Managing Remote Presence

This chapter includes the following sections:

Configuring Serial Over LAN

Serial over LAN enables the input and output of the serial port of a managed system to be redirected over IP. Configure and use serial over LAN on your server when you want to reach the host console with Cisco IMC.

Before you begin

You must log in as a user with admin privileges to configure serial over LAN.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Serial over LAN** tab.

Step 4 In the **Serial over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, Serial over LAN (SoL) is enabled on this server.

Name	Description
Baud Rate drop-down list	The baud rate the system uses for SoL communication. This can be one of the following: • **9600 bps** • **19.2 kbps** • **38.4 kbps** • **57.6 kbps** • **115.2 kbps**
Com Port drop-down list	The serial port through which the system routes SoL communication. **Note** This field is only available on some C-Series servers. If it is not available, the server always uses COM port 0 for SoL communication. You can select one of the following: • **com0**—SoL communication is routed through COM port 0, an externally accessible serial port that supports either a physical RJ45 connection to an external device or a virtual SoL connection to a network device. If you select this option, the system enables SoL and disables the RJ45 connection, which means that the server can no longer support an external serial device. • **com1**—SoL communication is routed through COM port 1, an internal port accessible only through SoL. If you select this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0. **Note** Changing the Com Port setting disconnects any existing SoL sessions. **Note** This option is available only on some C-Series servers.
SSH Port filed	The port through which you can access Serial over LAN directly. The port enables you to by-pass the Cisco IMC shell to provide direct access to SoL. The valid range is 1024 to 65535. The default value is 2400. **Note** Changing the SSH Port setting disconnects any existing SSH sessions.

Step 5 Click **Save Changes**.

Configuring Virtual Media

Before you begin

You must log in as a user with admin privileges to configure virtual media.

Procedure

Step 1 In the **Navigation** pane, click the **Compute** tab.

Step 2 In the **Compute** tab, click the **Remote Management** tab.

Step 3 In the **Remote Management** tab, click the **Virtual Media** tab.

Step 4 In the **Virtual Media Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, virtual media is enabled. **Note** If you clear this check box, all virtual media devices are automatically detached from the host.
Active Sessions field	The number of virtual media sessions that are currently running.
Enable Virtual Media Encryption check box	If checked, all virtual media communications are encrypted.
Low Power USB enabled check box	If checked, low power USB is enabled. If the low power USB is enabled, after mapping the ISO and rebooting the host, the virtual drives appear on the boot selection menu. But, while mapping an ISO to a server that has a UCS VIC P81E card and the NIC is in Cisco Card mode, this option must be disabled for the virtual drives to appear on the boot selection menu.

Step 5 Click **Save Changes**.

Creating a Cisco IMC-Mapped vMedia Volume

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **Cisco IMC-Mapped vMedia** area, click **Add New Mapping**.

Step 5 In the **Cisco IMC-Mapped vMedia** dialog box, update the following fields:

Name	Description
Volume field	The identity of the image mounted for mapping.
Mount Type drop-down list	The type of mapping. This can be one of the following: **Note** Ensure that the communication port of the mount type that you choose is enabled on the switch. For example, when you are using CIFS as your mount type, ensure port 445 (which is its communication port) is enabled on the switch. Similarly, enable ports 80 for HTTP, 443 for HTTPS and 2049 for NFS when you use them. • **NFS**—Network File System. • **CIFS**—Common Internet File System. • **WWW(HTTP/HTTPS)**—HTTP-based or HTTPS-based system. **Note** Before mounting the virtual media, Cisco IMC tries to verify reachability to the end server by pinging the server.
Remote Share field	The URL of the image to be mapped. The format depends on the selected **Mount Type**: • **NFS**—Use **`serverip:/share`**. • **CIFS**—Use **`//serverip/share`**. • **WWW(HTTP/HTTPS)**—Use **`http[s]://serverip/share`**.
Remote File field	The name and location of the .iso or .img file in the remote share.

Name	Description
Mount Options field	

Name	Description
	Industry-standard mount options entered in a comma separated list. The options vary depending on the selected **Mount Type**. If you are using **NFS**, leave the field blank or enter one or more of the following: • **ro** • **rw** **Note** The folder, which is shared, should have write permissions to use read-write option. Read-write option is available only for .img files. • **nolock** • **noexec** • **soft** • **port=VALUE** • **timeo=VALUE** • **retry=VALUE** If you are using **CIFS**, leave the field blank or enter one or more of the following: • **soft** • **nounix** • **noserverino** • **guest** • **username=VALUE**—ignored if **guest** is entered. • **password=VALUE**—ignored if **guest** is entered. • **sec=VALUE** The protocol to use for authentication when communicating with the remote server. Depending on the configuration of CIFS share, **VALUE** could be one of the following: • **None**—No authentication is used • **Ntlm**—NT LAN Manager (NTLM) security protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **Ntlmi**—NTLMi security protocol. Use this option only when you enable Digital Signing in the CIFS Windows server. • **Ntlmssp**—NT LAN Manager Security Support Provider (NTLMSSP) protocol. Use this option only with Windows

Name	Description
	2008 R2 and Windows 2012 R2. • **Ntlmsspi**—NTLMSSPi protocol. Use this option only when you enable Digital Signing in the CIFS Windows server. • **Ntlmv2**—NTLMv2 security protocol. Use this option only with Samba Linux. • **Ntlmv2i**—NTLMv2i security protocol. Use this option only with Samba Linux. If you are using **WWW(HTTP/HTTPS)**, leave the field blank or enter the following: • `noauto` **Note** Before mounting the virtual media, Cisco IMC tries to verify reachability to the end server by pinging the server. • `username=VALUE` • `password=VALUE`
User Name field	The username for the specified **Mount Type**, if required.
Password field	The password for the selected username, if required.

Step 6 Click **Save**.

Viewing Cisco IMC-Mapped vMedia Volume Properties

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Remote Presence**.
Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.
Step 4 In the **Cisco IMC-Mapped vMedia** area, select a row from the **Current Mappings** table.
Step 5 Click **Properties** and review the following information:

Name	Description
Volume field	The identity of the image mounted for mapping.

Name	Description
Mount Type drop-down list	The type of mapping. This can be one of the following: • **NFS**—Network File System. • **CIFS**—Common Internet File System. • **WWW(HTTP/HTTPS)**—HTTP-based or HTTPS- based system. **Note** Before mounting the virtual media, Cisco IMC tries to verify reachability to the end server by pinging the server.
Remote Share field	The URL of the image to be mapped.
Remote File field	The name and location of the .iso or .img file in the remote share.
Mount Options field	The selected mount options.
User Name field	The username, if any.
Password field	The password for the selected username, if any.

Removing a Cisco IMC-Mapped vMedia Volume

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **Cisco IMC-Mapped vMedia** area, click **Unmap**.

When you are prompted to save the mapping, click **Save**.

Remapping an Existing Cisco IMC vMedia Image

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Remote Presence**.
Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.
Step 4 In the **Cisco IMC-Mapped vMedia** area, select a row from the **Current Mappings** table.
Step 5 Click **Remap**.

Deleting a Cisco IMC vMedia Image

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Remote Presence**.
Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.
Step 4 In the **Cisco IMC-Mapped vMedia** area, select a row from the **Current Mappings** table.
Step 5 Click **Delete**.

KVM Console

The KVM console is an interface accessible from Cisco IMC that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The KVM console allows you to connect to the server from a remote location.

Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer
- CD/DVD or floppy drive on the network
- Disk image files (ISO or IMG files) on the network
- USB flash drive on the network

You can use the KVM console to install an OS on the server.

Note When launching the KVM Console from Internet Explorer 6 SP1 on Windows Server 2003, the browser will report that it cannot download a required file. If this occurs, click the browser Tools menu and select Internet Options. Click the Advanced tab and, in the Security section, uncheck the checkbox for "Do not save encrypted pages to disk." Launch the KVM Console again.

Configuring the Virtual KVM

Before you begin

You must log in as a user with admin privileges to configure the virtual KVM.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 4 On the **Virtual KVM** tab, complete the following fields:

Name	Description
Enabled check box	If checked, the virtual KVM is enabled. **Note** The virtual media viewer is accessed through the KVM. If you disable the KVM console, Cisco IMC also disables access to all virtual media devices attached to the host.
Max Sessions drop-down list	The maximum number of concurrent KVM sessions allowed. You can select any number between 1 and 4.
Active Sessions field	The number of KVM sessions running on the server.
Remote Port field	The port used for KVM communication.
Enable Video Encryption check box	If checked, the server encrypts all video information sent through the KVM.
Enable Local Server Video check box	If checked, the KVM session is also displayed on any monitor attached to the server.

Step 5 Click **Save Changes**.

Enabling the Virtual KVM

Before you begin

You must log in as a user with admin privileges to enable the virtual KVM.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Remote Presence**.
Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.
Step 4 On the **Virtual KVM** tab, check the **Enabled** check box.
Step 5 Click **Save Changes**.

Disabling the Virtual KVM

Before you begin

You must log in as a user with admin privileges to disable the virtual KVM.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Remote Presence**.
Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.
Step 4 On the **Virtual KVM** tab, uncheck the **Enabled** check box.
Step 5 Click **Save Changes**.