have its own Ethernet NIC, it shares one with the operating system. This NIC is configured with two IP addresses, one of the operating system, and one for communication with the BMC.

Console redirection and serial over LAN (SOL)

The BMC can be used to redirect input and output of the serial port through its shared NIC. When coupled with console redirection, it allows you to remotely access BIOS configuration and see the boot messages as your server boots or reboots.

If you also run a operating system console on the redirected serial port, after the system has booted you also have out-of-band access to the operating system for disaster recovery, monitoring, rebooting the system, etc. There are several steps for setting up SDTConnector and your operating system for SOL:

- Configure the xSeries/System x BMC and BIOS to enable console redirection
- Install the Systems Management Bridge program on the client PC that will be running SDTConnector
- Enable your operating system's serial console on the xSeries/System x server
- Configure the Opengear SSH gateway to permit SOL
- Configure SDTConnector to access the BMC using Systems Management Bridge
- Connect to the BMC using SOL

Configuring BMC console redirection on the xSeries/System x server

This process is detailed in the IBM technote entitled "Enabling Serial Over LAN for a Remote Windows Text Console using OSA SMBridge" and the Redbook entitled "IBM eServer xSeries and BladeCenter Server Management", available from the IBM web site. Below is a brief walk through. Refer to the IBM documents for a more thorough guide.

- ➢ Ensure you have a suitable Telnet client. For Windows users, download the HyperTerminal Private Edition (6.3) and install it of the client PC that will be running SDTConnector. The built is Windows telnet command and built in HyperTerminal client are not suitable. Otherwise, your operating system's built in Telnet client should be suitable.

- ➢ Enable BMC and console redirection in the BIOS by rebooting the xSeries/System x server and press F1 during POST to enter BIOS setup

    - Select Advanced Options -> Baseboard Management Control -> (BMC) Settings
    - Enter a unique, static IP address on your management network for the BMC. In this example we use 192.168.0.200. Enter the Subnet Mask of your management network, in this example we use 255.255.255.0.
    - Select Default Gateway and enter the IP address of your Opengear unit, in this example the Opengear unit resides at 192.168.0.1.
    - Return to the main menu and select Devices and I/O Ports.
    - Set Serial Port A and Serial Port B to Auto-configure.
    - Select Remote Console Redirection.
    - Set Remote Console Active to Active, Remote Console Text Emulation and Remote Console Keyboard Emulation to VT100/VT220, Remote Console Active After Boot to Enabled, and Remote Console Flow Control to Hardware. Ensure the Baud Rate is set to 19200, and Data Bits/Parity/Stop Bits are set to 8/None/1.
    - Hit Esc twice to return to the main menu, select Start Options.
    - If available, set the following options. Set Planar Ethernet 1 PXE to Disabled, Planar Ethernet 2 PXE to Enabled, Planar Ethernet PXE/DHCP to Planar Ethernet 2, and Run PXE only on Select Planar NIC to Enabled.

- Hit Esc to return to the main menu, select Advanced Options -> Baseboard Management Control (BMC) Settings.
- Set System-BMC Serial Port Sharing to Enabled, and BMC Serial Port Access Mode to Dedicated.
- Save your changes and reboot.

Installing the Systems Management Bridge on the PC running SDTConnector

Connecting to the BMC requires the use of the Systems Management Bridge (SMBridge) service. SMBridge runs on the client PC running SDTConnector, and allows you to use a Telnet client to communicate with the redirected serial port. SMBridge is used in loopback mode, as SDTConnector takes care of securely transporting the SOL traffic across the network or Internet.

For Windows:

- On the PC running SDTConnector, insert the Systems Management Bridge Installation CD that shipped with your xSeries/System x server. If you do not have this CD, SMBridge can be downloaded from: http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/license?filename=system_x/39r6689.zip&root=/systems/support/&brandind=5000004

- Follow the on screen prompts, accepting the default settings.

- Once installed, check the Systems Management Bridge is running by clicking Start -> Run and typing telnet 127.0.0.1 623. If the Systems Management Bridge prompt is displayed, it has installed correctly.

For Linux:

- On the PC running SDTConnector, insert the Systems Management Bridge Installation CD that shipped with your xSeries/System x server. If you do not have this CD, SMBridge can be downloaded from: http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/license?filename=system_x/39r6689.zip&root=/systems/support/&brandind=5000004

- Locate the osasmbridge-*.rpm package and install it. If you are using a distribution other than Redhat, use a tool such as alien to rpm2targz to convert the package. The important files are /etc/smbridge.cfg and /usr/bin/smbridge.

- Start SMBridge by running as root: /etc/init.d/smbridge start

- If this fails, you can run the following command as root: /usr/bin/smbridge -d -c /etc/smbridge.cfg

- Check SMBridge is running by opening and terminal and typing telnet 127.0.0.1 623. If the SMBridge prompt menu is displayed, it has installed correctly.

Enable your operating system's console on the xSeries/System x server

In order to access your operating system using SOL, you must tell it to run a console on the serial port when the OS starts.

For Windows 2003 Server:

(Emergency Administration Services (EMS) and the Special Administration Console (SAC) are discussed at length in articles available at Microsoft's MSDN site.)

- Use the bootcfg command to start Emergency Administration Services (EMS) on the serial port.

- From a command prompt (Start -> Run -> cmd.exe), type:

```
bootcfg /ems ON /port COM1 /baud 19200 /id 1
```

This enables EMS if you only have one Windows operating system installed, or for the first operating system in the Windows boot menu. Otherwise use /id 2 for the second operating system, /id 3 for the third, and so on.

This also assumes that you are using the first serial port (COM1) as per the step Enabling console redirection in the BIOS.

- Reboot your system to enable console redirection.

For Linux:

This process is detailed in the document entitled "IBM eServer xSeries and BladeCenter Server Management" published as part of the IBM Redbooks series, and available at the IBM web site.

Warning: It is not recommended you rely solely on this document to complete this step, the following is an example only to give you a rought idea of what is involved. Following these steps verbatim may render your system unable to boot.

Refer to the IBM documentation and your Linux distribution's documentation for a more thorough guide.

- Configure your bootloader to redirect to the serial port. Using GRUB, you would add the following lines to the top of your grub.conf or menu.lst file:

```
serial --unit=0 --speed=19200
terminal --timeout=10 console serial
```

- Find the entry for the kernel image you are using, and add the kernel options: console=tty0 console=ttyS0,19200, e.g.:

```
title Linux
root (hdx,x)
kernel /vmzlinux-x.y.z ro root=/dev/hdxx console=ttyS0 console=tty0
```

This also assumes that you are using the first serial port (/dev/ttyS0) as per the step Enabling console redirection in the BIOS.

- Modify the boot scripts to automatically spawn a login prompt on the serial port once Linux has booted. This varies from distribution to distribution. You may be able to add the following line to the top of /etc/inittab:

```
0:12345:/sbin/agetty ttyS0 19200
```

- Also ensure ttyS0 is listed in /etc/securetty to allow root to login through the serial console.
- Reboot your system to enable console redirection.

Configuring the Opengear SSH gateway to permit SOL

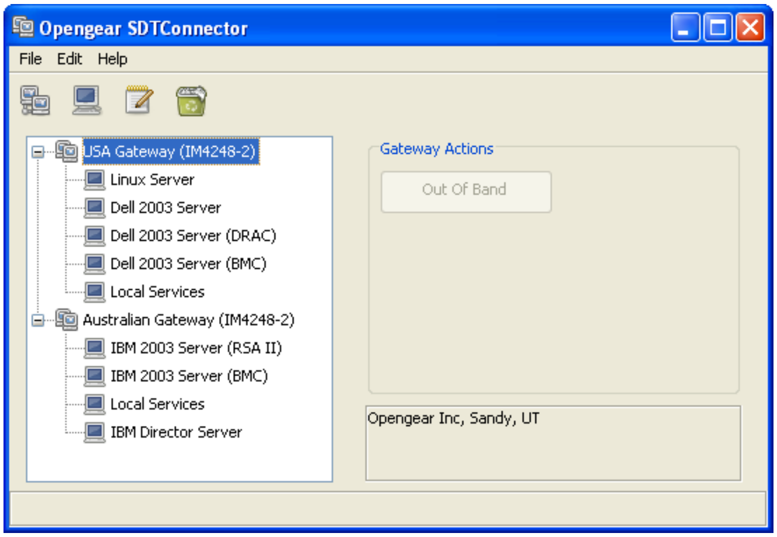
Ensure your Opengear unit is running firmware version 2.2.3 or later. The latest firmware is available from: ftp.opengear.com

- From the Serial & Network menu, select Network Hosts. Click Add Host. Enter the IP Address of the BMC, as per the step Configuring the BMC (in this example we used 192.168.0.200).
- Remove the Permitted Services you do not require, select the UDP radio button and enter Port 623. Click Add. Scroll to the bottom of the page and click Apply.
- From the Serial & Network menu, select Users & Groups. Click Add User. Enter a username for the new user, e.g. ibmadmin. Enter and confirm a gateway Password for this user. Note that this is separate from the BMC password.

- In Accessible Host(s), select the IP address for the BMC (192.168.0.200). Click Apply.

Configuring SDTConnector to connect the SOL session

- Install and launch SDTConnector (1.2.x or later) on the client PC.
- Select File -> New Gateway
- Enter the IP address through which the Opengear unit/management LAN gateway is accessible to this client PC (e.g. 192.168.0.1). Enter the gateway username (e.g. ibmadmin) and password you set in the previous step. Click OK.
- Right click on the newly created gateway and select New Host. Enter the BMC's IP address (192.168.0.200) in Host Address. Select the SOL service and click OK.



Connecting the SOL session

- Select the newly created host and click the SOL button. A Telnet window with the SMBridge prompt is displayed:

```
OSA System Management Bridge (SMBridge), Version 1.0.3.8
Copyright (c) 2004 - OSA Technologies, an Avocent Company. All Rights Reserved.

SMBridge>
```

- Type:

```
connect -ip 127.0.0.1 -u USERID -p PASSW0RD
```

Substitute the BMC username after -u, and password after -p.
The defaults are USERID and PASSW0RD.
The serial over LAN session is now connected.

Troubleshooting/FAQ

Why do I need to run SMBridge?

Systems Management Bridge converts TCP based Telnet traffic into UDP based SOL traffic and vice versa, so you can talk to the BMC using a standard Telnet client. SMBridge listens on local TCP port 623.

How does SDTConnector transport the UDP based SOL traffic to the BMC?

In order to transport the UDP traffic over the SSH tunnel, it must convert it into TCP traffic at the SDTConnector end of the tunnel, then convert it back into UDP at the Opengear end of the tunnel.

The SDTConnector end of this tunnel is listening on local UDP port 623, so when you connect to 127.0.0.1 (localhost) from the SMBridge prompt, it converts and transports it down the tunnel, converts it back, and forwards it to the BMC.

When I click the SOL button or type telnet localhost 623, the Telnet window closes immediately.

Ensure there are no other Telnet sessions to SMBridge already running on the client PC.

When I click the SOL button or type telnet localhost 623, I get a connection refused error or the Telnet window closes immediately.

First, ensure SMBridge is running.

Under Windows, click Start -> Run -> and type services.msc. Scroll down to find OSA SMBridge. If the status is not Started, right click it and click Start.

Under Linux, as root type /etc/init.d/smbridge start or run: /usr/bin/smbridge -d -c /etc/smbridge.cfg

Ensure your firewall settings aren't preventing you from connecting to TCP port 623.

Also ensure there are no other running programs using TCP port 623.

When I click the SOL button or when I click Start -> Run -> and type telnet localhost 623, it appears to connect but I never see the SMBridge prompt.

Ensure your firewall settings aren't preventing you from communicating on TCP port 623.

Under Windows, this problem can occur when the TCP/IP stack has become corrupted. Follow the steps at this link to reset the TCP/IP stack:

http://support.microsoft.com/kb/299357

Also ensure there are no conflicting services running on TCP port 623.

When I try to connect from the SMBridge prompt, the connection times out.

Ensure the Opengear SSH gateway is configured to allow SOL for the gateway user you are using with SDTConnector (e.g. ibmadmin), as per the section Configuring the Opengear SSH gateway to permit SOL.

You can confirm this is working by checking the Opengear system logs, search for output by udpgw and ensure UDP port 623 is being allowed for your user.

If this is working, the problem is with your BMC or network configuration. To troubleshoot this, install SMBridge on a system local to the BMC (e.g. on the management LAN itself) and ensure you can connect directly to the BMC by clicking Start -> Run -> and type telnet localhost 623, then type:

```
connect -ip 192.168.0.200 -u USERID -p PASSW0RD
```

Substitute the IP address of the BMC after -ip, and the BMC username and password after -u and -p. The values above are the defaults used in this document.

When I click the SOL button SDTConnector displays the error, Couldn't redirect port ... ?

Ensure UDP port 623 is not in use by another running program.

In Linux, ensure you are running SDTConnector with super user privileges, as port 623 is a privileged port and you will be unable to bind it otherwise.

3. *Connect to RSA II services*

xSeries/System x servers may be configured with an optional remote access card (Remote Supervisory Adapter II, or RSA II) that contains a sytems service processor. It provides out of band and remote access and control of the xSeries/System x server, independent of the operating system.

This is similar to the onboard BMC, however the add on remote access cards and more full featured and powerful. Advantages over the BMC include providing remote graphical access to the xSeries/System x server using a virtual KVM, ability to mount remote media, and remote server monitoring via a web page. The RSA II also has its own Ethernet network port, while the BMC shares a port with the system.

Configuring the RSA II

By default, the RSA II Ethernet port uses DHCP to acquire an address, with a static fall back address of 192.168.70.125. We suggest you use a static IP address rather than relying on a DHCP server, as this eliminates a possible point of failure.

In this example, we will set the RSA II's IP address to 192.168.0.125, subnet mask to 255.255.255.0 and gateway and 192.168.0.1, so it is compatible with the Opengear's default network settings.

- If you know the RSA II's IP address, you may browse to it to apple these network settings. Refer to IBM's RSA II user guide for detailed instructions.
- Otherwise, reboot the xSeries/System x server. During the POST messages, press F1 to enter the Configuration/Setup Utility menu. Select Advanced Setup, then RSA II Settings.
- Set DHCP Control to Use Static IP, Static IP Address to 192.168.0.125, Subnet Mask to 255.255.255.0 and Gateway to 192.168.0.1. Select Save Values and Reboot RSA II. Press Esc twice and exit the Setup Utility.

Refer to the IBM documentation for other setup tasks such as configuring users. In this example we use the default username/password, USERID/PASSW0RD (note the zero instead of "O" in PASSW0RD).

Configuring the Opengear SSH gateway to permit access to the RSA II

Ensure your Opengear unit is running firmware version 2.2.3 or later. The latest firmware is available from: ftp.opengear.com

- From the Serial & Network menu, select Network Hosts. Click Add Host. Enter the IP Address of the RSA II, as per the step Configuring the RSA II (in this example we used 192.168.0.125).

- Remove the Permitted Services you do not require, but do not remove HTTP (TCP port 80). Select TCP, enter Port 1044 and click Add. Select TCP, enter Port 1045 and click Add. Select TCP, enter Port 2000 and click Add. Select UDP, enter Port 2000 and click Add. Scroll to the bottom of the page and click Apply.

- From the Serial & Network menu, select Users & Groups. If you have not already, click Add User, otherwise Edit the user and skip to the next paragraph. Enter a username for the new user, e.g. ibmadmin. Enter and confirm a gateway Password for this user. Note that this is separate from the RSA II password.

- In Accessible Host(s), select the IP address for the RSA II (192.168.0.125). Click Apply.

Configuring SDTConnector to access the RSA II

Install and launch SDTConnector (1.4.x or later) on the client PC. If you haven't previously added the Opengear SSH gateway, select File -> New Gateway. Otherwise skip the next paragraph.

- Enter the IP address through which the Opengear unit/management LAN gateway is accessible to this client PC (e.g. 192.168.0.1). Enter the gateway username (e.g. ibmadmin) and password you set in the previous step. Click OK.

- Right click on the newly created gateway and select New Host. Enter the RSA II's IP address (192.168.0.125) in Host Address. Select the RSA II service and click OK.

Connecting to the RSA II

- Select the newly created host and click the RSA II button. A browser window is launched. Login to the RSA II using your RSA II username and password (USERID/PASSW0RD).

- From this page you can monitor you system, power it on and off, and access the virtual KVM and mount remote media using Remote Control. Note that Remote Control performs best when "Encrypt disk and KVM data during transmission" box is left unchecked. SDTConnector is already encrypting this data, so there is typically no need to encrypt it a second time.

4. *Connecting to IBM Director Server*

Director is IBM's tool for monitoring and administering of network-connected systems. When the Director client (Director Console) is installed alongside SDTConnector, you can connect to a Director server running on your management LAN.

The installation and setup of Director is outside the scope of this document. The following instructions assume you have a Director server running on your management LAN, and the Director Console installed on the same PC that is running SDTConnector.

Typically, your management LAN will have a dedicated Director server, independent from the hosts being managed. In this example, the Director server is assumed to be up and running on your management LAN with an IP address of 192.168.0.10.

Configuring the Opengear SSH gateway to permit access to Director

Ensure your Opengear unit is running firmware version 2.2.3 or later. The latest firmware is available from: ftp.opengear.com

- From the Serial & Network menu, select Network Hosts. Click Add Host. Enter the IP Address of the Director server as displayed in Control Panel -> Network Settings -> Local Area Connection -> Properties, in this example we will assume it is at 192.168.0.10.

- Remove any Permitted Services you do not require, select the TCP radio button and enter Port 2033 and click Add. Scroll to the bottom of the page and click Apply.

- From the Serial & Network menu, select Users & Groups. If you have not already, click Add User, otherwise Edit the user and skip to the next paragraph. Enter a username for the new user, e.g. ibmadmin. Enter and confirm a gateway Password for this user. Note that this is separate from the operating system or Director password.

- In Accessible Host(s), select the IP address of the Director server (192.168.0.10). Click Apply.

Configuring SDTConnector to connect to Director

Install and launch SDTConnector (1.4.x or later) on the client PC. If you haven't previously added the Opengear SSH gateway, select File -> New Gateway. Otherwise skip the next paragraph.

- Enter the IP address through which the Opengear unit/management LAN gateway is accessible to this client PC (e.g. 192.168.0.1). Enter the gateway username (e.g. ibmadmin) and password you set in the previous step. Click OK.

- Right click on the newly created gateway and select New Host. Enter the Director server's IP address (192.168.0.10) in Host Address.

- Select the Director service and click OK.

5. *Connecting to Director*

- Select the Director server host and click the Director button. The Director Console is launched, with the IBM Director Server address set to localhost or 127.0.0.1.

- Leave this IP address as localhost or 127.0.0.1, and enter the User ID and Password you use to connect to the Director server. It is possible this User ID and Password is the same as your operating system username and password on the Director server

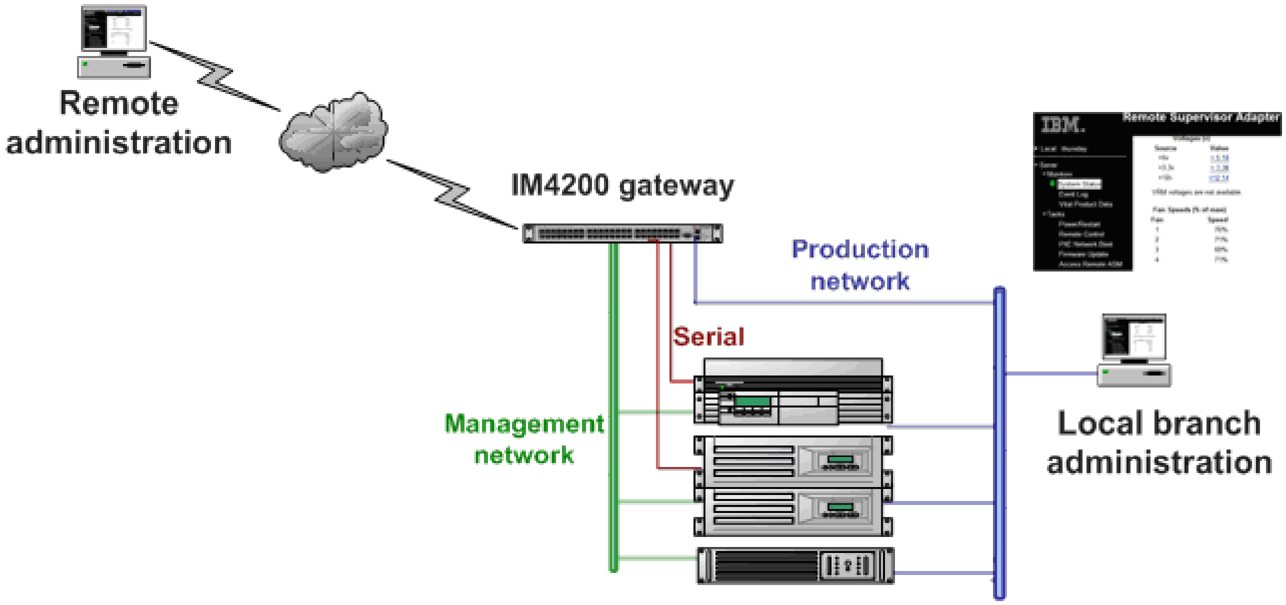
- Leave Use SSL unchecked, SDTConnector is already encrypting the traffic so it is not typically necessary to encrypt it a second time.

- Click OK to establish the connection.

6. *The IBM +Opengear solution*

Opengear IM4200 gateways and SDTConnector client ship preconfigured with support for IBM's BMCs and RSA cards and associated Director tools. IBM best practice recommends that the RSA cards not be connected directly to the production network, and the IM4200 gateway provides the ideal solution for securely accessing and controlling these service processors.

For enterprises with distributed branch offices the IM4200 family provides a powerful integrated solution. In the smaller branches with only a few racks of servers and network devices to administer, the IM4200 offers a single point of local and remote access to all the serial consoles, network consoles, service processors and power units at the site. In larger branches with racks of servers to administer, the IM4200 can serve as the management LAN gateway that securely isolates the service processors.



For the SMB customer the IM4216-25 + SDTConnector offers integrated out-of-band management fabric for RSAs/BMCs and remote access to IBM tools as well as management of non-IBM serial console equipment. It also delivers alternate connectivity for the out of band access with broadband and dial-up support. And for data center customers with racks of serial console devices to administer, the IM4248-2 (with its redundant power supplies, Ethernet failover, authentication and logs of all accesses) provides a most reliable solution, while the CM4148 provides a most affordable solution.

When locally administering an IBM server the Director application addresses the server at one TCP/IP address on the LAN, the RAC Services tools address the RSA at another IP address and the BMC is access for SOL and for IPMI connection using yet other UDP and TCP IP address. A selection of authentication and encryption options will then have been configured for each of these accesses. Administering this server remotely requires all the firewalls and routers in the enterprise network to be configured to allow communications through all these ports. Administering a distributed network of such servers remotely adds another layer of complexity.

The SDTConnector client that is supplied with each IM/CM4000 provides a simple centralized solution for administration of such distributed networks. With an IM4200 solution all the Director, IPMI and SOL access to each remote IBM server is securely tunneled thru SSH over the one selectable port. SDTConnector then gives the sys admin secure access to all these local and remote servers and sites from the one screen on his/her desktop, and appropriate tool for accessing a particular server can then be opened with a simple *point-n-click*

For remote administration, the SDTConnector client provides a simple centralized solution. RSA II, BladeCenter and BMC each use a variety of TCP/IP and UDP ports for communication only some of which the administrator can change. So the enterprise network firewalls and routers would need to allow communications through all these ports for the adapters to function properly.

However with an IM4200 solution all TCP and UDP access to the distributed servers is securely tunneled thru SHH over the one selectable port. SDTConnector also then gives the sys admin secure access to all these local and remote servers and sites from the one screen on his/her desktop, and the RSA management software for each of these servers can then be initiated with a simple *point-n-click*

For data center customers, with rows of racked IBM servers, the IM4200 family provides the most reliable solution for accessing the service processors - with redundant power supplies, Ethernet failover, authentication and logs of all accesses.

IBM's service processors can accessed with the IM4200 then managed using Director, IBM's integrated system management tools that provides a central platform for monitoring and managing all the IBM hardware resources. And the IBM + Opengear service management can be extended even further as Director also will seamlessly integrate with higher-level systems management offerings such as Tivoli, HP OpenView, Microsoft SMS and MOM, CA Unicenter, BMC and Altiris.