CommandCenter Secure Gateway

User Guide

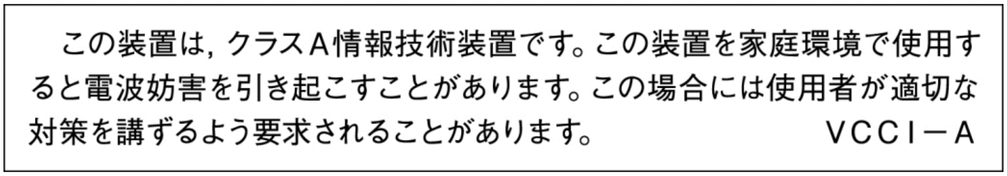
Release 11.0

CC-1F-v11.0-E
March 2023
255-80-3100-00

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)



この装置は，クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　ＶＣＣＩ－Ａ

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.

1F61
I.T.E.

Contents

Node Chat 100

My Profile 102

Appendix A Keyboard Shortcuts 106

Appendix B Troubleshooting 107

Index 111

What's New in the CC-SG User Help

The following sections have changed or information has been added to the CommandCenter Secure Gateway User Help based on enhancements and changes to the equipment and/or user documentation.

- AKC client launch needs trusted certificate
- Strong passwords are enabled in CC-SG by default
- CIM details are displayed
- Custom view set as system view can be set as default for all users
- Support for new iLO and DRAC versions

Please see the Release Notes for a more detailed explanation of the changes applied to this version of the CommandCenter Secure Gateway.

Introduction

This guide is intended for users who have been granted the Node In-Band Access, Node Out-of-Band Access, and Node Power Control privileges. With these privileges, you can connect to nodes, control power to nodes, create custom views, search for nodes, and use node chat to talk to other users who are connected to the same node.

In This Chapter

Prerequisites

Before connecting to a node, the nodes must be configured. The application that is used to connect to the node must also be configured. See Raritan's **CommandCenter Secure Gateway Administrator Guide** for additional information on nodes and applications.

Terminology/Acronyms

- iLO/RILOE - Hewlett Packard's Integrated Lights Out/Remote Insight Lights Out servers that can be managed by CC-SG. Targets of an iLO/RILOE device are powered on/off and recycled directly.
- In-band Access - using the TCP/IP network to correct or troubleshoot a node in your network. You can access nodes connected to KVM and Serial devices via these in-band applications: RemoteDesktop Viewer, SSH Client, VNC Viewer.
- IPMI Servers - Intelligent Platform Management Interface servers that can be controlled by CC-SG.
- Out-of-band Access - using applications such as Virtual KVM Client to correct or troubleshoot a node connected to KVM and Serial devices in your network.
- Ports - connection points between a Raritan Device and a node. Ports exist only on Raritan devices and identify a pathway from that device to a node.
- Nodes - the target systems such as servers, desktop PCs, or other networked equipment that CC-SG users can access.

Accessing CC-SG

You can access CC-SG in several ways:

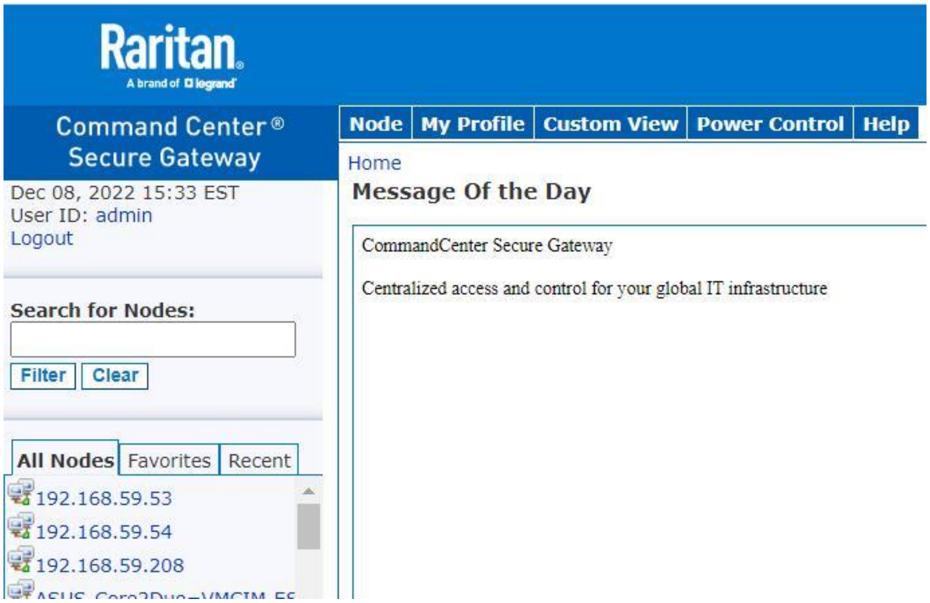
- Browser Access for Users and Admins: The CC-SG Access Client and Admin Client can be accessed with numerous supported web browsers. For a complete list of supported browsers, choose Administration > Compatibility Matrix.
- Desktop Admin Client: The Windows, Mac, and Linux desktop versions of the Admin Client are installed on your client computer and function exactly like the browser-based Admin Client, but uses an embedded Java library. You are not required to install Java on your PC.
- Thick Client: You can install a Java Web Start thick client on your client computer. The thick client functions exactly like the browser-based Admin Client.
- SSH: Remote devices connected via the serial port can be accessed using SSH.
- Diagnostic Console: Provides emergency repair and diagnostics only and is not a replacement for the browser-based GUI to configure and operate CC-SG.

Note: Users can be connected simultaneously, using the browser, thick client, and SSH while accessing CC-SG.

In This Chapter

CC-SG Access Client Using a Browser

The CC-SG Access client is an HTML-based client that provides non-administrator CC-SG users with a GUI for access tasks, based on your permissions.



Dec 08, 2022 15:33 EST
User ID: admin

192.168.59.53
192.168.59.54
192.168.59.208

Message Of the Day

CommandCenter Secure Gateway

Centralized access and control for your global IT infrastructure

1. Using a supported Internet browser, type the URL of the CC-SG: http(s)://*IP address*, for example, ***http://10.0.3.30*** (***https://10.0.3.30***) or https://10.0.3.30. The login page opens.
2. If the CC-SG Administrator has enabled the Restricted Service Agreement, read the agreement text, and then select the I Understand and Accept the Restricted Service Agreement checkbox.
3. Type your Username and Password then click Log In.
4. Upon valid login, the CC-SG Access Client's Home page opens.

Possible Error Messages

If you have access to a large number of nodes, you may see the following error messages while CC-SG loads.

Internet Explorer

A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive. Do you want to abort the script?

FireFox

A script on this page may be busy, or it may have stopped responding. You can stop the script now, or you can continue to see if the script will complete.

These warning messages occur when a script is taking longer than the default time to run.

▶ To resolve these errors:

- When the message appears, select the option that allows the script to continue running.

  Depending on your particular client and server speeds and the amount of data loading, the message may recur.

▶ To change the default time that scripts are allowed to run in Internet Explorer:

Refer to Microsoft Knowledge Base article 175500 for instructions.

▶ To change the default time that scripts are allowed to run in Firefox:

Refer to the MozillaZine Knowledge Base article about `dom.max_script_run_time` for details on this configuration: ***http://kb.mozillazine.org/Dom.max_script_run_time***
http://kb.mozillazine.org/Dom.max_script_run_time

1. Access the hidden configuration page in Firefox.
   a. Type `about:config` in the Firefox address bar.
   b. A list of hidden configurations appears.
2. In the Filter field, type `dom.max_script_run_time.` The list refreshes to display only one item.
3. Right-click the `dom.max_script_run_time` item, and choose Modify.
4. In the Enter Integer value dialog that appears, type a higher value, such as 100. The default value is 10.

Accessing Another CC-SG Unit in the Same Neighborhood

The Neighborhood feature groups multiple CC-SG units.

NOTE: Use the Access Client in Internet Explorer--this is the only browser/client combination that supports the drop-down list for the Neighborhood feature.

After the CC-SG Administrator configures the Neighborhood feature in the CC-SG Admin Client, the Secure Gateway drop-down list displays at the top of the Access Client if the CC-SG you access is an activated member in a Neighborhood.

If you accept the Restricted Service Agreement once in any Neighborhood member, it is implicitly accepted for all members in the Neighborhood.

Access from a Mobile Device

You can run the CC-SG Access Client using your IOS mobile device's browser.

When you connect to CC-SG on your IOS mobile device, you can access KX3 v3.4 and later targets using the HKC client, and SX2 2.1 and later targets using the HSC client.

See ***Connecting to Nodes using a Mobile Device*** (on page 71).

Log Out from the Access Client

When you are finished using the Access Client, you should click one of the Logout links to log out. Closing the browser window without clicking a logout link first does not log you out of the Access Client.

When you log out of a CC-SG that is an active member of the Neighborhood, it logs you out of all the CC-SG units and terminates all node connections within the Neighborhood.

CC-SG Admin Client Using a Browser

The CC-SG Admin client is a Java-based client that provides a GUI for both administrative and access tasks, depending on your permissions.

1. Using a supported Internet browser, allow pop-ups, then type the URL of the CC-SG and then type /admin: http(s)://*IP address*/admin, for example, ***http://10.0.3.30/admin*** (***https://10.0.3.30/admin***) or https://10.0.3.30/admin.

   If you see the JRE Incompatibility Warning window, select the JRE version that is appropriate for your client computer and install it. Once JRE is installed, try this procedure again. See **JRE Incompatibility** *(on page 6) and* **Install a Supported Java Runtime Environment (JRE) Version** *(on page 6).*

   Or, you can continue without installing a new JRE version.

2. If you see a Restricted Service Agreement, read the agreement text and select the I Understand and Accept the Restricted Service Agreement checkbox.
3. Type your Username and Password and click Log In.
4. Upon valid login, the CC-SG Admin Client opens.

Install a Supported Java Runtime Environment (JRE) Version

The browser must have the correct version of JRE installed before you can access the CC-SG Admin Client. Your administrator can recommend a JRE version that is different than the CC-SG minimum version. Check with your administrator to find out what JRE version is required.

▶ To check the JRE version in a Windows OS:

1. Open Control Panel.
2. Click Add or Remove Programs. Check the list of currently installed programs for the J2SE or Java 2 Runtime Environment version number.

▶ To verify that the JRE version is compatible with your CC-SG release:

Choose Administration > Compatibility Matrix. Look for Oracle JRE in the Application list.

▶ To upgrade JRE:

Go to https://www.java.com/en/download/manual.jsp

JRE Incompatibility

If you do not have the minimum required version of JRE installed on your client computer, you will see a warning message before you can access the CC-SG Admin Client. The JRE Incompatibility Warning window opens when CC-SG cannot find the required JRE file on your client computer.

If you see the JRE Incompatibility Warning window, select the JRE version that is appropriate for your client computer and install it, or you can continue without installing a new JRE version.

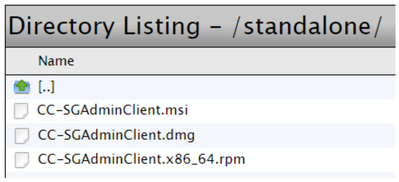
You must launch CC-SG again once JRE is installed.

Administrators can configure the JRE minimum version that is recommended and the message that appears in the JRE Incompatibility Warning window. See Configuring Custom JRE Settings.

CC-SG Desktop Admin Clients

Desktop Admin Clients are installed onto your client machine. A desktop icon is provided to launch the client.

Installation files can be downloaded directly from your CommandCenter Secure Gateway by going to: **https://<CC-SG IP address or hostname>/standalone**



Directory Listing – /standalone/

Name
[..]
CC-SGAdminClient.msi
CC-SGAdminClient.dmg
CC-SGAdminClient.x86_64.rpm

Follow these links to specific instructions for your client type.

- ***Windows Desktop Admin Client*** (on page 7)
- ***Mac Desktop Admin Client*** (on page 9)
- ***Linux Desktop Admin Client*** (on page 11)

Windows Desktop Admin Client

The Windows Desktop Admin Client is a version of the Admin Client that does not require Java to be installed on your PC. The Windows Admin Client is installed with a standard Windows installer onto your PC. A desktop icon is provided to launch the client.

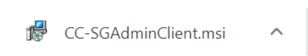
The client uses an embedded Java library that is internal to the client, so you can have all the features of the Java-based Admin Client, and avoid issues surrounding Java.

- No Java Applets. Insecure NPAPI protocol is not used.
- No Java virtual machine running on your PC.
- No Java updates required.
- No Java incompatibility between applications.
- No browser used.
- No Java/browser security issues.

Install the Windows Desktop Admin Client

▶ **To install the Windows Desktop Admin Client:**

1. Download the install file directly from the CC-SG by going to: **https://<CC-SG IP address or hostname>/standalone**
2. For the Windows client, choose the **.msi file.**



CC-SGAdminClient.msi

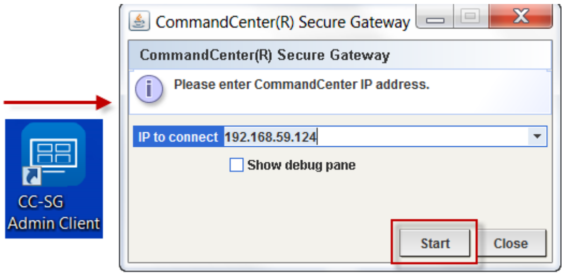
3. Launch the installer and click Next to start the installation.

4. Follow the prompts to setup the installation. Accept security prompts if they appear.
5. When the installation is complete, you will find the CC-SG Admin Client icon on your desktop.

Launch the Windows Desktop Admin Client

To launch the Windows Desktop Admin Client:

1. Double-click the desktop icon, then enter a CC-SG IP address and click Start.



CommandCenter(R) Secure Gateway

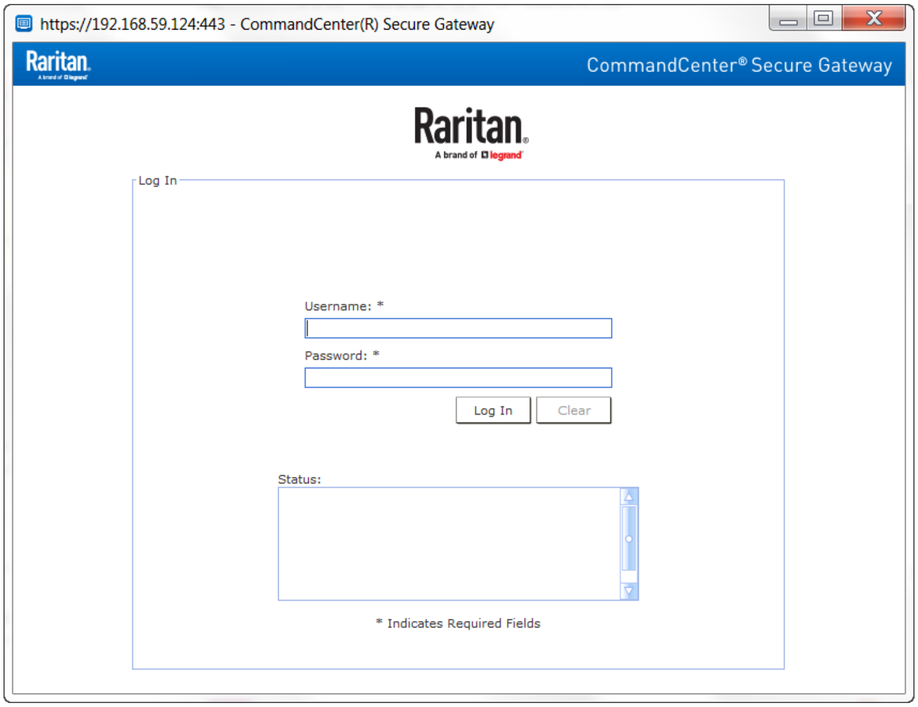
CommandCenter(R) Secure Gateway

Please enter CommandCenter IP address.

IP to connect 192.168.59.124

□ Show debug pane

2. The Admin Client login page opens.



https://192.168.59.124:443 - CommandCenter(R) Secure Gateway
Raritan.
CommandCenter® Secure Gateway
Raritan.
A brand of legrand
Log In
Username: *
Password: *
Log In
Clear
Status:
* Indicates Required Fields

Interface Support in CC-SG Desktop Admin Client

The CC-SG Desktop Admin Client does not support connections to the following interfaces because they require JRE add-ons in a browser:

- DRAC5
- DRAC6

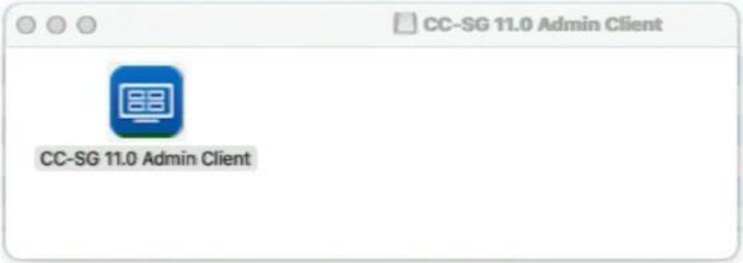
Mac Desktop Admin Client

▶ To download

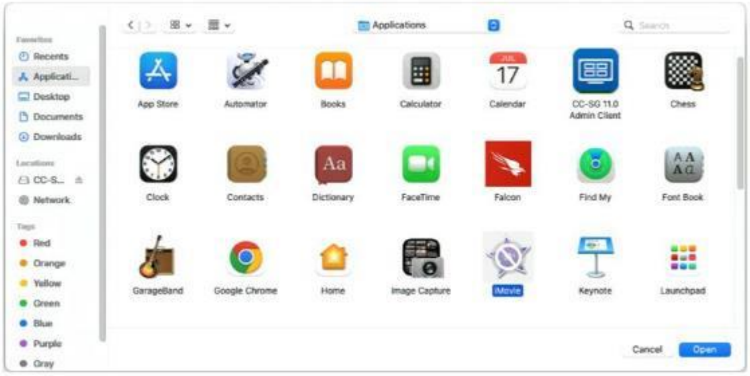
1. Download the install file directly from the CC-SG by going to: **https://<CC-SG IP address or hostname>/standalone**
2. For the Mac client, choose the **.dmg file.**

To install

- Double-click the downloaded Mac Desktop Admin Client installation file (.dmg).



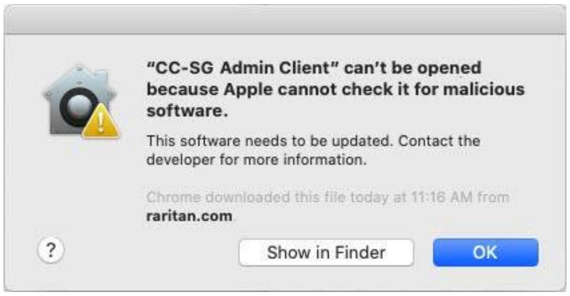
To allow all users to run the client, drag it to the Applications folder:



To launch:

- Double-click client icon to launch the Mac Desktop Admin Client.

You may see the following warning upon first launch, **without** an Open button that allows you to continue. Choose one of the options below to fix this if needed.



"CC-SG Admin Client" can't be opened because Apple cannot check it for malicious software.

This software needs to be updated. Contact the developer for more information.

Chrome downloaded this file today at 11:16 AM from **raritan.com**

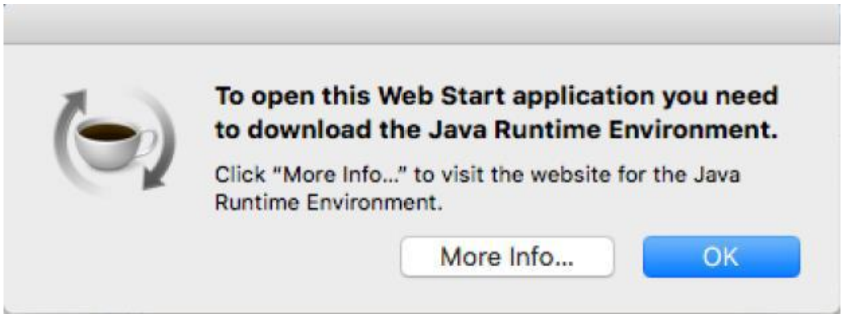
- Option #1:

  Go to System Preference > Security & Privacy, select "App Store and identified developers" under "Allow apps downloaded from." The warning will display with a button to "Open Anyway".

- Option #2:

  Instead of downloading the .dmg file directly from the Mac machine, download it on a Windows machine, save the file to a USB drive, then copy the file back to the MAC machine to install; or SCP from another machine into MAC to install the client.

Note: When making a target connection with a Java web start application (jnlp), install the latest Java runtime from the Java website.



To open this Web Start application you need to download the Java Runtime Environment.

Click "More Info..." to visit the website for the Java Runtime Environment.

Linux Desktop Admin Client

To download

1. Download the install file directly from the CC-SG by going to: **https://<CC-SG IP address or hostname>/standalone**
2. For the Linux client, choose the **.rpm file.**

To install

- Run the following command as root user on any Linux that supports rpm installation:

  ```
  rpm -i CC-SGAdminClient.x86_64.rpm
  ```

  Or run with sudo if you are not logged in as system administrator:

  ```
  sudo rpm -i CC-SGAdminClient.x86_64.rpm
  ```

To launch:

- Find CC-SG Admin Client under Applications/Internet.

  Or
- Run `ccadmin` command.

Note for Fedora 29 or later:

- If Java Web Start applications, such as VKC, SSH, and so on do not launch when you connect to a target from CC-SG, install the following package:

  ```
  dnf install libnsl
  ```

To uninstall:

- `rpm -e CC-SGAdminClient`

  Or

- `sudo rpm -e CC-SGAdminClient`

Note: When making a target connection with a Java web start application, a warning message about Java upgrade might appear at the background of the CC-SG client. Click the Later button for connection to be launched properly and prevent further warning messages.

Thick Client

The CC-SG thick client allows you to connect to CC-SG by launching a Java Web Start application instead of running an applet through a web browser. The advantage of this is that the client can outperform the browser in terms of speed and efficiency. The CC-SG thick client provides the same functions as the Java-based Admin Client, a GUI for both administrative and access tasks, depending on your permissions.

Check the Compatibility Matrix for your CC-SG version for the supported Java versions.

Install the Thick Client

1. To download the thick client from CC-SG, launch a web browser and type this URL: http(s)://<IP_address>/install, where <IP_address> is the IP address of the CC-SG.
2. If a security warning message appears, click Start to continue the download.
3. When the download is complete, a new window in which you can specify the CC-SG IP address appears.
4. Type the IP address of the CC-SG unit you want to access in the IP to Connect field.

   Once you have connected, this address will be available from the IP to Connect drop-down list. The IP addresses are stored in a properties file that is saved to your desktop.
5. Click Start.

   A warning message appears if you are using an unsupported Java Runtime Environment version on your machine. Follow the prompts to either download a supported Java version or continue with the currently installed version.
6. The login screen appears and the thick client looks and behaves just like the browser-based Java client. If the Restricted Service Agreement is enabled, read the agreement text, and then select the I Understand and Accept the Restricted Service Agreement checkbox.

7. Type your Username and Password in the corresponding fields and click Login to continue.

Access CC-SG with the Thick Client

Once the thick client is installed, there are different ways to access it on your client computer.

▶ **To access the thick client:**

- Launch the thick client from the Java Control Panel's Java Application Cache Viewer.
- Use the Java Control Panel's Java Application Cache Viewer to install a shortcut icon on your desktop for the thick client.

Internet Explorer Access

When accessing CC-SG using the Internet Explorer browser, you must add the CC-SG IP address or hostname to the Intranet Zone. In the browser, choose Tools > Internet Options > Trusted Sites > Sites. Click "Add this website to the zone" and click Add.

Mac and Safari Access

VKC KVM target connections are not automatically launched from the latest Safari versions. Instead, the JNLP app is saved to the downloads folder.

To open, go to the Downloads folder. Holding down the Ctrl button, click on file and select Open. Then click the Open button on the warning message that OS cannot verify the developer of the JNLP app.

Finding and Viewing Nodes

There are several ways to find and view nodes, depending on which client you are using.

See ***Finding and Viewing Nodes in the Access Client*** (on page 14) and ***Finding and Viewing Nodes in the Admin Client*** (on page 18) to learn how to use each client's navigation and search features to find and view nodes.

See ***Using Custom Views in the Access Client*** (on page 23) and ***Using Custom Views in the Admin Client*** (on page 25) to learn how to use each client's custom view feature to specify different ways to display the nodes in the left panel.

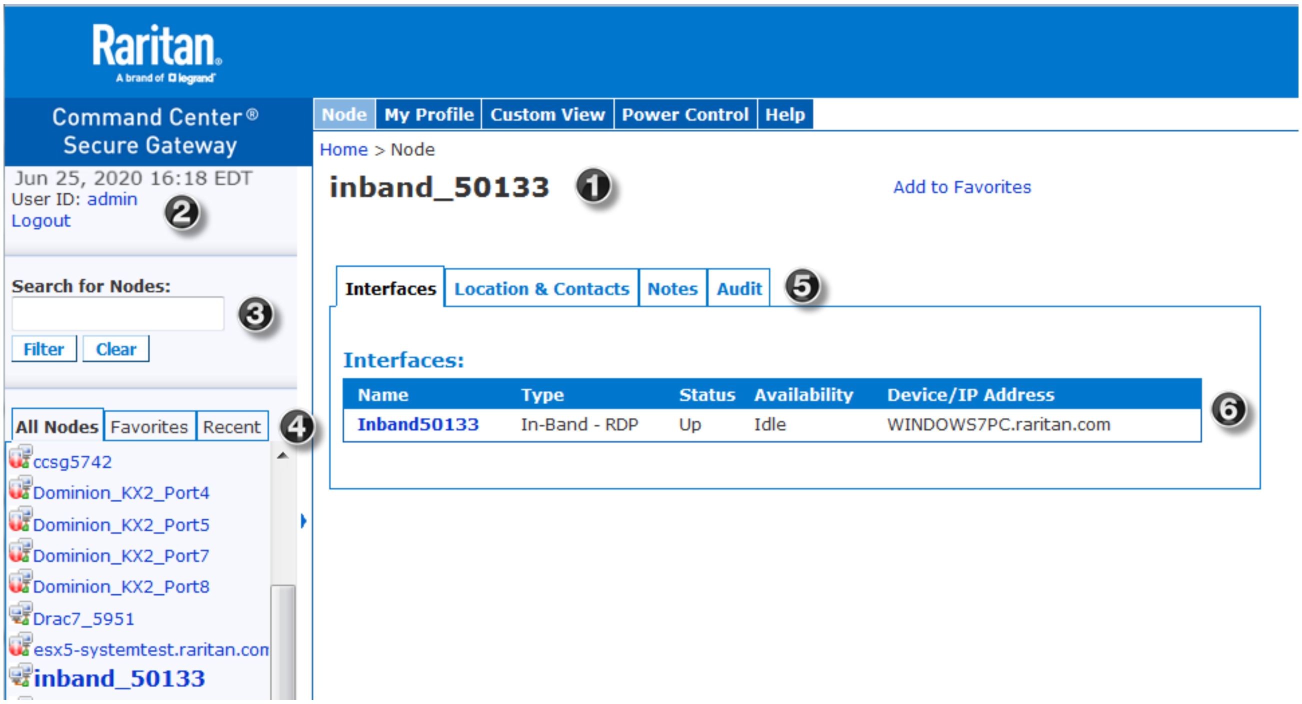
In This Chapter

Finding and Viewing Nodes in the Access Client

In the CC-SG Access Client, you can connect to nodes through their associated interfaces. Each node has a Node details screen, which lists all associated interfaces to which you have access. If a node has virtual media capabilities, the Node details screen displays whether virtual media is enabled or disabled for the node.

Click a node in one of the node lists in the left panel (All Nodes, Favorites, and Recent) to open the Node details screen for the selected node. Click the Node tab at the top of the screen to return to the selected node's Node details screen after viewing other tabs.

CC-SG Access Client Overview



Name	Type	Status	Availability	Device/IP Address
Inband50133	In-Band - RDP	Up	Idle	WINDOWS7PC.raritan.com

1. Current node name: The name of the CC-SG node you are viewing appears at the top of the page.
2. User ID and Date: Your CC-SG system date and time and User ID appear at the top of the left panel. Click the User ID link to open the My Profile tab.
3. Search: The Search function allows you to search for nodes in two ways. If the CC-SG is a neighborhood member, and extended network search is enabled, you can specify local or neighborhood searches. See ***Searching for Nodes*** (on page 17).
4. Node lists: Node lists appear below the search field. In each list, icons show the status of each node. The All Nodes list includes all nodes to which you have access. The Favorites list contains your personalized list of nodes. You can add nodes, delete nodes, and sort the list of Favorite nodes. The Recent list displays the ten nodes accessed most recently. Click a node to open the Node tab. The Node tab contains the Node profile, which displays details on the selected node. The Node tab also allows you to connect to an interface and perform power control.
5. Navigation tabs: The Navigation tabs are located at the top of every screen. Click a tab to open the related screen.
6. Node tabs: Details about the selected node are in each tab.

Node Lists

The left panel of the CC-SG HTML Client contains several ways to locate nodes. Three lists offer different views of the nodes: All Nodes, Favorites, and Recent. In each list, icons display show the status of each node. You can click a node in one of the lists to open the Node Profile.

You can also create Custom Views to specify different ways to display the nodes. See ***Using Custom Views in the Access Client*** (on page 23).

All Nodes List

The All Nodes list displays all nodes to which you have access. If you have applied a Custom View, the All Nodes list will display according to the specification of the Custom View. See ***Custom Views*** (on page 22).

Sort Nodes by Name or Status

You can sort the All Nodes list by node name or node status.

▶ **To sort nodes by Name:**

1. Open the All Nodes list.
2. Choose Sort Nodes By > Name.

▶ **To sort nodes by Status:**

1. Open the All Nodes list.
2. Choose Sort Nodes By > Status.

Favorite Nodes List

You can create a personalized list of the nodes you access most often in the Favorites list. You can add nodes, delete nodes, and sort the list of Favorite nodes.

Add a Node to Favorites

1. Click the All Nodes or Recent list in the left panel.
2. Click the node you want to add to Favorites. The Node details screen appears.
3. In the Node details screen, click Add to Favorites. The status bar at the bottom of the browser window displays a confirmation message and the Add to Favorites link disappears from the Node details screen.

Sort Nodes in Favorites

1. Click the Favorites list in the left panel.
2. Click Sort. The Sort Favorites window appears.

3. Arrange the nodes in the Favorite Nodes list in the order in which you would like them to appear in the Favorites list. Select a node and click the up and down arrows to move the node into the desired sequence. Click Sort by Name to arrange the nodes in alphanumeric order.
4. Click OK to save your changes.

Delete a Node from Favorites

1. Click the Favorites list in the left panel.
2. Click the node you want to delete. The Node details screen for the selected node appears.
3. Click Delete in the Favorites list to delete the node from the list.

Recent Nodes List

The Recent list displays the ten nodes you accessed most recently. Each node you click on is added to the top of the Recent list.

Clear the Recent Nodes List

1. Click the Recent list in the left panel.
2. Click Clear All to clear the Recent list.

Searching for Nodes

If the CC-SG is a neighborhood member, and extended network search is enabled, you can specify local or neighborhood searches.

See ***Extended Network Neighborhood Search*** (on page 18).

▶ **To search for nodes:**

1. If extended neighborhood search is enabled, two radio buttons display, Local Only and In Neighborhood. Select the radio button for the search range.
   - Local Only: searches only for nodes on the currently selected member. See the Secure Gateway drop-down list for your currently selected member.
   - In Neighborhood: searches for nodes in all member CC-SG units. See the Secure Gateway drop-down list to review all members.
2. Type the search terms, such as node name, in the Search for Nodes field at the top of the left panel.
3. As you type, the node that most closely matches your search terms is highlighted in the selected node list.
   - Click Filter to load a list that includes only the nodes that match your search terms.
   - Click Clear to reload the complete node list and remove your search terms.

Extended Network Neighborhood Search

When enabled, extended network neighborhood search gives users the option to search for and access nodes on any member of the neighborhood, using the Access Client only, across all supported browsers.

When performing the search, you can specify whether the search is extended to all members "In Neighborhood" or "Local Only".

Status and availability and node data for neighbor nodes is displayed when neighborhood search results are retrieved as the result of performing an extended network neighborhood search. This data is not updated in real-time for neighbor nodes while search results are displayed.

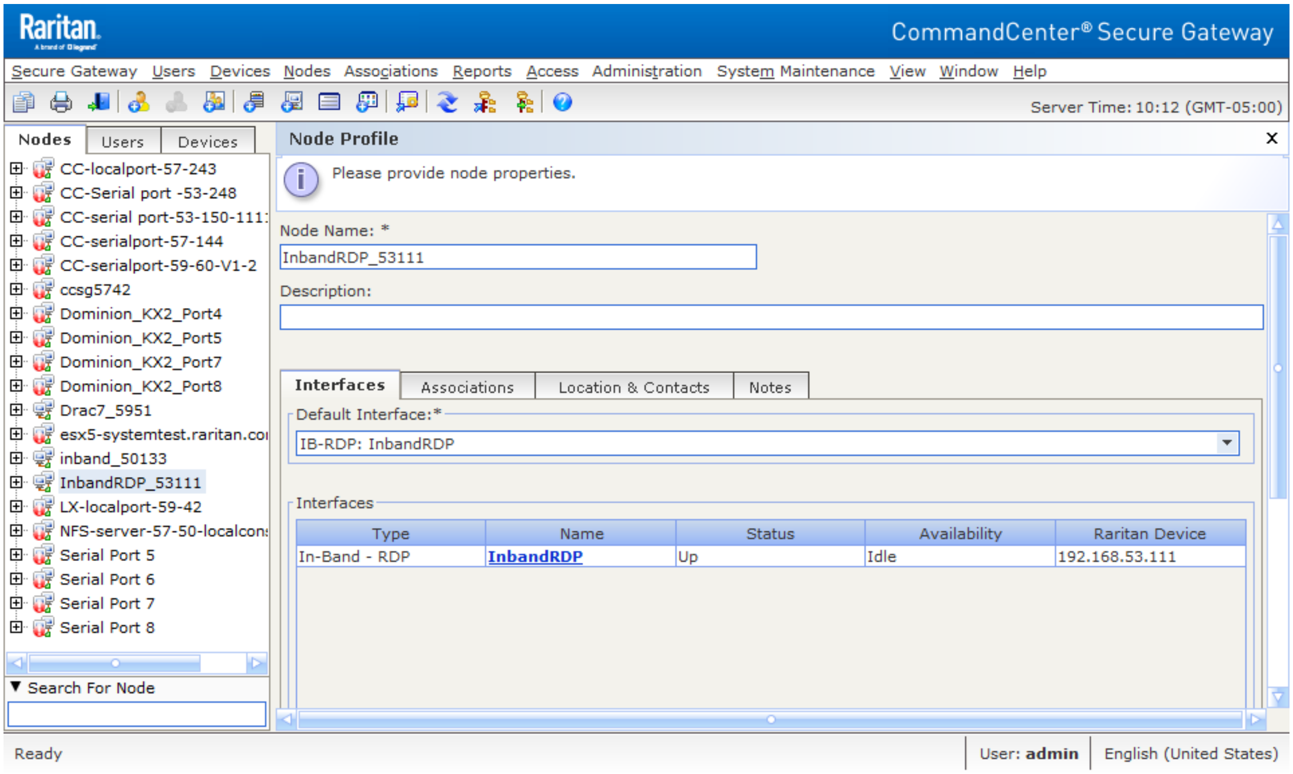
Note: The node's Virtual Machine Data will only be displayed for VM nodes on the home CC-SG, not for the VM nodes from a neighbor CC-SG.

When performing power control operations on the All Nodes group, while extended neighborhood search is in effect, nodes from neighbor CC-SG units will not be included. The All Nodes group is created on the "home" CC-SG only, and cannot contain neighbor nodes.

Finding and Viewing Nodes in the Admin Client

When you log into the Admin Client as a user without administrative permissions, the Nodes tab on the left will be populated with all the nodes you can access. The menus will vary based on your other permissions.

CC-SG Admin Client Screen Overview



Server Time: 10:12 (GMT-05:00)

Please provide node properties.

Node Name: * InbandRDP_53111

Description:

Default Interface:* IB-RDP: InbandRDP

Interfaces

Type	Name	Status	Availability	Raritan Device
In-Band - RDP	InbandRDP	Up	Idle	192.168.53.111

User: admin

English (United States)

1. Nodes tab: Click the Nodes tab to display all nodes in a tree view. Interfaces are grouped under their parent nodes. Click + and - to expand or collapse the tree. Click a node to view the Node Profile. Right-click an interface and select Connect to connect to that interface. You can sort the nodes by Node Name (alphabetically) or Node Status (Available, Busy, Unavailable). Right-click the tree view, click Node Sorting Options, and then click By Node Name or By Node Status.
2. Quick Commands toolbar: This toolbar offers shortcut buttons for executing common commands.
3. Operation menu bar: These menus contain commands to operate CC-SG. You can access some of these commands by right-clicking on the icons in the Nodes selection tab. The menus and menu items you see are determined by your user access privileges.
4. Main Display area: The commands you select from the menu bar and the tool bar display in this main area.
5. Server Time: The current time and time zone as configured on CC-SG. This time may be different than the time used by the client.

Node Icons

For easier identification of status, different-colored icons appear in the nodes tree.

Icon	Meaning
🖥	Node available - the node has at least one interface that is available.
🖥	Node unavailable - all interfaces for the node are busy.

Node Views

All nodes to which you have access appear in the Nodes tab in the left panel of the CC-SG Admin Client.

By default, nodes are arranged in a standard Tree View. The standard Tree View displays nodes in alphabetical order. If you want nodes to appear in a different order, you can create a Custom View. Custom Views allow you to specify different grouping of nodes, based on the categories they have been assigned to by the CC-SG Administrator. See ***Using Custom Views in the Admin Client*** (on page 25).

In both the Tree View and the Custom Views, you can also sort nodes by name or by status.

Tree View

The standard Tree View displays nodes in alphabetical order. To apply the Tree View to the Nodes tab:

- Choose Nodes > Change View > Tree View. The Tree View of the Nodes tree appears.
  - Nodes are arranged alphabetically by name.
  - Interfaces are grouped under their parent nodes. Click the + and - signs to expand or collapse each grouping.
  - Click the Expand and Collapse icons in the toolbar at the top of the screen to expand and collapse the entire tree.

Node Sorting Options

In both Tree View or Custom View, you can sort nodes either alphabetically or by availability status.

- Right-click in an empty area of the Nodes tab, click Node Sorting Options, and then click By Node Name or By Node Status.
  - By Node Name arranges nodes alphabetically by their names.

- By Node Status arranges nodes by their availability status: Available, Busy, and Unavailable.

Searching for Nodes

The CC-SG Search function allows you to search for nodes that match your search terms. CC-SG offers two search types, Filter by Search Results and Find Matching String.

- Filter by Search Results: type search terms and then click Search to display a list of nodes that match your search terms. You can use wildcards (*) with this search type.
- Find Matching String: type search terms and as you type, the node in the list that best matches your search is highlighted. There is no Search button. You cannot use wildcards with this search type.

You can set your search preference in your CC-SG profile. To access your profile, choose Secure Gateway > My Profile. See ***Set Search Preference*** (on page 104).

Search for a Node

1. Click the Nodes tab.
2. Type a search string in the Search for Node field.
3. Depending on your search preference, the Nodes tree will either highlight the first node that matches your search terms, or you can click Search to filter the list of nodes to display only those nodes that match your search terms.

Supported Wildcards for Node Search

These wildcards are supported when you have Filter by Search Results set as your search preference in My Profile. See ***Set Search Preference*** (on page 104).

Wildcard	Description	Sample Search Terms	Sample Search Result
?	Indicates any character.	Solaris?	Locates Solaris1, and SolarisN, but not Solaris1Z
[-]	Indicates a character in range.	Windows[0-9][0-9][0-9][0-9]	Locates Windows2016 only
*	Indicates zero or more characters.	Windows*	Locates Windows2016 and Windows2019 Server

Bookmarking an Interface

If you frequently access a node via a particular interface, you can bookmark it so that it is readily available from your browser.

► **To bookmark an interface in any browser:**

1. In the Nodes tab, select the interface you want to bookmark. You must expand the node to view the interfaces.
2. Choose Nodes > Bookmark Node Interface.
3. Select Copy URL to Clipboard.
4. Click OK. The URL is copied to your clipboard.
5. Open a new browser window and paste the URL into the address field.
6. Press the Enter key to connect to the URL.
7. Add the URL as a bookmark (also known as a Favorite) to your browser.

► **To get bookmark URLs for all nodes:**

- You can get bookmark URLs for all nodes in the Node Asset Report. See Node Asset Report.

Custom Views

Custom Views enables you to specify different ways to display the nodes in the left panel, using Categories and Node Groups set up by the Administrator.

CC-SG also includes a Tree View, which sorts the nodes in alphabetical order. You cannot change or delete the Tree View.

Types of Custom Views

There are two types of custom views: Filter by Node Group and View by Category.

View by Category

All nodes described by the categories you specify will appear in the nodes list when a View by Category custom view is applied. Nodes that do not have a category assigned will appear as "unassociated."

What are Categories?

CC-SG Administrators can set up Associations to help organize equipment. Each Association includes a Category, which is the top-level organizational group, and its related Elements, which are subsets of a Category. If the administrator has assigned Categories and Elements to nodes, you can set up custom views that display nodes according to the categories to which they belong.

All Categories and Elements assigned to a node are listed in the node details screen. See ***CC-SG Access Client Overview*** (on page 15).

Filter by Node Group

Only the node groups you specify will appear in the nodes list when a Filter by Node Group custom view is applied. The first level of organization is the node group name. A node may appear several times in the list if the node belongs to more than one node group defined in the custom view. Nodes that do not belong to a node group specified by the custom view will not appear in the list.

What are Node Groups?

CC-SG Administrators can set up Node Groups to help organize nodes. If the administrator has set up Node Groups, you can define custom views that specify which Node Groups you want to see in the nodes lists, and in what order the groups appear in the list.

Using Custom Views in the Access Client

Add a Custom View

1. Click the Custom View tab.
2. Click Add to open the Add View window.
3. Select Filter by Node Group to create a custom view that displays only the node groups you specify. Select View by Category to create a custom view that displays nodes according to the categories you specify.
4. Type a name for the custom view in the View Name field, and then click OK. The new custom view name displays in the View Name field in the Custom View screen.
5. In the Available list, select the item that you want to add to the custom view, and then click Add to move it to the Selected list. Repeat this step until you have added all necessary categories or node groups to the Selected list.
6. Arrange the items in the Selected list in the order in which each grouping will appear in the All Nodes list. Select an item in the Selected list and click the up and down arrows to move the item into the desired sequence.

7. If you have the Device, Port, and Node Management Privilege, you can select the System View checkbox to assign this custom view as a system-wide default view. **Optional**
8. Click Save to save the new custom view.

Apply a Custom View

1. Click the Custom View tab.
2. Click the View Name drop-down arrow and select from the list the custom view you want to apply to the All Nodes list.
3. Click Apply View to sort the All Nodes list according to the selected custom view.

Change a Custom View

You cannot change the Tree View.

1. Click the Custom View tab.
2. The View Name field displays the name of the custom view whose categories are listed in the View by Category section of the screen.
3. To change the sequence in which each category or node group appears in the All Nodes list, click an item in the Selected list and click the up and down arrows to move the item into the desired sequence.
4. To add an item to the custom view, select it in the Available list and click Add to move the item into the Selected list.
5. To remove an item from the custom view, select it in the Selected list and click Remove.
6. Click Save to save your changes.

Change a Custom View's Name

1. Click the Custom View tab.
2. Click the View Name drop-down arrow and select the custom view whose name you want to change from the list.
3. Click Edit to open the Edit View dialog.
4. Type a new name for the custom view in the View Name field, and then click OK.

Delete a Custom View

1. Click the Custom View tab.
2. Click the View Name drop-down arrow and select the custom view you want to delete from the list.
3. Click Delete. You cannot delete the Tree View.

Assign a Default Custom View

1. Click the Custom View tab.
2. Click the View Name drop-down arrow and select the custom view you want to assign as the default view from the list.
3. Click Set as Default.

Assign a Default Custom View for All Users

If you have CC Setup and Control privileges, you can assign a default custom view for all users.

1. Click the Custom View tab.
2. Click the View Name drop-down arrow and select the custom view you want assign as a system-wide default view.
3. Check the System View checkbox.
4. Click Save.

   All users who log into CC-SG will see the All Nodes list sorted according to the Categories specified in the selected custom view. Users can still change the custom view.

All Nodes List in Extended Network Neighborhood

When Extended Network Neighborhood is enabled, the CC-SG Access Client does not provide the ability to extend the use of node groups or categories, such as in a Custom View, beyond the "home" CC-SG the user is logged into.

The All Nodes list is a local group and only comprises nodes on the "home" CC-SG.

Using Custom Views in the Admin Client

Add a Custom View for Nodes

To add a custom view for nodes:

1. Click the Nodes tab.
2. Choose Nodes > Change View > Create Custom View. The Custom View screen appears.
3. In the Custom View panel, click Add. The Add Custom View window opens.
4. Type a name for the new custom view in the Custom View Name field.
5. In the Custom View Type section:
   - Select Filter by Node Group to create a custom view that displays only the node groups you specify.
   - Select View by Category to create a custom view that displays nodes according to the categories you specify.

6. Click OK.
7. In the Custom View Details section:
    a. In the Available list, select the item you want to include in the custom view, and then click Add to add the item to the list. Repeat this step to add as many items as you want.
    b. Arrange the items in the Selected list in the order you would like each grouping to display in the Nodes tab. Select an item and click the up and down arrow buttons to move the item into the desired sequence.
    c. If you must remove an item from the list, select it and click Remove.
8. Click Save. A message confirms that the custom view has been added.
9. To apply the new custom view, click Apply View.

Apply a Custom View for Nodes

▶ To apply a custom view to the nodes list:

1. Choose Nodes > Change View > Custom View. The Custom View screen appears.
2. Click the Name drop-down arrow and select a custom view from the list.
3. Click Apply View.

or

- Choose Nodes > Change View. All defined custom views are options in the pop-up menu. Choose the custom view you want to apply.

Change a Custom View for Nodes

1. Click the Nodes tab.
2. Choose Nodes > Change View > Create Custom View. The Custom View screen appears.
3. Click the Name drop-down arrow and select a custom view from the list. Details of the items included and their order appear in the Custom View Details panel

▶ To change a custom view's name:

1. In the Custom View panel, click Edit. The Edit Custom View window opens.
2. Type a new name for the custom view in the Enter new name for custom view field, and then click OK. The new view name appears in the Name field in the Custom View screen.

▶ To change the custom view's contents:

1. In the Custom View Details section:
    a. In the Available list, select the item you want to include in the custom view, and then click Add to add the item to the list. Repeat this step to add as many items as you want.

    b. Arrange the items in the Selected list in the order you would like each grouping to display in the Nodes tab. Select an item and click the up and down arrow buttons to move the item into the desired sequence.
    c. If you must remove an item from the list, select it and click Remove.
2. Click Save. A message confirms that the custom view has been added.
3. To apply the new custom view, click Apply View.

Delete a Custom View for Nodes

To delete a custom view for nodes:

1. Click the Nodes tab.
2. Choose Nodes > Change View > Create Custom View. The Custom View screen appears.
3. Click the Name drop-down arrow, and select a custom view from the list. Details of the items included and their order appear in the Custom View Details panel
4. In the Custom View panel, click Delete. The Delete Custom View confirmation message appears.
5. Click Yes.

Assign a Default Custom View for Nodes

To assign a default custom view for nodes:

1. Click the Nodes tab.
2. Choose Nodes > Change View > Create Custom View. The Custom View screen appears.
3. Click the Name drop-down arrow, and select a custom view from the list.
4. In the Custom View panel, click Set as Default. The next time you log in, the selected custom view will be used by default.

Assign a Default Custom View of Nodes for All Users

If you have the CC Setup and Control privilege, you can assign a default custom view for all users. The System View is set as default view for all user until each user sets their own default view.

To assign a default custom view of nodes for all users:

1. Click the Nodes tab.
2. Choose Nodes > Change View > Create Custom View.
3. Click the Name drop-down arrow, and select the custom view you want assign as a system-wide default view.
4. Select the System View checkbox, and then click Save.

All users who log into the CommandCenter Secure Gateway will see the Nodes tab sorted according to the selected System View (Custom View set as System View).

Connecting to Nodes

There are several methods for connecting to nodes, depending on which client you are using. However, once you connect, the workflow for each interface type is the same with either client. See ***Understanding Interfaces*** (on page 75).

See ***Connecting to Nodes using the Access Client*** (on page 30), ***Connecting to Nodes using a Mobile Device*** (on page 71), and ***Connecting to Nodes using the Admin Client and the Desktop Admin Client*** (on page 72) to learn each client's connection methods.

Then review the following sections to learn the workflow and see the typical applications for each interface type. See ***Applications for Accessing Nodes*** (on page 73).

- ***Connect to a Node via an Out-of-Band KVM Interface*** (on page 77)
- ***Connect to a Node via an Out-of-Band Serial Interface*** (on page 80)
- ***Connect to an iLO Processor Enabled Node*** (on page 81)
- ***Connect to a Node via an In-Band KVM Interface*** (on page 81)
- ***Connect to a Node via a Web Browser Interface*** (on page 88)

Power Control for nodes is handled differently, based on which client you are using. See ***Power Control for Nodes Using the Access Client*** (on page 93) and ***Power Control for Nodes Using the Admin Client*** (on page 96).

See Interface Types and Abbreviations for details on identifying interfaces that have the same name.

In This Chapter

Connecting to Nodes using the Access Client

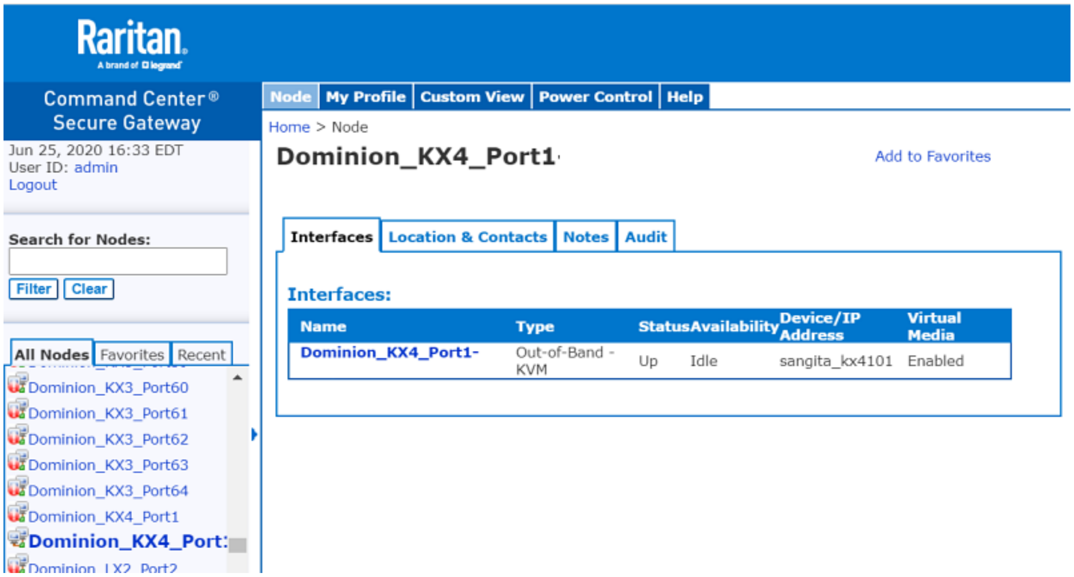
There are two ways to connect to a node in the Access Client. Each of these options launches the associated application and connects to the node.

- Double-click the node in one of the nodes lists in the left panel.
- Click the Name link in the Interfaces section of the node details screen.

Node Profile Screen Overview: Access Client

In the Access Client, you can view all node details in the Node tab.

Click a node in one of the node lists in the left panel (All Nodes, Favorites, and Recent) to open the Node profile screen. Click the Node tab at the top of the screen to return to the Node profile screen after viewing other tabs.



Jun 25, 2020 16:33 EDT
User ID: admin
Logout

Dominion_KX4_Port1

Name	Type	Status	Availability	Device/IP Address	Virtual Media
Dominion_KX4_Port1-	Out-of-Band - KVM	Up	Idle	sangita_kx4101	Enabled

Displayed Information and Features

- The selected node’s name appears at the top of the Node profile screen. You can add the node to the Favorites list by clicking Add to Favorites. See ***Favorite Nodes List*** (on page 16).
- If the selected node is a blade chassis, the name of the device managing the blade chassis appears below the node name.
- If the selected node is a blade server, the name of the blade chassis where the server resides appears. A slot number may also appear based on the blade server model.
- You can chat with other users who are connected to the same node as you. See ***Node Chat Using the Access Client*** (on page 100).
- You can access help by expanding the Help section at the bottom of the node profile or by clicking the Help tab to view all help topics.

Tabs

- The Interfaces tab lists the connection Type, Name, Status, Availability, and Device/IP Address for interfaces associated with the selected node. The Device/IP Address column lists device names for out-of-band interfaces and embedded server IP address for in-band interfaces. If a node has virtual media capabilities, a Virtual Media column lists the status, Enabled or Disabled. If you want to connect to the node, click the Name link to open the associated application and connect to the node. The Power Control section lists all power sources for the selected node. When a node has two or more power interfaces, the Advanced link displays next to the Power Control section. See ***Power Control for Nodes Using the Access Client*** (on page 93).
- The Associations tab lists the Categories and Elements associated with the selected node. CC-SG Administrators can set up Associations to help organize the equipment that CC-SG manages. Each Association includes a Category, which is the top-level organizational group, and its related Elements, which are subsets of a Category. You can use Associations to create Custom Views that help you organize the All Nodes list in different ways. See ***Custom Views*** (on page 22) for details.
- The Location & Contacts tab contains information about a node's location and contact information, such as phone numbers, that you may need when working on a node.
- The Notes tab contains a tool to add notes about a node for other users to read. All notes appear in the tab with the date, username, and IP address of the user who added the note.
- The Audit tab contains a list of the reasons that a node was accessed. You must enter a reason for access before connecting to a node when the administrator has enabled node auditing for your user group. The Audit tab is hidden if the feature is disabled, or if no reasons for access have been entered.

- The Control System Data tab, Virtual Host Data tab, and Virtual Machine Data tabs appear on nodes in your virtual infrastructure with information about the virtual node. Each tab contains information specific to the Control System, Virtual Host, or Virtual Machine.
- The Blades tab appears on blade chassis nodes and contains information about the blade servers residing in the blade chassis.

Chrome and Edge Browser Limitations

The Chrome and Edge browsers cannot launch in-band interfaces in the Access Client, with one exception. Chrome 53 can launch in-band SSH interfaces.

If you must use the Chrome or Edge browsers for other in-band interfaces, use the Admin client to access.

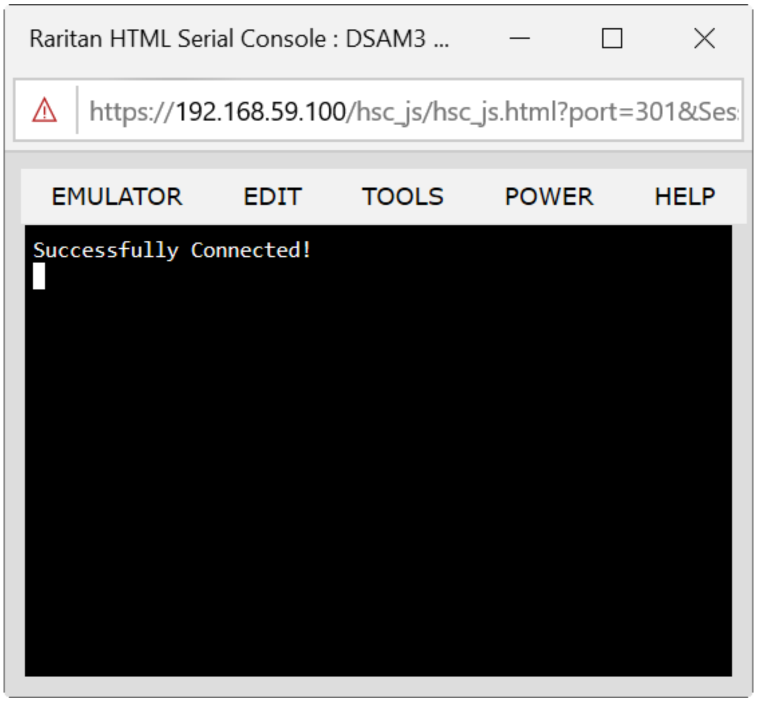
Launching AKC from CC-SG in Edge Browser

To launch the AKC from the Edge browser target device must be:

- KX4-101
- KX3 - 3.2 or later

HTML Serial Console (HSC) Help

You can connect to serial targets using HSC. HSC is supported with several Raritan products that offer serial connections. Not all products support all HSC features. Differences are noted.


Raritan HTML Serial Console : DSAM3 ...
https://192.168.59.100/hsc_js/hsc_js.html?port=301&Ses
EMULATOR
EDIT
TOOLS
POWER
HELP

```
Successfully Connected!
```

Support for CC-SG Proxy and Direct Mode

HKC and HSC support both connection modes, direct and proxy.

HSC Functions

Emulator

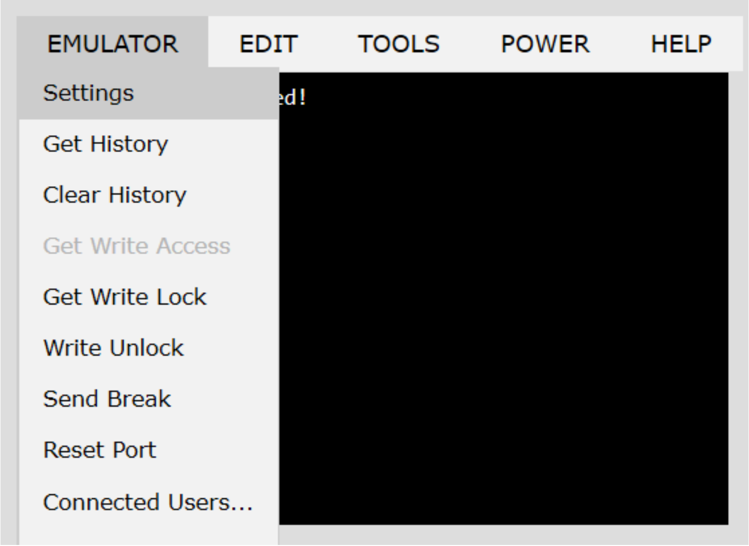
IMPORTANT: HSC sessions are affected by the CommandCenter Secure Gateway Idle Timeout.

If you have not changed the CommandCenter Secure Gateway Idle Timeout setting from the default, your session could be closed automatically if it exceeds the Idle Timeout period.

Change the default Idle Timeout setting and then launch the HSC. See Login Limitations for details on changing the Idle Timeout setting.

Access Emulator Options

1. Select the Emulator drop-down menu to display a list of options.



Settings

Note:

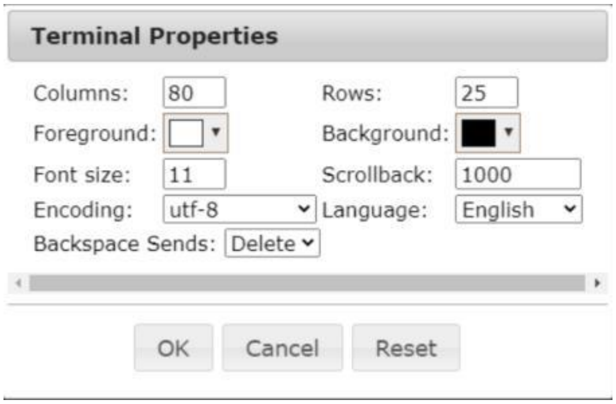
KX3 administrators can set Terminal emulation settings in Setup > Serial Port Configuration.

KX4-101 administrators can set terminal emulation settings in DSAM Serial Ports > Settings.

SX2 administrators can set terminal emulation settings in Device Settings > Port Configuration.

---

1. Choose Emulator > Settings. The Terminal Properties dialog displays the default settings.



Terminal Properties

Columns: 80 Rows: 25

Foreground: □ Background: ■

Font size: 11 Scrollback: 1000

Encoding: utf-8 Language: English

Backspace Sends: Delete

2. Set the terminal size by selecting the number of Columns and Rows. Default is 80 by 25.
3. Set the Foreground and Background colors. Default is white on black.
4. Set the Font size. Default is 11.
5. Set the Scrollback number to indicate the number of lines available for scrolling.
6. Choose one of the following from the Encoding drop-down menu:
   - UTF-8
   - 8-bit ascii
   - ISO-8859-1
   - ISO-8859-15
   - Shift-JIS
   - EUC-JP
   - EUC-KR
7. Choose one of the following from the Language drop-down menu:
   - English
   - Japanese
   - Korean
   - Chinese
   - Bulgarian

8. The Backspace Sends default is ASCII DEL, or you can choose Control-H from the Backspace Sends drop-down menu.
9. Click OK to save. If you changed the Language setting, the HSC changes to that language when the Display Settings window is closed.

The emulator settings are saved on a per port basis in the browser used for HSC, so make sure your browser is not set to delete history on exit.

Get History

History information can be useful when debugging, troubleshooting, or administering a target device. The Get History feature:

- Allows you to view the recent history of console sessions by displaying the console messages to and from the target device.
- Displays up to 512KB of recent console message history. This allows a user to see target device events over time.

When the size limit is reached, the text wraps, overwriting the oldest data with the newest.

Notes: History data is displayed only to the user who requested the history.

To view the Session History, choose Emulator > Get History.

Clear History

- To clear the history, choose Emulator > Clear History.

Get Write Access

Only users with permissions to the port get Write Access. The user with Write Access can send commands to the target device. Write Access can be transferred among users working in the HSC via the Get Write Access command.

To enable Write Access, choose Emulator > Click Get Write Access.

- You now have Write Access to the target device.
- When another user assumes Write Access from you:
  - The HSC displays a red block icon before Write Access in the status bar.
  - A message appears to the user who currently has Write Access, alerting that user that another user has taken over access to the console.

Get Write Lock

Write lock prevents other users from taking the write access while you are using it.

1. To get write lock, choose Emulator > Get Write Lock.
2. If Get Write Lock is not available, a request rejected message appears.

Write Unlock

To get Write Unlock, choose Emulator > Write Unlock.

Send Break

Some target systems such as Sun Solaris servers require the transmission of a null character (Break) to generate the OK prompt. This is equivalent to issuing a STOP-A from the Sun keyboard.

Only users with Write Access privileges can send a break.

To send an intentional “break” to a Sun Solaris server:

1. Verify that you have Write Access. If not, follow the instructions in the previous section to obtain write access.
2. Choose Emulator > Send Break. A Send Break Ack (Acknowledgement) message appears.
3. Click OK.

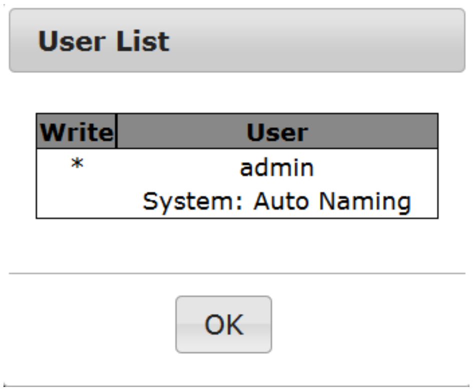
Reset Port

Reset Port resets the physical serial port on the SX2 and re-initializes it to the configured values regarding bps/bits, and so on.

Connected Users

The Connected Users command allows you to view a list of other users who are currently connected on the same port.

1. Choose Emulator > Connected Users.



Write	User
*	admin
	System: Auto Naming

2. A star appears in the Write column for the User who has Write Access to the console.

Exit

1. Choose Emulator > Exit to close the HSC.

Copy and Paste and Copy All

Data on the current visible page can be selected for copying. Copy and Paste are accessible in the HSC by right click in the terminal window. Select Copy or Paste in the context menu that appears.

To copy all text, use the Copy All option in the Edit menu.

If you need to paste a large amount of data, it is better to save the data in a file and use the Send a Text File function. Pasting a large amount of data in a browser windows can cause the browser to hang as it processes the data. See ***Send Text File*** (on page 37).

When pasting data to a port, the end of a line is sent as a carriage return.

The Cut option on the right-click menu is disabled.

Do not use the Delete option that appears in the right-click menu of IE and some versions of Firefox. This Delete option will remove display lines entirely from the emulator window.

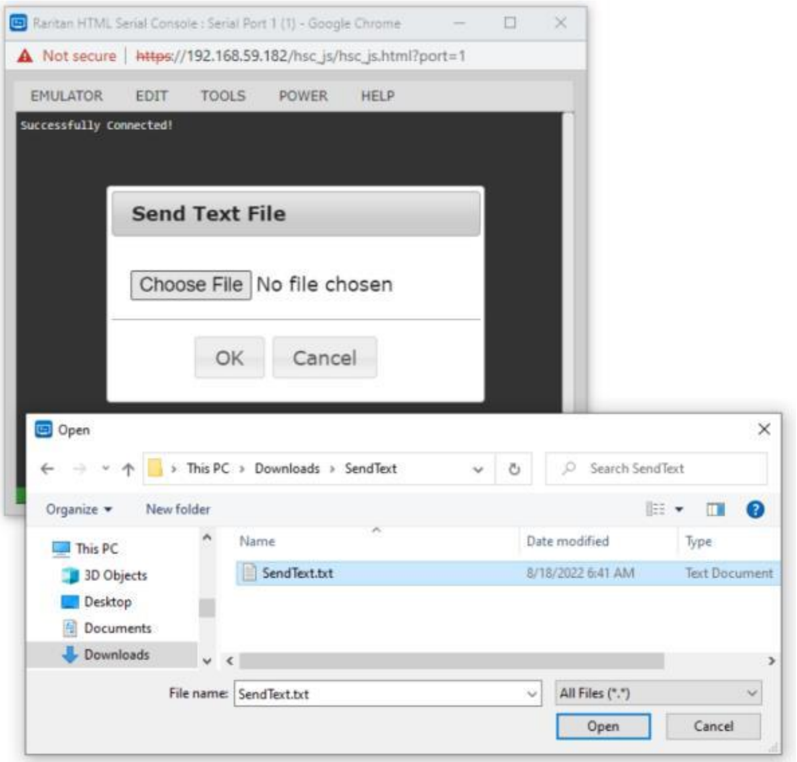
▶ Browser-specific behaviors

When copying from IE or Edge browsers, there are no end of line characters in the copied data. The pasted data appears to be all in one line and contains many spaces. When pasting back into a HSC window, the data may appear to be misaligned, but the data is complete.

Send Text File

1. Select Edit> Send Text File.
2. In the Send Text File dialog, click Browse to find the text file.
3. Click OK.
   - When you click OK, the selected file sends directly to the port.

- If there is currently no target connected, nothing is visible on the screen.



Raritan HTML Serial Console : Serial Port 1 (1) - Google Chrome

Not secure | ~~https~~://192.168.59.182/hsc_js/hsc_js.html?port=1

```
Successfully Connected!
```

Send Text File

Choose File No file chosen

This PC › Downloads › SendText

Name	Date modified	Type
SendText.txt	8/18/2022 6:41 AM	Text Document

File name: SendText.txt

All Files (*.*)

▶ **Note, if you are using a Mac® and/or Safari®, do the following in order to use this feature:**

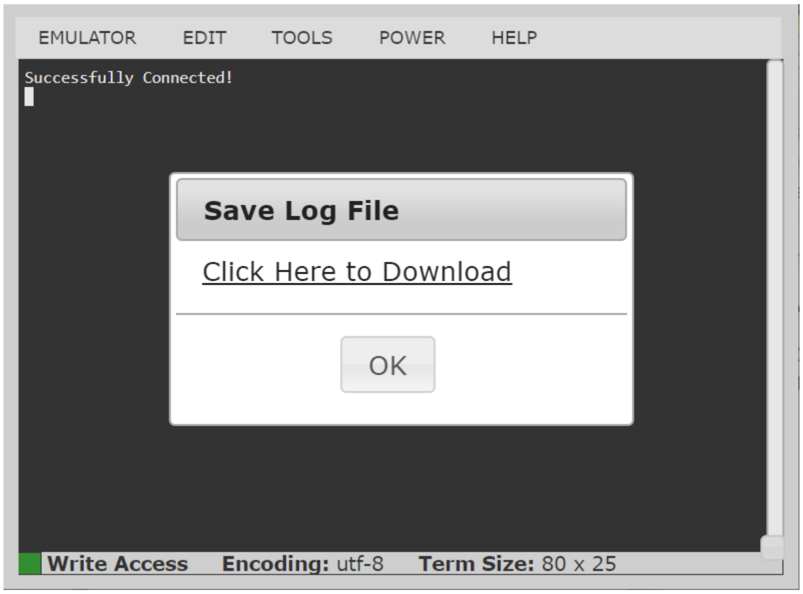
1. In Safari, select Preferences.
2. Under the Security tab, select "Manage Website Settings"
3. Click on the CommandCenter Secure Gateway website.
4. Select "Run in unsafe mode" from the drop-down box.
5. Restart Safari.

Tools: Start and Stop Logging

The Tools menu contains options for creating a data history file and downloading it.

1. Choose Tools > Start Logging to start the storage of serial port data in memory.

2. Click Stop Logging to save the log file. A pop up message appears with a download link. Click to download the memory buffer into a text file.



```
Successfully Connected!
```

Save Log File

Click Here to Download

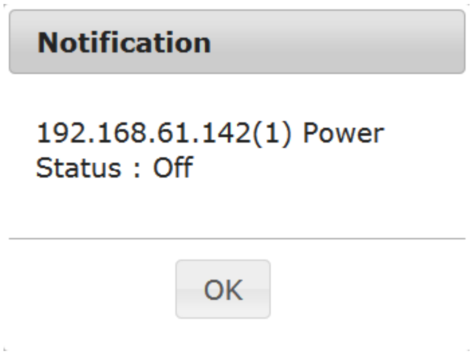
🟩 Write Access Encoding: utf-8 Term Size: 80 x 25

Power Status

Power Status in HSC shows the status of the outlet the target is plugged into.

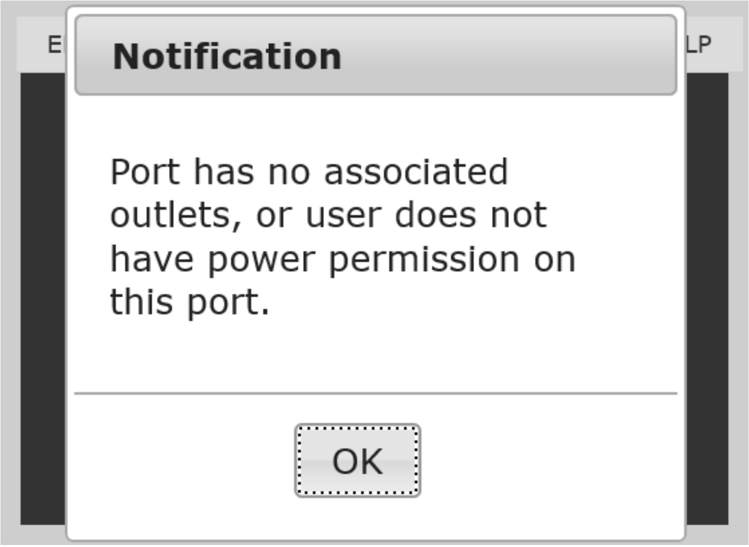
1. Choose Power > Power Status.
2. The Notification dialog shows the status of the outlet as ON or OFF.

Status may also show no associated outlet, or no power permission to the port.



Notification

192.168.61.142(1) Power Status : Off



Notification

Port has no associated outlets, or user does not have power permission on this port.

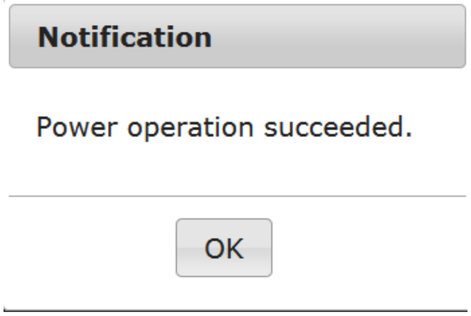
Power on a Target

Use this option to power on a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power On.

2. Click OK in the success message.



Notification

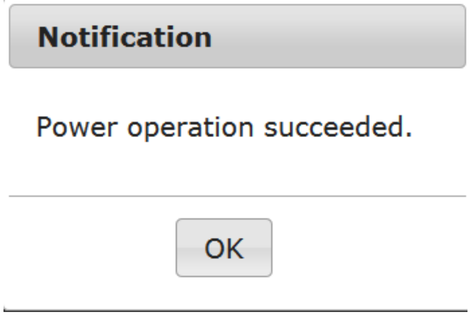
Power operation succeeded.

Power Off a Target

Use this option to power off a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power Off.
2. Click OK in the success message.



Notification

Power operation succeeded.

Power Cycle a Target

Power cycling allows you to turn a target off and then back on through the outlet it is plugged into.

This option is visible only when -

- there are one or more power associations to the target
- the target is already powered on (the port status us Up)
- you have permission to manage the target's power

1. Choose Power> Power Cycle.
2. Click OK in the success message.

HTML KVM Client (HKC)

The HTML KVM client (HKC) provides KVM over IP access that runs in the browser without the need for applets or browser plugins. HKC uses Javascript, NOT Java.

HKC runs on Linux and Mac clients, and on Windows clients in Internet Explorer 11, Edge, Firefox, Chrome and Safari browsers.

A mobile version of HKC also runs on iOS v10 and higher. See KVM Client Launching for a full matrix of clients.

Many KVM features are supported. Future releases will provide more advanced KVM features.

▶ **Supported Features:**

- Connection Properties
- USB Profiles
- Video Settings
- Input Settings
- Audio Playback
- Virtual Media
- Dual Video Targets
- Keyboard Macros
- Import and Export of Keyboard Macros
- Send Text to Target
- Keyboard and Mouse Settings
- Single Mouse Mode - not available on IE browser
- Power Control

▶ **Not supported:**

- Port Scanning
- Smartcard
- Limited Tools Menu options.
- Limited keyboard support: US-English, UK-English, French, German, Swiss-German, and Japanese are supported
- Hotkeys for keyboard macros
- Pre-populated keyboard macros for Sun targets
- Can only create Macros from keys that exist on the client PC (US-English, UK-English, French, German), no special function keys except for delay key.
- Single Mouse mode - not available on IE
- Virtual Media write not supported
- Local file transfer not supported on IE11.
- USB drive connects

- Favorites
- Audio capture, No audio support on IE.

Tips and Known Issues:

- Ensure that the device certificate is installed and trusted. The certificate Common name should match the IP address/Hostname used to connect to the device. See SSL and TLS Certificates for information on creating and installing certificates
- When Single Mouse Mode in the Edge browser is selected for the first time, the user is prompted to turn off the local mouse pointer. Select the bottom part of the Yes button.
- Target connections from Chrome 61 running on Fedora requires HardWare Acceleration to be enabled.
- If erratic mouse response is seen in Single Mouse mode on Fedora clients using the default Gnome desktop, use the Gnome classic desktop.
- To enable scrollbars on Mac Browser target connections: On the OS menu bar, choose System Preferences > General > Show scroll bars: Always.
- Internet Explorer and Edge support only 6 sessions at a time. The error displayed when attempting to connect to a seventh target is "Error could not connect to target." For IE11, you can increase the sessions allowed in the Group policy editor. See https://jwebsocket.org/documentation/reference-guide/internet-explorer-tips.
- For IE11 and Edge IPv6 device connections, either use device hostname or literal IPv6 as UNC. See https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names
- For Mac/Safari IPv6 device connections, use device hostname.
- Client Keyboard input selection should be set for each device individually.
- If encountering issues on browsers that have previously connected to an older version, it may be necessary to clear the Cache Web Content from the browser.
- To launch HKC automatically in Safari browser: Use http://<IP Address>/hkc, OR use http://<IP Address>/ if "Java content on browser" is disabled in Java Control Panel, and "Java Plugin" is disabled in the browser.
- From Chrome running on Linux, to get ´ ` or ^, the key needs to be hit three times, or twice followed by a space.
- On a default build of Redhat 7/Firefox ESR 24.5, there is no target video displayed on HKC connections. Older versions of Firefox lack HTML5 functions needed to support HKC. Upgrade Firefox to the latest available version.
- If HKC does not load, but rather displays a white screen, your browser memory may be full. Close all browser windows and try again.

- In Chrome, disable the background throttling to prevent background tabs from disconnecting after a certain amount of time. Go to chrome://flags, then search for "throttle". Set "Throttle Javascript timers in backgound" and "Calculate window occlusion on Windows" to "Disabled". Restart chrome to apply settings.

Support for CC-SG Proxy and Direct Mode

HKC and HSC support both connection modes, direct and proxy.

Known Issues: HKC with CC-SG

- Audio pauses on Chrome and Safari HTML Client connections if HTML menu displays a pop-up message. If message is left for over 30 seconds without a response, the KVM connection is closed
- Unable to launch HKC connections over IPv6.
- Unable to launch HKC connection from IE if port has # character in name.
- When accessing using a mobile device, HKC target connections are closed after about 1 min if browser is in background.
- A blank page with the message "Please wait, connecting to KVM" is displayed from HKC proxy connections from Firefox thick client and also from FF and Chrome bookmark HKC proxy launches.

HKC Versions for Different Devices

HKC menus and options will vary between different devices, such as KX3 versus KX4-101. For specific instructions for your device, check the device user guide.

Connection Properties

Connection properties manage streaming video performance over remote connections to target servers.

The properties are applied only to your connection - they do not impact the connection of other users accessing the same target servers.

If you make changes to connection properties, they are retained by the client.

▶ **To view connection properties:**

- Choose File > Connection Properties.

Default Connection Properties

The CommandCenter Secure Gateway comes configured to provide optimal performance for the majority of video streaming conditions.

KX3 default connection settings:

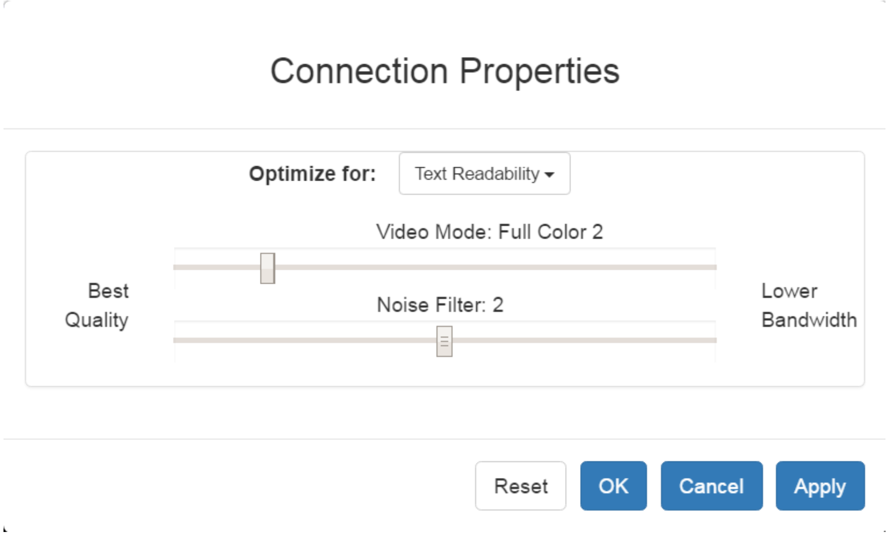
- Optimized for: Text Readability - video modes are designed to maximize text readability.

  This setting is ideal for general IT and computer applications, such as performing server administration.
- Video Mode - defaults to Full Color 2.

  Video frames transmit in high-quality, 24-bit color. This setting is suitable where a high-speed LAN is used.
- Noise Filter - defaults to 2.

  The noise filter setting does not often need to be changed.

Click Reset to regain the default connection properties.



Connection Properties

Optimize for: Text Readability

Video Mode: Full Color 2

Noise Filter: 2

Text Readability

Text Readability is designed to provide video modes with lower color depth but text remains readable. Greyscale modes are even available when applying lower bandwidth settings.

This setting is ideal when working with computer GUIs, such as server administration.

When working in full color video modes, a slight contrast boost is provided, and text is sharper.

In lower quality video modes, bandwidth is decreased at the expense of accuracy.

Color Accuracy

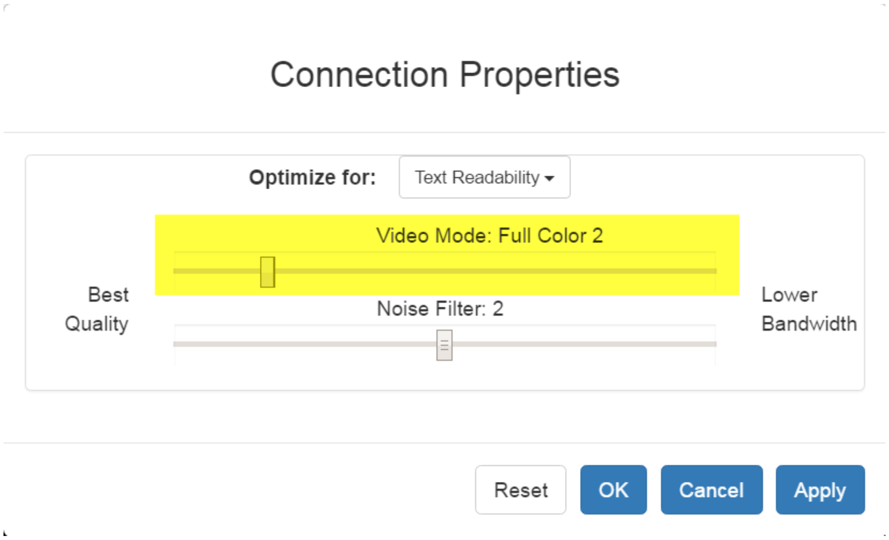
When Color Accuracy is selected, all video modes are rendered in full 24-bit color with more compression artifacts.

This setting applies to viewing video streams such as movies or other broadcast streams.

In lower quality video modes, sharpness of fine detail, such as text, is sacrificed.

Video Mode

The Video Mode slider controls each video frame's encoding, affecting video quality, frame rate and bandwidth.



Connection Properties

Optimize for: Text Readability

Video Mode: Full Color 2

Noise Filter: 2

In general, moving the slider to the left results in higher quality at the cost of higher bandwidth and, in some cases, lower frame rate.

Moving the slider to the right enables stronger compression, reducing the bandwidth per frame, but video quality is reduced.

In situations where system bandwidth is a limiting factor, moving the video mode slider to the right can result in higher frame rates.

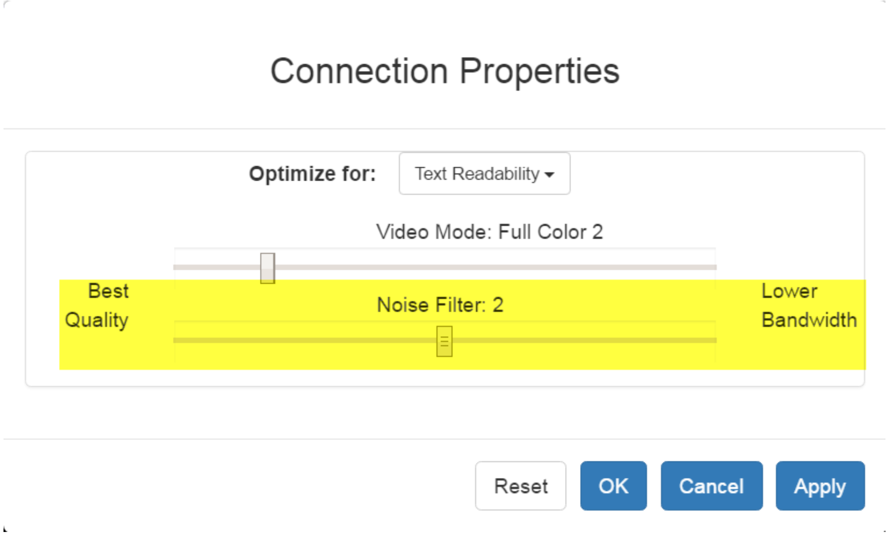
When Text Readability is selected as the Optimized setting, the four rightmost modes provide reduced color resolution or no color at all.

These modes are appropriate for administration work where text and GUI elements take priority, and bandwidth is at a premium.

Noise Filter

Unless there is a specific need to do so, do not change the noise filter setting. The default setting is designed to work well in most situations.

The Noise Filter controls how much interframe noise is absorbed by the CommandCenter Secure Gateway.


Connection Properties

Optimize for: Text Readability

Video Mode: Full Color 2

Noise Filter: 2

Moving the Noise Filter slider to the left lowers the filter threshold, resulting in higher dynamic video quality. However, more noise is likely to come through, resulting in higher bandwidth and lower frame rates.

Moving the slider to the right raises the threshold, allows less noise and less bandwidth is used. Video artifacts may be increased.

Moving the noise filter to the right may be useful when accessing a computer GUI over severely bandwidth-limited connections.

Connection Info

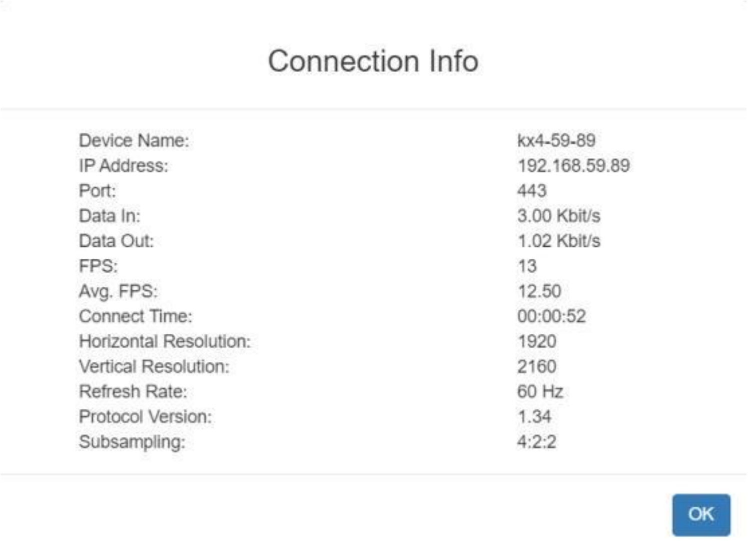
Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See ***Default Connection Properties*** (on page 45) for help configuring the connection properties.

- Name of the device
- IP address of the device
- Port - The KVM communication TCP/IP port used to access the device
- Data In/Second - Data rate received from the device
- Data Out/Second - Data rate sent to the device
- FPS - Video frames per second from the device.
- Average FPS - Average number of video frames per second.
- Connect Time - The duration of the current connection.
- Resolution - The target server's horizontal and vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - communications protocol version.
- Subsampling - Adaptive color subsampling
- Audio Playback Sample Rate - Audio playback sample rate seen if audio is connected.

▶ **To view connection info:**

- Choose File > Connection Info.



Connection Info

Device Name:	kx4-59-89
IP Address:	192.168.59.89
Port:	443
Data In:	3.00 Kbit/s
Data Out:	1.02 Kbit/s
FPS:	13
Avg. FPS:	12.50
Connect Time:	00:00:52
Horizontal Resolution:	1920
Vertical Resolution:	2160
Refresh Rate:	60 Hz
Protocol Version:	1.34
Subsampling:	4:2:2

USB Profile

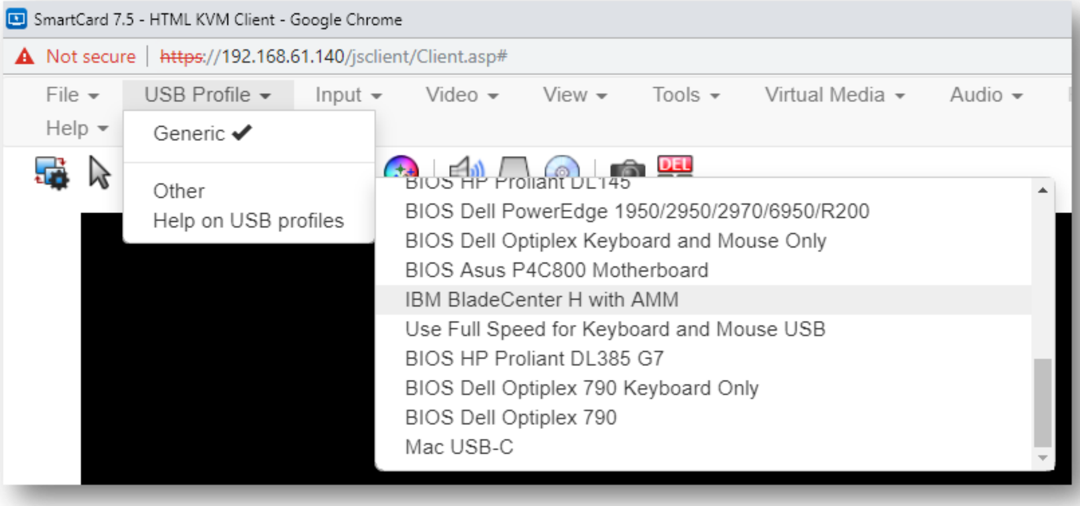
Select a USB profile that best applies to the KVM target server.

For example, if the server is running Windows® operating system, it would be best to use the Generic profile.

Or, to change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

To set a USB profile for a target server:

- Choose USB Profile, then choose Generic, or choose Other Profiles to select from a menu.


SmartCard 7.5 - HTML KVM Client - Google Chrome
Not secure
https://192.168.61.140/jsclient/Client.asp#
File
USB Profile
Input
Video
View
Tools
Virtual Media
Audio
Help
Generic ✔
Other
Help on USB profiles
BIOS HP Proliant DL145
BIOS Dell PowerEdge 1950/2950/2970/6950/R200
BIOS Dell Optiplex Keyboard and Mouse Only
BIOS Asus P4C800 Motherboard
IBM BladeCenter H with AMM
Use Full Speed for Keyboard and Mouse USB
BIOS HP Proliant DL385 G7
BIOS Dell Optiplex 790 Keyboard Only
BIOS Dell Optiplex 790
Mac USB-C
DEL

Note: When using the D2CIM-VUSB-USBC on Mac targets, you must select the "Mac USB-C" profile.

To view details on USB profiles:

Choose USB Profile > Help on USB Profiles.

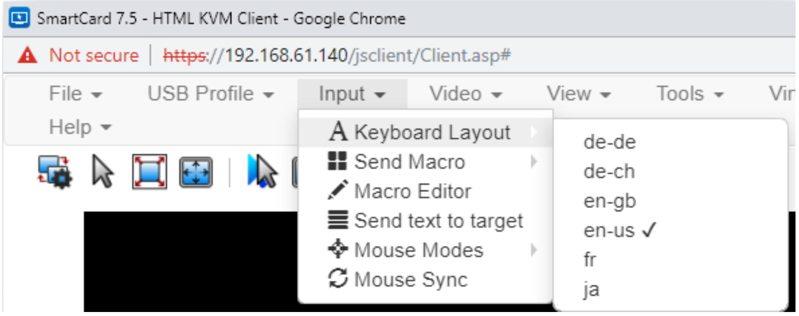
Input Menu

Keyboard Layout

To set your keyboard type.

- Choose Input > Keyboard Layout, then select your keyboard type.
  - de-de
  - de-ch
  - en-gb

- en-us
- fr
- ja

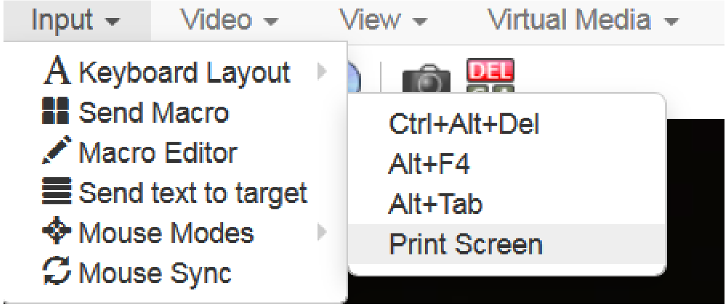


Send Macro

Due to frequent use, several keyboard macros are preprogrammed.

To send a preprogrammed macro:

- Choose Input > Send Macro, then select the macro:
  - Ctrl+Alt+Del: Sends the key sequence to the target without affecting the client.
  - Alt+F4: Closes a window on a target server.
  - Alt+Tab: Switch between open windows on a target server.
  - Print Screen: Take a screenshot of the target server.



Macro Editor

Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by your client PC.

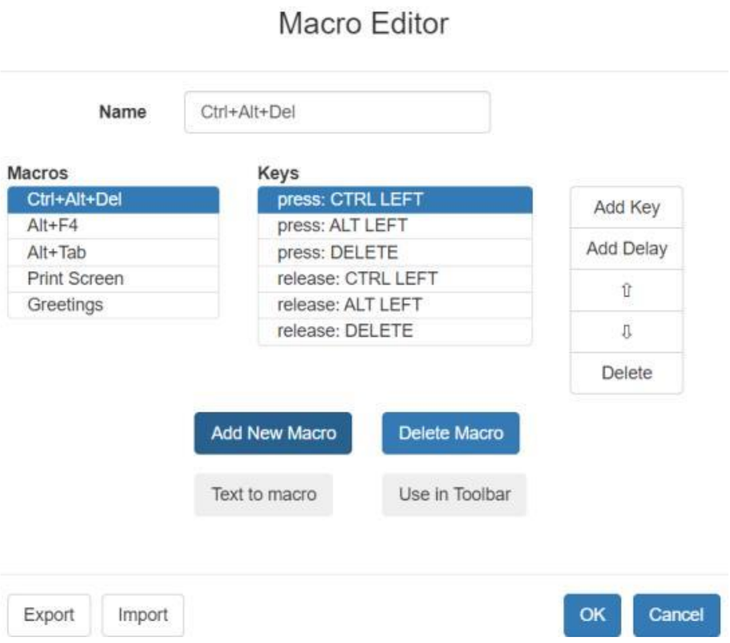
Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one CommandCenter Secure Gateway, your macros will only be available on the browser and CommandCenter Secure Gateway where they were created. To reuse your macros in another CommandCenter Secure Gateway device, you can import and export the macro files. See ***Import and Export Macros*** (on page 54).

To access the Macro Editor:

- Choose Inputs > Macro Editor.
- Select a macro from the Macros list to view the key combination.



Macro Editor

Name: Ctrl+Alt+Del

Macros
- Ctrl+Alt+Del
- Alt+F4
- Alt+Tab
- Print Screen
- Greetings

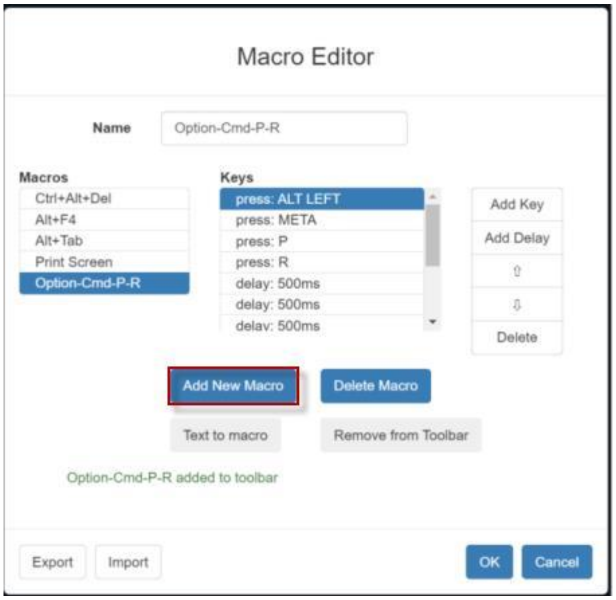
Keys
- press: CTRL LEFT
- press: ALT LEFT
- press: DELETE
- release: CTRL LEFT
- release: ALT LEFT
- release: DELETE

Add New Macro

To add a new macro:

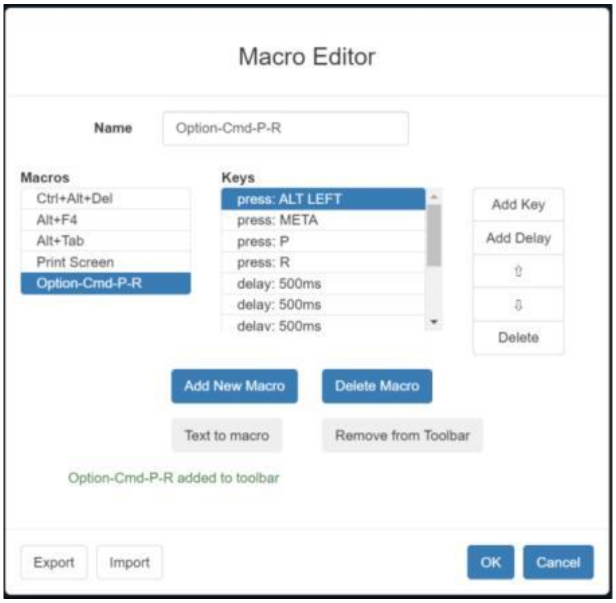
1. Choose Input > Macro Editor.

2. Click Add New Macro.



3. Enter a Name for the new macro. The name will appear in the Send Macro menu once the macro is saved.
4. Click Add Key, then press the key you want to add to the macro. The key press and key release appear in the Keys list.
   - To add more keys, click Add Key again, and press another key.
   - To remove a key, select it in the Keys list and click Delete.
5. To put the keys in the correct sequence, click to select a key in the Keys list, then click the up and down arrows.
6. To add a 500 ms delay to a key sequence, click Add Delay. A delay in the middle of a press-and-release key sequence indicates holding down a key. Add multiple delays to indicate a longer press-and-hold of a key. Click the up and down arrows to move the delays into the correct sequence.

7. Click OK to save. To use this macro from your toolbar, click Use in Toolbar. See Add a Macro to the Toolbar for more details.



Name: Option-Cmd-P-R

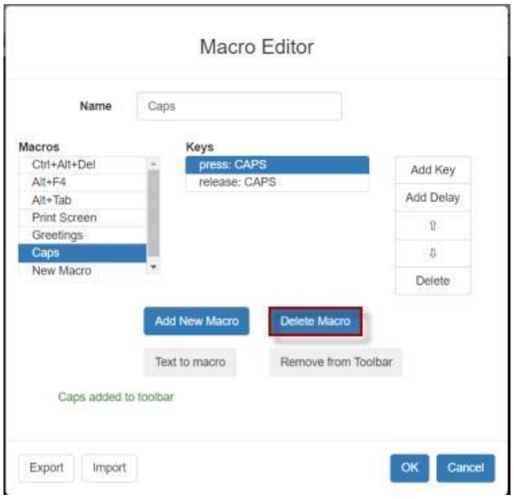
Option-Cmd-P-R added to toolbar

This example shows a macro for a Mac bootup sequence that requires a 2-second delay.

Delete a Macro

▶ To delete a macro:

1. Choose Inputs > Macro Editor.
2. Select the macro, then click Delete Macro.
3. Click OK.



Name: Caps

Caps added to toolbar

Import and Export Macros

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one CommandCenter Secure Gateway, your macros will only be available on the browser and CommandCenter Secure Gateway where they were created. To reuse your macros in another CommandCenter Secure Gateway device, you can import and export the macro files. Imported and exported macro files created on HKC are only compatible with HKC, and cannot be used on AKC or VKC. Likewise, macro files created on AKC or VKC cannot be imported for use on HKC.

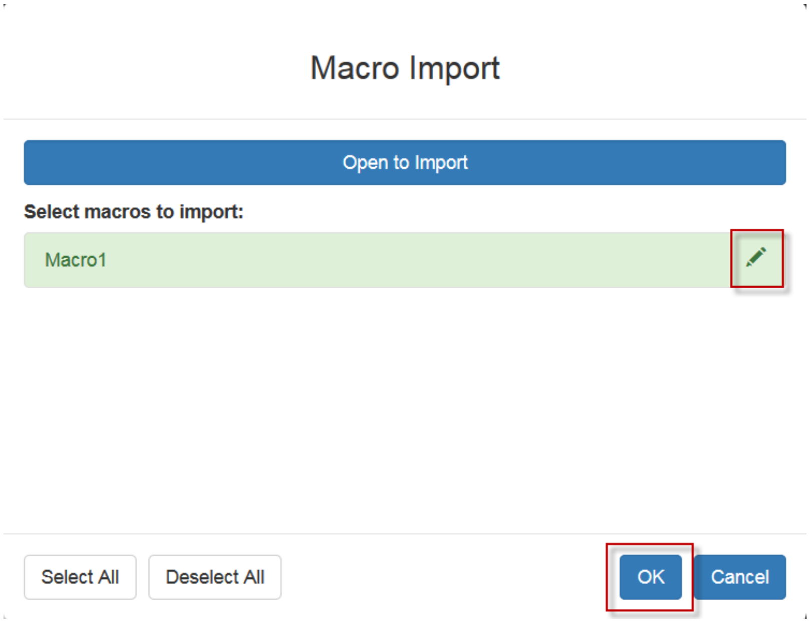
Macros are exported to an xml file named "usermacros.xml". Files are saved in your browser's default download location. Default macros are not exported.

Note: When exporting macros from Edge browser, a Down arrow is briefly displayed at the bottom of the KVM window and a file named "unconfirmed.crdownload" is saved to the default download directory. To use this file as a macro input file, rename it with a .xml extension.

▶ To export and import macros:

1. Choose Input > Macro Editor. The list of macros created for your browser and CommandCenter Secure Gateway displays in the Macro Editor dialog.
2. To export the list, click the Export button, then save the file.
3. Log in to the CommandCenter Secure Gateway where you want to import the macros.
4. Choose Input > Macro Editor.
5. Click Import, then click Open to Import and select the usermacros.xml file, and click OK.
6. The macros found in the file display in the list. Select the macros you want to import, then click OK.

- Macro names must be unique. If a macro with the same name already exists, an error message appears. Click the Edit icon to rename the macro, then click the checkmark to save the name.



Send Text to Target

Use the Send Text to Target function to send text directly to the target. If a text editor or command prompt is open and selected on the target, the text is pasted there.

To send text to target:

1. Choose Input > Send Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target. Supported keyboard characters only.
3. Click OK.

Mouse Modes

You can operate in either single mouse mode or dual mouse mode.

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

When controlling a target server, the Remote Console displays two mouse cursors - one belonging to your CommandCenter Secure Gateway client workstation, and the other belonging to the target server.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

Single mouse mode allows you to view only the target server's pointer. You can use Single mouse mode when other modes don't work.

You can toggle between these two modes (single mouse and dual mouse).

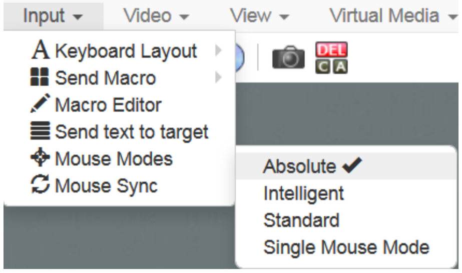
Absolute Mouse Synchronization

In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed. This mode is supported on servers with USB ports and is the default mode for virtual media CIMs.

- Absolute Mouse Synchronization requires the use of a virtual media CIM - D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP, D2CIM-VUSB-USBC

▶ To enter Absolute Mouse Synchronization Mode:

- Choose Input > Mouse Modes > Absolute.

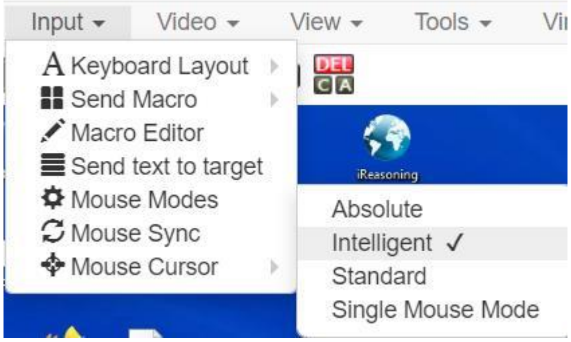


Intelligent

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target.

To enter Intelligent mouse mode:

- Choose Input > Mouse Mode > Intelligent. The mouse will synch. See ***Intelligent Mouse Synchronization Conditions*** (on page 59).



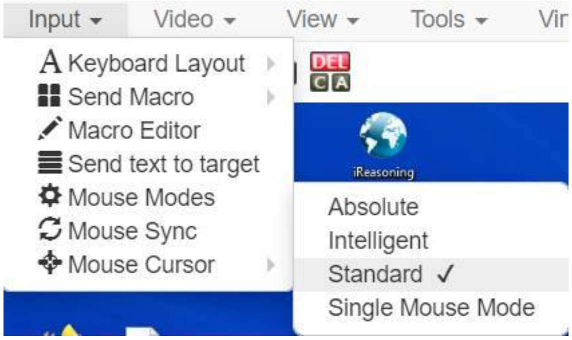
Standard

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target server.

In order for the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

To enter Standard mouse mode:

- Choose Input > Mouse Modes > Standard.



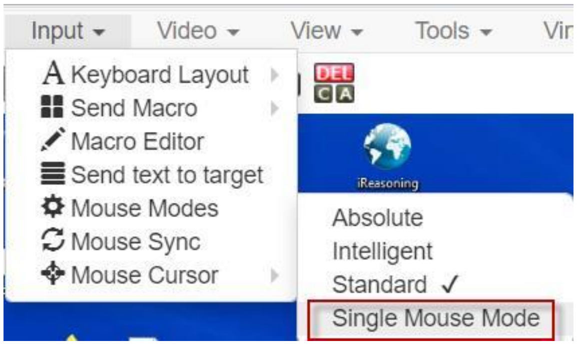
Single

Single Mouse mode uses only the target server mouse cursor; the client mouse cursor no longer appears onscreen.

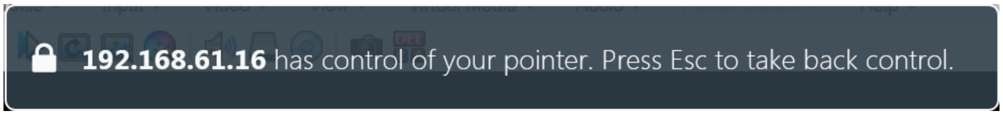
Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine. Single mouse mode is not available on Internet Explorer.

To enter Single mouse mode:

- Choose Inputs > Mouse Modes > Single.



- A message appears at the top of the client window: Press Esc to show your cursor.



192.168.61.16 has control of your pointer. Press Esc to take back control.

To exit Single mouse mode:

- Press Esc.
- Mouse mode changes back to dual mode.

Mouse Sync

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse cursor with the client mouse cursor.

Note: This option is available only in Standard and Intelligent mouse modes.

To synchronize the mouse cursors:

- Choose Inputs > Mouse Sync.

Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- The target advanced mouse properties such as “Enhanced pointer precision" or “Snap mouse to default button in dialogs” should be disabled.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

Video Menu

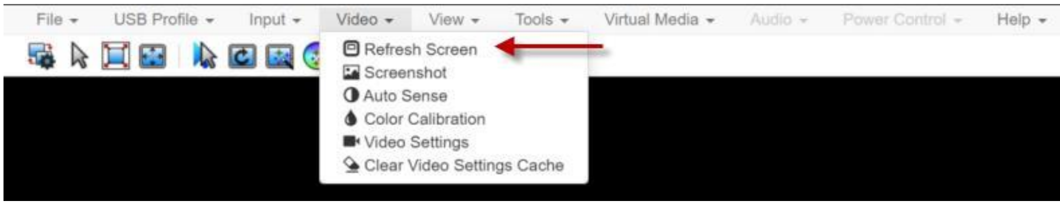
Refresh Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

- The Refresh Screen command forces a refresh of the video screen.
- The Auto-Sense command automatically detects the target server's video settings.
- The Color Calibration command calibrates the video to enhance the colors being displayed.
- In addition, you can manually adjust the settings using the Video Settings command.

▶ To force a refresh of the video screen:

- Choose Video > Refresh Video.



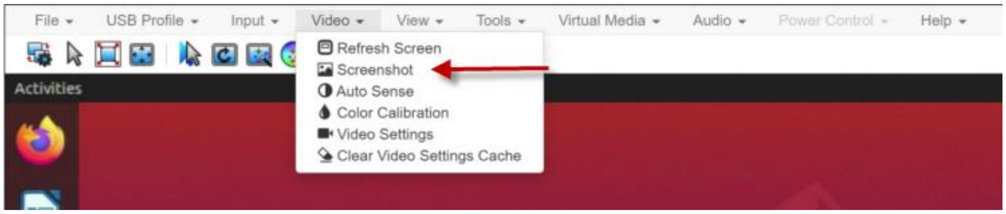
-

Screenshot

Take a screenshot of a target server using the Screenshot command.

▶ To take a screenshot of the target server:

1. Choose Video > Screenshot.
2. The screenshot file appears as a download to view or save. Exact options depend on your client browser.



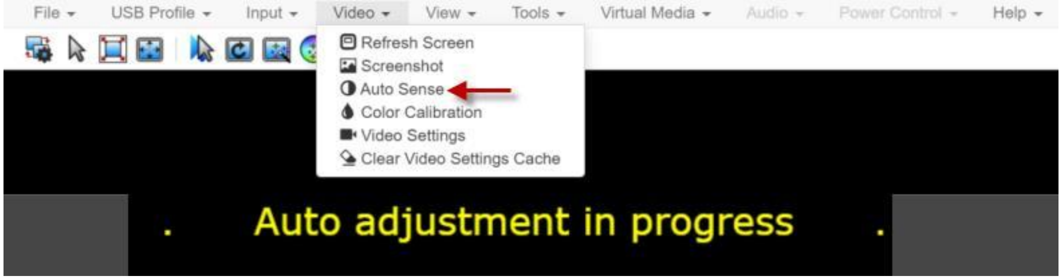
Auto Sense

The Auto Sense command forces a re-sensing of the video settings, such as resolution and refresh rate, and redraws the video screen.

To automatically re-sense the video settings:

- Choose Video > Auto Sense .

  A message stating that the auto adjustment is in progress appears.



Auto adjustment in progress

Color Calibration

The Color Calibration command optimizes the color levels, such as hue, brightness, and saturation, of the transmitted video images.

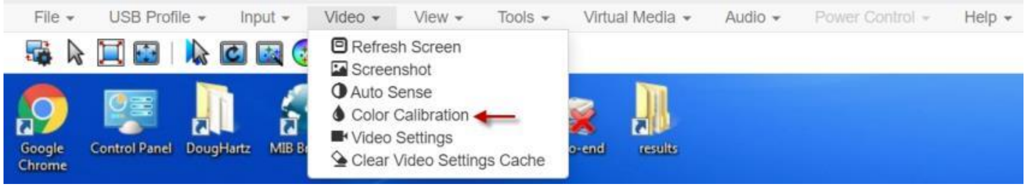
The color settings are on a target server-basis.

Note: When color is successfully calibrated, the values are cached and reused each time you switch to the target. Changes to the brightness and contrast in Video Settings are not cached. Changing resolution resets the video to the cached values again. You can clear the cached values in Video > Clear Video Settings Cache. See Clear Video Settings Cache.

To calibrate color:

- Choose Video > Color Calibration.

  A message stating that the color calibration is in progress appears.



Video Settings

Use the Video Settings command to manually adjust the video settings.

To change the video settings:

1. Choose Video > Video Settings to open the Video Settings dialog.

2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:

   a. PLL Settings

      Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances, this setting should not be changed because the autodetect is usually quite accurate.

      Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

   b. Brightness: Use this setting to adjust the brightness of the target server display.

      Brightness Red - Controls the brightness of the target server display for the red signal.

      Brightness Green - Controls the brightness of the green signal.

      Brightness Blue - Controls the brightness of the blue signal.

   c. Contrast Red - Controls the red signal contrast.

      Contrast Green - Controls the green signal.

      Contrast Blue - Controls the blue signal.

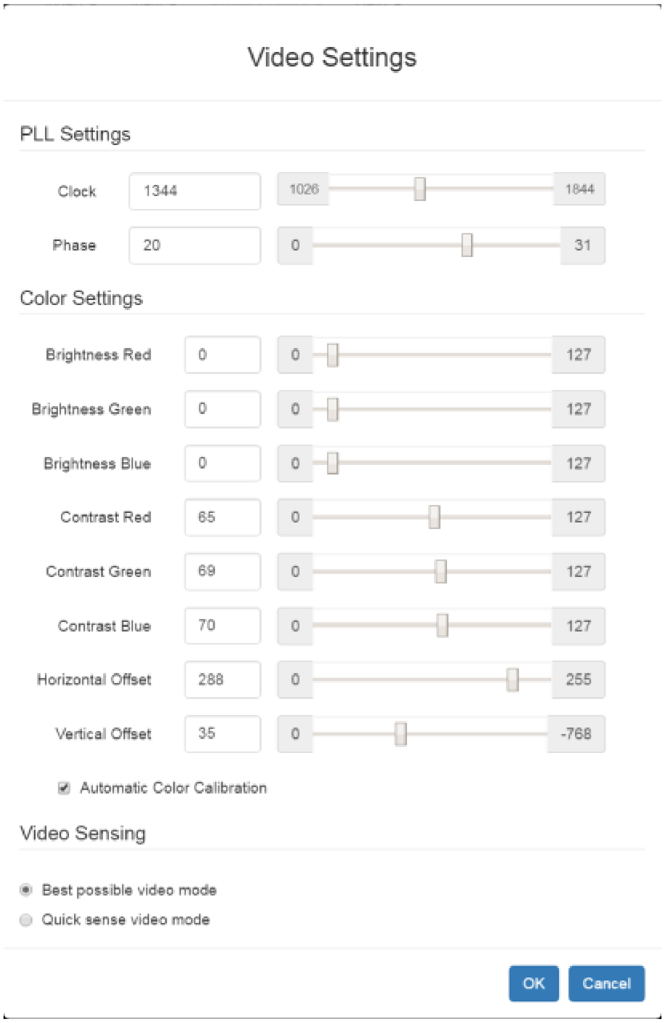
      If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Technical Support before making any changes.

---

   d. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.

e. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.



Video Settings

PLL Settings

Clock	1344	1026	1844
Phase	20	0	31

Color Settings

Brightness Red	0	0	127
Brightness Green	0	0	127
Brightness Blue	0	0	127
Contrast Red	65	0	127
Contrast Green	69	0	127
Contrast Blue	70	0	127
Horizontal Offset	288	0	255
Vertical Offset	35	0	-768

☑ Automatic Color Calibration

Video Sensing

● Best possible video mode

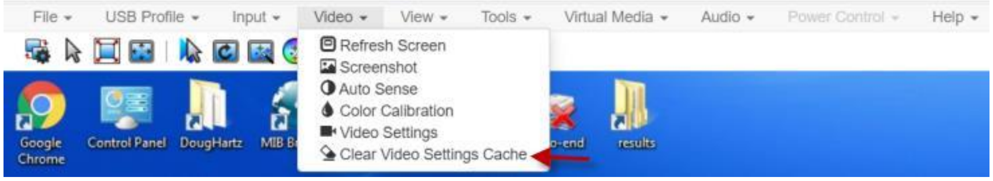
○ Quick sense video mode

Clear Video Settings Cache

You can clear the video settings cache to delete old settings that do not apply anymore, such as when a target server is replaced. When you clear the video settings cache, the server automatically does a video auto-sense and color calibration. The new values are cached and reused when the target is accessed again.

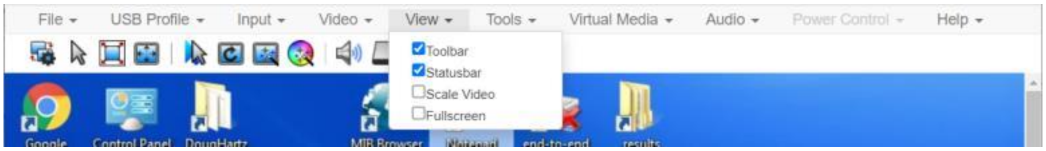
To clear the video settings cache:

- Choose Video > Clear Video Settings Cache in the toolbar.



View Menu

The View Menu contains options to customize your HKC display.



Toolbar and Statusbar:

The toolbar contains icons for some commands. The Statusbar displays screen resolution at the bottom of the client window.

Scale Video:

Scale Video scales your video to view the entire contents of the target server window in your HKC window. The scaling maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

Fullscreen:

Fullscreen sets the target window to the size of your full screen, removing your client from the view.

- Press Esc to exit fullscreen.

Virtual Media Menu

Due to browser limitations, HKC supports a different set of virtual media functions than the other KVM Clients.

Due to browser resources, virtual media file transfer is slower on HKC than the other KVM clients.

Connect Files and Folders

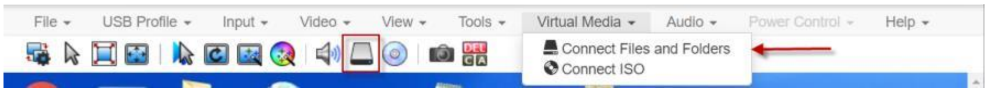
The Connect Files and Folders command provides an area to drag and drop files or folders that you want to connect by means of virtual media.

Supported browsers: Chrome, Firefox, Safari, Edge.

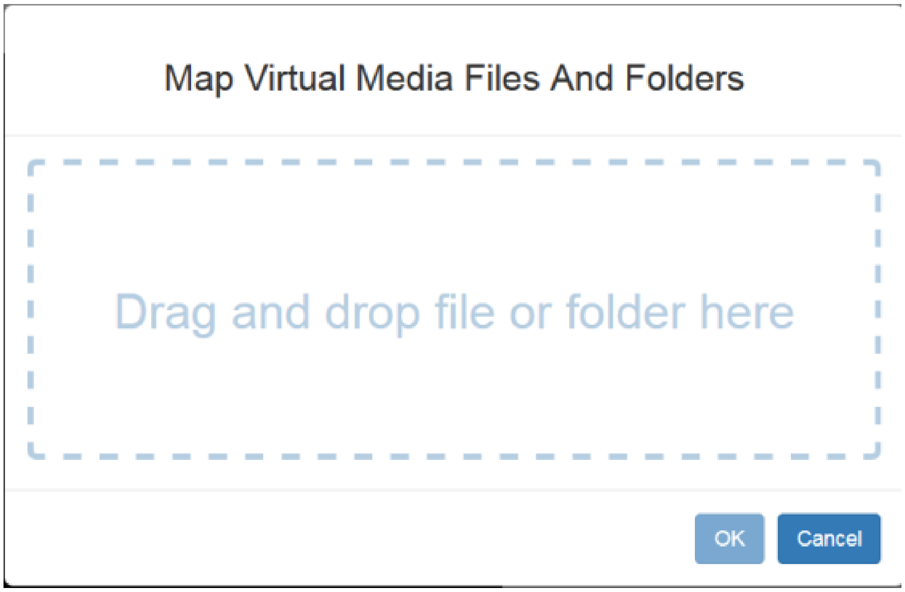
File size limit: 4GB per file

▶ To connect files and folders:

1. Choose Virtual Media > Connect Files and Folders. Or, click the matching icon in toolbar.



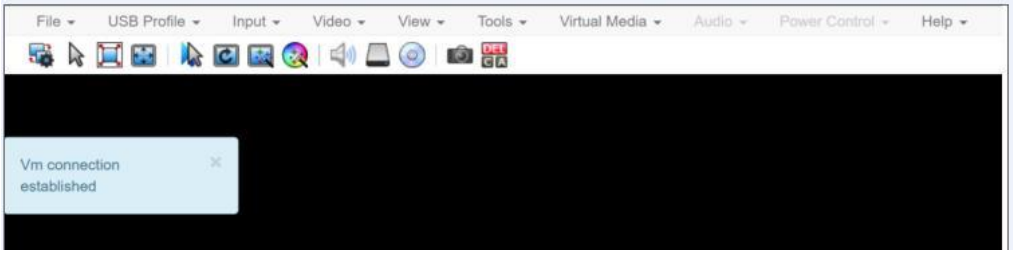
2. Drag files or folders onto the Map Virtual Media Files and Folders dialog. Click OK.



Map Virtual Media Files And Folders

Drag and drop file or folder here

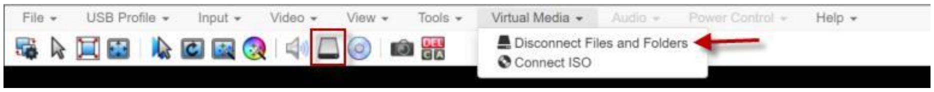
3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.



Vm connection established

To disconnect files and folders:

- Choose Virtual Media > Disconnect Files and Folders. Or, click the matching icon in the toolbar.



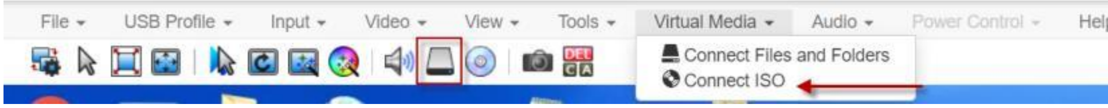
Connect ISO

The Connect ISO command maps a virtual media image file to the target. You can connect ISO, DMG or IMG files from your client PC or ISO files from a remote server.

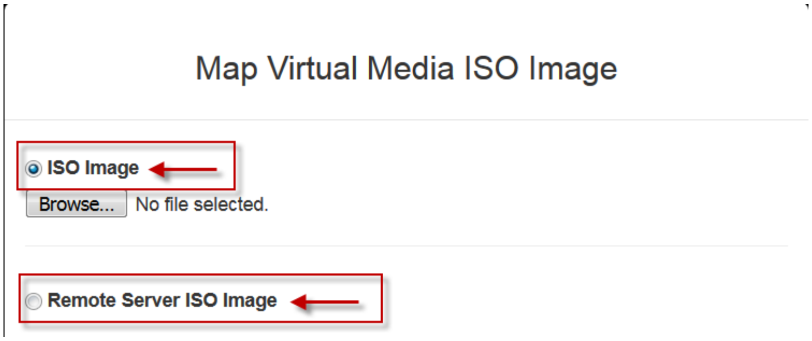
Note: If connection to your SAMBA server is lost while transferring files from your image file to the target, keyboard and mouse control will be lost for several minutes, but will recover.

To map virtual media image files:

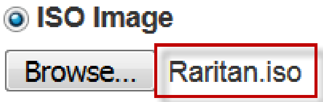
1. Choose Virtual Media > Connect ISO. Or, click the matching icon in the toolbar.



2. Select the option for your file's location:

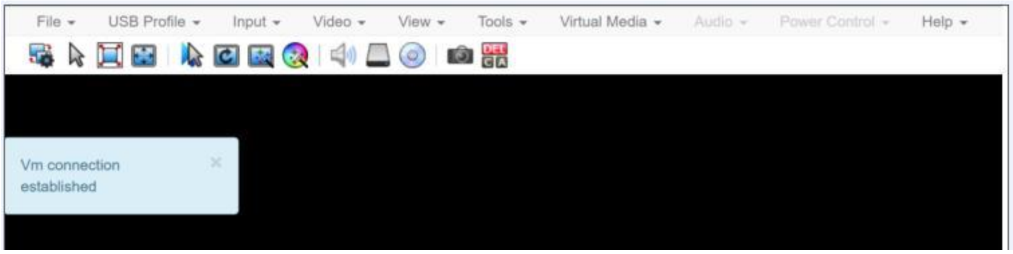


   - Select ISO Image if the image file is directly accessible on your client. Click Browse, select the ISO, DMG or IMG file, and click OK. The filename appears next to the Browse button.



  - Select Remote Server ISO Image for ISO files on a remote server. Remote ISO files must be pre-configured by an administrator for the mapping to appear here. See Virtual Media File Server Setup (File Server ISO Images Only). Select the Hostname, then select the image file from the Image list. Enter the file server's username and password.

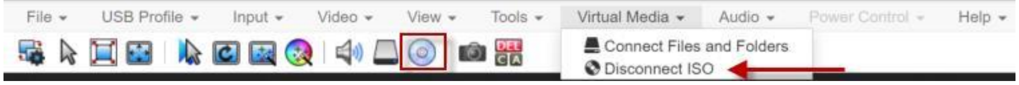
3. Click OK to map the selected file to the target. A message appears to show virtual media is connected.



Vm connection established

To disconnect ISO:

- Choose Virtual Media > Disconnect ISO. Or, click the matching icon in the toolbar.



Audio Menu

The Audio menu contains audio connection and settings.

Audio quality deteriorates if multiple target connections are open. To preserve quality, limit to four target connections open on HKC when an audio session is running.

Note: IE does not support audio. The menu will appear grayed out.

Connect Audio

The Connect Audio command connects your playback device, selects audio format and gives an option to mount the selected playback device automatically when you connect to the target.

HKC connects the client PC's default audio playback device. To use a different device, it must be set as default in the client OS.

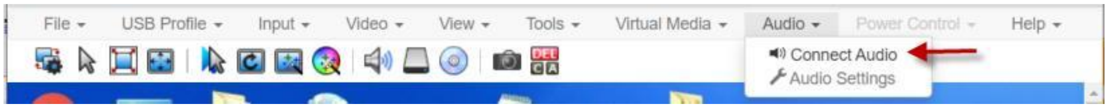
Supported audio sample rates differ depending on your connecting device and browser:

- On Windows Edge - 11,025, 22,050 and 44,100 Hz
- On Mac/Windows and Linux Chrome - 11,025, 22,050 and 44,100 Hz
- On Mac/Windows and Linux Firefox only 44.1 kHz available
- On Mac Safari - only 44.1 kHz available
- On IOS devices - only 44.1 kHz available

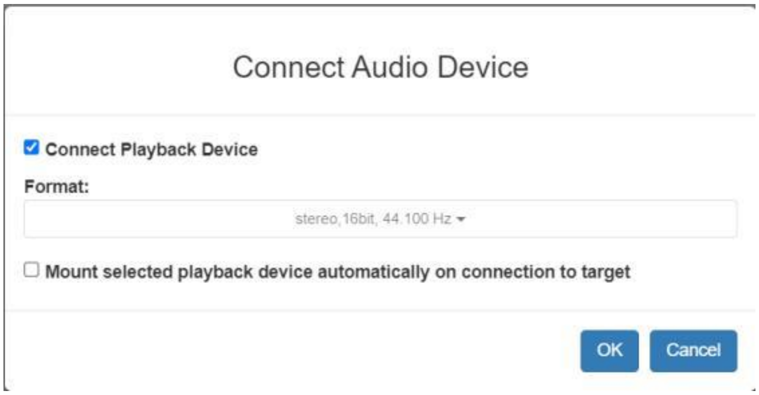
Note: For best quality, limit the number of audio sessions to a maximum of four KVM sessions.

To connect audio:

1. Choose Audio > Connect Audio, or click the matching icon in the toolbar.



2. In the Connect Audio Device dialog, select the Connect Playback Device checkbox.



Connect Audio Device

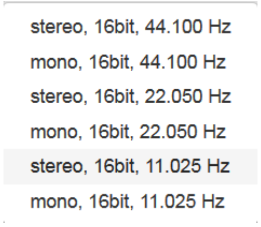
☑ Connect Playback Device

Format:

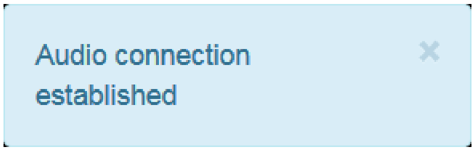
stereo,16bit, 44.100 Hz

☐ Mount selected playback device automatically on connection to target

3. Select the Format.



4. Select the "Mount selected playback device automatically on connection to target" checkbox to enable the option. This setting will connect audio automatically the next time you connect to the target.
5. Click OK. A success message appears.



Audio connection established

To disconnect audio:

1. Choose Audio > Disconnect Audio, or click the matching icon in the toolbar.

Audio Settings

The Audio Settings option is enabled when audio is connected. Use the Audio Settings to set the buffer and volume.

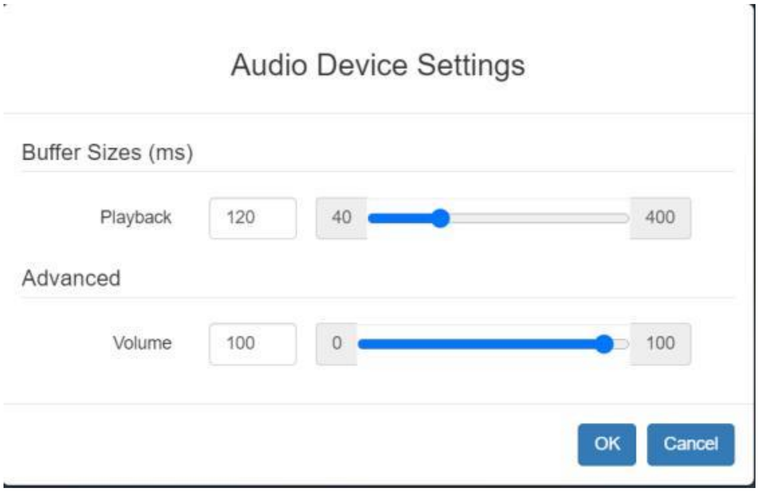
Increasing the buffer size improves the audio quality but may impact the delivery speed.

The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

To configure audio settings:

1. Choose Audio > Audio Settings while Audio is connected.

2. Set the Buffer and Volume using the arrows or sliders.



Audio Device Settings

Buffer Sizes (ms)

Playback 120 40 400

Advanced

Volume 100 0 100

3. Click OK.

Auto Play in Safari

For HKC connections in the Safari browser that have auto mounted audio devices, make sure that the "Auto Play" setting is "Allow all Auto Play".

https://support.apple.com/guide/safari/customize-settings-per-website-ibrw7f78f7fe/mac

Auto Play in Chrome

For HKC connections in the Chrome browser that have auto mounted audio devices, make sure that the "Autoplay policy" is set to "No user gesture is required". To find this setting, go to chrome://flags.

For more details, see https://www.theoplayer.com/blog/chrome-autoplay-policy-what-you-need-to-know

Power Control Menu

You can power on, power off, and power cycle a target through the outlet it is connected to.

Access the target, and then select a power control option from the Power Control menu.

The menu option is disabled if you do not have permission for power control, and when outlets are not associated with the port.

Connecting to Nodes using a Mobile Device

When using your IOS mobile device, such as an iPhone or iPad, you can connect to nodes using the Access Client.

Accessible interfaces include out-of-band KVM and Serial interfaces, in-band power control interfaces, and web browser interfaces. See ***Mobile Device Accessible Interfaces*** (on page 71) for the complete list of accessible interfaces.

Interfaces that are not available when connecting to CC-SG on your mobile device will be disabled.

Connect to a Node via an Out-of-Band KVM Interface on an IOS Mobile Device

Only Dominion KX3 v3.4 and later, and SX2 v2.1 and later targets can be accessed using an IOS mobile device. See the Compatibility Matrix for the most up-to-date list of supported targets.

▶ **To connect to a node via an out-of-band KVM or Serial interface on an IOS mobile device:**

1. Login to the Access Client using your mobile device browser.
2. Touch the node you want to access in the node list, then touch the blue interface link in the Node Profile to the right.
3. The client opens and connects to the target.

Mobile Device Accessible Interfaces

Interfaces that are accessible using your mobile device have enabled links. Interfaces that are not accessible using your mobile device will have disabled links.

▶ **Mobile device accessible interfaces:**

- Out-of-Band - KVM

  Targets of Dominion KXIII (3.4 and higher), SX2, and KX4-101. See the Compatibility Matrix for the most up-to-date list of supported targets.

- Power Control - DRAC
- Power Control - ILO Processor
- Power Control - Integrity iLO2
- Power Control - IPMI
- Power Control - Managed Power Strip
- Power Control - Power IQ Proxy
- Power Control - RSA
- VMware Power
- Web Browser

Connecting to Nodes using the Admin Client and the Desktop Admin Client

The Admin Client and the Desktop Admin Client work the same way for connections to nodes, except that a few interfaces are not supported on the Desktop version. See ***Interface Support in CC-SG Desktop Admin Client*** (on page 9).

There are several ways to connect to nodes in the Admin Client. Each of these options launches the associated application and connects to the node.

- When a node is selected in the Nodes tab, press the Enter key to connect to the node using the default interface.
- When an interface is selected in the Nodes tab, press Enter to connect to the node using the selected interface.
- When a node's status is Available, double-click the node in the Nodes tab to connect to the node using the default interface. If the node's status is Unavailable, double-clicking the node has no effect.
- When an interface is up and the availability is idle or connected, double-click the interface label in the Nodes tab to connect to the node using the selected interface. If the interface is down or the availability is busy, double-clicking the interface has no effect.
- Click an interface link in the Node profile screen to connect to the node using the interface.
- Right-click an interface in the Nodes tab, then choose Connect.

Node Profile Overview: Admin Client

In the Admin Client, you can view all node details in the Node profile page. Select a node in the Nodes tab to open the Node profile page.

- The selected node’s name displays at the top of the Node profile screen.
- The Interfaces tab lists the connection Type, Name, Status, Availability, and Device/IP address for interfaces associated with the selected node. If a node has virtual media capabilities, a Virtual Media column lists the status, Enabled or Disabled. Interfaces for power control are also listed in the Interfaces section. See ***Power Control for Nodes Using the Admin Client*** (on page 96).

  Note: In-Band - iLO Processor KVM, In-Band - DRAC KVM and In-Band - RSA KVM will not display any Availability.

- The Associations tab lists the Categories and Elements associated with the selected node. CC-SG Administrators can set up Associations to help organize the equipment that CC-SG manages. Each Association includes a Category, which is the top-level organizational group, and its related Elements, which are subsets of a Category. You can use Associations to create Custom Views that help you organize the All Nodes list in different ways. See ***Custom Views*** (on page 22) for details.
- The Location & Contacts tab contains information about a node's location and contact information, such as phone numbers, that you may need when working on a node.
- The Notes tab contains a tool to add notes about a node for other users to read. All notes appear in the tab with the date, username, and IP address of the user who added the note.
- The Audit tab contains a list of the reasons that a node was accessed. You must enter a reason for access before connecting to a node when the administrator has enabled node auditing for your user group. The Audit tab is hidden if the feature is disabled, or if no reasons for access have been entered.
- The Control System Data tab, Virtual Host Data tab, and Virtual Machine Data tabs appear on nodes in your virtual infrastructure with information about the virtual node. Each tab contains information specific to the Control System, Virtual Host, or Virtual Machine.
- The Blades tab appears on blade chassis nodes and contains information about the blade servers residing in the blade chassis.

Interface Support in CC-SG Desktop Admin Client

The CC-SG Desktop Admin Client does not support connections to the following interfaces because they require JRE add-ons in a browser:

- DRAC5
- DRAC6

Applications for Accessing Nodes

- When you connect to an out-of-band node, the default Raritan application for the node opens.

Applications include:

- Active KVM Client (AKC)
- Raritan Serial Console (RSC)
- HTML KVM Client (HKC) - available for KX3 and KX4
- HTML Serial Console (HSC) - available for SX2 and DSAM
- Virtual KVM Client (VKC)
- Mobile KVM Client (MKC) - only on mobile devices

- When you connect to an in-band or virtual node, the vendor's application for the node opens.

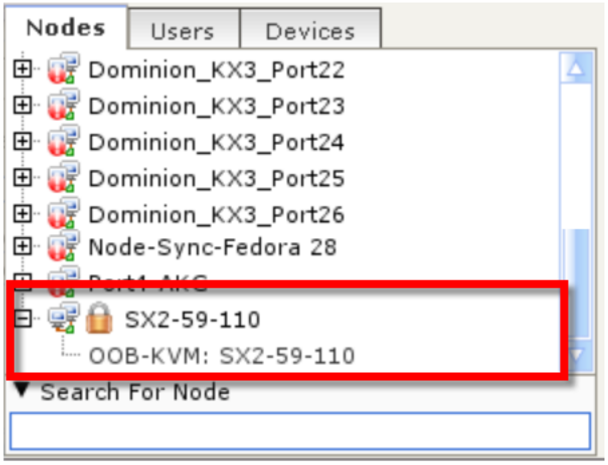
Applications include:

- DRAC
- Integrity ILO2 Power Control
- ILO

Node Lockout on Disconnect Setting

The Node Lockout on Disconnect setting prohibits access to a node for a set amount of time after a disconnected session. This temporary lockout can prevent a security issue that may occur if a user disconnects from the node without first logging out from the target, which may allow another user to connect to the target and have access that they should not have. The delay before allowing new connections allows the target's timeout to end any sessions before a new user connects. Default setting is disabled.

The setting applies to all KX/SX/LX/KSX node connections. Other interface and node types are not supported.



When enabled and a user disconnects from a supported node, the Admin Client shows a Lock icon on the node in the Nodes list. When locked, the same user can re-connect to the node, and the lockout time resets on disconnection.

The lockout applies to the following tasks and an error message that the node is locked will be presented to the user :

- any other user attempting to access the node interfaces
- attempts to perform a power operation
- attempts to access on any client, including Admin, Access, or using a Bookmark
- attempts to access using the SSH 'connect' command to connect to serial ports
- User Station connections
- WS-API connections as well.

When a node is locked, a user with the CC Setup and Control pemission can unlock the node by:

- Right clicking the node, or an interface in the node, and choosing Unlock Disconnect Lock.
- Selecting the node, or an interface in the node, and choosing Nodes > Unlock Disconnect Lock.

Understanding Interfaces

Each node has one or more interfaces through which you can connect to it.

▶ To view the interfaces associated with a node

Select a node to open the Node Profile screen. All interfaces associated with the node are listed in the Interfaces section.

In the Access Client, power control interfaces are listed in the Interfaces section.

▶ To check an interface's Availability

You can see whether an interface is available by checking the Availability column in the Node Profile's Interface section.

Availability	Meaning
Idle	The interface is not in use.
Connected	The interface is in use, but it is available to additional users.
Busy	The interface is busy and cannot accept any additional users.
Inaccessible	There are no available paths to the Blade Server node as they are all in use.

Note: Nodes connected to KX 1.4 devices do not use the "Busy" Availability category described above. If an interface to a node connected to a KX 1.4 displays the "Connected" Availability category, the interface may be either Connected or Busy.

Interface Types and Abbreviations

There are many interface types, each providing different types of access to nodes. The abbreviations in this table are used in the Admin Client's Nodes tab as a prefix to the interface name, and in the Node profile for each node, in the Interfaces tab.

Interface Type	Interface Abbreviation	Supports Proxy Mode?
Out-of-Band KVM	OOB-KVM	Yes
Out-of-Band Serial	OOB-Serial	Yes
In-Band DRAC KVM	IB-DRAC	No
In-Band RSA KVM	IB-RSA	No
In-Band iLO Processor KVM	IB-ILO Processor	No
In-Band SSH	IB-SSH	Yes
In-Band VNC	IB-VNC	Yes
In-Band RDP	IB-RDP	MultiPlatform and Java RDP: No Microsoft RDP: Yes
In-Band Telnet	IB-TELNET	Yes
In-Band UCS KVM	IB-UCS	No
Power Control: iLO Processor	PWR-ILO Processor	Yes
Power Control: Integrity ILO2	PWR-Integrity ILO2	Yes
Power Control: DRAC	PWR-DRAC	Yes
Power Control: IPMI	PWR-IPMI	Yes
Power Control: Managed Power Strip	PWR-PDU	Yes
Power Control: Power IQ Proxy	PWR-PIQ	Yes
Power Control: RSA	PWR-RSA	Yes
Web Browser	WEB	No
VI Client	VIC	No
VMware Viewer	VMV	No

Interface Type	Interface Abbreviation	Supports Proxy Mode?
Virtual Power	Virtual PWR	Yes

Connect to a Node via an Out-of-Band KVM Interface

1. Select the node to which you want to connect. The Node profile screen appears.

   In the Node profile screen, all configured interfaces appear in the Interface section.
2. In the Name column, click the hyperlink of the Out-of-Band KVM interface you want to use to connect to the node.
3. If node auditing is enabled for your user group, the Access Information dialog appears. Enter your reason for accessing the node and then click OK.
4. The Virtual KVM Client (VKC), Active KVM Client (AKC) or HTML KVM Client (HKC) opens in a new window. Default client is selected based on your PC.
5. A Connection Status window opens. Once a connection is established, the client opens.

   Note: If the KVM node is on sleep mode and indicates “no video signal,” press the space bar on your keyboard until the node exits sleep mode.

   Note: The .NET AKC client looks and operates like VKC, with a few exceptions.
6. To disconnect from VKC, choose Connection > Exit.

Prerequisites for Using AKC

- Ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone and that Protected Mode is not on when accessing the device.
- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.
- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

Note: The AKC launching will always need a trusted certificate on the CC-SG.

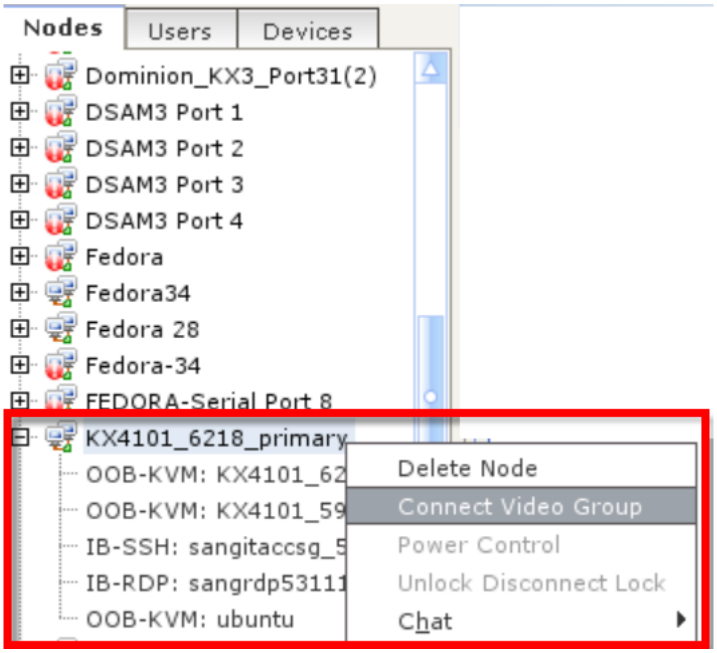
Launch a Video Group Connection

Video groups are configured when a target server has 2 or more video card outputs. CC-SG will provide a video group to include all these video card outputs so that you can launch all these KVM connections at once. There may be up to 6 KVM connections per video group.

Video Group connections are supported in AKC/VKC.

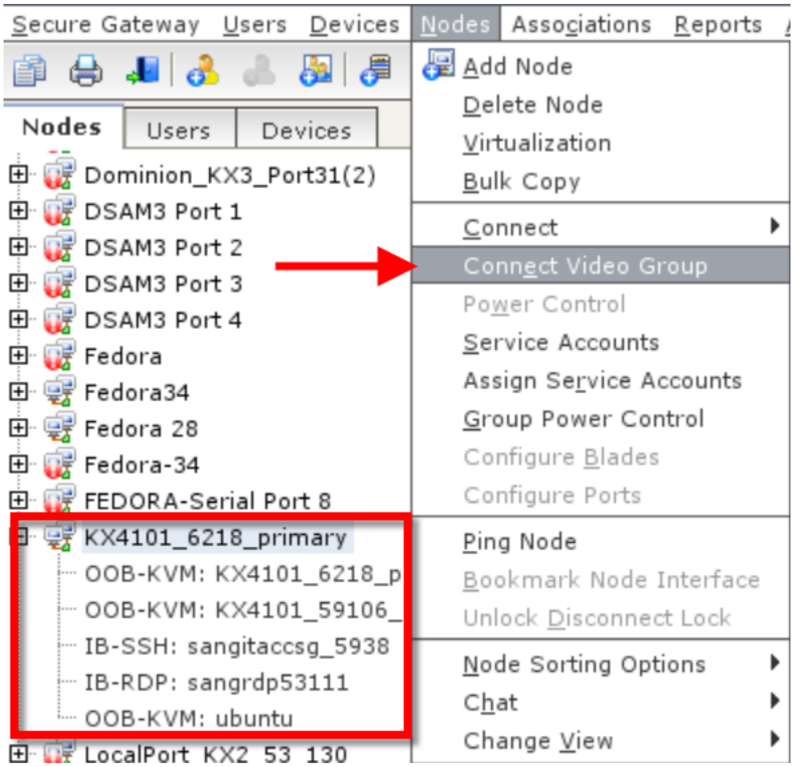
Launching Video Groups in the Admin Client:

1. In the Nodes list, right-click the node whose video group you want to launch, then select Connect Video Group.



or

2. Select the node with the video group in the Nodes list, then choose Nodes > Connect Video Group.

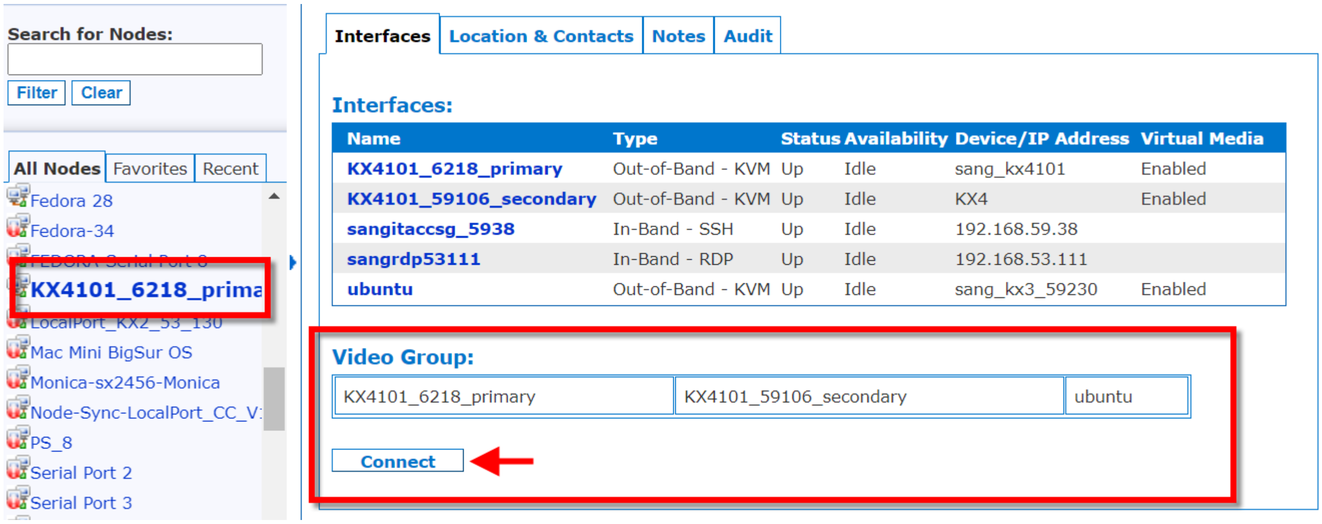


3. The Video Group connection launches in the application configured in the first interface of Video Group.

▶ Launching Video Group Connections in the Access Client:

1. Select the node whose video group you want to launch in the All Nodes list.

2. Below the Interfaces tab, the video group configuration is shown. Click Connect.



Interfaces:

Name	Type	Status	Availability	Device/IP Address	Virtual Media
KX4101_6218_primary	Out-of-Band - KVM	Up	Idle	sang_kx4101	Enabled
KX4101_59106_secondary	Out-of-Band - KVM	Up	Idle	KX4	Enabled
sangitaccsg_5938	In-Band - SSH	Up	Idle	192.168.59.38	
sangrdp53111	In-Band - RDP	Up	Idle	192.168.53.111	
ubuntu	Out-of-Band - KVM	Up	Idle	sang_kx3_59230	Enabled

Video Group:

KX4101_6218_primary	KX4101_59106_secondary	ubuntu

3. The Video Group connection launches in the application configured in the first interface of the Video Group.

Connect to a Node via an Out-of-Band Serial Interface

1. Select the node to which you want to connect. The Node profile screen appears.

   In the Node profile screen, all configured interfaces appear in the Interface section.

2. In the Name column, click the hyperlink of the serial interface you want to use to connect to the node.
3. If node auditing is enabled for your user group, the Access Information dialog appears. Enter your reason for accessing the node and then click OK.
4. The RSC or HTML Serial Console (HSC) application opens in a new window. Default client is selected based on your PC.

Accessing a Serial Interface for the First Time

If the node is configured for a console application, a Security Warning appears, indicating that the console applet is a signed applet from Raritan Systems. Click Yes and the console appears.

Important: The security warning (appearing in IE only) appears the first time the user connects to a serial interface. Click Yes when this display appears; if you click No, the console application does not launch and you must exit CC-SG, close the browser, re-launch the browser, and connect to CC-SG again.

Connect to an iLO Processor Enabled Node

To access the Integrated Remote Console, which includes the Virtual Media functions, make sure you access CC-SG by Internet Explorer with a DNS name, rather than an IP address, or access the CC-SG by Internet Explorer with the system's default browser set to Internet Explorer. The Java app will load first, then launch the Integrated Remote Console in a new window.

Note: You must accept a security warning before connecting to an iLO3 interface. This warning occurs because the HP applet is not signed, and CC-SG detects this.

▶ **To connect to an iLO Processor-enabled node:**

1. In the Nodes tree, select the iLO/RILOE node you want to connect to and manage. The Node details screen appears.
2. In the Node details screen, all configured interfaces appear in the Interface section.
3. In the Name column, click the hyperlink of the KVM interface you want to use to connect to the node.
4. If node auditing is enabled for your user group, the Access Information dialog appears. Enter your reason for accessing the node and then click OK.
5. The HP Remote Console applet launches. When the applet loads, you have KVM access to the iLO/RILOE-enabled server. If you accessed CC-SG by Internet Explorer with a DNS name, or by Internet Explorer set as your default browser, the Integrated Remote Console launches from the applet in a new window.
6. When you are finished, close the browser window to disconnect.

Connect to a Node via an In-Band KVM Interface

CC-SG supports SSH Keyboard Interactive Authentication, so this authentication mechanism can be enabled in a SSH server.

1. In the Nodes tree, select the node you want to connect to and manage. The Node Profile page opens.
2. In the Node Profile screen, all configured interfaces display in the Interfaces section.
3. In the Name column, click the hyperlink of the In-Band KVM interface you want to use to connect to the node.
4. If node auditing is enabled for your user group, the Access Information dialog appears. Enter your reason for accessing the node and then click OK.
5. Depending on the interfaces, this step varies.

- For SSH, TELNET, and VNC interfaces, the Application Startup Parameters dialog appears if CC-SG Administrators have not configured the username and password in the interfaces. Type the Username and Password, and click OK.
- For RDP interfaces, the Application Startup Parameters dialog appears. Options vary by RDP type.
  - If CC-SG Administrators have not configured the username and password in the interfaces, you must type the Username and Password in the dialog.
  - For Microsoft and Java, select the Screen Size and Color Depth you want to use for this session.
  - For Microsoft RDP only, select the Use Local Drives in Remote Session checkbox to enable drive mounting from the local client to the target.
  - For Microsoft RDP users with smart cards, such as RSA SecurID, select the Use Local Smart Cards in Remote Session checkbox to enable mounting your smart card on a target. Click OK.
  - For MultiPlatform RDP, select the Screen Size. If you have not already downloaded and installed the client, click the download link. See ***Install MultiPlatform RDP Client*** (on page 83) for details.

6. The Remote Console applet launches in a new window. When the applet loads, you have KVM access to the node.

   Note: If you cannot connect to an in-band KVM interface, it may already be occupied by another user.

7. When you are finished using Remote Console, close the browser window.

MultiPlatform RDP Client Connection Details

The MultiPlatform RDP client does not require Java. It is the default RDP client option for new interfaces. You must install MultiPlatform RDP client before CC-SG can use it for connections: See ***Install MultiPlatform RDP Client*** (on page 83). Your browser may ask for permission to run MultiPlatform RDP.

- Targets supported: Windows 10, Windows 2012, Windows 2016, Windows 2019.
- Add square brackets around IPv6 addresses in the interface's address field.
- The error dialog box for a failed client connection may appear behind the browser window. The dialog is visible in the Windows task bar.
- If MultiPlatform RDP client has not been installed, and a connection is attempted, the connection fails, but an error does not appear.

Does not support:

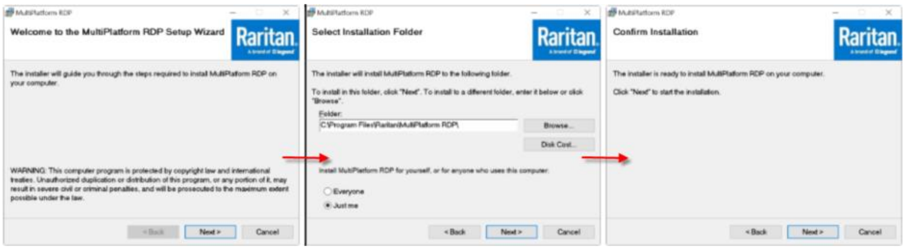
- Full screen
- Proxy mode (always uses direct mode)
- Smart card
- Drive sharing
- USB device sharing
- Control-Alt-Delete support. Control-Alt-Delete will be sent to the target but the client host will also receive it. You can use Control-Alt-Delete and cancel the local response.

Install MultiPlatform RDP Client

To download and install:

The MultiPlatform RDP client runs on Windows only. You must download and install it before CC-SG can use it for connections.

1. Download the .msi from the CC-SG by going to: http://CCSG-IP/download
2. Run the installer. You will choose the install location and specify to install only for current user or all users. Confirm permission to install. Restart the browser to recognize the new application association.



The installer will guide you through the steps required to install MultiPlatform RDP on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

The installer will install MultiPlatform RDP to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Raritan\MultiPlatform RDP\

Install MultiPlatform RDP for yourself, or for anyone who uses this computer:

○ Everyone

● Just me

The installer is ready to install MultiPlatform RDP on your computer.

Click "Next" to start the installation.

Java RDP Connection Details

- The Java RDP interface supports Windows 2003 targets.
- Java RDP can be used for proxy mode connections. See ***About Connection Modes*** (on page 87).
- When adding RDP interfaces to Windows 7, make sure that ICMPv4 and ICMPv6 are allowed by the Windows 7 firewall.

Microsoft RDP Connection Details

- Internet Explorer only.
- Microsoft RDP cannot be used for proxy mode IPv6 connections. See ***About Connection Modes*** (on page 87).
- Targets supported: Windows 10, Windows server 2012, Windows server 2016.
- When connecting to a Microsoft RDP interface with "Use Local Drives in Remote Session" selected, make sure the CC-SG's IP address is included in the browser's Trusted Sites Zone.

VNC Connection Details

► Support for IPv6:

Not all VNC versions support IPv6.

RealVNC supports IPv6. You must select Prefer On in the RealVNC server settings or IPv6 and VNC will not work with CC-SG.

The TightVNC client will work with CC-SG if the server setting is changed to Prefer On.

Free edition of RealVNC does NOT support IPv6

Personal Edition of RealVNC supports IPv6, but it is a 30 day trial version, and then you must buy a license.

Enterprise edition of RealVNC supports IPv6 when you buy a license.

► VNC connections to Windows 7:

When adding VNC interfaces for Windows 7, make sure that ICMPv4 and ICMPv6 are allowed by the Windows 7 firewall.

DRAC 5 Connection Details

Tip for Hostnames:

In CC-SG, when adding the DRAC interface, make sure hostname is entered exactly as it is on the DRAC machine locally, including case-sensitivity. Verification will fail if the case does not match.

2020 update:

By default, the DRAC5 applet is not able to be launched with a current JRE. However, modification of the java.security file to enable currently disabled functions can be done on the client that will allow the application to launch properly. These edits are required as of JRE 1.8.0_131 and newer.

- Comment out the following lines in the java.security file:
  - jdk.certpath.disabledAlgorithms=....
  - jdk.tls.disabledAlgorithms=....
  - jdk.jar.disabledAlgorithms=....

Certificate information:

When using Internet Explorer and connecting to DRAC 5 servers, you must have a valid certificate installed on DRAC 5, or Internet Explorer will give an error. If the certificate is not signed by a trusted CA, also install the certificate of the CA used to sign the DRAC certificate into the Trusted Root CA of the browser. You must also disable the information bar for Internet Explorer downloads to allow the DRAC5 .jnlp file to be accessed.

Note: Java applets are blocked by all the browsers except IE11.

To disable the Internet Explorer downloads information bar:

1. Choose Tools > Internet Options.
2. In the Security tab, select the Internet zone.
3. Click Custom Level. Scroll down to Downloads.
4. Under "Automatic prompting for file downloads" click Enable.
5. Click OK. You are returned to the Internet Options dialog.
6. In the Security tab, select the Intranet zone.
7. Click Custom Level. Scroll down to Downloads.
8. Under "Automatic prompting for file downloads" click Enable.
9. Click OK.

DRAC 6 Connection Details

Launching a DRAC interface may fail with the error message "Unsigned application requesting unrestricted access in Java console". DRAC6 applets are signed with MD5 jar signatures. Some JRE versions find this insecure, causing the error. Editing the java.security file may resolve this issue. On Windows, this file can be found at C:\Program Files (x86)\Java\jre7\lib\security\java.security. Comment out the jdk.jar.disabledAlgorithms line of the file.

DRAC 8/9 Connection Details

Tip for Hostnames:

In CC-SG, when adding the DRAC interface, make sure hostname is entered exactly as it is on the DRAC machine locally, including case-sensitivity. Verification will fail if the case does not match.

Tip for SSL Certificates:

Upon connection, you may see the following message: "You have an SSL certificate for remote presence port. You have to close this window now."

To prevent this in Internet Explorer, add the DRAC IP/hostname to Trusted Sites in IE. Internet Options> Security> "Trusted sites". Other browsers may show this message briefly before making a connection.

Note: DRAC applications fail to launch from MAC clients with Safari, Chrome or Firefox. The DRAC java application requires native libraries to function, and uses specific dynamic libraries which are unavailable on MAC OS installs.

iLO 4 Connection Details

Due to a limitation in some iLO devices, ILO4 KVM targets require a workaround to launch in the following browser/client configurations:

- Firefox browser on MAC
- Firefox browser on Windows 10

The required JNLP file is downloaded, but the file extension is not recognized so the associated application does not launch.

Workaround:

1. Locate the downloaded file in your Finder or Downloads folder (depending on your browser/client).
2. Rename the file with a .jnlp extension, and and then open the file with Java Web launcher.
3. The KVM connection is launched.
4. A Client Security Warning Message displays   in red “Running this application maybe a security risk.” After accepting, the client launches successfully.

iLO 3 Connection Details

The iLO3 interface cannot be accessed directly from some browser/client configurations because TLS 1.2 is not supported in the server. A General Exception error displays and the connection fails.

The following browser/client configurations cannot be used successfully:

▶ Browsers:

- Firefox
- Safari
- Chrome

▶ Clients:

- Linux
- MAC

About Connection Modes

CC-SG offers three connection modes for in-band and out-of-band connections: Direct, Proxy, and Both.

- Direct mode allows you to connect to a node or port directly, without passing data through CC-SG. Direct mode generally provides faster connections.
- Proxy mode allows you to connect to a node or port by passing all data through CC-SG. Proxy mode increases the load on your CC-SG server, which may cause slower connections. However, Proxy mode is recommended if you are more concerned about the security of the connection. You need to keep the CC-SG TCP ports 80, 443, 2400 and 2401, and ports assigned for Microsoft RDP, open in your firewall.
- Both mode allows you to configure CC-SG to use a combination of Direct mode and Proxy mode. In Both mode, Proxy mode is the default, but you can configure CC-SG to use Direct mode when connections are made using client IP addresses in specified ranges.

Note: Some interfaces only work in Direct mode even though you configure CC-SG to use Proxy mode. These interfaces include ILO, RSA, DRAC, Web Browser and VMware Viewer. Java RDP interfaces can be used in proxy mode. See About Interfaces.

Connect to a Node via a Web Browser Interface

A web browser interface allows you to launch a browser and connect to web applications associated with a node. Some examples of web-enabled nodes include the Raritan Dominion PX or nodes that contain RSA, DRAC, or ILO Processor cards.

▶ To connect to a node via a web browser interface:

1. Select the node whose web application you want to use in one of the node lists in the left panel. The Node details screen appears.

   In the Node details screen, all configured interfaces appear in the Interface section.
2. In the Name column, click the hyperlink of the web browser interface you want to use to connect to the node.
3. If node auditing is enabled for your user group, the Access Information dialog appears. Enter your reason for accessing the node and then click OK.
4. Your default browser launches and opens the URL associated with the Web Browser interface. You may have to log in to gain access.
5. When you are finished using the web application, close the browser window to end the connection.

Connect to a Control System or Virtual Host Node via a VI Client Interface

If you are using Internet Explorer, you must enable the following options for cookie handling. In the browser, choose Tools > Internet Options. In the Privacy tab, click Advanced. Select "Override automatic cookie handling." Select Accept for First-party Cookies and Third-party Cookies. Select "Always allow session cookies."

▶ To connect to a Control System or Virtual Host Node via a VI Client Interface:

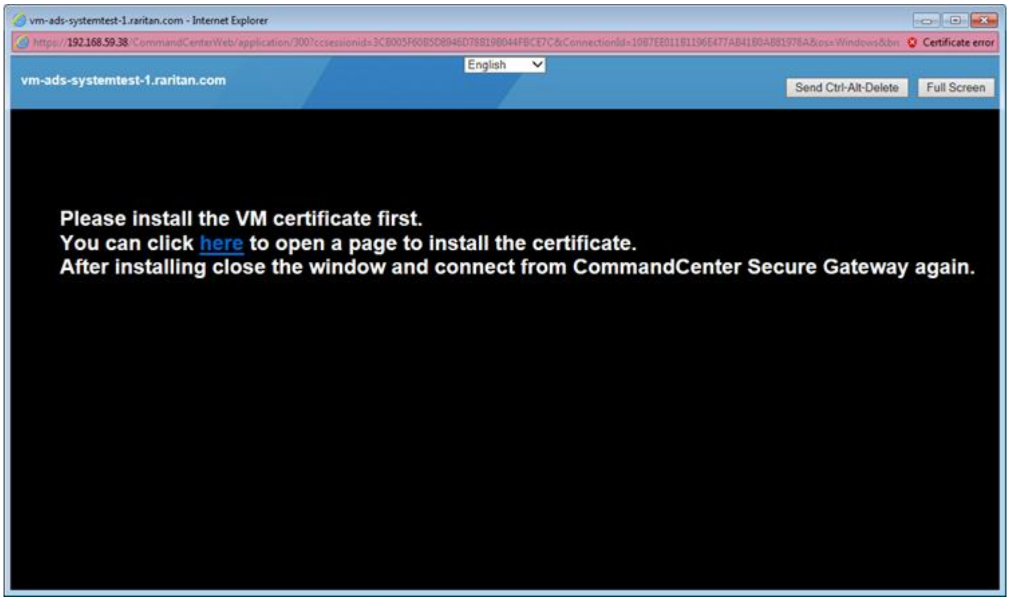
1. Select the control system or virtual host node you want to connect to in one of the node lists in the left panel.
2. In the Interfaces tab, click the VI Client interface.
3. If node auditing is enabled for your user group, the Access Information dialog appears. Enter your reason for accessing the node and then click OK.
4. Enter your username and password if requested. If single sign-on is enabled, you are connected directly to the VMware Virtual Infrastructure Web Access client.

Connect to a Virtual Machine Node via a VMW Viewer Interface

If you are using Firefox on Windows, you must add the IP address of the CC-SG to the Allowed Sites for Add-ons list and the Allowed Sites for Pop-ups list in the browser before connecting to a VMW Viewer interface.

If you are using Internet Explorer 11, you must add CC-SG to the list of Intranet IP addresses before the VMviewer is launched from CC-SG. If this is not done, you may see a message, "Please install the VMware Remote Console Plug-in". The message may display repeatedly even when the plugin is installed. Or, you may see a message "The required VMware Remote Console Plug-in version is not supported by Netscape." Add CC-SG's IP address in the browser under Tools > Internet Options > Security > Local intranet. Click Sites > Advanced, and add the CC-SG IP address to the list. Close all browsers.

The first time you connect to a virtual machine, using any supported browser, you may be asked to download an add-on from VMware.


vm-ads-systemtest-1.raritan.com - Internet Explorer
https://192.168.59.38/CommandCenterWeb/application/300?ccsessionid=3CB005F60B5D8946D78B198044FBCE7C&Connectionld=1087EE011B1196E477AB4180AB81978A&os=Windows&bn
Certificate error
English
vm-ads-systemtest-1.raritan.com
Send Ctrl-Alt-Delete
Full Screen

Please install the VM certificate first.
You can click here to open a page to install the certificate.
After installing close the window and connect from CommandCenter Secure Gateway again.

Once the add-on is installed, restart your browser. If the add-on installation fails, see ***Install VMware Plugins for Firefox 3.0*** (on page 109).

To connect to a Virtual Machine Node via a VMW Viewer Interface:

1. Select the virtual machine node you want to connect to in one of the node lists in the left panel.
2. In the Interfaces tab, click the VMW Viewer interface.
3. If node auditing is enabled for your user group, the Access Information dialog appears. Enter your reason for accessing the node and then click OK.
4. The Virtual Machine Remote Console window opens.

Send Ctrl-Alt-Delete to a Virtual Machine

Even when the virtual machine has control of the keyboard and the mouse, Ctrl-Alt-Delete is processed by both the virtual machine and the host operating system.

To send Ctrl-Alt-Delete only to the virtual machine, type Ctrl-Alt-Insert instead.

Disconnect from a Node

There are several ways to disconnect from a node. Please follow the instructions for the client you are using.

▶ **To disconnect from a node using the Access Client:**

Close the application that you are using to manage the node.

▶ **To disconnect from a node using the Admin Client:**

- In the Nodes tab, select the active node you want to disconnect from. Choose Nodes > Disconnect.
- In the Nodes tab, right-click the active node you want to disconnect from, and choose Disconnect.
- In the Nodes tab, right-click the active interface through which you are connected to the node, and choose Disconnect.
- Close the application that you are using to manage the node.

Note 1: A user with the "Device, Port, and Node Management" privileges can Disconnect users from a Node, except those initiated by a CC Super-User.

Note 2: As a CC Super-User, you can terminate any user's node connection sessions, including those initiated by another CC Super-User, in the Admin Client.

Connections that Exceed the Maximum Number of Sessions Available

CC-SG user groups can be configured so that, when members access Dominion KX, KXII and KSXII devices, a limit is imposed on the number of KVM sessions allowed per user for a given device. This prevents any single user from using all available channels at once.

When you reach the limit, a warning message displays with information on the current sessions.

```
Connection Denied: Exceeds the allotted number of sessions
for the KVM switch this node is attached to.
```

You must disconnect a session on the device before starting another new session.

Older Version of Application Opens After Upgrading

If you attempt a connection and the newest versions of applications are supposed to be working, but the incorrect, older versions are opening, clear the Java cache. This can happen if the cache hasn't been cleared since a CC-SG upgrade.

See ***Clear the Java Cache*** (on page 108)

Power Control

CC-SG enables you to control power for single nodes or node groups that have power interfaces associated with them.

You can perform power on, power off, cycle power, and graceful shutdown operations. You can also perform suspend operations for virtual nodes.

Graceful shutdown allows the node to complete any processes it is currently running, while not allowing any new processes to begin, so that the node can shutdown without interrupting anything. Graceful shutdown is not available for all node types.

In This Chapter

What are Power Control Interfaces?

Power control interfaces provide control of each power supply to the node.

Power control interfaces include:

- In-band power control interfaces, such as IPMI, iLO, Integrity ILO2, DRAC, and RSA, which control the node power directly.
- Managed power strip interfaces, which control node power via an outlet on a power strip or Dominion PX device.
- Virtual power interfaces, which control power to virtual machines.
- Power IQ Proxy interfaces, which control power to IT devices managed by Power IQ.

Tips on Controlling Power to Nodes with Multiple Interfaces

Follow these tips when cycling power to:

- servers with dual power supplies
- servers with embedded management cards that are also connected to outlets of managed power strip

1. When you must Cycle the power of a server with dual power supplies, make sure that both managed power strip interfaces are selected, and that these interfaces appear close to each other in the list of selected interfaces, as the order of execution is based on their order in the group.

2. When you must Cycle the power of a server with an embedded management card that is also connected to a Raritan managed power strip, select **either** the managed power strip interface, or the embedded power interface, but not both, to perform the power control operation. If both interfaces are selected, the timing of the commands may not allow the server's power to cycle.
3. It takes approximately one second to issue a power control command to a managed power strip or an embedded server management card.

See ***Power Control for Nodes Using the Access Client*** (on page 93) and ***Power Control for Nodes Using the Admin Client*** (on page 96).

Power Status Messages

The Power Status Messages window opens when you begin a power control operation. You should keep this window open until all power control operations are completed.

You can resize, minimize, or maximize the Power Status Messages window. You can select and then copy and paste the text in the window.

The messages in the Power Status Messages window are updated as new information is received about the status of the power control operation.

A new message appears in the Power Status Messages window when:

- Power control operation request is sent
- Power control operation fails
- Power control operation completes successfully
- All power control operations requested complete successfully

▶ How to get status updates if you close the Power Status Messages window:

- When a power control operation fails, an alert message containing information about the failed operation appears.
- The status bar at the bottom of your browser window displays an alert message when the entire operation completes successfully.
- Alert messages appear only for failed operations. Alert messages do not appear for successful operations.

Power Control for Nodes Using the Access Client

The Access Client offers several methods for controlling power to nodes and node groups.

Single Node Power Control

Single node power control allows you to control power for all or selected interfaces within a single node.

See ***Tips on Controlling Power to Nodes with Multiple Interfaces*** (on page 92) for details on setting up power control operations for nodes with more than one power control interface.

▶ Control power for all interfaces of a single node:

1. Click the node for which you want to control power in one of the node lists in the left panel. The Node details screen appears.
2. In the Power Control section, click On, Off, Cycle, Graceful Shutdown, or Suspend to perform the corresponding power control operation for all interfaces associated with the node.
3. A Power Status Messages window opens to show you the status of the power control operation. Messages populate the window as new information is received about the power control operation. Keep this window open until all power control operations are complete, so that you can monitor progress.
4. See ***Power Status Messages*** (on page 93) for details on how CC-SG alerts you to successful and failed power control operations.

▶ Control power for multiple interfaces of a single node:

If a node has dual power supplies, you should have a power control interface for each power supply. Single Node Power Control enables you to perform a power control operation on only one or multiple interfaces.

1. There are two ways to access Single Node Power Control for multiple interfaces:
   a. Click the Power Control tab at the top of the screen, and then click Single Node Power Control to open the Single Node Power Control screen.
   b. Click the node for which you want to control power in one of the node lists in the left panel, and then click Advanced in the Power Control section of the Node details screen for the selected node.
2. Click the Node drop-down arrow and select the node for which you want to control power from the list. The Available list displays all interfaces in the selected node.
3. In the Available list, select the specific interface upon which you want to perform power control and click Add to move the interface to the Selected list. Repeat this step until you have added all necessary interfaces to the Selected list.

4. Arrange the interfaces in the Selected list in the order you would like CC-SG to perform the power operation. Select an interface in the Selected list and click the up and down arrows to move the interface into the desired sequence.
5. Click the Operations drop-down arrow, and select On, Off, Cycle, Graceful Shutdown, or Suspend from the list.
6. If you selected multiple interfaces, type the number of seconds (from 0-120) that should elapse between interfaces in the Sequence Interval (seconds) field.
7. Click OK to begin the power control operation. Click OK in the confirmation message to start the operation.
8. A Power Status Messages window opens to show you the status of the power control operation. Messages populate the window as new information is received about the power control operation. Keep this window open until all power control operations are complete, so that you can monitor progress.

   See ***Power Status Messages*** (on page 93) for details on how CC-SG alerts you to successful and failed power control operations.

Node Group Power Control

Node Group Power Control allows you to control power for all or selected interfaces associated with nodes in a node group. For power on and power off operations, you can select the order in which interfaces are powered on and off.

See ***Tips on Controlling Power to Nodes with Multiple Interfaces*** (on page 92) for details on setting up power control operations for nodes with more than one power control interface.

▶ **Control power for all or selected interfaces in a node group:**

1. Click the Power Control tab at the top of the screen, and then click Node Group Power Control to open the Node Group Power Control screen.
2. Click the Node Group drop-down arrow and select the node group for which you want to control power from the list. The Interfaces for Power Control table lists all interfaces in the selected node group.
3. Select options from the Node, Interface Type, and Device drop-down menus if you want to filter the list of available interfaces. As you make selections, the Interfaces for Power Control table updates the list of interfaces that will be included in the power operation. **Optional**
4. Deselect the checkboxes next to power interfaces you want to exclude from the power operation. **Optional**
5. Click the Operations drop-down arrow, and select On, Off, Cycle, Graceful Shutdown, or Suspend from the list.

6. If you selected multiple interfaces, type the number of seconds (from 0-120) that should elapse between interfaces in the Sequence Interval (seconds) field.
7. Click OK to begin the power control operation.
8. A Power Status Messages window opens to show you the status of the power control operation. Messages populate the window as new information is received about the power control operation. Keep this window open until all power control operations are complete, so that you can monitor progress.

   See ***Power Status Messages*** (on page 93) for details on how CC-SG alerts you to successful and failed power control operations.

Power Control for Nodes Using the Admin Client

The Admin Client offers several methods for controlling power to nodes and node groups.

Single Interface Power Control

In the CC-SG Admin Client, you can select the power operation you want to perform on a specific power control interface using the interface's right-click menu.

1. In the Nodes tab, right-click the power control interface, and then click the power operation you want to perform. The Power Control screen opens.
2. The selected interface name displays in the Selected list. The power operation you selected on the right-click menu is populated in the Operation field.
3. Click OK to send the power operation request to the node. A confirmation message appears in the screen.
4. A Power Status Messages window opens to show you the status of the power control operation. Messages populate the window as new information is received about the power control operation. Keep this window open until all power control operations are complete, so that you can monitor progress.
5. See ***Power Status Messages*** (on page 93) for details on how CC-SG alerts you to successful and failed power control operations.

Single Node Power Control

You can power on, power off, cycle power, and perform graceful shutdown to a single node that has an associated power interface. If a node has more than one power interface, you can select which interfaces you want to use in the power control operation.

See ***Tips on Controlling Power to Nodes with Multiple Interfaces*** (on page 92) for details on setting up power control operations for nodes with more than one power control interface.

1. Click the Nodes tab.
2. Select the node upon which you want to perform power control.
3. Choose Nodes > Power Control. The Power Control screen opens.
4. The selected node's name appears in the Node field.
5. The node's power interfaces appear in the Selected list.
6. Arrange the interfaces in the Selected list in the order you would like CC-SG to perform the power operation. Select an interface in the Selected list and click the up and down arrows to move the interface into the desired sequence.
7. Click the Operation drop-down arrow, and select Power On, Power Off, Power Cycle, Graceful Shutdown, or Suspend from the list.
8. If you selected Power On, Power Off, Graceful Shutdown, or Suspend in the Operation field, and more than one interface in the Selected list, type the number of seconds (from 0-120) that should elapse between interfaces in the Sequence Interval (seconds) field.
9. Click OK to send the power operation request through the interface. A confirmation message appears.
10. A Power Status Messages window opens to show you the status of the power control operation. Messages populate the window as new information is received about the power control operation. Keep this window open until all power control operations are complete, so that you can monitor progress.
11. See ***Power Status Messages*** (on page 93) for details on how CC-SG alerts you to successful and failed power control operations.

Node Group Power Control

You can power on, power off, cycle power, and perform graceful shutdown for all nodes that have associated power interfaces in a node group.

This is useful if you need to power down all nodes in a node group so that you can rewire the rack on which they are mounted or if you need to perform other types of maintenance on a node group.

See ***Tips on Controlling Power to Nodes with Multiple Interfaces*** (on page 92) (in the **CC-SG User Guide**) for details on setting up power control operations for nodes with more than one power control interface.

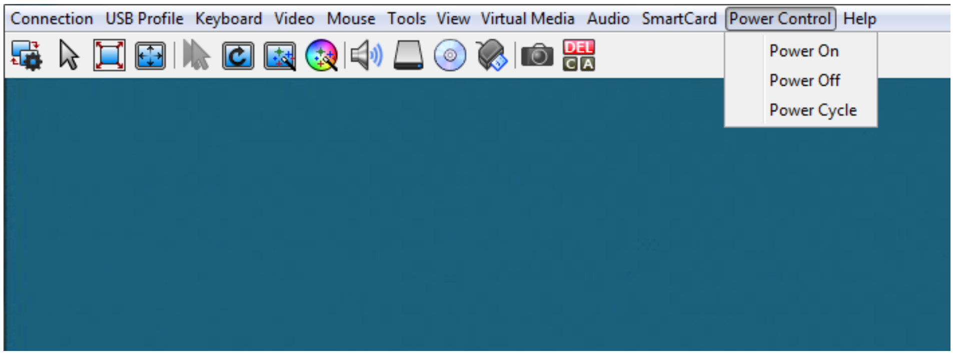
1. Click the Nodes tab.
2. Choose Nodes > Group Power Control. The Group Power Control screen appears.
3. Click the Node Group drop-down arrow and select the node group whose power you want to control from the list.
4. In the Available list, select the specific interface on which you want to perform power control, and then click Add to move the interface to the Selected list. Repeat this step until you have added all necessary interfaces to the Selected list. If you must remove an interface, select the interface in the Selected list, and then click Remove.
5. Arrange the interfaces in the Selected list in the order you would like CC-SG to perform the power operation. Select an interface in the Selected list and click the up and down arrows to move the interface into the desired sequence.
6. Click the Operation drop-down arrow, and select Power On, Power Off, Power Cycle, Graceful Shutdown, or Suspend from the list.
7. If you selected Power On, Power Off, Graceful Shutdown, or Suspend in the Operation field, type the number of seconds (from 0-120) that should elapse between interfaces in the Sequence Interval (seconds) field.
8. Click OK to send the power operation request through the selected interfaces. A confirmation message appears.
9. A Power Status Messages window opens to show you the status of the power control operation. Messages populate the window as new information is received about the power control operation. Keep this window open until all power control operations are complete, so that you can monitor progress.

   See ***Power Status Messages*** (on page 93) for details on how CC-SG alerts you to successful and failed power control operations.

Power Control Using VKC, VKCS, and AKC

You can power on, power off, and power cycle a target through the outlet it is connected to.

Access the target, and then select a power control option from the Power Control menu.



The menu option is disabled if you do not have permission for power control, and when outlets are not associated with the port.

Node Chat

Web Interfaces do not allow node chat.

In This Chapter

Node Chat Using the Access Client

You can chat with other users who are connected to the same node as you. Any participant can end a chat session. However, if the user who initiated the chat ends the session, then the entire chat session is terminated and all chat windows are closed. If you end a chat session and you are not the initiator, then you can rejoin the session later if it is still active.

1. Click the connected node whose other users you want to chat with in one of the node lists in the left panel. The Node details screen opens.
2. Click Open Chat beneath the Interface section. The Chat dialog appears.
3. Type your message in the bottom box and click Send.
4. To end the chat session, click Close.

Node Chat Using the Admin Client

Chat provides a way for users connected to the same node to communicate with each other. You must be connected to a node to start a chat session for that node. Only users on the same node will be able to chat with each other.

▶ **To participate in a chat session:**

1. Click the Nodes tab.
2. Right-click on a node to which you are currently connected and select Chat. Click Start Chat Session if no session has been created yet. A Chat session will be created.

   If a chat session is in progress, right-click on the node, select Chat, then Show Chat Session to join the chat session.

   The chat session window will appear with the message fields on the left and a list of users in the chat session on the right.
3. Type a message in the new message (lower left) field and either press the Enter key or click Send. The message will appear in the chat (upper left) field for all users to see.
4. Click Clear to clear any message you have typed in the new message field but have not sent. Clear will not clear the chat field.
5. Click Close to leave or end the chat session.

6. You will be prompted if you want to close the chat session. Click Yes to close the chat session for all participants, click No to exit the chat session but leave it running for others.

   You can also close a chat session for all participants from the nodes tab. Right click on the node with the chat session, select Chat, then End Chat Session.

My Profile

In This Chapter

My Profile in the Access Client

The My Profile tab allows you to change your password, email address, and default node list.

Change Your Password

You can change your password if your account is locally authenticated. If your account uses remote authentication, contact the administrator to change your password.

▶ **To change your password:**

1. Click the My Profile tab. The My Profile page opens.
2. Select the Change Password (For Local Authentication Only) checkbox to activate the change password fields.
3. Type your current password in the Old Password field.
4. Type your new password in the New Password and Retype New Password fields.
5. Click OK.

Note: If you see a Strong passwords are required text label next to the New Password field, the Administrator has enabled strong passwords. Strong passwords must contain a minimum of 8 characters and satisfy other requirements as defined by the Administrator.

If you see a Strong passwords are not required text label next to the New Password field, the Administrator has not enabled strong passwords. Your password must contain 6-16 characters.

Change Your Email Address

The Email Address field in the My Profile screen displays the email address currently associated with your CC-SG User ID.

1. Click the My Profile tab. The My Profile screen opens
2. Type your new email address in the Email Address field.
3. Click OK.

Set Default Node List

The Default Node List field in My Profile allows you to define which node list appears in the left panel upon login.

1. Click the My Profile tab. The My Profile screen opens
2. Click the Default Node List drop-down arrow, and then select All Nodes, Favorite Nodes, or Recent Nodes from the list.
3. Click OK to save your default node list selection.

My Profile in the Admin Client

My Profile allows you to change your CC-SG password and email address, adjust the CC-SG display's font size, and set your default search type preference. You can also view information about how long you can use your password before you are forced to change it.

Change Your Password

You can change your CC-SG password whenever you want, provided your account is locally authenticated. If your account uses remote authentication, contact the administrator to change your password.

The CC-SG Administrator can configure CC-SG to force you to change your password periodically.

▶ **To change your password:**

1. Choose Secure Gateway > My Profile. The Change My Profile screen appears.
2. Select the Change Password (For Local Authentication Only) checkbox to activate the change password fields.
3. Type your current password in the Old Password field.
4. Type your new password in the New Password and Retype New Password fields.

   Note: If you see a Strong passwords are required text label next to the New Password field, the Administrator has enabled strong passwords. Strong passwords must contain a minimum of 8 characters, and satisfy other requirements as defined by the Administrator. If you see a Strong passwords are not required text label next to the New Password field, the Administrator has not enabled strong passwords. Your password must contain 6-16 characters.

5. Click OK to set your new password.

Change Your Email Address

1. Choose Secure Gateway > My Profile. The Change My Profile screen appears.

2. Type your new email address in the Email address field.
3. Click OK.

Change the CC-SG Font Size

CC-SG will use the font size you select for all text in its screens.

1. Choose Secure Gateway > My Profile. The Change My Profile screen appears.
2. Click the Font Size drop-down arrow and select the font size that you want CC-SG to use in its screens.
3. Click OK.

Set Search Preference

CC-SG offers two search types, Filter by Search Results and Find Matching String. You can set your search preference in My Profile.

- Filter by Search Results: type search terms and then click Search to display a list of nodes that match your search terms. You can use wildcards (*) with this search type.
- Find Matching String: type search terms and as you type, the node in the list that best matches your search is highlighted. There is no Search button. You cannot use wildcards with this search type.

To set your search preference:

1. Choose Secure Gateway > My Profile. The Change My Profile screen appears.
2. In the Search Preference panel, click the radio button that corresponds to the search type you want to use.
3. Click OK.

Devices Port Sorting Options

CC-SG offers several port sorting options to determine how ports are listed in the Devices tab. You can set your preference in My Profile in the Admin Client only.

To select port sorting options:

1. Choose Secure Gateway > My Profile. The Change My Profile screen appears.
2. In the Devices Port Sorting Options box, click the radio button for the sorting option you prefer:
   - By Port Name
   - By Port Status
   - By Port Number
3. Click OK.

Appendix A Keyboard Shortcuts

The following keyboard shortcuts can be used in the Admin Client.

Operation	Keyboard Shortcut
Refresh	F5
Print panel	Ctrl + P
Help	F1

Appendix B Troubleshooting

- Launching CC-SG from your web browser requires a Java plug-in. If your machine has an incorrect version, CC-SG will guide you through the installation steps. If your machine does not have a Java plug-in, CC-SG cannot automatically launch. In this case, you must uninstall or disable your old Java version and provide serial port connectivity to CC-SG to ensure proper operation.
- If CC-SG does not load, check your web browser settings.
  - In Internet Explorer, ensure Java (Oracle) is enabled.
  - Open Java plug-in in the Control Panel and adjust the settings for your browser.
- If you have problems adding devices, ensure the devices have the correct firmware versions.
- If the network interface cable is disconnected between the device and CC-SG, wait for the configured heartbeat minutes, and then plug the network interface cable back in. During the configured heartbeat period, the device operates in standalone mode and can be accessed through VKC.
- If you receive an error message that states your client version is different from the server version and that behavior may be unpredictable, you should clear the browser's cache and the Java cache and restart the browser. See ***Clear the Browser's Cache*** (on page 108) and ***Clear the Java Cache*** (on page 108).
- If the memory usage is rising dramatically or the browser session stops responding to your actions, you may need to increase your Java Heap size for your client.

  a. Open Java plug-in in the Control Panel.

  b. Click the Java tab.

  c. Click View inside the Java Applet Runtime Settings group box.

  d. Select the row of the current Java version you are running and type `-Xmx<size>m` in the Java Runtime Parameters column. For example, type `-Xmx300m` if you want to increase the Java Heap size to a maximum of 300MB.

  It's not recommended to set the Java Heap size higher than half of the client computer's memory. For example, if the client computer has 4.0 GB of RAM, set the parameter to -Xmx2048m maximum.
- If you access more than one CC-SG unit using the same client and Firefox, you may see a "Secure Connection Failed" message that says you have an invalid certificate. You can resume access by clearing the invalid certificate from your browser.

  a. In Firefox, choose Tools > Options.

  b. Click Advanced.

  c. Click the Encryption tab.

d. Click View Certificates and find "Raritan" in the list.

e. Select the CommandCenter item and click Delete. Click OK to confirm.

In This Chapter

Clear the Java Cache

These instructions may vary slightly for different Java versions and different operating systems.

► **In Windows:**

1. Choose Control Panel > Java.
2. On the General tab, click Settings.
3. In the dialog box that opens, click Delete Files.
4. Make sure the Applications and Applets checkbox is selected then click OK.

Clear the Browser's Cache

These instructions may vary slightly for different browser versions.

► **Internet Explorer:**

1. Choose Tools > Internet Options.
2. On the General tab, click Delete Files then click OK to confirm.

► **In FireFox:**

https://support.mozilla.org/en-US/kb/how-clear-firefox-cache#w_clear-the-cache

Install VMware Plugins for Firefox 3.0

You must install the VMware MKS plugin before you can access a VM Viewer interface. If you use the Firefox 3.0 browser, this plugin installation fails.

An error message appears.

```
Error: Firefox could not install the file at
https://<sm_server_hostname>/StageManager/ControlPane
l/Machines/MachineDetails/ActiveXControls/xpihandler.
ashx?filename=vmware-mks-windows-ff-3.xpi  because:
Install script not found -204
```

Go to VMware knowledge base article number 1006950 for details and workaround.

The VMware knowledge base is at kb.vmware.com.

Workaround for Issues with RDP and Chrome Access to KX3

When KX3 v3.4 is launched directly via latest version Chrome browser from an RDP session and KVM launching of target is attempted, the HKC target window opens to a blank white screen. The same behavior is seen when the KX3 device is under CC-SG management and launched in Chrome browser using HTML client via RDP session. This is due to WebGL.

Google has disabled WebGL support for some old GPUs and graphics drivers.

▶ **Workaround:**

Enable "Override software rendering list" in chrome://flags

Index