Raritan.

A brand of **legrand®**

CommandCenter Secure Gateway

User Guide

Release 6.2

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.

CE c(UL)us 1F61
LISTED   I.T.E.

Contents

Chapter 4   Connecting to Nodes   26

Cannot Write To/From a File from a Mac Client   64

Chapter 5   Power Control   65

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.

Connect to a Virtual Machine Node via a VMW Viewer Interface (on page 60)

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

Chapter 1   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.

Chapter 2 Accessing CC-SG

You can access CC-SG in two ways:

- Through a browser: CC-SG offers two browser-based access options, a Java-based CC-SG Admin Client and an HTML-based CC-SG Access Client.

  For a complete list of browsers and platforms, refer to the CC-SG Compatibility Matrix on the Raritan web site in the Support section under Firmware and Documentation.

- Through a thick client: You can install a Java Web Start thick client on your client computer. The thick client functions exactly like the browser-based CC-SG Admin Client.

Note: Multiple users can be connected simultaneously, using any client.

In This Chapter

Before You Begin

CC-SG is accessed via a web browser from a user's PC. Verify that you have installed a supported Java Runtime Environment (JRE) version and disabled pop-up blockers.

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 Sun JRE in the Application list.

▶ **To upgrade JRE:**

Go to *http://java.sun.com/products/archive* (*http://java.sun.com/products/archive*).

Disable Pop-up Blockers

The client PC and the browser should have all pop-up blockers disabled.

Browser-Based Access via the CC-SG Access Client

The CC-SG Access client is an HTML-based client that provides a GUI for access tasks, based on your permissions.
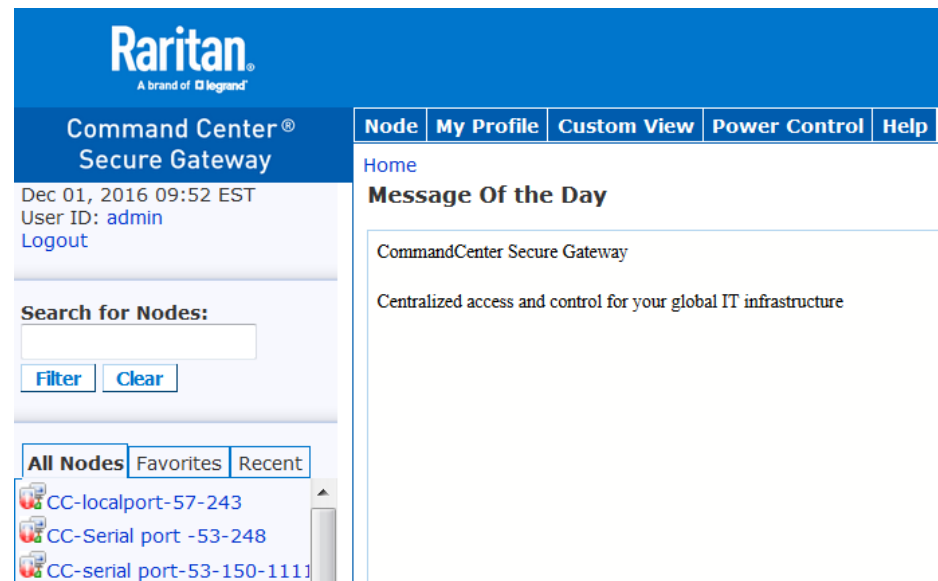
1. Using a supported Internet browser, type the URL of the CC-SG: http(s)://*IP address*, for example, *http://10.0.3.30* (*https://10.0.3.30*) or https://10.0.3.30. The login page opens.
2. If the CC-SG Administrator has enabled the Restricted Service Agreement, read the agreement text, and then select 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 1.5 or 2.0

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

Only the Access Client supports the drop-down list for the Neighborhood feature. The Neighborhood feature groups multiple CC-SG units and enables you to switch among these CC-SG units with single sign-on.

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.

When you switch to another CC-SG, you also need to have an account on that system. Otherwise, the authentication will fail.

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

▶ **To access another CC-SG unit in the same Neighborhood**

1. Click the Secure Gateway drop-down arrow, and select the CC-SG unit you want to access from the list.

2. Click Go.

The node lists in the All Nodes, Favorites, and Recent tabs all change to display the nodes available in the new CC-SG if the access to the new CC-SG unit is successful.

Access from a Mobile Device

You can run the CC-SG Access Client using your mobile device's browser. In CC-SG version 5.2, Safari browser on iPhone and iPad are supported. Other mobile devices will be supported in future releases.

Your CC-SG's browser connection protocol must be configured for HTTPS/SSL for mobile device access. To set, log in to the Admin Client, choose Administration>Security, click the Encryption tab, then select HTTPS/SSL and click Update.

When you connect to CC-SG on your iPhone or iPad, you access targets using the Mobile KVM Client (MKC). See *Connecting to Nodes using a Mobile Device* (on page 39).

Browser-Based Access via the CC-SG Admin Client

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, 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).*

   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.

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.

Thick Client Access

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. If the CC-SG is configured for secure browser connections, you must select the Secure Socket Layer (SSL) checkbox. If the CC-SG is not configured for secure browser connections, clear the Secure Socket Layer (SSL) checkbox. This setting must be correct or the thick client will not be able to connect to CC-SG.

   ▪ To check the setting in CC-SG: Choose Administration > Security. In the General tab, look at the Browser Connection Protocol field. If the HTTPS/SSL option is selected, then you must select the Secure Socket Layer SSL checkbox in the thick client's IP address specification window. If the HTTP option is selected, then you must deselect the Secure Socket Layer SSL checkbox in the thick client's IP address specification window.

6. 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.

7. 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.

8. 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.

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.

Internet Explorer 10 and 11 Access

When accessing CC-SG using the Internet Explorer 10 or 11 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.

Raritan.
A brand of legrand

Mac and Safari Access

KVM target connections are not automatically launched from the latest Safari versions.

The following steps will correct this.

Option 1:

When connecting to a target, click "Open the Finder" from your Mac's Download icon, select the downloaded jnlp file, then right click Open.

Option 2:

Choose System Preferences > Security & Privacy > Allow apps downloaded from: Anywhere.

Chapter 3   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 10) and *Finding and Viewing Nodes in the Admin Client* (on page 14) 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 20) and *Using Custom Views in the Admin Client* (on page 22) 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

1. Current CC-SG name: The name of the CC-SG unit you are accessing appears at the top of the left panel.

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 13).

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 20).

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 19).

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 14)/

▶ **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.

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

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 22).

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 79).

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 79).

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 Windows2000, and Windows2003 Server
*	Indicates zero or more characters.	Windows*	Locates Windows2000, but not Windows2003 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 bookmark an interface in Internet Explorer (add an interface to your Favorites):**

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 Add Bookmark (IE Only).
4. A default name for the bookmark appears in the Bookmark Name field. You can change the name, which will appear in your Favorites list in Internet Explorer.
5. Click OK. The Add Favorite window opens.
6. Click OK to add the bookmark to your Favorites list.

▶ **To access a bookmarked interface:**

1. Open a browser window.
2. Choose the bookmarked interface from the list of bookmarks in the browser.
3. When the CC-SG Access Client appears, log in as a user who has access to the interface. The connection to the interface opens.

▶ **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 Screen Overview* (see "*CC-SG Access Client Overview*" on page 11).

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.

Raritan.
A brand of legrand

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:

Raritan.
A brand of ☐ legrand®

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.

▶ **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 CC-SG will see the Nodes tab sorted according to the selected custom view. Users can change the custom view.

Chapter 4 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 51).

See *Connecting to Nodes using the Access Client* (on page 27), *Connecting to Nodes using a Mobile Device* (on page 39), and *Connecting to Nodes using the Admin Client* (on page 49) 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 50).

- *Connect to a Node via an Out-of-Band KVM Interface* (on page 52)
- *Connect to a Node via an Out-of-Band Serial Interface* (on page 54)
- *Connect to an iLO Processor Enabled Node* (on page 55)
- *Connect to a Node via an In-Band KVM Interface* (on page 55)
- *Connect to a Node via a Web Browser Interface* (on page 59)

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 67) and *Power Control for Nodes Using the Admin Client* (on page 69).

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.

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 12).
- 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 73).
- 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 67).
- 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 19) 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.

Raritan.
A brand of legrand

- 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:

1. Target device must be
   - KX3 - 3.2 or 3.4
   - KX2 - 2.7
   - KX2-101 V2 3.7
   - KSX - 2.7 GA
2. "Enable AKC Download Server Certificate Validation" must be enabled in CC-SG. Choose Administration > Configuration > Device Settings. Device certificates should be trusted by client PC.

HTML Serial Console (HSC) Help

Use HSC to connect to serial targets from SX2. HSC is also launched when accessing SX2 targets in CC-SG. **Note:** HSC does not support CC-SG's proxy mode in release 6.2.

Note: You can also access targets via Direct Port Access, command line interface (CLI), local port GUI, and SSH.

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.
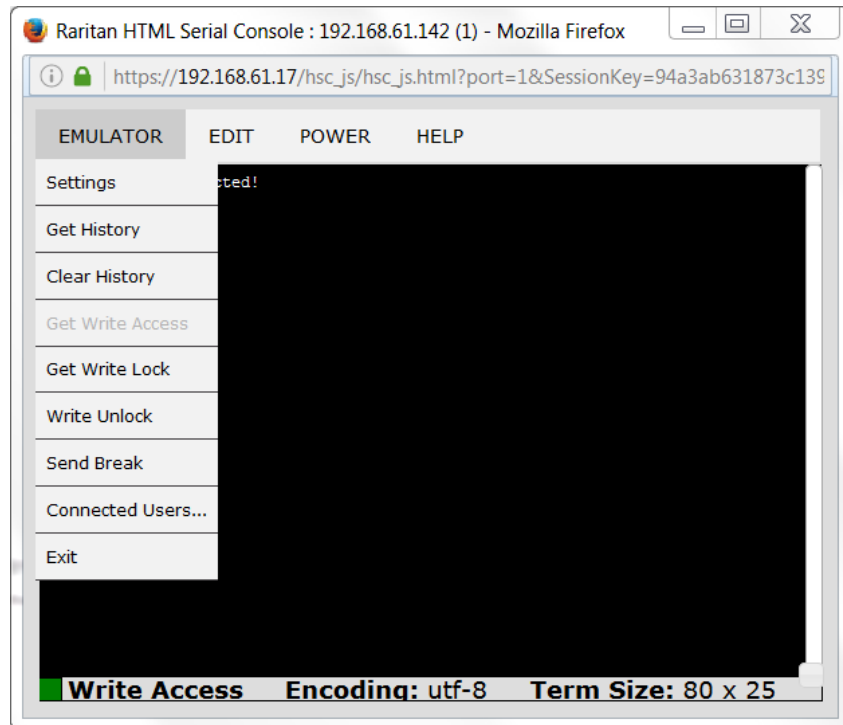
Settings

Note: An Administrator can set Terminal emulation settings using Setup > Port Configuration.

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

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:
   - US-ASCII
   - ISO-8859-1
   - ISO-8859-15
   - UTF-8
   - 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.

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.

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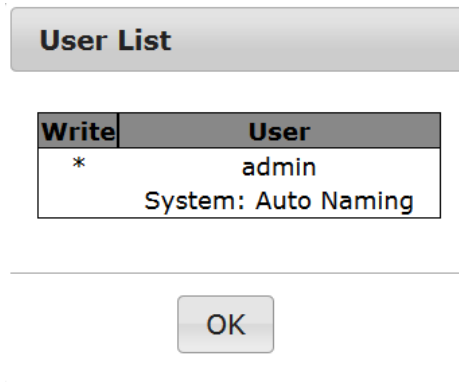
2. A star appears in the Write column for the User who has Write Access to the console.

Exit

1. Choose Emulator > Exit to close the HSC.

Copy and Paste

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.

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 a Text File* (see "*Send Text File*" on page 35).

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, Raritan Serial Console (RSC) sends whatever file you selected directly to the port.

- If there is currently no target connected, nothing is visible on the screen.
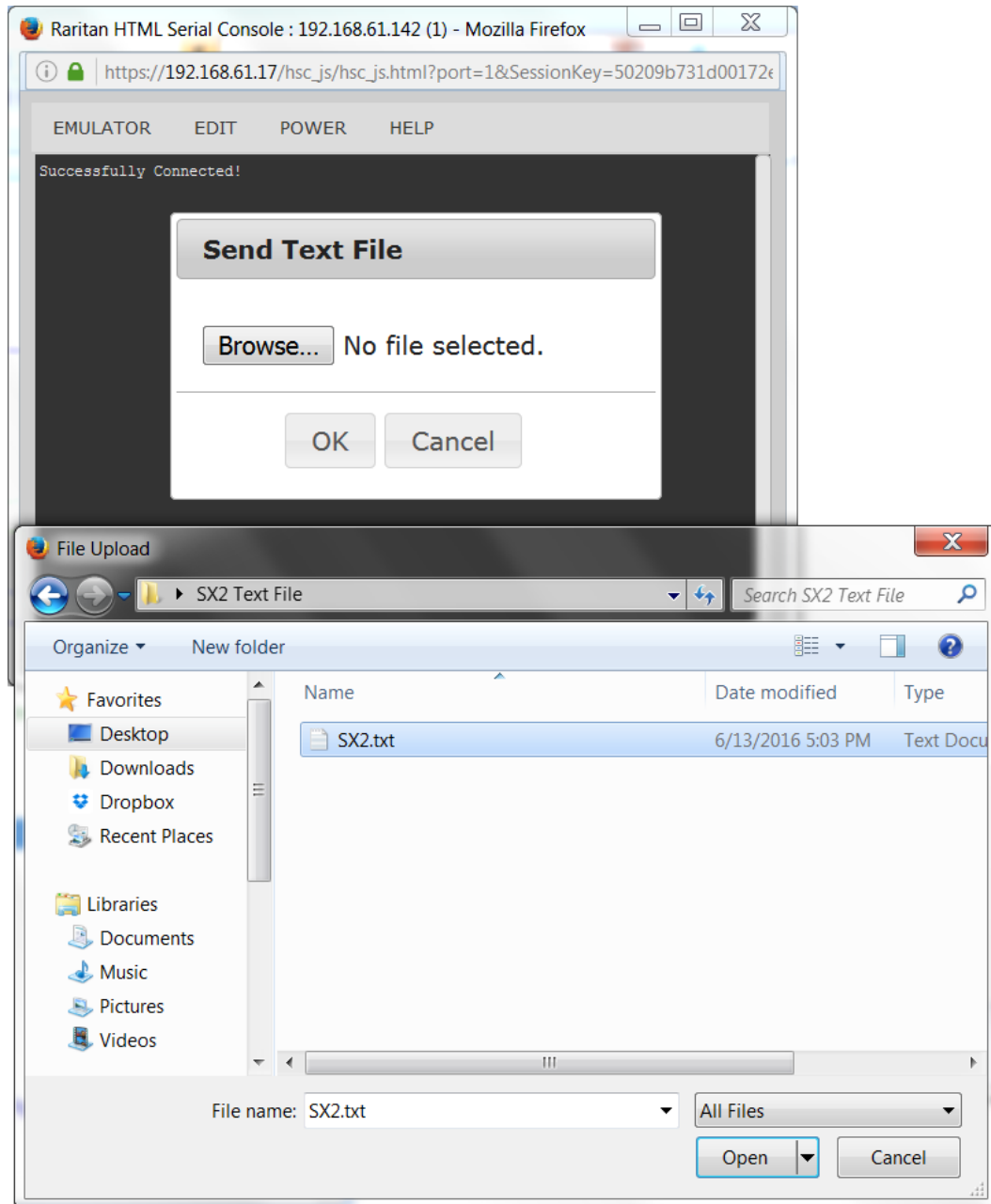
▶ Note, if you are using a Mac® and/or Safari®, do the following in order to use this feature:

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.

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.
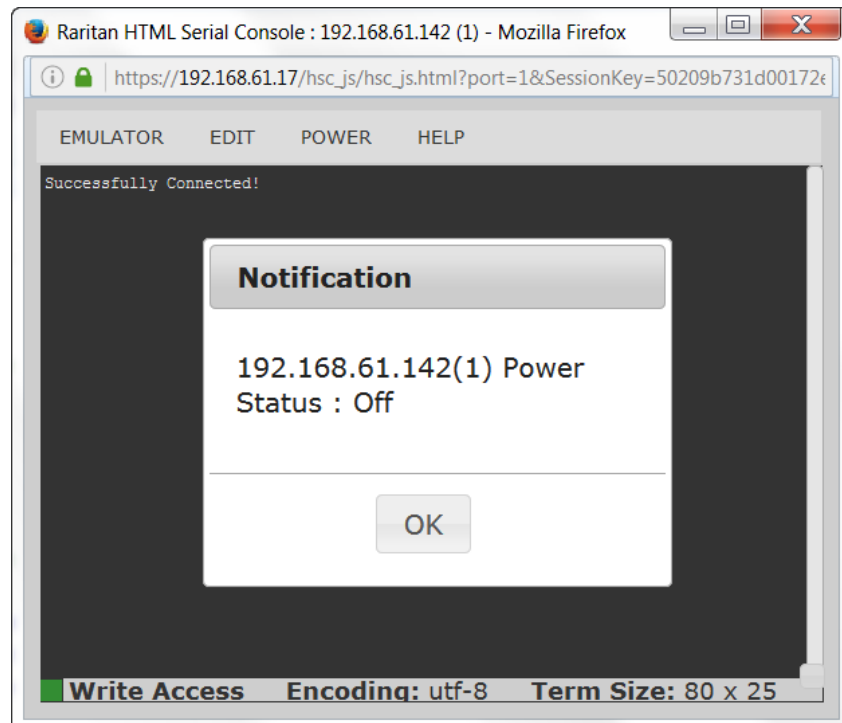
Power on a Target

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.

OK
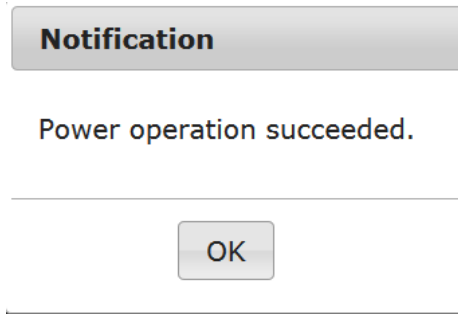
Power Off a Target

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.

OK
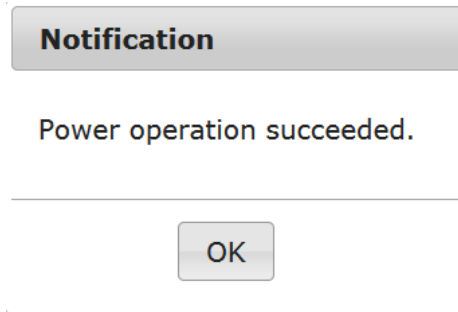
Power Cycle a Target

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.

Raritan.
A brand of ☐legrand®

Connecting to Nodes using a Mobile Device

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

Accessible interfaces include out-of-band KVM interfaces, in-band power control interfaces, and web browser interfaces. See *Mobile Device Accessible Interfaces* (on page 40) for the complete list of accessible interfaces.

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

Out-of-Band KVM interfaces are accessible using the Mobile KVM Client (MKC), rather than AKC or VKC.

MKC launches automatically for all out-of-band KVM interfaces accessed from mobile devices. There is no configuration or selection of MKC required. See *Connect to a Node via an Out-of-Band KVM Interface on a Mobile Device* (on page 39) and *Mobile KVM Client* (on page 41).

You connect to each interface using the same links as when accessing from PC. When MKC opens, use the touch screen equivalent to each mouse click operation for navigating. See *Touch Mouse Functions* (on page 41).

The mobile device does not provide file storage for keyboard macros, so keyboard macros that you have created and would like to use in MKC can be stored on CC-SG with your profile data. You must import user-defined keyboard macros, using the desktop Access Client, before they will be available in MKC. See *Manage Mobile Client Keyboard Macros* (on page 76).

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

Only Dominion KX2 2.4 or later, and KX3 connected targets can be accessed on a mobile device using MKC. See the Compatibility Matrix for the most up-to-date list of supported targets.

See *Mobile KVM Client* (on page 41) for details on using the client.

▶ **To connect to a node via an out-of-band KVM interface on a 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 Mobile KVM Client opens and connects to the target.

Use Exit to Close Mobile KVM Client Sessions

Connections to nodes made from your mobile device should be properly closed using the Exit menu command in the Mobile KVM Client (MKC). This ensures that resources are quickly released and made available for other connections.

If sessions are not properly closed, they will be automatically closed after a period of inactivity. Sessions will not be closed if they are active. The mobile client timeout period is configured in the Admin Client, in Administration > Security. The default mobile client timeout is 8 minutes. The mobile client timeout is always enabled.

This timeout applies to mobile client access only and is in addition to the Inactivity Timer and any device specific idle timeout value. It is intended to allow a shorter timeout period to be defined and applied to mobile client access.

Examples of closing a session improperly include touching the X in the top left corner to close a browser window, leaving a browser window open and turning your device off, or putting a browser window in the background.

▶ **To use exit to close a mobile KVM client session:**

- In the MKC toolbar, touch Menu, then touch Exit.

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 KXII 2.4 only. 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

Mobile KVM Client

The Mobile KVM Client (MKC) is used to connect to out-of-band KVM nodes when you are using your mobile device, such as an iPad or iPhone.

Enable pop-ups in your mobile device browser before accessing the CC-SG Mobile Access Client and MKC.

MKC does not support connections over IPv6.

Touch Mouse Functions

Use the touchscreen equivalent for each mouse function to navigate the Mobile KVM Client (MKC) on your mobile device.

To view this chart in MKC, touch the Help icon (?) in the MKC toolbar.

Single Finger Touch	Mouse Equivalent
touch down - move - release	move mouse pointer
short tap	left click
double short tap	left double-click
short tap - touch down - move - release	hold down left mouse button and move, as in drag and drop or select

Two Finger Touch	Mouse Equivalent
touch down - move - release	move screen
touch down - change distance - release	resize screen (short pause at 100% zoom)
short tap	right click
double short tap	right double-click
short tap - touch down - move - release	hold down right mouse button and move, as in right drag and drop

Using the MKC Toolbar

The MKC toolbar may not be completely visible at one time, depending on the resolution of your mobile device.

▶ **To view the whole toolbar:**

• Touch and swipe to move the toolbar icons to the left and right, bringing different icons into view.

▶ **To use the keyboard button icons:**

The toolbar contains icons for each keyboard button you may need. Touch and swipe left and right to view all icons.

• Touch an icon for a button press.
• For a button hold, such as for Control and Alt used in Control+Alt+Delete, touch the icon once to activate it. The icon color will darken to indicate it is currently pressed. To release the icon, touch again.

MKC Toolbar Icons

Depending on your mobile device screen size and resolution, you may not see all toolbar icons at once. For example, on tablet device, such as an iPad you may see F4 as the final icon to the right.

Touch and swipe the toolbar to the left, to view the F5 through F12 icons. Swipe the toolbar back to the right to return to the default view.

On a mobile phone device, such as an iPhone, you will see fewer icons. Use the same touch-and-swipe motion left and right to view additional icons.

▶ Keyboard Icon

Provides access to the mobile device's native soft keyboard. See *Display Mobile Device Keyboard* (on page 44).

▶ Shift (SHIFT) – Control (CTRL) – Alternate (ALT)

Provide the modifier keys to be used together with other keys on the toolbar. See *Using the MKC Toolbar* (on page 42).

▶ Windows (WIN)

Provides access to the Windows Start menu. This is the equivalent of the Windows key on a standard Windows keyboard.

▶ Application Key or "Right-Click" Key

Provides access to a right-click menu. This is the equivalent of the Application key on a standard Windows keyboard. The Application key has an image of a mouse pointer on a menu, and it is positioned between the Alt and Ctrl keys to the right of the spacebar.

Touch the Application icon to display the selected item's right-click menu.

▶ Left Arrow, Up Arrow, Down Arrow, Right Arrow

Provide document navigation.

▶ Tab (TAB) – Escape (ESC) – Delete (DEL) – Function 1 (F1) thru Function 12 (F12)

Provide standard press and release key operation.

Display Mobile Device Keyboard

Toggle on and off the MKC keyboard to display or hide it.

The keyboard is configured on the mobile device. For example, on iPad choose Settings > General > Keyboard > International Keyboards to see the available keyboards or to add a keyboard. From the soft keyboard touch the globe icon to toggle between available keyboards.

► **To display/hide mobile device keyboard:**

- In the MKC toolbar, touch the keyboard icon, next to the Menu button to display the keyboard.
- In the keyboard, touch the icon in the bottom right corner to hide the keyboard.

Display Connection Info

Display information about your connection to see how much bandwidth is being used in transmitting and receiving data.

This information can be helpful in determining how much of the available bandwidth is being consumed, the effect of selecting a lower video quality setting, or for troubleshooting if image updates are slower than expected. See *Set Video Connection Quality* (on page 48).

Incoming	kpx/s	pixel updates per second
	kB/s	bytes per second
Outgoing	msg/s	messages per second
	kB/s	bytes per second

► **To display connection info:**

- In the MKC toolbar, touch Menu, then touch Connection Info.

  The connection information appears in the viewer.

  To turn off the connection information display, touch Menu, then touch Connection Info. The display toggles off.

Set Keyboard Type

The default keyboard in MKC is US/International English. Select the language keyboard to match the language keyboard setting of the target you are accessing. This is required to provide the correct keyboard mapping in the target.

You must correctly set the keyboard type in MKC based on the language mapping required by the target. This setting is in addition to the keyboard language setting on your mobile device itself.

▶ **To set keyboard type:**

1. In the MKC toolbar, touch Menu, then touch Keyboard Type.
2. Touch the keyboard language to set it.

Keyboard Languages

- Danish (Denmark)
- English (UK)
- English (US/Int'l)
- French (Belgium)
- French (France)
- German (Germany)
- German (Switzerland)
- Hungarian
- Italian (Italy)
- Japanese
- Korean (Korea)
- Norwegian (Norway)
- Portuguese (Portugal)
- Slovenian
- Spanish (Spain)
- Swedish (Sweden)

Launch Keyboard Macro

Pre-defined macros are always available in MKC. You must import user-defined macros using the desktop Access Client before they are available on MKC. See *Manage Mobile Client Keyboard Macros* (on page 76).

SUN macros are available in MKC if you are connected to a target that has the SUN CIM.

► **To launch keyboard macro:**

1. In the MKC toolbar, touch Menu, then touch Keyboard Macros.
2. Touch the macro you want to launch.

   The macro is launched and the results display on the target.

Set Mouse Mode

When controlling a target server, the MKC displays two mouse cursors: a red bullseye indicates where the mobile touch gestures are relative to the target, and the cursor that belongs to the target server.

Single mouse mode is not available in MKC.

Your mouse will operate in dual mouse mode only. When properly configured, the two mouse cursors align.

There are several mouse modes when in dual mouse mode. Mouse modes are available based on the attached CIM and selected USB profile.

- See *Absolute Mouse Mode* (on page 47).
- See *Intelligent Mouse Mode* (on page 47).
- See *Standard Mouse Mode* (on page 47).

► **To set mouse mode:**

1. In the MKC toolbar, touch Menu, then touch Mouse.
2. Touch Mouse Mode, then touch Absolute, Intelligent, or Standard.

Absolute Mouse Mode

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

Note: For KX II, Absolute Mouse Synchronization is available for use with the virtual media-enabled USB CIM (D2CIM-VUSB and D2CIM-DVUSB) only.

Intelligent Mouse Mode

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

During synchronization, the mouse cursor does a "dance" in the top left corner of the screen and calculates the acceleration. For this mode to work properly, certain conditions must be met.

See the Dominion KXII User Guide for more details on Intelligent Mouse mode.

Standard Mouse Mode

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.

Sync Mouse in Intelligent or Standard Mouse Mode

In Intelligent or Standard mouse mode, the Sync Mouse command forces realignment of the target server mouse pointer with the MKC mouse pointer.

▶ **To sync mouse:**

1. In the MKC toolbar, touch Menu, then touch Mouse.
2. Touch Sync Mouse. Wait several seconds while the synchronization occurs.

Auto-Sense Video Settings

The Auto-sense Video Settings command forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.

Auto-sensing video settings can eliminate target video misalignment and sometimes mouse synchronization problems.

▶ **To auto-sense video settings:**

1. In the MKC toolbar, touch Menu, then touch Video.
2. Touch Auto Sense Video Settings.

Set Video Connection Quality

Adjust the bandwidth consumed by the connection by setting the video connection quality.   A lower quality setting will consume less bandwidth by providing lower video quality.

Use the connection information display to get bandwidth information to help adjust the video connection quality. See *Display Connection Info* (on page 44).

▶ **To set video connection quality:**

1. In the MKC toolbar, touch Menu, then touch Video.
2. Touch Connection Quality Settings, then touch High, Medium, or Low. The default setting is High.

View MKC Help

Descriptions of the touchscreen techniques can be accessed in MKC.

▶ **To view MKC help:**

* Touch the Help icon (?) icon in the toolbar. The help opens.
* See *Touch Mouse Functions* (on page 41) to view this information.

Connecting to Nodes using the Admin Client

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 69).

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 19) 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.

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 only
- HTML Serial Console (HSC) - available for SX2 and DSAM only
- 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

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

Interface Type	Interface Abbreviation	Supports Proxy Mode?
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	Java RDP, Microsoft RDP
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
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.

Raritan.
A brand of legrand

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.
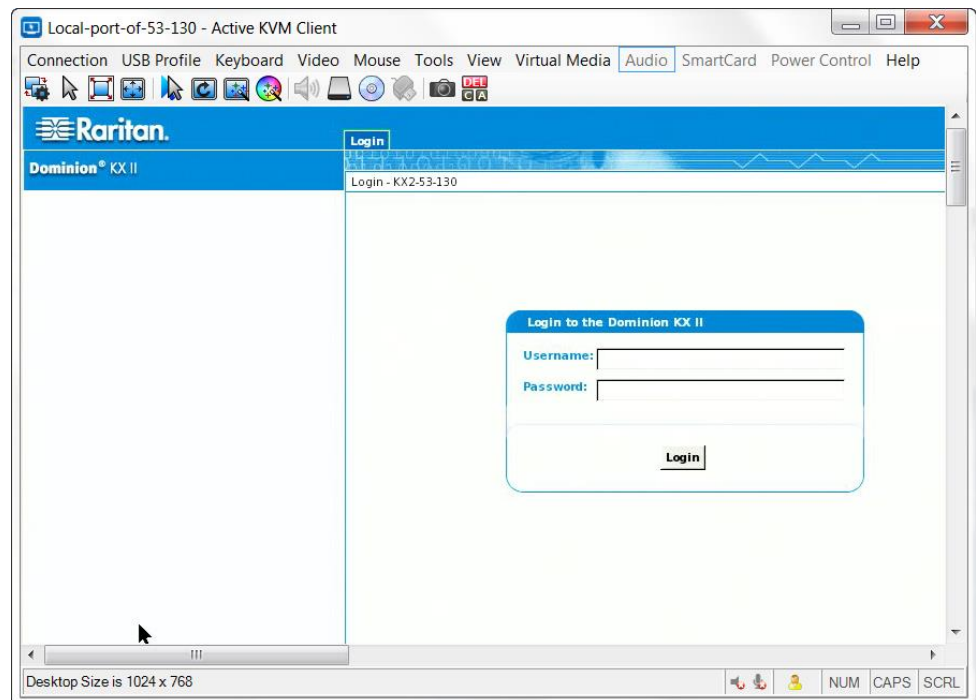
> Note: The .NET AKC client looks and operates like VKC, with a few exceptions.

6. To disconnect from VKC, choose Connection > Exit.

Prerequisites for Using AKC

- Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.
- Windows Vista, Windows 7 and Windows 2008 server users should 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.

Enable AKC Download Server Certificate Validation

If the device (or CC-SG) administrator has enabled the Enable AKC Download Server Certificate Validation option:

- 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.

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.

        ▪ If CC-SG Administrators have not configured the username and password in the interfaces, you must type the Username and Password in the dialog.

        ▪ 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.

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.

DRAC 5 Connection Details

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.

▶ **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.

▶ **To connect DRAC interfaces with Internet Explorer 9:**

1. In Internet Explorer 9, choose Tools > Options.

2. In the Privacy tab, set the slider to Low for cookies to access the DRAC Interface.

3. At the "Do you want to open or save vkvm.jnlp" prompt, click Open to launch the DRAC interface.

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 58).
- When adding RDP interfaces to Windows 7, make sure that ICMPv4 and ICMPv6 are allowed by the Windows 7 firewall.

Microsoft RDP Connection Details

- If using a Windows XP client, you must have Terminal Server Client 6.0 or higher to connect a Microsoft RDP interface from CC-SG. Update the Terminal Server Client to 6.0 using this link: http://support.microsoft.com/kb/925876.
- Internet Explorer only.
- Microsoft RDP cannot be used for proxy mode IPv6 connections. See *About Connection Modes* (on page 58).
- Targets supported include Vista, Win2008 server, Windows 7, Windows 8, Windows 8.1, Windows 10, Win server 2012, and all prior Windows releases.
- For more information on Microsoft RDP, including usage information, see: http://www.microsoft.com/downloads/details.aspx?FamilyID=469eee3a-45b4-4b40-b695-b678646a728b&displaylang=en
- When adding RDP interfaces to Windows 7, make sure that ICMPv4 and ICMPv6 are allowed by the Windows 7 firewall.
- 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.

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, 8080, 443, and 2400 open in your firewall.

  Note: Beginning with CC-SG 4.2, proxy mode supports encryption of KVM data when using Dominion KXII release 2.1.10 and higher. In this configuration, KVM data is encrypted according to the security setting in the KXII device. Encryption is not supported with devices other than Dominion KXII 2.1.10.

- 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 10 or 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.
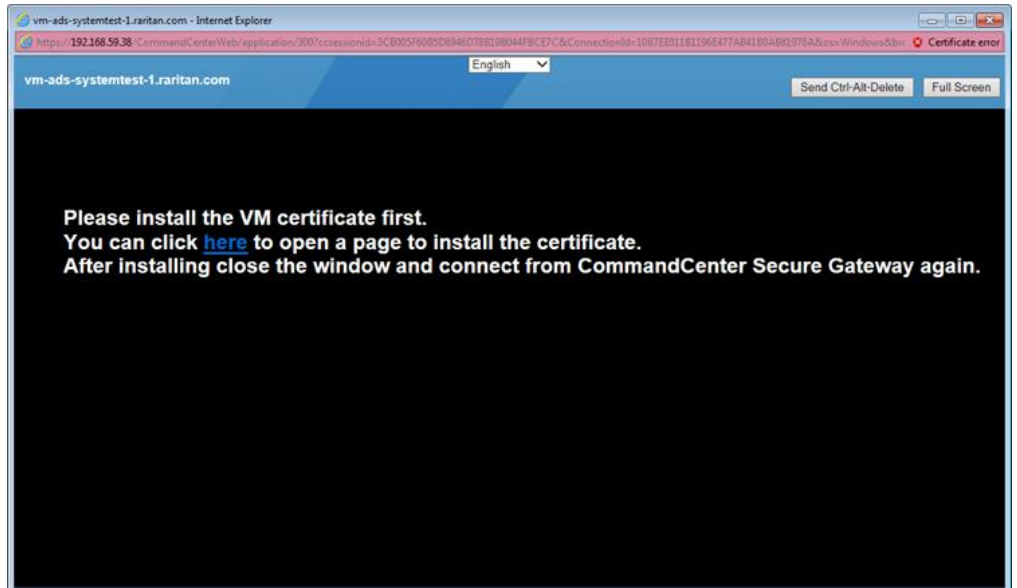
Once the add-on is installed, restart your browser. If the add-on installation fails, see *Install VMware Plugins for Firefox 3.0* (on page 83).

▶ **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.

vSphere 4 Users Must Install New Plug-In

When upgrading your virtual environment from a previous version to vSphere 4, you must remove the VMware Remote Console plug-in from the browser. After removing the plug-in, the correct plug-in for vSphere4 will be installed the next time you connect to a Virtual Machine from CCSG.

▶ **To remove the old plug-in from Internet Explorer:**

1. Choose Tools > Manage Add-Ons > Enable or Disable Add-Ons.

2. Select "Add-Ons that have been used by Internet Explorer" in the Show list.

3. Scroll down to the "VMware Remote Console Plug-in" and select it.

4. The Delete Active-X button should become enabled. Click to delete the old plug-in.

   ▪ If the Delete button is not enabled, go to Control Panel > Add/Remove Programs and look for an older VI Client. If VI client 2.5 is installed, uninstall it. After the uninstalling the VI client 2.5, the plug-in will be removed.

▶ **To remove the old plug-in from Firefox users:**

1. Choose Tools >Add-Ons.

2. Click the Plug-Ins tab.

3. Select the old plug-in then select it and click Disable.

▶ **To install the new plug-in:**

1. After removing the old plug-in, login to CCSG and connect to a Virtual Machine.

2. You will be prompted to install the plug-in for vSphere 4.

Mount a Drive or Drive Image via a VMW Viewer Interface

The virtual machine remote console Devices menu supports the following functions, when launched via a VMW Viewer Interface. This is supported only for vSphere 4.0.

- Mount a CD/DVD Drive from an ESX host or client computer
- Browse for an ISO image
- Mount a floppy drive from an ESX host
- Browse for a floppy image

▶ **To access the virtual machine remote console's mounting functions:**

1. Connect to the virtual machine. See *Connect to a Virtual Machine Node via a VMW Viewer Interface* (on page 60).

2. Choose Devices in the remote console to view the menu choices for mounting.

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: As a normal user, you cannot disconnect from nodes whose connections you did not initiate.

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.

Note 3: As a CC-SG Administrator, you can terminate any user's node connection sessions, except those initiated by a 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.

Cannot Write To/From a File from a Mac Client

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 82)

If you are connecting to the CommandCenter Secure Gateway from a Mac® 10.8.5 client running Safari with   and cannot write to/from a file on a KX2 or KX3 target server or access virtual media, do the following to correct this:

1. In Safari, select Preferences.
2. Under the Security tab, select Manage Website Settings.
3. Click on "Website for KX2 or KX3".
4. Select "Run in unsafe mode" from the drop-down.

    Note: In Safari 10.0, "Run in safe mode" is now hidden as an option for Plugin-Settings. Hold the Mac Option/Alt key while clicking on the site to list the option.

    If running MacOS Sierra 10.12, Java version must be 1.8.0.121 or higher.

5. Restart Safari.

Chapter 5 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 67) and *Power Control for Nodes Using the Admin Client* (on page 69).

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 66) 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 66) 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 66) 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 66) 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 66) 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 66) 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 66) 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 66) 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 66) (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 66) 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.

Chapter 6 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.

Raritan.
A brand of legrand

Chapter 7   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.

Manage Mobile Client Keyboard Macros

Each user must import their user-defined keyboard macros to make them available for use while connected to targets using the Mobile KVM Client (MKC).

Export the file from Virtual KVM Client (VKC), then import it using the desktop Access Client. You cannot import macros using a mobile device. Imported macros are available per user in MKC when you connect to a target using your mobile device.

Export Keyboard Macros in VKC

Export your keyboard macros from the Virtual KVM Client (VKC) to create an XML file that you can import in the Access Client to make user-defined macros available in the Mobile KVM Client (MKC).

▶ **To export keyboard macros in VKC:**

1. Log in to the Access Client.
2. Connect to an out-of-band KVM interface that uses VKC.
3. Choose Tools > Export Macros to open the Select Keyboard Macros to Export dialog.
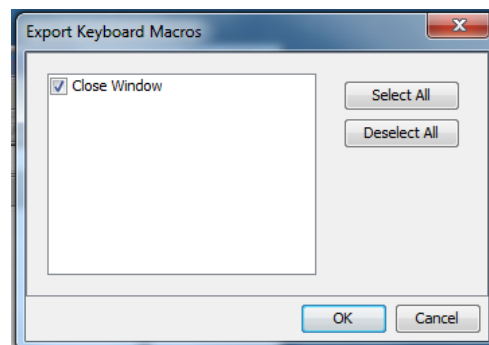
4. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.

5. Click Ok. An "Export Keyboard Macros to" dialog is displayed. Locate and select the macro file. By default, the macro exists on your desktop.

6. Select the folder to save the macro file to, enter a name for the file and click Save. If the macro already exists, you receive an alert message.

7. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.

Import Keyboard Macros for Mobile KVM Client

Import a keyboard macro .XML file to make user-defined macros available in the Mobile KVM Client (MKC).

When you import a new file, all previously imported macros are overwritten.

The maximum file size is 4KB. The file type must be .XML. The file must have been exported from Virtual KVM Client (VKC). See *Export Keyboard Macros in VKC*. (see "*Export Keyboard Macros in VKC*" on page 76)

▶ **To import keyboard macros for Mobile KVM Client:**

1. Log in to the desktop Access Client.

2. Click the My Profile tab. The My Profile page opens.

3. In the Manage Mobile Client Keyboard Macros section, click Browse, then select the .XML file you exported from the Virtual KVM Client (VKC) and click Open.

4. Click Import File. Imported macro names display in the Available Keyboard Macros list.

   To verify the import, log in to the Access Client using your mobile device, connect to an out-of-band KVM target, then touch Menu in the toolbar. In the Menu, touch Keyboard Macros. The list of available macros displays. Macros are organized by type: pre-defined macros, SUN macros, then user-defined, imported macros.

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.

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 (Sun) 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 82) and *Clear the Java Cache* (on page 82).
- If you have problems accessing a KX2 port via the VKC interface when using Internet Explorer, you should clear the browser's cache and then re-access the port. See *Clear the Browser's Cache* (on page 82).
- 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 1.0 GB of RAM, set the parameter to –Xmx512m 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 XP with Java 1.6:**

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.

Index

A

About Connection Modes • 57, 58
Absolute Mouse Mode • 46, 47
Access CC-SG with the Thick Client • 8
Access from a Mobile Device • 5
Accessing a Serial Interface for the First Time
 • 54
Accessing Another CC-SG Unit in the Same
 Neighborhood • 5
Accessing CC-SG • 2
Add a Custom View • 20
Add a Custom View for Nodes • 22
Add a Node to Favorites • 12
All Nodes List • 12
All Nodes List in Extended Network
 Neighborhood • 22
Applications for Accessing Nodes • 26, 50
Apply a Custom View • 20
Apply a Custom View for Nodes • 23
Assign a Default Custom View • 21
Assign a Default Custom View for All Users •
 22
Assign a Default Custom View for Nodes • 24
Assign a Default Custom View of Nodes for All
 Users • 25
Auto-Sense Video Settings • 48

B

Before You Begin • 2
Bookmarking an Interface • 18
Browser-Based Access via the CC-SG Access
 Client • 3
Browser-Based Access via the CC-SG Admin
 Client • 6

C

Cannot Write To/From a File from a Mac Client
 • 64
CC-SG Access Client Overview • 11, 19
CC-SG Admin Client Screen Overview • 15
Change a Custom View • 21
Change a Custom View for Nodes • 23

Change a Custom View's Name • 21
Change the CC-SG Font Size • 78
Change Your Email Address • 75, 78
Change Your Password • 75, 78
Chrome and Edge Browser Limitations • 29
Clear the Browser's Cache • 81, 82
Clear the Java Cache • 64, 81, 82
Clear the Recent Nodes List • 13
Connect to a Control System or Virtual Host
 Node via a VI Client Interface • 59
Connect to a Node via a Web Browser
 Interface • 26, 59
Connect to a Node via an In-Band KVM
 Interface • 26, 55
Connect to a Node via an Out-of-Band KVM
 Interface • 26, 52
Connect to a Node via an Out-of-Band KVM
 Interface on a Mobile Device • 39
Connect to a Node via an Out-of-Band Serial
 Interface • 26, 54
Connect to a Virtual Machine Node via a VMW
 Viewer Interface • vii, 60, 62
Connect to an iLO Processor Enabled Node •
 26, 55
Connecting to Nodes • 26
Connecting to Nodes using a Mobile Device • 5,
 26, 39
Connecting to Nodes using the Access Client •
 26, 27
Connecting to Nodes using the Admin Client •
 26, 49
Connections that Exceed the Maximum
 Number of Sessions Available • 63
Copy and Paste • 35
Custom Views • 12, 19, 28, 50

D

Delete a Custom View • 21
Delete a Custom View for Nodes • 24
Delete a Node from Favorites • 13
Disable Pop-up Blockers • 3
Disconnect from a Node • 63
Display Connection Info • 44, 48

Raritan.
A brand of legrand

85

Raritan.
A brand of legrand