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.

☞

Important You cannot use native serial redirection and serial over LAN simultaneously.

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 **Compute** menu.
Step 2	In the **Compute** menu, select a server.
Step 3	In the work pane, click the **Remote Management** tab.
Step 4	In the **Remote Presence** pane, click the **Serial over LAN** tab.
Step 5	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. 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.

Step 6   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 **Compute**.

Step 2   In the **Compute** menu, select a server.

Step 3   Click the **Remote Management** tab.

Step 4   In the **Remote Management** tab, click the **Virtual Media** tab.

Step 5   In the **vKVM Console Based vMedia 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.

Step 6   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 **Compute** menu.

Step 2   In the **Compute** menu, select a server.

Step 3   In the work pane, click the **Remote Management** tab.

Step 4   In the **Remote Management** tab, click the **Virtual Media** tab

Step 5   In the **Current Mappings** area, click **Add New Mapping**.

Step 6   In the **Add New Mapping** dialog box, update the following fields:

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:
	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**

- **rsize=VALUE**

- **wsize=VALUE**

- **vers=VALUE**

If you are using **CIFS**, 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. |

- **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

Name	Description
	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 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. • `vers=VALUE` **Note** The format of the VALUE should be *x.x* 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 7   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 **Compute** menu.

Step 2   In the **Compute** menu, select a server.

Step 3   In the work pane, click the **Remote Management** tab.

Step 4   In the **Remote Management** tab, click the **Virtual Media** tab

Step 5   Select a row from the **Current Mappings** table.

Step 6   Click **Properties** and review the following information:

Name	Description
Add New Mapping button	Opens a dialog box that allows you to add a new image.
Properties button	Opens a dialog box that allows you to view or change the properties for the selected image.
Unmap button	Unmaps the mounted vMedia.
Last Mapping Status	The status of the last mapping attempted.
Volume column	The identity of the image.
Mount Type drop-down list	The type of mapping.
Remote Share field	The URL of the image.
Remote File field	The exact file location of the image.
Status field	The current status of the map. This can be one of the following: • **OK**—The mapping is successful. • **In Progress**—The mapping is in progress. • **Stale**—Cisco IMC displays a text string with the reason why the mapping is stale. • **Error**—Cisco IMC displays a text string with the reason for the error.

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 **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **Remote Management** tab.

Step 4 In the **Remote Management** tab, click the **Virtual Media** tab

Step 5 Select a row from the **Current Mappings** table.

Step 6 Click **Unmap**.

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 **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **Remote Management** tab.

Step 4 In the **Remote Management** tab, click the **Virtual Media** tab

Step 5 Select a row from the **Current Mappings** table.

Step 6 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 **Compute** menu.

Step 2	In the **Compute** menu, select a server.
Step 3	In the work pane, click the **Remote Management** tab.
Step 4	In the **Remote Management** tab, click the **Virtual Media** tab
Step 5	Select a row from the **Current Mappings** table.
Step 6	Click **Delete**.

Virtual KVM Console

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

Here are a few major advantages of using Cisco KVM Console:

- The Cisco KVM console provides connection to KVM, SOL, and vMedia whereas the Avocent KVM provides connection only to KVM and vMedia.

- In the KVM Console, the vMedia connection is established at the KVM Launch Manager and is available for all users.

- The KVM console offers you an advanced character replacement options for the unsupported characters while pasting text from the guest to the host.

- The KVM console provides you an ability to store the vMedia mappings on CIMC.

Instead of using CD/DVD or floppy drives physically connected to the server, the vKVM 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 vKVM console to install an OS on the server.

Note   To configure the vKVM console successfully for the S3260 Storage Server, you need to configure IP addresses for the Cisco IMC, CMC, and BMC components. You can configure the IP addresses for these components using the CLI interface or Web UI. For the CLI, use the command **scope network**, or view the setting using **scope <chassis/server1/2><cmc/bmc><network>**.

To configure IP addresses for network components on the web interface, see the steps described in the section **Configuring Network-Related Settings**.

Launching KVM Console

You can launch the KVM console from either the Home page or from the Remote Management area.

Procedure

Step 1	To launch the console from Home page, in the **Navigation** pane, click the **Chassis** menu.
Step 2	In the **Chassis** menu, click **Summary**.
Step 3	From the tool bar, click **Launch vKVM**.
Step 4	In the **Servers** drop-down menu, select a server.
Step 5	Alternatively, in the **Navigation** pane, click the **Compute** menu.
Step 6	In the **Compute** menu, select a server.
Step 7	In the work pane, click the **Remote Management** tab.
Step 8	In the **Remote Management** pane, click the **Virtual KVM** tab.
Step 9	In the **Virtual vKVM** tab, click **Launch vKVM console**.
Step 10	Required: Click the URL link displayed in the pop-up window to load the client application. You need to click the link every time you launch the vKVM console.

Virtual KVM Console

The vKVM console is an interface accessible from Cisco IMC that emulates a direct keyboard, video, and mouse (vKVM) connection to the server. It allows you to connect to and control the server from a remote location and to map physical locations to virtual drives that can by accessed by the server during this vKVM session.

Cisco IMC provides Cisco based vKVM console for M5 servers with the following options:

File Menu

Menu Item	Description
Paste Text From File / Send Text	Opens the dialog box that allows you to paste content.
Capture to File	Opens the **Save** dialog box that allows you to save the current screen as a JPG image.
Exit	Closes the vKVM console.

View Menu

Menu Item	Description
Keyboard	Displays the virtual keyboard for the vKVM console, which you can use to input data.

Menu Item	Description
Refresh	Updates the console display with the server's current video output.
Full Screen	Expands the vKVM console so that it fills the entire screen.

Macros Menu

Choose the keyboard shortcut you want to execute on the remote system.

Menu Item	Description
Static Macros menu	Displays a predefined set of macros.
Manage	Opens the **Configure User Defined Macros** dialog box, which allows you to create and manage macros.
	System-defined macros cannot be deleted.

Tools Menu

Menu Item	Description
Session Options	Opens the **Session Options** dialog box that lets you specify:
	• **Scaling**—Specify whether or not you want to maintain the aspect ratio of the screen. Check or uncheck the **Maintain Aspect Ratio** checkbox (checked by default).
	• **Mouse Acceleration**: The mouse acceleration to use on the target system. The default is **Absolute positioning (Windows, Newer Linux & MAC OS X)**. Other options are:
	• **Relative Positioning, no acceleration**
	• **Relative Positioning (RHEL, Older Linux)**
	• **Paste Text**: Allows you to select to paste text from clipboard or a file.
Session User List	Opens the **Session User List** dialog box that shows all the user IDs that have an active vKVM session.
Chat	Opens the **Chat** box to communicate with other users.

Menu Item	Description

Stats	Opens the **Stats** dialog box, and the **Live vKVM** displays the following:
	
	  • **Frame Rate**: Frame rate measured in the number of frames per second.
	
	  • **Bandwidth**: Bandwidth measured in the number of KBs per second.
	
	  • **Compression**: Compression measured in the percentage of compression being used.
	
	  • **Packet Rate**: Packet rate measured in number of packets per second.
	
	When vMedia is activated, the **Virtual Media** dialog box displays the following:
	
	  • **Target Device**: The type of local device.
	
	  • **Mapped to**: The type of local device or image file to which the host server device is mapped.
	
	  • **Duration**: The elapsed time of the device to map.
	
	  • **Read Bytes**: The number of bytes sent or received by the server.

Play Controls	Opens **Cisco vKVM Playback** window that allows you to choose a `.dvc` file.

Power Menu

Menu Item	Description
Power On System	Powers on the system. This option is disabled when the system is powered on and it is enabled when the system is not powered.
Power Off System	Powers off the system from the virtual console session. This option is enabled when the system is powered on and disabled when the system is not powered on.
Reset System (warm boot)	Reboots the system without powering it off. This option is enabled when the system is powered on and disabled when the system is not powered on.
Power Cycle System (cold boot)	Turns off system and then back on. This option is enabled when the system is powered on and disabled when the system is not powered on.

Boot Device Menu

Name	Description
No Override	Clicking this option enables the host to boot to the first device configured.
Boot Device list	A list of boot devices that the server uses to boot from only for the next server boot, without disrupting the currently configured boot order. Once the server boots from the one time boot device, all its future reboots occur from the previously configured boot order. A maximum of 15 devices are displayed on the vKVM console.

Virtual Media Menu

Name	Description
Create Image **Note** This option is available only if you use the Google Chrome web browser.	Allows you to create an ISO image. Drag and drop files or folders in the **Create Image** dialog box; these files or folders are converted to an ISO image. You can use the **Download ISO Image** button to save the ISO image to your local machine.
Activate Virtual Devices	Activates a vMedia session that allows you to attach a drive or image file from your local computer or network.

Help Menu

Name	Description
Help Topics	Clicking this option brings you back to this window.
About vKVM Viewer	Displays the version number of the vKVM viewer.

Settings

The **Settings** icon is located on the top right hand corner of the HTML vKVM viewer window.

Name	Description
Logged in as:	Displays your user role name.
Cisco IMC Host Name	Displays the host name.

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 **Compute** menu.

Step 2   In the **Compute** menu, select a server.

Step 3   In the work pane, click the **Remote Management** tab.

Step 4   In the **Remote Management** pane, click the **Virtual KVM** tab.

Step 5   In the **vKVM Properties** area 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 6   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 **Compute** menu.

Step 2   In the **Compute** menu, select a server.

Step 3   In the work pane, click the **Remote Management** tab.

Step 4   In the **Remote Management** pane, click the **Virtual KVM** tab.

Step 5   On the **Virtual KVM** tab, check the **Enabled** check box.

Step 6   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 **Compute** menu.

Step 2   In the **Compute** menu, select a server.

Step 3   In the work pane, click the **Remote Management** tab.

Step 4   In the **Remote Management** pane, click the **Virtual KVM** tab.

Step 5   On the **Virtual KVM** tab, uncheck the **Enabled** check box.

Step 6   Click **Save Changes**.