Avocent® DSView™ and Rack Power Manager Software Plug-in

Technical Bulletin

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. For additional assistance, visit https://www.VertivCo.com/en-us/support/.

TABLE OF CONTENTS

1 Introduction **1**
1.1 Plug-in Installation 1
2 Power Distribution Unit Plug-ins **3**
2.1 Additional Supported Appliances 3
2.2 Add Appliance Wizard 3
2.3 Appliance Names and Terminology 5
2.3.1 Naming Liebert® Rack PDU receptacles 5
2.4 Unit Views 5
2.4.1 Accessing the appliance 6
2.4.2 Configuring settings on the OBWI 6
2.5 Operations 6
2.5.1 Configuring SNMP 6
2.5.2 Granting access rights 7
2.5.3 Upgrading firmware 7
2.6 Appliance Setting Configuration 7
2.6.1 Using configuration tools 7
2.6.2 Applying appliance configuration template properties 9
2.6.3 Configuring appliance settings in the Rack Power Manager software 10
2.6.4 Configuring Liebert® UPS appliance settings 12
2.6.5 Configuring Liebert® PDU appliance settings 13
2.6.6 Configuring Rack PDU appliance settings 14
2.6.7 Configuring PDU and CDU appliance settings 15
2.7 Comparative and Status Reports 16
3 Appliance, Infrastructure and Virtualization Plug-ins **19**
3.1 Avocent® AutoView™ and MergePoint Unity™ Switches 19
3.2 Avocent® Universal Management Gateway Plug-in 20
3.3 Cyclades™ ACS5000 Advanced Console Server 20
3.4 Avocent® ACS6000 and ACS8000/ACS800 Advanced Console Server 20
3.5 Blade Chassis Plug-in 20
3.6 Infrastructure Plug-in 20
3.7 Virtualization Plug-in 21
3.8 System Requirements 21
3.9 System Configurations 21
3.9.1 Configuring a blade chassis system 21
3.9.2 Configuring a virtualization system 24
3.10 Unit Views 26
3.10.1 Accessing a blade chassis 26
3.10.2 Managing IBM® or HP® blade cards 27
3.10.3 Accessing a virtual environment unit 27
3.10.4 Deleting a virtual environment unit 27

3.11 Operations 28
3.11.1 Configuring SNMP 28
3.11.2 Granting access rights 28
3.11.3 Organizing units in an infrastructure 28
3.11.4 Launching KVM sessions in the DSView™ software 29
3.11.5 Avocent® Universal Management Gateway appliance 30
3.11.6 Avocent® ACS6000 and ACS8000/ACS800 advanced console servers 33
3.12 Adding an Appliance 33
3.13 Cyclades™ ACS5000 Advanced Console Server 38
3.13.1 Using configuration tools 38
3.13.2 Configuring console server properties 38
3.13.3 Configuring the console server serial port 43
3.13.4 Managing power devices 45
3.13.5 Configuring hostname discovery strings 51
3.13.6 Configuring the TCP Port 52
3.13.7 Configuring sessions settings 52
3.14 Virtualization 53
3.14.1 Managing a virtual machine 53
3.14.2 Enabling automatic virtual machine management 54
3.14.3 Using Unit Tools 54
3.14.4 Operating a virtual machine 57
3.14.5 Managing virtual environments in the DSView™ software 58
3.14.6 Logging data 64
3.14.7 Logging DSView™ software events 68

1 INTRODUCTION

The Avocent® DSView™ management software and the Avocent® Rack Power Manager software enable you to access, monitor and control various Avocent and Vertiv™ appliances and attached targets.

Appliance-specific plug-ins provide additional access, configuration and management functionality that is not native to the DSView software or the Rack Power Manager software.

NOTE: All instances of DSView software in this document refer to DSView software version 4 or later.

This document provides information about the plug-ins that are supported by the DSView and/or Rack Power Manager software, which are listed in the following table.

Table 1.1 DSView and Rack Power Manager Software Plug-ins

PLUG-IN	DSVIEW SOFTWARE	PRE-INSTALLED ON DSVIEW SOFTWARE	RACK POWER MANAGER SOFTWARE
Avocent® Power Management Distribution Unit	X	N/A	X
Liebert® MPH2 Rack Power Distribution Unit and MPX and MPH rack PDUs with RPC2 cards installed	X	X	X
Liebert® GXT4™ Uninterruptible Power Supply	X	N/A	X
Liebert® MPX and MPH Rack Power Distribution Units	X	X	X
APC Rack Power Distribution Unit	X	X	X
Liebert® MPI Intelligent Power Distribution Unit	X	X	X
Server Technology Sentry Switched Cabinet Distribution Unit	X	X	X
Infrastructure	X	X	X
Avocent® AutoView™ Switch	X	N/A	N/A
Avocent® MergePoint Unity™ Switch	X	X	X
Avocent® Universal Management Gateway Appliance	X	X	N/A
Blade Chassis	X	X	N/A
Cyclades™ ACS5000 Advanced Console Server	X	N/A	X
Avocent® ACS6000 Advanced Console Server	X	X	X
Avocent® ACS8000 Advanced Console Server	X	X	X
Avocent® ACS800 Advanced Console Server	X	X	X
Virtualization	X	X	N/A

1.1 Plug-in Installation

Some appliance-specific plug-ins are pre-installed in your Avocent DSView software and the Avocent Rack Power Manager software. See the previous table for a detailed list of pre-installed plug-ins. If the plug-in for your appliance is not pre-installed, check with Vertiv Technical Support to ensure your version of DSView or Rack Power Manager software is compatible with the plug-in.

NOTE: You can add the Liebert® GXT4 UPS plug-in or the Liebert® MPI PDU plug-in to the DSView software from the optional plug-in list at www.VertivCo.com. For a list of the optional plug-ins, see the DSView and Rack Power Manager software release notes.

Please read these instructions in their entirety prior to plug-in installation.

NOTE: You must have DSView™ or Rack Power Manager software administrator access rights to add or manage plug-ins.

To download and install plug-ins for the DSView management software:

1. Visit https://www.VertivCo.com/en-us/support/software-download/software/avocent-dsview-software-downloads/ to access the appliance-specific DSView software plug-ins.

NOTE: A current DSView software maintenance contract is not required to download appliance plug-ins. An active maintenance contract is only required for downloading the DSView software and DSView software updates. Contact your Sales representative to renew your maintenance contract or request maintenance renewal from the DSView download software portal at www.VertivCo.com.

2. Select the plug-in from the list that corresponds to your appliance.
3. Download and save the plug-in to your PC or server.
4. Select the *System* tab.
5. Click *Plug-ins - Add*.
6. Click *Next* and browse to the plug-in you downloaded in step 3.
7. Click *Next* and click *Next* again to install the plug-in.
8. Click *Finish*.

NOTE: The plug-in must be added to each hub and spoke within the DSView software system.

2 POWER DISTRIBUTION UNIT PLUG-INS

Power distribution unit plug-ins for the Avocent® Power Management (PM) Power Distribution Unit (PDU), APC Rack PDU, MPI PDU, the Liebert® MPX and MPH Rack PDUs, GXT4 UPS, the Liebert® RPC2™ and the Server Technology Sentry Cabinet Distribution Unit (CDU) allow you to access, configure and manage PDUs, CDUs and UPSes from the Avocent® DSView™ software and the Avocent® Rack Power Manager software. These plug-ins also enable the software to collect and use power-related parameters from the PDUs, CDUs and UPSes.

When you install a plug-in for the DSView or Rack Power Manager software for any of the units previously listed, you can log into the appliance web interface to add single or multiple appliances. You can view all of the added devices on the Appliances-All screen. Most PDU, CDU or UPS administration tasks can be accomplished either locally or remotely with the DSView or Rack Power Manager software which provide a real-time view of all connected devices.

Using the DSView or Rack Power Manager software web interface, the administrator can configure the PDU, CDU or UPS and modify appliance settings. Other authorized users have access to troubleshoot, perform maintenance on, cycle power to or reboot connected devices.

2.1 Additional Supported Appliances

The APC Rack PDU plug-in allows you to manage the APC Rack PDU Series 78xx or 79xx from the DSView or Rack Power Manager software. The Server Technologies Sentry CDU plug-in allows you to manage the following Server Technology Sentry Switched CDUs without attaching the CDU to another appliance:

- CW-48V5Z454-A1P
- CW-24VY-L30M
- CWG-24V4Z423A9/QR
- CW-8H1A413
- CW-24V4K425A9
- STV-4501C
- STV-6502M

You can also manage the following Server Technology Sentry Switched CDUs from the plug-in but the CDUs must be attached to another appliance:

- CW-8H1
- CW-8H2
- CW-16V1
- CW-16V2
- CW-24V2
- CW-24V3
- CW-32VD1
- CW-32VD2

2.2 Add Appliance Wizard

The Add Appliance Wizard guides you through the steps to add a PDU, CDU or UPS to the network. See the Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power

Manager Installer/User Guide for details on using the Add Appliance Wizard.

The following procedures detail the steps necessary to launch the Add Appliance Wizard, add appliances by type or IP address, discover appliances on a network and delete an appliance.

To launch the Add Appliance Wizard:

Click *Add* from the Appliances - All screen.

To add a single appliance by type:

1. Click *Add* from the Appliances - All screen.
2. Select the Add a single appliance by type radio button.
3. Select the PDU, CDU or UPS in the Product list and click *Next*.
4. Enter the IP address for the appliance to be added and go to Step 5.

   -or-

   Enable the Appliance does not have an IP Address assigned yet checkbox, enter network information and click *Next - Finish* to complete this procedure.
5. Select the Use SNMPv1 radio button and enter either **public** or **private** in the Read Community and Write Community fields.

   -or-

   Select the User SNMPv3 radio button and enter network information and credentials.
6. When the appliance is found, click *Next - Finish*.

To add one or more appliances by IP address:

1. Click *Add* from the Appliances - All screen.
2. Select the Add one or more appliances by IP address radio button and click *Next*.
3. Enter the IP address for the appliances to be added in the Addresses field and port information in the HTTP Port and HTTPS Port fields.
4. Select the Use SNMPv1 radio button and enter either **public** or **private** in the Read Community and Write Community fields.

   -or-

   Select the User SNMPv3 radio button and enter network information and credentials.
5. Enable the checkboxes for the required plug-ins in the Available plug-ins list and click *Next*.
6. When the PDUs, CDUs or UPSes are found, select the appliances to be added in the Appliances Found field, click *Add* to move them to the Appliances to Add field and click *Next*.
7. Select the options applicable to the appliance from the Select Options screen and click *Next - Finish*.

To discover appliances on the network:

1. Click *Add* from the Appliances - All screen.
2. Select the Discover appliances on the network from an IPv4 address range or from an IPv6 subnet radio button.

NOTE: IPv6 is not supported by APC Rack PDUs, MPI PDUs, Server Technology PDUs or GXT4 UPSes.

3. Click the Use IPv4 address range radio button and enter the IPv4 address range.

   -or-

   Click the Use IPv6 subnet radio button and enter the IPv6 network prefix.

4. Enter additional information in the HTTP Port and HTTPS Port fields for the search as required.
5. Select the Use SNMPv1 radio button and enter either **public** or **private** in the Read Community and Write Community fields.

   -or-

   Select the User SNMPv3 radio button and enter network information and credentials.

6. Enable the checkboxes for the required plug-ins in the Available plug-ins list and click *Next*.
7. Select the PDU from the Appliances Found field and click *Add*.
8. Repeat step 4 for each added PDU, CDU or UPS and click *Next*.
9. Select the options applicable to the added appliance and click *Next* - *Finish*.

To delete an appliance:

1. Click the checkbox to select an appliance in the Appliances - All screen and click *Delete*.
2. Press *OK* in the confirmation box.

2.3 Appliance Names and Terminology

Depending on the appliance type, naming and terminology can differ. You can find more information on name synchronization, naming target devices and renaming a managed appliance in the Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power Manager Installer/User Guide.

2.3.1 Naming Liebert® Rack PDU receptacles

Liebert® Rack PDU outlets are called receptacles, while Avocent® PDU outlets are called sockets or outlets. All Liebert Rack PDU receptacles have the same name. For MPH vertical models, receptacles are also organized into three branches of nine receptacles per branch, and the branch number is displayed as part of the PDU name in the DSView™ or Rack Power Manager software database.

The name format is: PDU-Branch-Receptacle; for example, if the Liebert Rack PDU reports an asset named "Receptacle 1," the default name assigned to the receptacle in the DSView or Rack Power Manager software database is "Receptacle 1-2-3" for PDU 1, Branch 2, Receptacle 1. However, to avoid confusion, add one PDU at a time and assign unique names to receptacles in the DSView or Rack Power Manager software database before adding the next PDU.

2.4 Unit Views

All added appliances are listed on the Unit Views screen and in the Unit Views - Appliances-All menu in the side navigation bar of the Avocent DSView software and the Avocent Rack Power Manager software. The Unit Views screen allows you to access the Operations drop-down menu and the Unit Overview screen for a selected appliance.

From the Operations drop-down menu you can hide a unit from view, view versions, push names to the appliance, pull names from the appliance, view properties, cycle power to the appliance or turn the appliance off or on.

To access the Operations drop-down menu:

Click the checkbox to select an appliance, outlet or receptacle on the Unit Views screen and click *Operations*.

2.4.1 Accessing the appliance

The Unit Overview screen allows you to view and change the target device name, type and icon or merge target devices. From this screen, you can also cycle wall outlet power or turn it on and off.

The following table lists the information fields that appear on the Unit Overview screen for an appliance and a description for each field.

Table 2.1 Appliance Unit Overview Information

FIELD	DESCRIPTION
Name	Name of the PDU.
Type	Type of PDU.
Tools	Tools to reboot, resync, turn on, turn off or power cycle the PDU; or opens a command line prompt to access the appliance via Telnet.

When you open the PDU Unit Overview screen, a list of the links to the PDU menus appears in the side navigation bar.

To open the Unit Overview screen for an appliance:

Click an individual appliance, outlet or receptacle.

2.4.2 Configuring settings on the OBWI

You can view and configure additional PDU settings on the OBWI. The following OBWI procedures are only supported by Liebert® GXT4 UPSes, MPI PDUs and newer versions of the Server Technology PDUs.

To configure a PDU or UPS by launching the OBWI:

1. From the Unit Overview screen, click the PDU or UPS name.
2. Click *Overview - Browser session*.
3. Configure PDU or UPS settings listed on the OBWI.

To access the OBWI through a proxy:

1. From the Units View screen, click the PDU or UPS name.
2. Click *Browse Session*.

2.5 Operations

For more information about operations, access rights, appliance configuration templates, configuration tools and tabs not listed in this document, see the Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power Manager Installer/User Guide.

2.5.1 Configuring SNMP

Some appliances require SNMP configuration for the device to communicate with the DSView or Rack Power Manager software.

Configuring SNMP settings for Vertiv™ rack PDUs

For instructions to configure SNMP settings for the Vertiv™ rack PDU device with an Liebert® RPC2™ Communications module, see the RPC2 Communications Module Rack PDU SNMP OIDs Technical Bulletin.

Configuring SNMP settings for Liebert rack PDUs

You must also configure SNMP settings from the Liebert MPX and Liebert MPH PDU web interface for the PDUs to communicate with the DSView or Rack Power Manager software.

To configure SNMP for the PDU:

1. In the PDU interface, select the *configure* tab.
2. On the side navigation bar, select *Management Protocol - SNMP - Access*.
3. Enter 0.0.0.0 in the Network Name field for both the public and private community, or for a more secure setting, enter the IP address for the DSView or Rack Power Manager server.

NOTE: Any rack PDUs that are daisy-chained also need to be configured in their web interface.

2.5.2 Granting access rights

Administrators can adjust user or user group access rights in the DSView or Rack Power Manager software. The Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power Manager Installer/User Guide provides details about access rights and procedures for assigning and viewing effective access rights.

2.5.3 Upgrading firmware

The following procedure details the steps necessary to upgrade firmware specifically for a Liebert® GXT4 UPS. For firmware update and managing procedures for selected appliances, see the Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power Manager Installer/User Guide.

To upgrade Liebert GXT4 UPS firmware:

1. On the desktop, click *System - Appliance files - Add*.
2. Upload the GXT4 firmware file.
3. Click *UPS in Appliances*.
4. In the Tools section, click *Upgrade Firmware*.
5. Choose the firmware file to use and click *Finish*.

NOTE: Firmware upgrades can also be scheduled using the System - Tasks screen.

2.6 Appliance Setting Configuration

You can configure appliance settings in the Avocent DSView software and the Avocent Rack Power Manager software using configuration tools or by applying appliance configuration templates. The Appliance Settings link appears in the side navigation bar after you select an appliance from the Unit Views Appliances - All screen.

2.6.1 Using configuration tools

The plug-ins are integrated with the DSView™ or Rack Power Manager software tools and depending on the appliance type, the configuration tools can differ. The tools and their functions are listed in the

following table.

Table 2.2 Configuration Tools

APPLIANCE / TOOLS	DESCRIPTION
Reboot	Terminate all active sessions and reboot the PDU.
Upgrade Firmware	Upgrade the firmware through the DSView or Rack Power Manager server.
Resync	Synchronize the configuration information of the PDUs and outlets with the DSView or Rack Power Manager server database.
Save Configuration (Legacy)	Back up the PDU configuration data to the DSView or Rack Power Manager server database. The saved configuration includes the configuration not exposed in the Web Manager.
Restore Configuration (Legacy)	Restore a previously saved PDU configuration. The restored configuration includes the configuration not exposed in the Web Manager.
Save Configuration Template	Create a configuration template with a specific name. The saved configuration template includes the Web Manager screens and can later be used to replicate this PDU configuration to multiple PDUs, or to restore the configuration to a replacement PDU.
Apply Configuration Template	Restore a configuration saved while using the Save Configuration Template.
Save Last Known Good Configuration	Save a configuration template with a pre-defined name of Last Known Good Configuration.
Apply Last Known Good Configuration	Restore the configuration template saved as Last Known Good Configuration.
Save Current Configuration	Save a configuration template with a pre-defined name of Current Configuration.
Apply Current Configuration	Restore the configuration template saved as Current Configuration.
Appliance Replacement	Replace a faulty PDU with another one by applying the configuration template from the faulty one to the replacement PDU.
Appliance Session	Launch a viewer with an SSH connection using the DSView software.
Restore to Factory Configuration	Restore to factory default values and reboot the PDU. Only the configuration of the running image will be restored to factory default. After reboot, the PDU will need to be deleted and then added again to the DSView or Rack Power Manager software if it was previously added in Secure mode or if the PDU gets a different IP from DHCP.
Shutdown Appliance	Shut down the PM PDU.

In addition to the configuration tools described in the previous table, you can also perform the following tasks by selecting an appliance on the Unit Views screen and selecting the *Operations* drop-down.

Table 2.3 Operations Available on Unit Views Screen

OPERATION	DESCRIPTION
Hide Units From View	Hides the unit from displaying in the Unit Views or Appliances-All screens.
Reboot	Terminate all active sessions and reboot the PDU.
Show Version	Display current PDU boot and firmware versions.
Push Names to Appliance	The DSView or Rack Power Manager software pushes names stored in the database to the PDU and all targets.
Pull Names from Appliance	The DSView or Rack Power Manager software pulls PDU and all target names and synchronizes the DSView or Rack Power Manager server database.
Properties	Customize the unit configuration in the DSView or Rack Power Manager server database.
Move Units To Zone	Allows users who have purchased the requisite licenses to set up zones and move appliances from the default top level zone to a sub-zone.
Apply Configuration Template	Restore a configuration saved while using the Save Configuration Template.
Save Last Known Good Configuration	Save a configuration template with a pre-defined name of Last Known Good Configuration.
Save Current Configuration	Save a configuration template with a pre-defined name of Current Configuration.
Enable Secure Mode	Launches the appliance in secure mode.
Properties - Bulk Edit	Updates parameters on multiple selected devices at once.
Power PDU Off	Remotely powers off the PDU.
Power Cycle PDU Unit	Remotely cycles power to the PDU.
Power PDU On	Remotely powers on the PDU.

2.6.2 Applying appliance configuration template properties

Appliance configuration templates allow administrators to simultaneously configure multiple units from the DSView™ or Rack Power Manager software. An appliance configuration template can be used to configure new units or replace existing units.

These properties are applied to an appliance when the Appliance Replacement, Apply Configuration Template, Apply Last Known Good Configuration or Apply Current Configuration operations are executed.

A new “Template” node under the Power Management node creates templates for Avocent® and Cyclades™ PDUs. When a PDU configuration template is applied, the settings saved under the Template node are applied to all PDUs in the chain. The following table lists the Appliance Settings screens that are supported for the configuration templates.

Table 2.4 Appliance Configuration Template Supported Screens

APPLIANCE SETTINGS MAIN SCREENS	APPLIANCE SETTINGS SUBSCREENS
Power Management	PDUs - Settings - Outlets*
	PDUs - Settings - PDUs*
	PDUs - Settings - Phases*
	PDUs - Settings - Banks*
	PDUs - Settings - Environment*
	Settings
	Template

APPLIANCE SETTINGS MAIN SCREENS	APPLIANCE SETTINGS SUBSCREENS
System	Security - Security Profile
	Date and Time - Date & Time
	Date and Time - Timezone
	Language
Network	Settings*
	IPv4 Static Routes*
	IPv6 Static Routes*
	Hosts*
	Firewall - IPv4 Filter Table
	Firewall - IPv4 Filter Table - Rules
	Firewall - IPv6 Filter Table
	Firewall - IPv6 Filter Table - Rules
	IPSec (VPN)
	SNMP - System
	SNMP - v1, v2, v3
Authentication	Appliance Authentication
	Authentication Servers - RADIUS
	Authentication Servers -TACACS+
	Authentication Servers -Kerberos
	Authentication Servers -NIS
	Authentication Servers -DSView
Users	Local Accounts - User Name
	Local Accounts - Password Rules
	Groups - Members
	Groups - Log-in Profile
	Groups - Access Rights - Serial
	Groups - Access Rights - Power - PDU*
	Users - Groups - Access Rights - Power - Outlets*
	Users - Groups - Access Rights - Appliance
Events and Logs	Event List
	Event Destinations
	Data Buffering
	Appliance Session
	Sensors

*These screens are only applied when using the Appliance Replacement operation. The Appliance Replacement operation will restore the configuration of the master and chained PDUs, so make sure they share the same configuration when the configuration template was saved.

2.6.3 Configuring appliance settings in the Rack Power Manager software

The following configuration actions are available in the Avocent® Rack Power Manager software Rack Power Manager software.

To view Agent Information:

Click *Agent*.

To view information about the PDUs:

Click *PDU*.

To view PDU power information:

Click *Totals*.

To reset energy accumulation:

Click the checkbox to select a PDU and click *Reset Energy*.

To view and configure a phase setting:

1. Click *Phase*.
2. Click the checkbox to select a phase to configure and click *Configure*.
3. Configure the Over Current Alarm Threshold (%), Over Current Warning Threshold (%) and Low Current Alarm Threshold (%) fields and click *Save - Close*.

To view and configure branch settings:

1. Click *Branch*.
2. Click the checkbox to select a branch to be changed and click *Configure*.
3. Enter the branch's identification, User Tag 1 and User Tag 2 information.
4. Configure the Over Current Alarm Threshold (%), Over Current Warning Threshold (%) and Low Current Alarm Threshold (%) fields and click *Save*.

To reset branch energy accumulation:

1. Click the checkbox to select a branch.
2. Click *Reset Energy*.

To reset receptacle energy or adjust power:

1. Click *Receptacle*.
2. Click the checkbox to select a receptacle.
3. Click *Reset Energy*, *On*, *Off*, *Cycle*, *Lock* or *Unlock* to adjust receptacle power.

To flash the receptacle LED:

1. Click *Receptacle*.
2. Click the checkbox to select a receptacle.
3. Click *Blink LED*.

NOTE: The receptacle LED flashes for 10 seconds.

To configure the receptacle settings:

1. Click *Receptacle*.
2. Click the checkbox to select a receptacle and click *Configure*.
3. Enter the receptacle's name, User Tag 1 and User Tag 2 information.
4. Select a power up state, SWOTP state and level of criticality from the drop-down lists and configure values for On Delay, Post On and Post Off.

5. Configure the Over Current Alarm Threshold (%), Over Current Warning Threshold (%) and Low Current Alarm Threshold (%) fields and click *Save*.

NOTE: If the Branch Receptacle Module or the input power source is changed on an MPX PDU, you need to resync to update the topology view in the DSView™ or Rack Power Manager software. See the Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power Manager Installer/User Guide for more information.

To view a list of sensors:

Click *Sensor*.

To configure a sensor:

1. Click the checkbox to select a sensor and click *Configure*.
2. Enter the sensor's name, User Tag 1 and User Tag 2 information.
3. Configure the door, contact, temperature and differential pressure alarms and warning thresholds in the appropriate fields and click *Save*.

NOTE: The humidity thresholds are only available if the specific sensor supports it.

2.6.4 Configuring Liebert® UPS appliance settings

The following configuration actions are available for Liebert UPSes.

To view or modify the web interface:

1. Click *Web Interface Settings*.
2. Choose either HTTP or HTTPS as the OBWI protocol.
3. Specify the OBWI port number.
4. Specify the OBWI home screen relative URL path.

NOTE: The relative path follows the IP address of the UPS. For example, if the OBWI home screen URL is https://10.207.66.66/admin/index.html, then admin/index.html is the relative URL.

5. Click *Save*.

To view or modify SNMP settings:

Click *SNMP Settings* to view or change the SNMP version used by the DSView or Rack Power Manager software SNMP V1/V2 community strings and SNMP V3 settings.

NOTE: The configured SNMP settings are only saved to the DSView or Rack Power Manager software database and not to the UPS. These settings are used by the DSView or Rack Power Manager software to access the UPS. So, it should match what is configured on the OBWI.

To change the SNMP v1 settings:

1. Select the Use SNMPv1 radio button.
2. Enter **public**, **private** or the name of a group in the Read Community Name and Write Community Name fields for the Avocent® DSView™ software and the Avocent® Rack Power Manager software to use to access the UPS.
3. Click *Save*.

To change the SNMP v3 settings:

1. Select the Use SNMPv3 radio button.
2. Specify the User Name, Authentication Password, Privacy Password, Authentication Protocol, Privacy Protocol and Security Level that the DSView™ or Rack Power Manager software uses to access the UPS.
3. Click *Save*.

2.6.5 Configuring Liebert® PDU appliance settings

The following configuration actions are available for Liebert PDUs.

To view Agent Information:

Click *Agent Information*.

To view information about the PDUs:

Click *PDUs*.

To view information about the PDU's Power Sources:

Click *Power Sources*.

To reset energy accumulation:

Click the checkbox to select a PDU and click *Reset Energy Accumulation*.

To configure a phase:

1. Click *Power Source Line/Phases*.
2. Click a phase to open the Phase Information screen, configure the overcurrent alarm threshold, overcurrent warning threshold and low current alarm threshold and click **Save**.

To view and configure branch information:

1. Click *Branches* and click a branch to be changed.
2. Enter the branch name, tag 1 and tag 2 information in the appropriate fields and click *Save*.

To reset branch energy accumulation:

1. Click the checkbox to select a branch.
2. Click *Reset Energy Accumulation*.

To view a list of receptacles:

1. Click *Receptacles* and click the checkbox to select one or more receptacles.
2. Click the appropriate button in the content area to turn on, turn off, cycle, lock, unlock or configure the selected receptacles.

To configure the receptacle settings:

1. Click a receptacle.
2. Configure the Name, Tag 1, Tag 2, On Delay(s), Locked State, Over Current Alarm Threshold (%), Over Current Warning Threshold (%) and Low Current Alarm Threshold (%) fields.
3. Click *Save - Close*.

NOTE: If the Branch Receptacle Module or the input power source is changed on an MPX PDU, you need to resync to update the topology view in the DSView™ or Rack Power Manager software. See the Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power Manager Installer/User Guide for more information.

To view a list of sensors and sensor information:

Click *Sensors* and click a sensor to view a sensor's information, measurements and thresholds on the Sensor Information screen.

To configure a sensor:

1. Click the checkbox to select one or more thresholds and click *Configure Threshold*.
2. In the Information heading, enter the sensor's name and tag information in the appropriate fields.
3. In the Thresholds heading, enter the temperature and humidity thresholds in the appropriate fields and click *Save*.

NOTE: The humidity thresholds are only available if the specific sensor supports it.

2.6.6 Configuring Rack PDU appliance settings

The following configuration actions are available for APC Rack PDUs.

NOTE: The procedures in this section are only applicable to APC PDUs and older versions of the Server Technology PDUs.

To view and modify general PDU information:

1. Click *General Information* to verify the display orientation, line-to-line voltage and power factor.
2. Under Physical/Electrical Information, select either *Normal* or *Reverse* from the drop-down menu for the display orientation.
3. Under Power Information, enter the line-to-line voltage and power factor in the appropriate fields and click *Save*.

To view and modify phase settings:

1. Click *Phases* and click a phase.
2. In the Phase Information screen, set the low overload threshold, near overload threshold, overload threshold and overload restriction values.
3. Enter the values for the low load threshold, near overload threshold and overload threshold.
4. Select *None*, *On Alarm* or *On Warning* from the drop-down menu for overload restriction and click *Save*.

To view and modify bank settings:

1. Click *Banks* and click a bank.
2. In the Banks Information screen, set the low overload threshold, near overload threshold, overload threshold and overload restriction values.
3. Enter the values for the low load threshold, near overload threshold and overload threshold.
4. Select *None*, *On Alarm* or *On Warning* from the drop-down menu for overload restriction and click *Save*.

To view and modify switched outlets and their information:

1. Click *Switched Outlets* and click the checkbox to select one or more switched outlets.
2. Click *Immediate On* to turn on a switched outlet, *Immediate Off* to turn off a switched outlet or *Immediate Reboot* to reboot a switched outlet.

   -or-

   Click *Push Names* to push the Avocent® DSView™ software and the Avocent® Rack Power Manager software name for an outlet to the appliance or *Pull Names* to pull the name from an appliance to the DSView™ or Rack Power Manager software.

   -or-

   Click *Lock On*, *Lock Off* or *Unlock* to turn on, turn off or unlock an outlet lock, respectively.
3. Click an outlet and set the Outlet Name, Power On Delay, Power Off Delay and Reboot Duration.

To change outlet settings:

1. Enter the name of the outlet in the Outlet Name field.
2. In the Power On Delay field, select the Immediate power on, Never power on or Wait radio button. If you select Wait, enter the number of seconds to wait in the Seconds field.
3. In the Power Off Delay field, select the Immediate power off, Never power off or Wait radio button. If you select Wait, enter the number of seconds to wait in the Seconds field.
4. In the Reboot Duration field, enter the number of seconds for the PDU to remain off before rebooting and click *Save*.

To view and modify outlets and their information:

NOTE: This procedure is only applicable for PDUs that support outlet monitoring.

1. Click *Monitored Outlets*.
2. Click an outlet to set the outlet name, low overload threshold, near overload threshold and overload threshold.

2.6.7 Configuring PDU and CDU appliance settings

The following configuration actions are available for MPI PDU and Server Technology Sentry Switched CDU.

To view and modify the web interface:

1. Click *Web Interface Settings* and modify the OBWI protocol, port number and relative URL path.

NOTE: The relative path follows the IP address of the PDU. For example, if the OBWI home screen URL is https://10.207.66.66/admin/index.html, then admin/index.html is the relative URL.

2. Click *Save*.

To view and modify SNMP settings:

Click *SNMP Settings* and change the SNMP version used by the Avocent DSView software and the Avocent Rack Power Manager software, SNMP V1/V2 community strings and SNMP V3 settings.

NOTE: The configured SNMP settings are only saved to the DSView™ or Rack Power Manager software database and not to the PDU. These settings are used by the DSView or Rack Power Manager software to access the PDU and should match what is configured in the OBWI.

To change the SNMP v1 settings:

1. Select the Use SNMPv1 radio button.
2. Enter the Read and Write community name that the DSView or Rack Power Manager software uses to access the PDU.
3. Click *Save*.

To change the SNMP v3 settings:

1. Select the Use SNMPv3 radio button.
2. Enter the necessary information that the DSView or Rack Power Manager software uses to access the PDU.
3. Click *Save*.

2.7 Comparative and Status Reports

Comparative reports display data for multiple units of the same type while status and power range reports display data for an individual unit.

To view comparative reports in the Rack Power Manager software:

1. Click *Reports - Power*.
2. Select a report from the Reports menu.
3. Select a filter from the Filters menu and enter the appropriate values, then select the items to be included in the report and click >>.
4. Enter the date and time range for the report in the fields provided.
5. Click *Run Report*.
6. Click the bar chart or table view icons to change the view, or click the interpolation icon to show only data points.
7. Click *Export Data* to export and save the report data as a .csv file.
8. Click *Close*.

To view status reports in the Rack Power Manager Software:

1. Click *Reports - Power*.
2. Select *PDU Status* or *PDU Power Range* from the Reports menu and click *Run Report*.
3. Click on a PDU name to select the report and click *Export Data* to export and save the report data as a .csv file.
4. Click *Close*.

To view the Event Log report:

1. Click *Reports - Event Log*.
2. Click a column header to sort the rows in ascending or descending order.

To view the Data Log report:

1. Click *Reports - Data Log*.

2. Click a column header to sort the rows in ascending or descending order.

To view the Asset report:

1. Click *Reports - Asset*.
2. Click an icon to display the Asset report as a pie chart, bar graph or information table.
3. Click the print icon to print the report or click *Export Data* to export and save the report data as a .csv file.

To view the Usage report in the DSView™ software:

1. Click *Reports - Usage*.
2. Click an icon to display the Asset report as a pie chart, bar graph or information table.
3. Select a duration in the Report Range drop-down menu.
4. Click the print icon to print the report or click *Export Data* to export and save the report data as a .csv file.

This page intentionally left blank.

3 APPLIANCE, INFRASTRUCTURE AND VIRTUALIZATION PLUG-INS

When you install a plug-in for the Avocent® DSView™ software and the Avocent® Rack Power Manager software for any of the following appliances, blade chassis or virtual machines, you can log into the appliance's web interface to remotely configure and manage the target devices. You can view all of the added devices on the Appliances-All screen.

3.1 Avocent® AutoView™ and MergePoint Unity™ Switches

The plug-ins for the Avocent Autoview and MergePoint Unity KVM over IP and serial console switches allow you to discover, access and control rack PDUs that are attached serially to the switch within the DSView and Rack Power Manager software. Licenses are not required for Autoview or MergePoint Unity switch plug-in operations. For a complete list of switches supported by the DSView software, see the DSView software release notes.

The Autoview switch plug-in supports the following switch models:

- AV2108
- AV2216
- AV3108
- AV3216

The MergePoint Unity switch plug-in supports the following switch models:

- MPU104E
- MPU108E
- MPU108EDAC
- MPU1016
- MPU1016DAC
- MPU2016
- MPU2016DAC
- MPU2032
- MPU2032DAC
- MPU4032
- MPU4032DAC
- MPU8032
- MPU8032DAC

Several original equipment manufacturer (OEM) DSView software plug-ins are supported and should be used in conjunction with specific switches. The OEM plug-ins include:

- Dell® KVM Remote Console Switch Plug-In
- Avocent® MergePoint Unity for Dell KVM Over IP and Serial Console Switch Plug-In
- Fujitsu® KVM s4 Switch Plug-In
- Hewlett Packard Enterprise® Console Switch G2 Plug-In
- IBM® Global Console Manager (GCM) Appliance Plug-In

- Avocent® AutoView™ Switch for Dell
- Hewlett Packard Enterprise® KVM Console Switch G3 Plug-In
- Lenovo® Global Console Manager (GCM) Appliance Plug-In
- Lenovo® Local Console Manager (LCM) Appliance Plug-in

3.2 Avocent® Universal Management Gateway Plug-in

The Avocent Universal Management Gateway appliance plug-in allows you to access and control IT assets locally or remotely, launch KVM sessions to a target device from a single point of access and perform server management tasks.

You can also log in to the appliance's web interface to discover and add an appliance and other target devices and configure the appliance to discover service processors.

3.3 Cyclades™ ACS5000 Advanced Console Server

The Cyclades ACS5000 Advanced Console Server plug-in enables you to access, configure and manage the console servers from the DSView or Rack Power Manager software. The ACS5000 console server plug-in, version 3.3 or later, supports ACS5000 console servers.

3.4 Avocent® ACS6000 and ACS8000/ACS800 Advanced Console Server

The ACS6000 or ACS8000/ACS800 plug-in for the DSView software allows you to log in to the appliance's web interface to assign configuration template properties and perform configuration tasks. For some procedures, you will need to select the appropriate target device connected to the advanced console server. The ACS6000 and ACS8000/ACS800 console server plug-ins support all models of ACS6000 and ACS8000/ACS800 console servers, respectively, regardless of the number of ports.

3.5 Blade Chassis Plug-in

The Blade Chassis plug-in also allows you to access multi-vendor blade chassis and blades from the DSView™ software and launch a KVM session to any managed blade from a single point of access. When you install the Blade Chassis plug-in, you can log in to the appliance's web interface to discover and add MergePoint Unity™ switches or other target devices, view and manage appliances that are added, view DHCP status or apply a configuration template to the appliance. The Blade Chassis plug-in supports all Avocent KVM switches and the following blade chassis:

- IBM® Blade Chassis - BladeCenter (14 blades), BladeCenter T (8 blades), BladeCenter H (14 blades) or BladeCenter HT (12 blades)
- Dell® Blade Chassis - PowerEdge 1855 (10 blades) or PowerEdge 1955 (10 blades)
- HP® Blade Chassis - BladeSystem c-Class (16 blades) or BladeSystem p-Class (16 blades)
- Generic Blade Chassis

3.6 Infrastructure Plug-in

The Infrastructure plug-in allows you to visually organize units in a hierarchy based on the physical rack structure in a data center or lab. Configuring units in an infrastructure is required before utilizing the software. When you install the Infrastructure plug-in for the DSView or Rack Power Manager software, you can log in to the appliance's web interface to create an infrastructure hierarchy. After the hierarchy is created, you can view, modify and add units to the infrastructure.

3.7 Virtualization Plug-in

The Virtualization plug-in enables the access and control of virtual machines from the DSView™ software. Appliance plug-ins also allow authorized users access to troubleshoot, perform maintenance on, cycle power to or reboot connected devices. Supported unit types include VMware® VirtualCenters, ESX servers and virtual machines, as well as Citrix® XenServers™, Microsoft® Hyper-V servers, SCVMM and virtual machines. You can launch a Virtual Network Computing (VNC), Remote Desktop (RDP), Secure Shell 2 (SSH) or VMware viewer session to supported virtual machines from a single point of access.

NOTE: When the virtual environment units are selected, only the buttons and links for the supported operations are shown.

For detailed information on DSView software or Rack Power Manager software standard operations, procedures or particular functionality, refer to the Avocent® DSView™ 4.5 Management Software Installer/User Guide, the Avocent® Rack Power Manager Installer/User Guide or the installer/user guide for the corresponding appliance.

3.8 System Requirements

Prior to installing or running an appliance, infrastructure or virtualization plug-in, you must install Avocent DSView software version 4.0 or the Avocent Rack Power Manager software version 1.5.1 or later. If your appliance configuration contains hub and spoke servers, ensure the plug-in is installed on every hub and spoke server in the network.

Before installing and using the DSView software plug-in for virtualization, you must install the DSView software on a server that has access to a VMware or Xen environment.

NOTE: The servers must meet the minimum requirements and specifications for the DSView software. See the Avocent® DSView™ 4.5 Management Software Installer/User Guide for the minimum server requirements.

The Virtualization plug-in for the DSView software supports the following VMware vSphere, Xen environment and Microsoft Hyper-V entities:

- VMware® Virtual Center 5.5, 5.5u2 and 6.0
- VMware® ESXi 5.5, 5.5u2 and 6.0
- XenServer® 6.5
- Hyper-V2 (Windows® 2008) Hypervisors and SCVMMs
- Hyper-V3 (Windows® 2012) Hypervisors and SCVMMs

3.9 System Configurations

The following sections describe system configurations that must be in place prior to installing the appliance, infrastructure or virtualization plug-ins.

3.9.1 Configuring a blade chassis system

Connect a supported blade chassis to a KVM over IP appliance on a network accessible by the DSView software. The following list describes the connections required by Dell, IBM and HP blade chassis:

- For a Dell® blade chassis, connect the analog KVM card to the ACI port on the KVM over IP appliance. This single connection allows KVM sessions to all blades on the blade chassis.

NOTE: A connection to a digital KVM card on the Dell® blade chassis is not supported.

- For an IBM® blade chassis, connect the KVM card to a server port on the KVM over IP appliance through an Avocent PS/2 IQ module. This single connection allows KVM sessions to all blades on the blade chassis.
- For an HP® blade chassis, connect each blade to a server port on the KVM over IP appliance through an HP module. You must establish a connection for each blade that will launch a KVM session from the DSView™ software.

Figure 3.1 DSView Software System with a Connected IBM BladeCenter Blade Chassis

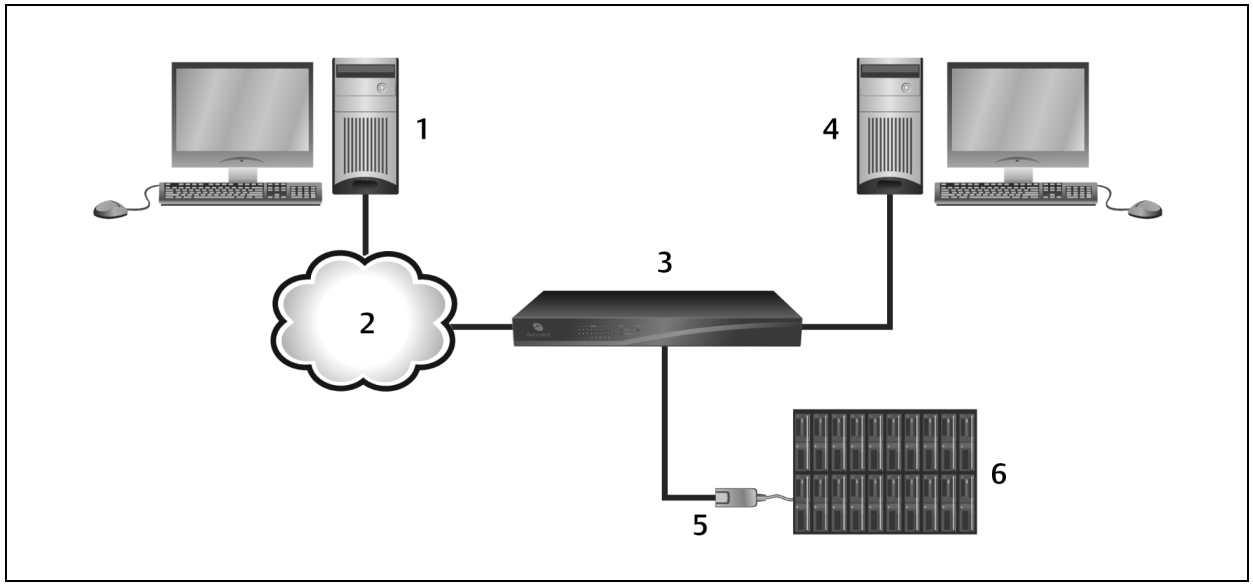

Table 3.1 System Configuration Descriptions

ITEM	DESCRIPTION	ITEM	DESCRIPTION
1	DSView Software System	4	PC running OSCAR™ Graphical User Interface
2	TCP/IP Connection	5	IQ Module
3	KVM over IP Appliance	6	Blade Chassis (IBM BladeCenter shown)

Adding a Dell® blade chassis

Before you add an attached Dell® blade chassis to the DSView™ software, use the Add Unit Wizard to add a KVM over IP appliance connected to the Dell® blade chassis.

To add a KVM over IP appliance with an attached Dell® blade chassis to the DSView software:

1. Click the *Units* tab and click *Blade Chassis* in the side navigation bar.
2. Click *Add*, select the appliance model from the product list and click *Next*.
3. Configure the Name and Address fields and click *Next*.
4. Click the Allow target devices with the same name to be merged into a single target device checkbox to merge the appliance in the DSView software database.
5. When adding target devices with default names, click the Blade checkbox under Allow target devices that contain default names to be added for these type of connection(s).
6. Click *Next - Finish*.

Adding an HP® blade chassis

Before you add an attached HP™ blade chassis to the DSView software, use the Add Unit Wizard to add a KVM over IP appliance connected to the HP blade chassis.

To add an HP™ blade chassis to the DSView software:

1. Click the *Units* tab and click *Blade Chassis* in the side navigation bar.
2. Click *Add - Next*.
3. Select the appropriate type of HP® blade chassis from the list and click *Next*.

   -or-

   If an HP™ blade chassis is already added, click *HP® BladeSystem - Add*, select the appropriate type of HP® BladeSystem blade chassis from the list and click *Next*.

NOTE: If you click *Add* from any Unit Views screen not described in steps 1-2, the Add Unit Wizard will not include options for adding a blade chassis.

4. Enter the name of the HP® blade chassis in the Name field.
5. Enter the IP address or URL of the HP® blade chassis in the IP address field.
6. When merging a blade that has multiple connections into a single blade in the DSView software database, click the Allow target devices with the same name to be merged into a single target device checkbox.
7. When adding target devices with default names, click the KVM checkbox under Allow target devices that contain default names to be added for these type of connection(s).
8. Click *Next - Finish*.

To use the Attach Device Wizard to associate a blade with a KVM over IP appliance port:

1. Click *Unit Views - Blade Chassis - HP® Blade System* in the side navigation bar.
2. Click the arrow to select and expand the information for the HP® blade chassis.
3. In the Action field of the port where the blade attaches, click the arrow to display the drop-down menu and click *Attach Device - Next*.
4. Select *Browse for an Existing Target Device - Next*.
5. Enter a valid filter string and click *Filter*.
6. Select a target device from the list and click *Next - Finish*.
7. Repeat steps 1-7 for additional HP® blades.

Adding an IBM® or generic blade chassis

Before you add an attached IBM® or generic blade chassis to the DSView™ software, use the Add Unit Wizard to add a KVM over IP appliance connected to the IBM® or generic blade chassis.

To add an IBM or generic blade chassis to the DSView software:

1. Click the *Units* tab and click *Blade Chassis* in the side navigation bar, then click *Add*.
2. Select the appropriate type of IBM® or generic blade chassis from the list and click *Next*.

   -or-

If an IBM® blade chassis has already been added, click *IBM® BladeCenter* or *Generic* in the side navigation bar, click *Add*, select the appropriate type of IBM® or generic blade chassis from the list and click *Next*.

NOTE: You must be on a Blade Chassis Unit Views screen so the Add Unit Wizard includes options for adding a blade chassis.

3. Enter the name of the blade chassis in the Name field.
4. Enter the IP address or URL of the blade chassis in the IP address field.
5. When merging a blade that has multiple connections into a single blade in the DSView software database, enable the Allow target devices with the same name to be merged into a single target device checkbox.
6. When adding target devices with default names, click the KVM checkbox under Allow target devices that contain default names to be added for these type of connection(s).
7. Click *Next - Finish*.

To use the Merge Chassis Wizard to associate each blade with a KVM over IP appliance port:

1. In a Unit Views screen containing the blade chassis to be merged, click the name of the blade chassis.
2. Click *Merge Chassis - Next*.
3. From the menu, select the KVM device and click *Next*.
4. From the menu, select the port to be merged with the blade chassis and click *Next*.
5. Click *Back* and repeat steps 4-5 to merge another blade.

NOTE: You must complete the Merge Chassis Wizard for each blade to be accessible from the DSView software.

-or-
Click *Finish* to close the screen.

3.9.2 Configuring a virtualization system

Connect the hypervisor managers and servers to a network accessible by the DSView™ software.

NOTE: (VMware only) If you do not need to access the VMware Viewer on an attached ESX server, you only need to connect the VirtualCenter to the network in order to access any attached ESX servers.

Figure 3.2 DSView Software Configuration with a Connected Virtual Environment

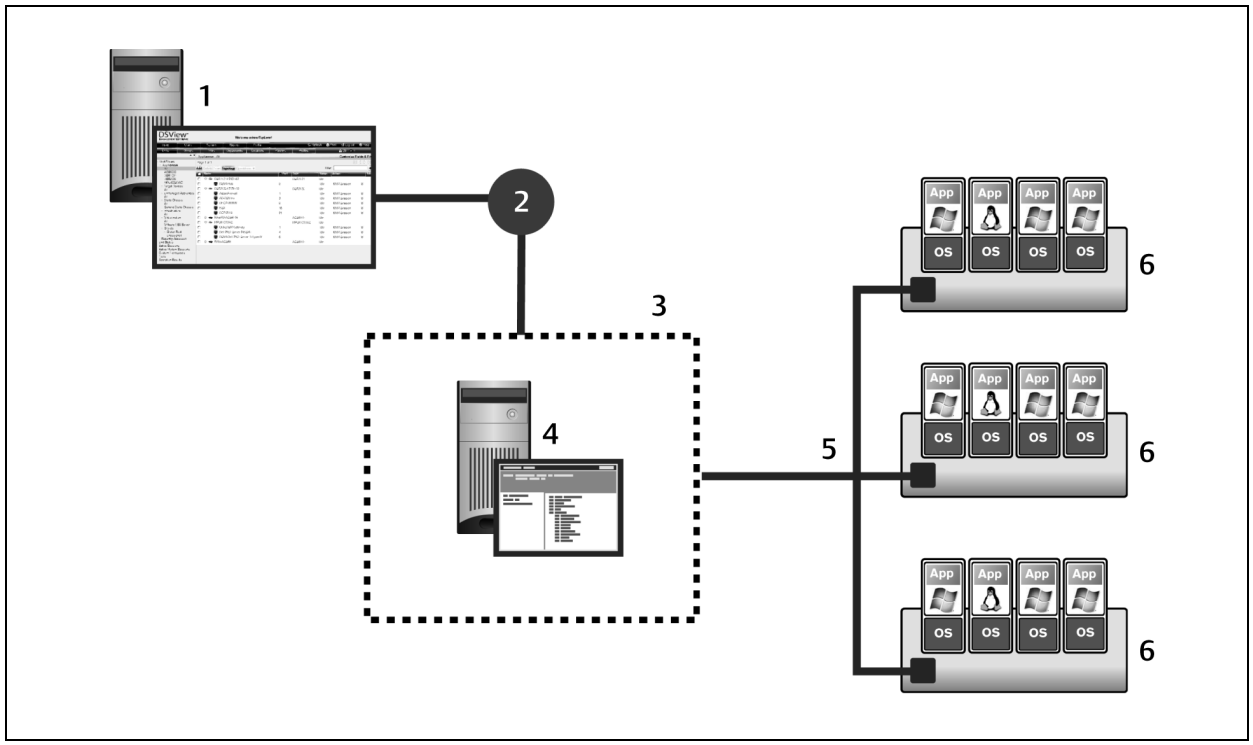

Table 3.2 Configuration Descriptions for DSView Software with a Connected Virtual Environment

ITEM	DESCRIPTION	ITEM	DESCRIPTION
1	DSView Software Client	4	Hypervisor Server
2	Virtualization Plug-In	5	SOAP/HTTPS Connection
3	Hypervisor Manager (Optional)	6	Virtual Machines

Adding a hypervisor manager or server

When you add a hypervisor manager to the DSView software, the attached hypervisor server(s) are added automatically. Hosted virtual machines are also added automatically, and you can specify which virtual machines are managed and accessible. You can access and control managed virtual machines from the Target Devices and Virtualization screens. From the hosted VMs screen, you can view unmanaged virtual machines and configure the status of managed or unmanaged machines.

NOTE: You cannot add a hypervisor manager or server by discovering units from a range of IP addresses.

To add a hypervisor manager or server to the DSView™ software:

1. In the side navigation bar, click *Units - Virtualization*.
2. Click *Add* in the content screen.
3. Select a unit type from the list and click *Next*.

   -or-

   Click a unit type in the side navigation bar and click *Add - Next*.

NOTE: You must be on the Virtualization Unit Views screen so the Add Unit Wizard includes options for adding a hypervisor manager or server.

4. Enter the IP address of the unit type selected in the Address field.
5. Select the *http* protocol.

   -or-

   Select the *https* protocol and click *Next* to accept the displayed certificate.

NOTE: The default TCP port number for the HTTP or HTTPS protocol is populated for you. If necessary, you can enter a different port number in the Port field.

6. Click *Next*.
7. Enter the username and password required to access the unit.
8. Select the Use DSView User Credentials for Operations checkbox and enable user credential caching in the DSView software to use DSView software user credentials for virtual environment operations.

NOTE: If the checkbox is not selected, the credentials provided for the hypervisor manager or server are used for all operations.

9. Select the hosted virtual machines to be managed and click *Add*.

   -or-

   Select *Manage all hosted virtual machines listed below* and click *Next*.

   -or-

   Click *Next* without adding any virtual machines to the managed list.

10. Click *Next - Finish*.

3.10 Unit Views

The Add Appliances Wizard allows you to add an appliance such as a switch to the DSView or Rack Power Manager software to manage the switch with the software. All added appliances are listed on the Unit Views screen. The Unit Views screen allows you to access the Operations drop-down menu and the Unit Overview screen to manage and configure a selected appliance.

3.10.1 Accessing a blade chassis

The added blade chassis and blades are available in the Unit Views screens in the DSView software and the blades are also available as target devices. From the Unit Views screens, you can manage properties, connections, session files and a variety of other functions for any unit, including blade chassis and blades.

NOTE: When the blade chassis or blades are selected, only the buttons and links for the supported operations are shown.

To access the Blade Chassis Unit Views screens:

1. Click the *Units* tab.
2. Click *Blade Chassis - All* to view all the blade chassis and connected blades.
   -or-
   Click *Dell PowerEdge*, *IBM BladeCenter*, *HP BladeSystem* or *Generic* to only display units of the respective type.

-or-

Click *Target Devices* in the side navigation bar to view all the target devices, including blades.

3. Click *Topology* and click the arrow to expand the blade chassis list and display all the connected blades.

3.10.2 Managing IBM® or HP® blade cards

The DSView™ software automatically detects the number of blade cards that a blade chassis supports. A target device name and port for each slot on the blade chassis are visible in the Unit Views screens, even if a blade is not physically in the slot. If you have empty slots for blades in an IBM or HP blade chassis, you can remove the associated blade name from the discovered blades list. If you add a blade to an empty slot on a blade chassis, you can add the blade back in the discovered blades list.

To manage IBM or HP blade cards:

1. In a Unit Views screen, click the name of the blade chassis.
2. Click *Manage Blade Cards* in the side navigation bar.
3. Select the blades from the right column and click *Remove* to remove blades from the discovered blades list.
   -or-
   Select the blades from the left column and click *Add* to add blades to the discovered blades lists.
4. Click *Save*.

3.10.3 Accessing a virtual environment unit

The added hypervisor managers, hypervisor servers and virtual machines are available in the Unit Views screens. When displaying these units, the DSView software uses the corresponding name reported by the virtual environment in the Add Unit Wizard. If the hypervisor manager and attached hypervisor server report a conflicting name for that server, the DSView software uses the name reported by the hypervisor manager.

To access the Unit Views screens:

1. Click *Units*.
2. Click *Virtualization - All* to view all components in the virtual environment.

   -or-

   Click a unit type to only display units of the respective type.

   -or-

   Click *Target Devices* to view all target devices, including virtual machines.

   -or-

   Click *Topology* to enable Topology view and click the arrow to expand the virtual environment unit list and display all connected units.

3.10.4 Deleting a virtual environment unit

Deleting the hypervisor managers or servers from the DSView™ software removes the unit from the DSView software but does not affect the virtual environment.

To delete the hypervisor managers or servers from DSView:

1. Click the *Units* tab and select the units to be deleted.
2. Click *Delete*.

NOTE: As a best practice, delete virtual machines from the virtual environment instead of clicking *Delete* in the DSView software. When virtual machines are added or removed from the virtual environment, the DSView software is automatically resynchronized with the virtual environment.

3.11 Operations

For more information about licensing, configuration tools and operations not listed in this document, see the Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power Manager Installer/User Guide.

3.11.1 Configuring SNMP

SNMP v1/v2 protocol is used to communicate management information between the DSView software server and the console server. However, the DSView software configures only one SNMP read and write community and SNMPv3 cannot be configured through the DSView software.

3.11.2 Granting access rights

The appliance plug-in is integrated with the DSView software licensing feature to control access privileges. In addition to assigning access rights to managed devices, the DSView server uses the plug-in to control access to specific functionality of the appliance. An administrator controls user or group access to the following tasks:

- View unit information
- Reboot appliance and disconnect sessions
- Flash upgrade the console server
- Configure unit settings
- Establish viewer sessions
- Control target device power
- View data logging

To configure access rights:

1. From the Unit Views screen, click *Access Rights* in the side navigation bar.
2. Select a value from the User and User Groups screen.
3. If the desired user or user group is not shown, click *Edit List*. Add a user or user group from the Available dialog box to the List to Update screen and click *OK*.
4. For each access right, check to enable the Allow, Deny or Inherit checkbox.

NOTE: When *Inherit* is selected, the Allow and Deny checkboxes are grayed out and the access right is inherited from the unit to which the selected user/group belongs. If none of the checkboxes are selected, the access right is neither allowed nor denied.

3.11.3 Organizing units in an infrastructure

Units must be organized in an infrastructure in the DSView™ software or Rack Power Manager software for the plug-in to accurately collect and aggregate historical data. Power operations and power monitoring

reports are available through the Rack Power Manager software. Each infrastructure can contain up to four levels in the following hierarchy: company, data center, row of racks and rack.

For a software system consisting of hub and spoke servers, a row of racks and the racks and devices it contains must be assigned to the same server. For example, a row of racks assigned to a hub server must not contain racks that are assigned to a spoke server.

To modify an infrastructure membership:

1. Click the *Units* - *Units* tabs.
2. Click *Infrastructure* or *Rack Power Manager* in the side navigation bar.
3. Click a company, data center, row of racks or rack.
4. Click *Membership* and select a unit from the Member of menu to configure the parent unit for the selected infrastructure level.
5. Select the unit(s) from the list and click *Add* to add members to the infrastructure level.
6. Select the unit(s) from the list and click *Remove* to detach members from the infrastructure level.
7. Select *Add data monitoring to selected units* - *Next* to monitor power data for the selected power devices.
8. Click *Finish*.

3.11.4 Launching KVM sessions in the DSView™ software

NOTE: Virtual media sessions to blades are not supported.

To open a KVM session from the DSView software Explorer:

In a Unit Views screen, click the *KVM Session* link in the Action column of a blade.

To open a KVM session from the Unit Overview screen:

1. In a Unit Views screen, click the name of the blade.
2. Click the *KVM Session* name or icon.

KVM switch key sequence

Dell® and IBM® blade chassis allow users to enter a key sequence to switch to another blade from an open KVM session. To prevent unauthorized access to blades, the preset Dell® and IBM® key sequence is disabled when a KVM session is opened from the DSView software. DSView software administrators can change the KVM switch sequence configured on the blade chassis.

The right column of the KVM Switch Sequence screen contains the preset KVM switch key sequence for a selected blade chassis. This key sequence is blocked to prevent the user from switching to another blade during a KVM session. If a user-defined key sequence is configured on the blade chassis, block this key sequence by moving the appropriate keys to the right column.

To configure a disabled KVM switch sequence:

1. In a Unit Views screen, click the name of the blade chassis.
2. Click *KVM Switch Sequence* in the side navigation bar.
3. Select the keys from the left column and click *Add* to add keys to the blocked key sequence list and move them to right column.
   -or-

Select the keys from the right column and click *Remove* to remove keys from the blocked key sequence list and move them to left column.

4. Click *Save - Close*.

3.11.5 Avocent® Universal Management Gateway appliance

The following procedures are operations unique to the Universal Management Gateway appliance. For more information about operations not listed in this document, see the Avocent® Universal Management Gateway Appliance Installer/User Guide.

Configuring the appliance

You can access the added appliance and its target devices from the Units tab in the DSView™ software.

To run an appliance session:

1. In the Unit Overview screen for the appliance, click *Appliance session* in the Tools section.
2. Type **cli** to invoke the CLI utility.

NOTE: For more information on the CLI utility, see the Vertiv™ Universal Management Gateway Appliance Command Reference Guide.

To run an appliance web user interface (UI) session:

In the Unit Overview screen for the appliance, click *Appliance WebUI session* in the Tools section.

Mapping appliance associations

There are corresponding appliance and target settings listed in the DSView software and the appliance web UI. Although the settings are the same in both, they are listed differently depending on which interface you are using. The following table lists the settings as they appear in the DSView software and then lists the equivalent settings as they appear in the appliance web UI. For more information on these associations, see the Avocent® Universal Management Gateway Appliance Installer/User Guide.

Table 3.3 UI Associations

DSVIEW SOFTWARE UI	APPLIANCE WEB UI
Appliance Settings	
Date and Time	Administration - Appliance Settings
Network - Settings	Administration - Network Settings
Network - Bridges	Administration - Network Settings - BGP
Network - Hosts	Administration - Network Settings - Hosts
Network - Static Routes	Administration - Network Settings - Routes
Users - Local Accounts - User Management	Administration - Users
Users - Authentication - Appliance Authentication	Administration - Users - Authentication
Users - Authentication Servers - Authentication - LDAP	Administration - Users - Authentication - LDAP
Users - Authentication Servers - Authentication - DSView	Administration - Users - Authentication - DSView
Users - Groups	Administration - Users - Groups
USB Ports	Administration - USB Devices
Security	Administration - Security

DSVIEW SOFTWARE UI	APPLIANCE WEB UI
Firewall and NAT - Policy - NAT	Firewall and NAT - Policy
Firewall and NAT - Policy - IP Forward Config	
Firewall and NAT - Policy - Firewall For System Defined	
Firewall and NAT - Policy - Firewall For User Defined	
Firewall and NAT - Interfaces - Outside Interfaces	Firewall and NAT - Interfaces
Firewall and NAT - Interfaces - Inside Interfaces	
Firewall and NAT - Hosts - UMG Defined Hosts	Firewall and NAT - Hosts
Firewall and NAT - Hosts - User Defined Hosts	
Firewall and NAT - Defined Networks	Firewall and NAT - Networks
Firewall and NAT - Services - UMG Defined Services	Firewall and NAT - Services
Firewall and NAT - Services - User Defined Services	
Target Settings	
Connected Targets	Administration - Targets
Target Ports - Port Assignments	Administration - Targets - Port Configuration - Port Assignment
Target Ports - Serial Management	Administration - Targets - Port Configuration - Serial Settings
Target Ports - Network Settings - System Interface	Administration - Targets - Port Configuration - Network Settings
Target Ports - Network Settings - Custom Interface	
Target Ports - DHCP Settings - DHCP Global Settings	Administration - Targets - Port Configuration - DHCP Settings
Target Ports - DHCP Settings - DHCP Dynamic Ranges	
Target Ports - DHCP Settings - DHCP Assignment By MAC	
Target Ports - DHCP Settings - DHCP Lease Bindings	
Target Ports - Discovery Settings - IP Ranges	Administration - Targets - SP Management - Discovery
Target Ports - Discovery Settings - Default Users	
Target Ports - Serial Settings - Serial Console Ports	Administration - Targets - Serial Management - Serial Console Ports
Target Ports - CAS Profile - Settings	Administration - Targets - Serial Management - CAS Profile
Target Ports - CAS Profile - Auto Answer	
Target Ports - CAS Profile - Probe Strings	
Target Ports - CAS Profile - Match Strings	
Target Ports - KVM Settings - KVM Devices	Administration - Targets - KVM Management - Devices
Target Ports - KVM Settings - Defaults	Administration - Targets - KVM Management - Default Settings
Target Ports - KVM Settings - Active Sessions	Administration - Targets - KVM Management - Active Sessions
Target Ports - KVM Settings - UMIQ Pass-Through	Administration - Targets - KVM Management - UMIQ Pass-Through
Target Ports - SP Settings - SP Management	Administration - Targets - SP Management - Service Processors
Target Ports - SP Settings - Access Settings	Administration - Targets - SP Management - Access Settings
Target Ports - PDU Settings - Serial PDU Ports	Administration - Targets - PDU Management - Serial PDU - Serial PDU Ports
Target Ports - PDU Settings - Logins	Administration - Targets - PDU Management - Serial PDU - Serial Login
Environmental Sensors	
Configure - COM Digital Inputs	Administration - Sensors - COM Digital Input
Configure - One-Wire Digital Inputs	Administration - Sensors - Digital Input

DSVIEW SOFTWARE UI	APPLIANCE WEB UI
Configure - One-Wire Environmental Sensor	Administration - Sensors - Environmental Sensor
Configure - RS-485 Environmental	Administration - Sensors - RS-485 Environment Sensor
View - Temperature Sensors	Sensors
View - Humidity Sensors	
View - Digital Inputs	
View - DI Alerts	
IP-based Access Licenses - Status	NA
Sessions	
Target Sessions	Administration - Sessions
Appliance Sessions	

The following table lists the events recorded in the DSView software and each equivalent event as shown in the appliance's web UI.

Table 3.4 Event Associations

DSVIEW SOFTWARE UI	APPLIANCE WEB UI
Appliance power device socket state off	Outlet is off
Appliance power device socket state on	Outlet is on
Appliance target name change	Change target name
Appliance target session started	A session has started
Appliance target session stopped	A session has ended
Appliance target SP power status off	The server controlled through the SP is turned off
Appliance target SP power status on	The server controlled through the SP is turned on
Appliance target topology change	Add or delete a target

Configuring a service processor

From the DSView™ software, you can configure the appliance to discover service processors (SPs) that reside on the same LAN as the appliance. Discovered service processors are displayed in the Managed SP list. You can also manually add a target device to the Managed Targets list if you know its IP address.

There are two discovery options, depending on the firmware version of the appliance.

If you are running appliance firmware version 2.0 or greater, you will be able to discover SPs via the Discovery (Current) node from the side navigation bar. Discovering SPs from this node is nearly identical to discovering SPs from the web UI of an appliance running firmware version 2.0 or greater.

If you are running appliance firmware 1.0, you will be able to discover SPs via the Discover (version 1.0) node from the side navigation bar. Discovering SPs from this node is nearly identical to discovering SPs from the web UI of an appliance running firmware version 1.0.

NOTE: Both nodes are available from the side navigation bar, however if you try to run a discovery method that is not compatible with your current firmware version, you will get an error message. For example, if your appliance is running firmware 2.0, you will get an error message if you try to discover via the Discovery (version 1.0) option.

3.11.6 Avocent® ACS6000 and ACS8000/ACS800 advanced console servers

The following procedures are operations unique to the ACS6000, ACS8000 and ACS800 advanced console servers. For more information about operations not listed in this document, see the Avocent® ACS6000 Advanced Console Server Installer/User Guide, the Avocent® ACS8000 Advanced Console Server Installer/User Guide or the the Avocent® ACS800 Advanced Console Server Installer/User Guide.

3.12 Adding an Appliance

Once you have logged on successfully, the Appliances-All screen displays all of the added devices and those available for adding in the DSView software.

To add an appliance:

1. On the Unit Views screen, click *Add - Next*.
2. Select either *Add a single appliance* or *Discover appliances on the network from an IPv4 address range or from an IPv6 subnet* and click *Next*.
3. Follow the specific instructions on your screen to either type a pre-configured IP address or enter an IP range for discovery and click *Next*.
4. Configure settings on the Select Options page:
    a. Select *Enable Secure Mode* to restrict access to the ACS6000 or ACS8000/ACS800 console server for this software installation.
    b. Select *Allow target devices with the same name to be merged into a single target device* to allow multiple target devices with the same name to be merged.
    c. Select *Allow target devices that contain default names to be added for these types of connections* to allow target devices with default names to be added, then select either or both of the connection type options (Serial and Power) and click *Next*.
5. Configure settings on the Configure Serial Ports page:
    a. For the Port Status, select either *Enable all ports and set to CAS* or *Keep current status*.

NOTE: Serial ports must be enabled to communicate with connected target devices.

    b. For Port Authentication, select either *Set authentication type of ALL ports* or *Keep current authentication*.
    c. If you chose to set the authentication type for all ports, select the authentication type from the drop-down menu and click *Next*.

NOTE: It is recommended that you change the factory default passwords to access the console server for administrator and root users.

6. Select a configuration template to apply to the console server, or select *None* to skip this step.
7. Click *Next - Finish* to return to the Unit Views page.

Using configuration tools

The ACS6000 and ACS8000/ACS800 console server plug-ins are integrated with the DSView™ management software tools to perform the following configuration tasks. You can access these tools from the Unit Views screen.

Table 3.5 Configuration Tools

APPLIANCE / TOOLS	DESCRIPTION
Reboot	Terminate all active sessions and reboot the console server.
Upgrade Firmware	Upgrade the firmware through the DSView server.
Resync	Synchronize the configuration information in the ACS6000 or ACS8000/ACS800 console server and connected target devices with the DSView server database.
Save Configuration (Legacy)	Back up the full console server configuration data to the DSView server database. The saved configuration includes the configuration not exposed in the web manager.
Restore Configuration (Legacy)	Restore a previously saved full console server configuration. The restored configuration includes the configuration not exposed in the web manager.
Save Configuration Template	Create a configuration template with a specific name. The configuration saved includes the web manager screens listed in Table 1.3 and can later be used to replicate this console server configuration to multiple console servers, or to restore the configuration to a replacement console server.
Apply Configuration Template	Restore a configuration saved during Save Configuration Template.
Save Last Known Good Configuration	Save a configuration template with a pre-defined name of Last Known Good Configuration.
Save Current Configuration	Save a configuration template with a pre-defined name of Current Configuration.
Appliance Replacement	Replace a console server with another one by applying the configuration template from the original one to the replacement console server.
Appliance Session	Launch a viewer with an SSH connection to the Linux command line of the ACS6000 or ACS8000/ACS800 advanced console server.
Shutdown Appliance	Terminate all active sessions and stop all services to prepare a console to be turned off.
Apply Last Known Good Configuration	Restore the configuration template saved as Last Known Good Configuration.
Apply Current Configuration	Restore the configuration template saved as Current Configuration.
HTTPS Certificate	Generates or downloads an individual HTTPS certificate for installation on the firmware.
Configuration Integrity	Generates and verifies a digital signature (MD5) of the appliance configuration to be used to automatically verify the integrity of an individual appliance configuration for change-detection capabilities.

In addition to the configuration tools described in the previous table, you can also perform the following tasks by selecting an appliance on the Unit Views screen and selecting the *Operations* drop-down.

Table 3.6 Operations Available on Unit Views Screen

OPERATION	DESCRIPTION
Hide Units From View	Hide the console server from view on the Appliances-All page.
Restore Hidden Units To View	Restore a hidden console server to view on the Appliances-All page. You can enable viewing of hidden items from the Customize Fields & Filter page.
Reboot	Terminate all active sessions and reboot the console server.
Show Version	Display current ACS6000 or ACS8000/ACS800 console server boot and firmware versions.

OPERATION	DESCRIPTION
Push Names to Appliance	The DSView software pushes names stored in the database to the console server and all targets.
Pull Names from Appliance	The DSView software pulls ACS6000 or ACS8000/ACS800 console server and all target names and synchronizes the DSView server database.
Properties	Customize the unit configuration in the DSView server database.
Apply Configuration Template	Restore a configuration saved during Save Configuration Template.
Apply Last Known Good Configuration	Restore the configuration template saved as Last Known Good Configuration.
Apply Current Configuration	Restore the configuration template saved as Current Configuration.
Save Current Configuration	Save a configuration template with a pre-defined name of Current Configuration.
Save Current Configuration	Save a configuration template with a pre-defined name of Current Configuration.
Properties - Bulk Edit	Edit multiple properties for the console server.
Disable FIPS mode	Disable the FIPS module.
Clear IP Change Token	Clears firmware tokens used in communication with DSView in a failover event.
Sync IP Change Token	Synchronizes tokens used in communication with DSView in a failover event.
Enable FIPs mode	Enable the FIPs module.

Configuring appliance settings

You can configure the following Appliance Settings for your ACS6000 or ACS8000/ACS800 advance console server system using the DSView™ software:

- System (security, boot configuration, login banner, language, date and time)
- Network (DNS, hostname, devices, firewall, SNMP and IPSec)
- Ports
- Pluggable devices
- Authentication
- Users
- Events and logs (event lists, event destinations, data buffering, appliance session and sensors)

Managing power devices

You can configure and manage power devices connected to an ACS6000 or ACS8000/ACS800 console server through the DSView software. Depending on the console server model, the following power devices are compatible with the ACS6000 or ACS8000/ACS800 server console:

- Avocent® Power Management Power Distribution Unit (PM PDU).
- Liebert® MPH2 rack Power Distribution Units (PDUs) as well as MPX and MPH rack PDUs with RPC2 cards installed.
- Cyclades™ PM Intelligent Power Distribution Units (IPDUs) - With Cyclades™ PM IPDUs, up to 128 outlets can be daisy chained and managed from a single serial port.
- Avocent™ SPC power control devices.
- Server Technology Sentry™ family of Switched Cabinet Power Distribution Units (CDUs), Smart Cabinet Power Distribution Units (Smart CDUs) and switched CDU Expansion Module (CW/CX) power devices.
- Server Technology Sentry Power Tower XL™ (PTXL) and Power Tower Expansion Module (PTXM) power devices.

- Eaton™ ePDU G3™ Power Distribution Units (PDUs). With Eaton ePDU G3 PDUs, up to eight ePDUs can be chained together and managed from a single serial port.
- Raritan™ PX G2™ Power Distribution Units (PDUs).
- APC™ Rack rPDU2™ Power Distribution Units (PDUs).

NOTE: Daisy chaining is not possible with SPC PDUs, Raritan PDUs or APC PDUs. ServerTech PDUs allow only one level (Master and Slave) of daisy chaining.

NOTE: Configuration and management of Server Technology Sentry CDU should be handled through the DSView™ software. The DSView™ server enables the Server Technology Sentry CDU licensing feature for the selected serial ports in the ACS6000 or ACS8000/ACS800 console server.

NOTE: Authorized users may also monitor and control a connected Liebert® GXT4 uninterruptible power device (UPS). The ACS8000/ACS800 advance console system automatically recognizes and supports Liebert® RPC2 cards, Avocent® PM PDUs, Cyclades™ PM PDUs or Avocent SPC devices when the corresponding serial port is configured for power management.

Applying appliance configuration template properties

Appliance configuration templates allow administrators to simultaneously configure multiple units from the DSView software. An appliance configuration template can be used to configure new units or to replace existing units. These properties are applied to an ACS6000 or ACS8000/ACS800 console server when the Appliance Replacement, Apply Configuration Template, Apply Last Known Good Configuration Template or Apply Current Configuration Template operations are executed.

In addition to supporting ACS8000/ACS800 appliance templates, the ACS8000/ACS800 plug-in also supports importing ACS6000 configuration templates. If an attribute is not specified or not present in the imported ACS6000 appliance configuration template, the ACS8000/ACS800 plug-in assigns default settings.

The following table lists the Appliance Settings screens that are supported for the ACS6000 or ACS8000/ACS800 console server configuration templates.

NOTE: Some models do not support all settings.

Table 3.7 Supported Appliance Settings Screens

MAIN NODES	SUBNODES
System	General
	Security - Security Profile
	Date and Time - Date & Time
	Date and Time - Timezone
	Help and Language
Network	Settings*
	IPv4 Static Routes*
	IPv6 Static Routes*
	Hosts*
	Firewall - IPv4 Filter Table
	Firewall - IPv4 Filter Table - Rules
	Firewall - IPv6 Filter Table
	Firewall - IPv6 Filter Table - Rules

MAIN NODES	SUBNODES
	IPSec (VPN)
	SNMP - System
	SNMP - v1, v2, v3
Ports	Serial Ports - Set CAS - Physical
	Serial Ports - Set CAS - CAS**
	Serial Ports - Set CAS - Data Buffering
	Serial Ports - Set CAS - Alerts
	Serial Ports - Set CAS - Power*
	Serial Ports - Set Dial-In
	Serial Ports - Set Power - Physical
	Serial Ports - Set Power - Power
	Aux Port - Set Dial-In
	Aux Port - Set Power - Physical
	Aux Port - Set Power - Power
	CAS Profile - Auto Discovery - Settings
	CAS Profile - Auto Discovery - Probe Strings
	CAS Profile - Auto Discovery - Match Strings
	CAS Profile - Auto Answer
	CAS Profile - Pool of Ports
	Dial-In Profile - Settings
	Dial-In Profile - Secure Dial-In - Callback Users
Authentication	Appliance Authentication
	Authentication Servers - RADIUS
	Authentication Servers - TACAS+
	Authentication Servers - Kerberos
	Authentication Servers - NIS
	Authentication Servers - DSView
Users	Local Accounts - User Names
	Local Accounts - Password Rules
	Groups - Members
	Groups - Log-in Profile
	Groups - Access Rights - Serial
	Groups - Access Rights - Power - PDU*
	Groups - Access Rights - Power - Outlets*
	Groups - Access Rights - Appliance
Events and Logs	Event List
	Event Destinations
	Data Buffering
	Appliance Session
	Sensors
Power Management	Log-in

*These screens are only applied when using the Appliance Replacement operation.
**The Port Name, Port IPv4 Alias and Port IPv6 Alias is used only during Appliance Replacement.
Default names is used when you use the Apply Configuration template.

3.13 Cyclades™ ACS5000 Advanced Console Server

The following procedures are operations unique to the ACS5000 Advanced Console Server. For more information about operations not listed in this document, see the Cyclades™ ACS5000 Advanced Console Server Installer/User Guide.

3.13.1 Using configuration tools

The console server plug-ins are integrated with the DSView™ software tools which are accessible from the Unit Overview screen. You must select the appropriate console server or connected target device from the Unit Views screen before you can perform the procedures in this document. Clicking the *Save* button saves your configurations in the DSView server database and in RAM on the console server. If the appliance has changes in RAM that are not saved in Flash, you must click the *Flash Required* button to store the changes permanently to the Flash memory card in the console server. The following table lists each tool and the task it performs.

Table 3.8 Configuration Tools

APPLIANCE / TOOLS	DESCRIPTION
Name	Rename a console server. Use alphanumeric characters, hyphen (-) or underscore (_) only.
Type	Non-editable field. It displays the console server type.
Reboot	Terminate all active sessions and reboot the console server.
Upgrade Firmware	Upgrade the firmware through the DSView software server. A valid Flash file must exist in the DSView server firmware repository.
Resync	Synchronize the console server and target device configuration information with the DSView server database.
Manage Power Devices	Configure and manage power devices connected to the console server and target devices.
Appliance Session	Launch a viewer with an SSH connection to the Linux command line of the console server. You can specify the application to be used for serial sessions to target devices. Select *Profile - Applications - Serial Sessions* for the options.
Save Configuration	Back up the console server configuration data to the DSView server database. The DSView server prompts you to enter a filename for the backup configuration file.
Restore Configuration	Restore a previously saved configuration. A valid configuration file must exist in the DSView server configuration files repository.
Save Configuration to Flash	Save the console server configuration data to Flash memory.

3.13.2 Configuring console server properties

You can configure the following console server settings using the DSView software:

- Network parameters
- Authentication method and DSView software authentication servers
- The console server web manager
- SNMP traps, Syslog or system events
- The console server ports
- Power devices and power management on target servers
- Data logging

The following tools are accessible from the Units Identification Properties screen.

Table 3.9 Properties Configuration

PROPERTY	DESCRIPTION
Identity	Identification properties which can be used for asset management.
Location	Information on physical location of the console server.
Contacts	Primary and secondary contacts responsible for administering the console server, who should be notified when there is an issue with the unit.
Custom Fields	Three custom fields in which you can specify information to better identify a console server on the network.
Notes	Any additional comments on the console server (for example, unit description or an associated accounting cost center).
Network	The IP address used by the DSView software to access the appliance.

To view or change properties:

1. From the Unit Views screen, select the console server to be configured.
2. Click *Properties* in the side navigation bar.
3. Change the desired property and click *Save - Close*.

Configuring network parameters

As a dual stack host, a single console server can manage servers configured for IPv4 and servers configured for IPv6.

NOTE: The console server must have firmware version 3.3 or later to configure IPv6 or DNS addresses.

To configure network parameters:

1. From the Unit Views screen, click *Appliance Settings - Network* in the side navigation bar.
2. Select *IPv4 Configuration - Enable IPv4* to enable and configure IPv4 for the appliance.
   a. Select *Static (User defined)* to define the address and enter the IPv4 address, subnet mask and gateway in the fields provided.

      -or-
      Select *DHCP* to acquire the values from the DHCP server.
   b. Click *Save*.
3. Select *IPv6 Configuration - Enable IPv6* to enable and configure IPv6 for the appliance.
   a. Select *Stateless Configuration Only* to automatically configure the appliance.

      -or-
      Select *Static (User defined)* to define the address and enter the IPv6 address, prefix and gateway in the fields provided.
      -or-
      Select *DHCP* to acquire the values from the DHCP server, then select *DNS* and/or *Domain*, respectively, to acquire server names and/or domain names from the DHCP server.
   b. Click *Save*.
4. Select *DNS* to configure two DNS servers for the console server.
   a. Select *Static (User defined)* in the IPv4 or IPv6 configuration to define the DNS addresses and enter IPv4 or IPv6 addresses in the fields provided.

      -or-

Select *DHCP* in the IPv4 or IPv6 configuration to acquire the server addresses from the DHCP server.

b. Click *Save*.

5. Click *Flash Required* to save your changes to the console server Flash memory.
6. Select *Units - Properties - Network* to update the unit network properties that were changed.

To push an IP address to a non-configured console server:

NOTE: The Avocent® Install and Discover Protocol (AIDP) allows the DSView™ software to use DHCP or assign a static IPv4 or IPv6 address to an unconfigured appliance.

1. Select an appliance from the Select Appliance Type menu and click *Next*.
2. If the console server does not have an IP address, select *No, the ACS 5000 was not configured yet* or *No, the ACS was not configured yet* and click *Next*.
3. Select *IPv4* and enter the IPv4 address and subnet mask in the fields provided. Select *Static* and enter a gateway in the field provided to define the address or select *DHCP* to acquire the address from the DHCP server then click *Save*.

   -or-

   Select *IPv6* and define the scope of where the multicast message will be sent. Select *Static* and enter the IPv6 address, prefix length and optionally enter a gateway in the fields provided or select *DHCP* to acquire the address from the DHCP server, then click *Save*.

4. Complete the Add Appliance Wizard.

Configuring dial-up connection

The console server plug-ins allow you to configure dial-up access via an external analog modem as a backup connection to the appliance.

The dial-up connection feature is configured from the Appliance Settings - Dial Up node on the Unit Views screen of a console server. You can access the Settings and External Modem screens from the Unit Views screen.

NOTE: To configure dial-up, you must have rights for Configure Unit Settings. Without those rights, you can only view the current settings.

The following table provides a summary of the fields on the Dial-up Configuration screen.

NOTE: Dial-up can be configured only when the appliance is reachable using the primary network.

Table 3.10 Dial-up Configuration

FIELD	CONTROL TYPE	DESCRIPTION
Enable Dial-up	checkbox	This refers only to the modem. When enabled, DSView software uses an external modem connection when the primary network is unavailable.
Modem Type	Radio Button	The only modem type supported is an external, analog modem.
Serial Modem Port	Combo box	This is the port number on the appliance where the external modem is connected.
Appliance Phone Prefix	Read-only text	This is the appliance's phone number prefix (required to reach the appliance), set by selecting *System - DSView Server - DSView Modem Sessions*.
Appliance Phone Number	Text	Enter the phone number that the DSView software uses to dial the appliance.
PPP User	Text	Enter the username of the modem user.

FIELD	CONTROL TYPE	DESCRIPTION
Change Password	checkbox	Check this field to be able to enter a password in the PPP password field; otherwise that field will be disabled.
PPP Password and Confirm PPP Password	Password	Use this password to authenticate the dial-up user. When disabled, the plug-in will use the previously-set password.
PPP Auth Protocol	Combo box	Select the authentication method: PAP or CHAP.
PPP User Auth (PAM)	Combo box	This is the desired authentication method for PPP user. It is recommended that *Local* authentication is selected since the PPP user is created as a Local user in the console server. If another authentication method is desired, the PPP user must be created in the authentication server and the authentication server must be accessible even if there is no connection between the dialer in DSView software and the console server.
PPP Local IP address	Display only	When first configured, these text areas are blank and you will have to select the Set PPP IP addresses checkbox to assign the PPP Local IP address. If previously configured, the PPP Local IP address will be displayed here.
PPP Appliance IP address	Display only	When first configured, these text areas are blank and you will have to select the Set PPP IP addresses checkbox to assign the PPP Appliance IP address. If previously configured, the PPP Appliance IP address will be displayed here.
Set PPP IP addresses	checkbox	Select this checkbox to assign new IP addresses for them or if the PPP Local IP and PPP Appliance IP address fields are blank. Selecting this checkbox will enable you to select one of the two radio buttons: Automatically or Choose Address Manually.
Automatically (Under Choose Address)	Radio button	Select this button to have the DSView software assign the PPP IP addresses from the address range in the System - DSView Server - DSView Modem Sessions screen.
Manually (Under Choose Address)	Radio button	Select this button to enter the PPP Local IP address and PPP Appliance IP address manually in the fields provided.
External Modem (sub screen)	drop-downs	Select the appropriate values for Baud, Data Bit, Flow Control, Parity, Stop Bits and DCD to configure the console server for dial-in connection using an external modem.

Configuring authentication

The console server plug-ins allow you to configure two authentication types: the DSView™ software or the Radius authentication server. When the DSView software centralized authentication service is configured, the DSView™ server is used to authenticate users accessing the console server.

To enable centralized authentication in the DSView software:

Select a DSView software authentication type.

To select a DSView software authentication type:

1. In the console server Unit Views screen, click *Appliance Settings - Authentication Type*.
2. Select an Authentication Type from the drop-down list and click *Save*.
3. Click *Flash Required* to save your changes to the console server Flash memory.

Use the Appliance Settings - Appliance Authentication Servers - DSView screen to configure up to four DSView software authentication servers for the authentication methods.

NOTE: The console server must have firmware version 3.3 or later to configure IPv6 addresses.

To configure DSView™ software authentication servers:

1. In the console server Unit Views screen, click *Appliance Settings - Authentication Servers - DSView*.
2. Enter the IPv4 or IPv6 addresses of up to four DSView software authentication servers on your network. Click *Save*.
3. Click *Flash Required* to save your changes to the console server Flash memory.

Radius authentication server configuration

The console server also supports the Radius authentication server. Use the Appliance Authentication Servers - Radius screen to configure up to four Radius authentication servers.

To configure Radius authentication servers:

1. In the console server Unit Views screen, click *Appliance Settings - Authentication Servers - Radius*.
2. Enter the IPv4 or IPv6 addresses of up to four Radius authentication servers on your network (up to two authentication servers and up to two accounting servers).
3. In the Secret field, enter the secret configured in the Radius Server.
4. In the Timeout field, enter the amount of time in seconds the console server will wait for the Radius server to respond before trying again.
5. In the Retries field, enter the number of retries to attempt if the Radius server does not respond before trying the secondary server.
6. Select the *Enable Service-Type attribute checking* checkbox to authorize the console server to retrieve the level of the user (admin or regular) based on the Service-Type attribute from the Radius server.
7. Click *Save*.
8. Click *Flash Required* to save your changes to the console server Flash memory.

Accessing the console server web manager

The console server web manager can be enabled or disabled from the Web Service screen. Enabling the web service is required for direct access to the console server. Otherwise, the web service is disabled.

To enable or disable access to the console server web manager:

1. In the console server Unit Views screen, click *Appliance Settings - Web*.
2. Select the new state for the web manager from the drop-down list and click *Save*.
3. Click *Flash Required* to save your changes to the console server Flash memory.

Configuring system events

The console server can be configured to send notifications for system events using the following modes of delivery:

- SNMP traps - System events are routed and logged in the DSView software event database, and optionally in the SNMP management systems.
- Syslog - System events are logged in the DSView software event database.

Configuring appliance alerts

You can configure and assign alert strings to system events. When a system event occurs, the alert string triggers an email notification. You can enter up to 10 alert strings in the displayed fields.

To enable appliance alerts and email notification:

1. In the console server Unit Views screen, click *Appliance Settings - Events - Appliance Alerts*.
2. Click *Enable Appliance Alert* and enter the desired text strings in the Alert String fields.
3. Click *Flash Required* to save your changes to the console server's Flash memory.

4. Click *Reports - Email Notifications* in the side navigation bar.
5. Click *Add - Next* to start the Add Email Notification Wizard.
6. Configure the email address properties and click *Next*.
7. (Optional) To assign a trigger email notification to an event, select an event, add it to the Events To Notify screen and click *Next*.
8. (Optional) To assign a trigger email notification to one or more unit groups, select a unit group and add it to the Events To Notify screen.
9. Click *Next - Finish*.

Configuring data logging

The Syslog protocol logs data between console servers and connected target devices. You can configure the following:

- Data logging on the console server or each individual serial port
- The DSView™ server receiving data logging messages
- The Syslog server and SSH server ports
- The SSH parameters on the console server

The Appliance Settings - Versions screen displays the boot code and firmware versions of the console server.

3.13.3 Configuring the console server serial port

You can perform the following tasks from the Ports screen:

- Enable or disable serial ports
- Rename serial ports and initiate a push or pull name operation
- Configure serial ports authentication method
- Configure serial ports connection protocol, break sequence and communication parameters
- Configure serial ports for multiple users and sessions
- Configure port alerts
- Configure data logging

Enabling or disabling a serial port

To enable or disable a serial port:

1. In the console server Unit Views screen, click *Appliance Settings - Ports - Serial*.
2. Click the checkbox to select a port and click *Enable Port* or *Disable Port*.
3. Click *Flash Required* to save your changes to the console server Flash memory.

NOTE: The Type (protocol) of each serial port is configurable through the console server web manager.

Configuring serial port general settings

To configure serial port general settings:

1. In the console server Unit Views screen, click *Appliance Settings - Ports - Serial*.
2. Click the desired port number.

3. Enter a desired name in the Name in Appliance field.
4. Select an Authentication Type for the serial port from the drop-down menu.
5. Select the desired protocol for connecting to a target device.

NOTE: Only SSH and SSH/Telnet are supported by the serial viewer.

6. Enter a desired character string for sending a break sequence to the serial port (the default is ~break [Ctrl-b]).
7. Select the linefeed suppression of *After a CR*, *None* or *Null After a CR* from the menu.
8. Enter the idle time-out in minutes.
9. Select the terminal type for the serial viewer session.
10. Select *screens EMS* for the serial viewer session to emulate a screens EMS terminal.
11. Click *Save* to store your changes in the DSView™ software database.
12. Click *Flash Required* to save your changes to the console server Flash memory.

Configuring serial communication parameters

In addition to the communication options available to serial devices in the DSView software, you can configure the following communication parameters on a serial port:

- Detect if a modem in use is still turned on and active.
- Monitor a Data Carrier Detect (DCD) signal. The system can generate an alarm if a serial console cable is removed from the console server or if a target device attached to the console server is powered down.

To configure serial communication parameters:

1. In the console server Unit Views screen, click *Appliance Settings - Ports - Serial*.
2. Click the serial port to be configured.
3. Click *Communication*.
4. Configure the communication parameters and the DCD signal.

NOTE: Communication settings must match the settings in the target device.

5. Click *Save* to store your changes in the DSView software database.
6. Click *Flash Required* to save your changes to the console server Flash memory.

Configuring multiple users and sessions

The console server allows multiple users to connect simultaneously to a single serial port. The following table describes the available options for configuring multiple users or sessions.

Table 3.11 Multiple Session Settings

MULTIPLE SESSION SETTING	DESCRIPTION
No	Multiple sessions are not allowed; however one shared session and one normal session are allowed. Only two users can connect to the same port simultaneously.
Read/Write	More than two simultaneous users can connect to the same serial port. A sniffer menu displays, in which you can choose to: • Open a sniff session • Open a read/write session • Cancel a connection • Send a message to other users connected to the same serial port
Read/Write	Read/write sessions are opened, and the sniffer menu does not display.
ReadOnly	Read only sessions are opened, and the sniffer menu does not display.

To configure multiple users and sessions:

1. In the console server Unit Views screen, click *Appliance Settings - Ports - Serial*.
2. Click the serial port to be configured.
3. Click *Multi-User* from the side navigation bar.
4. Select the *Enable Multiple Sessions* checkbox.
5. Select an option from the Multiple Sessions Settings drop-down menu.
6. In the Privileged Users field, enter the usernames or group names with access rights to a multiuser shared session.
7. In the Menu Hotkey field, enter the hotkey sequence for accessing the menu (the default sequence is ^Z [Ctrl-Z]).
8. Activate the Notify Users checkbox to inform users of session access.
9. Select an option from the Sniff Mode drop-down list to configure the type of data displayed on the monitor in a port-sharing session.
10. Click *Save* to store your changes in the DSView™ software database.
11. Click *Flash Required* to save your changes to the console server Flash memory.

Logging serial port data

The console server supports two methods of data logging and only one of the data logging methods can be enabled at a time. The two supported data logging methods are:

- DSView™ server centralized data logging of the serial console sessions and direct SSH/Telnet sessions to the console server.
- Console server local data logging where data is stored in circular format in a file or buffer. In a circular data logging format, data is written into a specified local data file until the maximum file size is reached then the data is overwritten sequentially as additional data log is stored. Circular buffering requires an administrator to set up a process to examine the data during the timeframe before the data logging file or buffer reach its maximum size.

3.13.4 Managing power devices

You can configure and manage the following power devices connected to a console server through the DSView™ software:

- Avocent® PM (Power Management) 1000/2000/3000 Power Distribution Units (PDUs)
- Avocent® SPC power control device
- Cyclades™ PM Intelligent Power Distribution Unit (IPDU)
- Server Technology Sentry™ Switched CDU, Smart CDU and PTXL models

NOTE: Configuration and management of Server Technology Sentry models should be handled through the DSView software. The DSView™ server enables the Server Technology Sentry licensing feature for the selected serial ports in the console server.

Adding or removing power management devices

To add or remove power management devices:

1. In the console server Unit Views screen, click *Appliance Settings - Ports - Power Devices*.
2. Click *Manage* to start the Power Management Wizard and click *Next*.
3. Select the Add Power Devices or Remove Power Devices radio button and click *Next*.
4. Select the console server serial port number where a power device is attached.
5. Select a Power Device Type from the drop-down menu to add a power device.

NOTE: The options include Avocent/Cyclades, Server Tech or SPC power device.

6. Click *Next - Finish*.
7. Click *Flash Required* to save your changes to the console server Flash memory.

Resetting Hardware (HW) overcurrent protection

If a PDU has overcurrent protection and an overcurrent situation occurs, the Reset HW Overcurrent Protection reactivates the circuits.

To reset HW overcurrent protection:

1. In the console server Unit Views screen, click *Appliance Settings - Ports - Power Devices*.
2. Select the PDU where the circuit breaker was tripped.
3. Click *Reset HW Overcurrent Protection*.

Configuring power device settings

Depending on the power device type, the configurable parameters can differ. The following tables describe the parameters viewable when an Avocent PM PDU, Cyclades PM IPDU, an Avocent SPC power control device or a Server Technology Sentry CDU or PTXL model is used.

Table 3.12 Avocent PM PDU and Cyclades PM IPDU Configuration Parameters

PARAMETER	DESCRIPTION
Name in Appliance	The name saved in the power device.
Name in DSView	The name assigned to the power device in the DSView software.
Firmware Version	The power device's firmware version.
Number of Sockets	Total number of outlets in the power device.
Model	The power device's model name.
Syslog	Enable or disable Syslog messages.
Buzzer	Enable or disable the buzzer.

PARAMETER	DESCRIPTION
SW Overcurrent Protection	Enable or disable Software Overcurrent protection. If the current on the power device exceeds the user-defined current high critical threshold, this function prevents outlets from being turned on.
Poll Rate (milliseconds)	The time value that the power device is polled for status and data. The value should be set between 500 and 10,000.
Vendor Name	The name of the power device manufacturer.
Default Voltage (Cyclades PM IPDU only)	The nominal input voltage feeding the power device. Some power devices do not have the capability to read the real input voltage using proper voltage sensors.
Power Factor (Cyclades PM IPDU only)	The ratio of the real power to the apparent power; a number between 0 and 1 that is frequently expressed as a percentage. Real power is the capacity of the circuit for performing work in a particular time. Apparent power is the product of the current and voltage of the circuit.
Cycle Interval	Number of seconds a socket's power stays off before it is turned back on.
Cold Start Delay	Number of seconds the socket's power stays off before the sockets are turned on during cold start of the PDU.
LED Display	The orientation (Normal or Inverted) set in the LED Display. The LED Display shows the Current (ampere). Valid for models that support this configuration.
LED Display Refresh Period (seconds)	Number of seconds that the LED Display shows the Current of a phase or bank before switching to the next phase or bank. Valid for models that support this configuration.

Table 3.13 Avocent® SPC Device, Server Technology Sentry CDU and PTXL Models Configuration Parameters

PARAMETER	DESCRIPTION
Name in Appliance	Avocent SPC power control device or Server Technology Sentry CDU or PTXL model name saved in the power control device.
Name in DSView	The name assigned to the power device in the DSView software.
Status	Status of the power device (enabled or disabled). This parameter appears only if the console server firmware is earlier than 3.3.
Version	Current firmware version.
Total Load (A)	Total current load on the power device. This parameter appears only if the console server firmware is earlier than 3.3.
Total Load Minimum (A)	Triggers an enabled trap when a drop in the current below the defined minimum current threshold is reached. This value should be set between 0 and 30. This parameter appears only if the console server firmware is earlier than 3.3.
Total Load Maximum (A)	Triggers an enabled trap when a reading above the defined maximum current threshold is reached. This value should be set between 0 and 30. This parameter appears only if the console server firmware is earlier than 3.3.
Number of Sockets	Total number of outlets in the power device.
Poll Rate (milliseconds)	The time value that the power device is polled for status and data. The value should be set between 500 and 10,000.
Vendor Name	The name of the power device manufacturer.
Input Feeds	Number of power inlets used by the power device.

PARAMETER	DESCRIPTION
Model	The power device model name.
Sequence Interval	When turning on multiple sockets at the same time, this is the delay time (in seconds) between operations on each socket (valid only on master Server Technology Sentry CDU and PTXL models).
Reboot Delay or Cycle Interval	Number of seconds that a socket's power stays off before it is turned back on (valid only on master Server Technology Sentry CDU and PTXL models).
Default Voltage	The nominal input voltage feeding the power device. Some power devices do not have the capability to read the real input voltage using proper voltage sensors.
Power Factor	The ratio of the real power to the apparent power; a number between 0 and 1 that is frequently expressed as a percentage. Real power is the capacity of the circuit for performing work in a particular time. Apparent power is the product of the current and voltage of the circuit.

To change power device settings:

1. In the console server Unit Views screen, click *Appliance Settings - Ports - Power Devices*.
2. Select the power device to be configured.
3. Modify the power device parameters.
4. Click *Save* to store your changes in the DSView software database.
5. Click *Flash Required* to save your changes to the console server Flash memory.
6. Click *Close*.

Configuring power device sockets

The Power Device Sockets screen allows you to perform the following operations on an individual or multiple power device sockets:

- Switch power sockets on or off.
- Lock a socket to prevent accidental power switch, or unlock a socket.
- Cycle power on an individual socket or on multiple sockets with a defined power up interval.
- Save configuration changes to Flash memory on the console server.

NOTE: Depending on the power device type, the configurable parameters can differ.

To configure individual power device sockets:

1. In the console server Unit Views screen, click *Appliance Settings - Ports - Power Devices*.
2. Select the power device to be configured.
3. Click *Sockets* from the side navigation bar.
4. Click the checkbox to select single or multiple sockets.
5. Click *On* or *Off* to switch the power on a socket.

   -or-

   Click Cycle to briefly switch a socket off and on.

   -or-

   Click *Lock* to prevent an accidental power switch, or click *Unlock* to unlock a socket.

   -or-

Click *Save Status* to save changes made to the outlet.

6. Click a single socket to modify the settings. See the following table.

Table 3.14 Power Device Socket Parameters

SETTING	DESCRIPTION
Socket	View the number of the outlet in the power device.
Name	Assign or change the name of an outlet in the power device.
Post-On Delay	Delay (in seconds) for turning on subsequent outlets after an outlet has been turned on.
Post-Off Delay	Delay (in seconds) for turning off subsequent outlets after an outlet has been turned off.
Minimum On Time (Avocent SPC power control devices only)	Minimum time an outlet stays on before it is turned off. Valid values are 0s, 15s, 30s, 45s, 1m, 1m15s, 1m30s, 1m45s, 2m, 3m, 4m, 5m, 10m, 15m, 30m and 1h.
Minimum Off Time (Avocent SPC power control devices only)	Minimum time an outlet stays turned off before it is turned on. Valid values are 0s, 15s, 30s, 45s, 1m, 1m15s, 1m30s, 1m45s, 2m, 3m, 4m, 5m, 10m, 15m, 30m and1h.
Wake-Up State	Outlet state after a cold boot. It can be set to on, off or the last saved state. Wake-Up State is not applicable for Server Technology and SPC PDUs.

Configuring power device current

Use the Current screen to view and configure current information for the PDU, outlets, phases and banks. This screen is present if the console server firmware version is 3.3 or later. The following table describes the parameters.

Table 3.15 Power Device Current Parameters

PARAMETER	DESCRIPTION
ID	The unique ID of the element.
Scope	The element type (PDU, phase, bank or outlet).
Name	Name of the element (PDU or outlets only).
Value (A)	The current value measured in amperes.
Max (A)	The maximum value recorded, measured in amperes. The Max (A) value can be reset with the Reset Values button.
Min (A)	The minimum value recorded, measured in amperes. The Min (A) value can be reset with the Reset Values button.

To configure power device current parameters:

1. In the console server Unit Views, click *Appliance Settings - Ports - Power Devices*.
2. Select the power device to be configured.
3. Click *Current* from the side navigation bar.
4. Select the Current to be configured.
5. Set the Current high and low critical and warning thresholds.

NOTE: You can set a trap to be sent when the high or low threshold is reached.

6. Click *Save*.

Configuring power device voltage

Use the Voltage screen to view voltage information for the PDU, outlets, phases and banks. This screen is present if the console server firmware version is 3.3 or later. The following table describes the parameters.

Table 3.16 Power Device Voltage Parameters

SETTING	DESCRIPTION
ID	The unique ID of the element.
Scope	The element type (PDU, phase, bank or outlet).
Name	Name of the element (PDU or outlets only).
Value (V)	The current value measured in volts.
Max (V)	The maximum value recorded, measured in volts. The Max (V) value can be reset with the Reset Values button.
Min (V)	The minimum value recorded, measured in volts. The Min (V) value can be reset with the Reset Values button.
Measurement	The voltage can be measured if the PDU supports voltage detection or it can be estimated if the PDU requires the user to configure the Nominal Voltage.

Configuring power consumption

Use the Power screen to view power consumption information for the PDU, outlets, phases and banks. This screen is present if the console server firmware version is 3.3 or later. The following table describes the parameters.

Table 3.17 Power Device Power Consumption Parameters

SETTING	DESCRIPTION
ID	The unique ID of the element.
Scope	The element type (PDU, phase, bank or outlet).
Name	Name of the element (PDU or outlets only).
Value (W)	The current value measured in watts.
Max (W)	The maximum value recorded, measured in watts. The Max (W) values can be reset with the Reset Values button.
Min (W)	The minimum value recorded, measured in watts. The Min (W) values can be reset with the Reset Values button.
Measurement	The power consumption can be measured if the PDU supports voltage detection or it can be estimated if the PDU requires the user to configure the Nominal Voltage.
Power Factor	The ratio of the real power to the apparent power; a number between 0 and 1 that is frequently expressed as a percentage. Real power is the capacity of the circuit for performing work in a particular time. Apparent power is the product of the current and voltage of the circuit.

Configuring power device environment

Use the Environment screen to view environmental information for the PDU. This screen is present if the console server firmware version is 3.3 or later. The following table describes the parameters.

Table 3.18 Power Device Environment Parameters

SETTING	DESCRIPTION
Sensor	The sensor ID.
Name	The sensor name.
Type	The sensor type.
Value	The current value of the sensor.
Max	The maximum value recorded by the sensor. The Max (W) values can be reset with the Reset Values button.
Min	The minimum value recorded by the sensor. The Min (W) values can be reset with the Reset Values button.
Threshold	The threshold value that caused the Alarm.
Alarm	Active alarm with the highest priority. It indicates the sensor value reached one of the configured thresholds.

To change power device environment parameters:

1. In a Unit Views screen containing an ACS5000 console server, click *Appliance Settings - Ports - Power Devices* in the side navigation bar.
2. Select the power device to be configured.
3. Click *Environment* from the side navigation bar and select the sensor to be configured.
4. Set the sensor high and low critical and warning thresholds and click *Save* to store your changes.

NOTE: You can set a trap to be sent when the high or low threshold is reached.

3.13.5 Configuring hostname discovery strings

NOTE: To configure hostname discovery strings, the console server must have firmware version 3.3 or later.

You can configure customized probe and answer strings to provide a framework for the console server when it attempts to discover hostnames. If configured, these strings are valid for all serial ports. Probe and answer strings appear in lists that are used to probe the device connected to the serial port and to extract the hostname.

NOTE: Using probe strings requires specific knowledge of C-like escape sequences. Using answer strings requires specific knowledge of POSIX extended regular expressions.

NOTE: Hostnames longer than 31 characters will be truncated. Only the first 31 characters of a hostname will be assigned to the serial port alias.

To configure hostname discovery probe and answer strings:

1. In the console server Unit Views, click *Appliance Settings - Ports - Hostname Discovery*.
2. In the Hostname Discovery Probe Strings field, enter the range of probe strings.
3. In the Hostname Discovery Answer string field, enter the range of answer strings.
4. Click *Save*.

3.13.6 Configuring the TCP Port

By default, the TCP port numbers start at 7001 for serial port 1 and increase incrementally by one (+1) up to the number of serial ports that your console server supports. For example, a console server with eight serial ports has TCP ports 7001 through 7008. If these ports are already in use within your system, the default settings can duplicate and fail. If this occurs, change the default TCP base port for the serial port.

To configure the default TCP base port number:

1. In the console server Unit Views, click *Appliance Settings - Ports - TCP Port*.
2. Enter the new base port in the field.
3. Click *Save* to store your changes in the DSView™ software database.
4. Click *Flash Required* to save your changes to the console server Flash memory.

Console server TCP and UDP ports usage

The communication between the DSView software plug-in and the console server is through a Secure Shell protocol (SSH). See the following table for port usage information.

Table 3.19 Console Server Communication Ports

PORT ID	DESCRIPTION
TCP 3871	Avocent DS Authentication Protocol (ADSAP2). Used for session authorization.
TCP 1078	Avocent serial viewer port in proxy mode.
TCP 4122 (default)	SSH Server port.
TCP 4514 (default)	Data Logging Server port.
UDP 3211	Avocent Install and Discovery Protocol (AIDP). Used for IP configuration.
UDP 162	SNMP trap port. Used if the console server is configured to send SNMP traps to the DSView server.

3.13.7 Configuring sessions settings

Using the Sessions menu, you can perform the following tasks:

- View the active sessions, logged in users for each target device and their connection duration.
- Terminate a user session and disconnect them from the target device.
- Set an idle time-out, which is the maximum time (in seconds) that a session is idle before the user is logged off.
- Configure multiuser settings that will be valid to all serial ports.

To monitor active sessions or set an idle time-out:

1. In the console server Unit Views, click *Appliance Settings - Sessions - Active*.
2. Click the checkbox to select a target device and click *Disconnect* to terminate a user's session.
3. Select *Sessions - Settings - Serial* to set an idle time-out.
4. In the Idle Timeout field, enter a value (in seconds).
5. Click *Save* to store your changes in the DSView software database.
6. Click *Flash Required* to save your changes to the console server Flash memory.

To configure multiuser settings:

1. In a console server Unit Views screen, click *Appliance Settings - Sessions - Settings - Multi-User*.
2. Select the Enable Multiple Sessions checkbox.
3. Select an option from the Multiple Sessions Settings drop-down menu.
4. In the Privileged Users field, enter the usernames or group names with access rights to a multiuser shared session.
5. In the Menu Hotkey field, enter the hotkey sequence for accessing the menu (the default sequence is ^Z [Ctrl-Z]).
6. Activate the Notify Users checkbox to inform users of session access.
7. Select an option from the Sniff Mode drop-down list to configure the type of data displayed on the monitor in a port-sharing session.
8. Click *Save* to store your changes in the DSView™ software database.
9. Click *Flash Required* to save your changes to the console server Flash memory.

3.14 Virtualization

The following procedures are operations unique to the virtual machine environments. For more

information about operations not listed in this document, see the Avocent® DSView™ 4.5 Management Software Installer/User Guide or the Avocent® Rack Power Manager Installer/User Guide.

3.14.1 Managing a virtual machine

Before you can access or control a virtual machine from the DSView software, the machine must be designated as managed, which makes the units available from the DSView Target Devices and Virtualization screens. Each managed virtual machine uses a managed device license in the DSView software. If a virtual machine is added, it is available in the Hosted VMs screen but remains unmanaged until you designate it as managed.

To designate virtual machines as managed devices:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor manager or server.
3. Click *Server Settings* in the side navigation bar.
4. Click *Hosted VMs*.
5. Select the virtual machines from the Hosted Virtual Machines list and click *Manage* to designate virtual machines as managed.

   -or-

   Select the virtual machines from the Hosted Virtual Machines list and click *Unmanaged* to designate virtual machines as unmanaged.
6. Click *Close*.

NOTE: A setting of N/A in the Managed column indicates the virtual machine was reported as a hosted virtual machine in the virtual environment but is not synchronized with the DSView database.

3.14.2 Enabling automatic virtual machine management

After performing a resync or during VMware operations such as VMotion, VMs are removed from DSView™ software and then added back when the virtual machine is placed on a different ESX server. This places the virtual machine in an unmanaged state. Enabling automatic virtual machine manageability prevents virtual machines from being placed in an unmanaged state.

To enable automatic virtual machine manageability:

1. Click *System* and select *Plug-ins* from the menu.
2. Select the *Virtualization* plug-in and select *Settings*.
3. Click the Automatically move VMs to Managed State checkbox.

NOTE: If automatic virtual machine manageability is enabled, any new or cloned virtual machines are automatically placed in a managed state.

3.14.3 Using Unit Tools

Merging virtual target device connections with physical target device connections allows all possible actions to be available from a single view, while the physical and virtual target devices remain distinct entities within the DSView database.

Establishing virtual machine sessions

You can establish a VNC, RDP, SSH, Hyper-V or VMware viewer session to a virtual machine. The VNC viewer service is automatically added when a virtual machine is added to the DSView software. The VMware viewer service is only added for VMware virtual machines and cannot be manually added or removed using the Add Services Wizard in the DSView software.

The RDP viewer service is added only for virtual machines reporting a Microsoft® Windows operating system. The SSH session viewer service is only added for virtual machines reporting a Portable Operating System Interface (POSIX) such as Linux® or Solaris®, and the SSH service must be configured on the virtual machine from the DSView software.

NOTE: Virtual media sessions to virtual machines are not supported.

The following parameters are required to establish sessions:

- The virtual machine must be configured to support the viewer to establish a VNC or RDP session.
- The virtual machine must be configured with an SSH server and be listening to SSH client requests to establish an SSH session.
- A current and compatible web browser is required to establish a VMware viewer session. See the Avocent® DSView™ 4.5 Management Software Release Notes for a list of supported browsers.

NOTE: By default, the VMware viewer uses ports 902 and 903 to communicate with ESX servers. If these ports are blocked by a firewall, the VMware viewer session fails to launch.

NOTE: Client viewer sessions using the VMware Viewer will fail on an ESXi server unless vSphere or VirtualCenter are installed.

To establish an initial RDP session:

1. In the DSView software, click *Units* and expand the appliance.

2. Select the target device.
3. Select *Services - Add* to add a new service.
4. Choose *Select services discovered running on the target device* and click *Next*.
5. Select the remote desktop service and click *Add - Next*.
6. Click *Finish - Close*.

To open an RDP session:

1. Click the name of the target device.
2. Click *RDP session*, choose the display settings and click *OK*.
3. Enter the username and password and click *OK*.

To open a virtual session:

1. Click *Units - Virtualization*.
2. Click *All* or *Virtual Machine* in the side navigation bar.
3. In the Action column, select the type of session to be opened.

   -or-

   Click the name of the virtual machine and select the type of session to be opened under Tools.

Session status (VMware only)

If a virtual machine has at least one active session through the VMware viewer, a status of In Use is listed and a yellow circle is displayed on the icon for the virtual machine. The In Use status and yellow circle are also displayed for the ESX server and/or VirtualCenter that hosts that virtual machine.

NOTE: Unit status polling must be enabled in the DSView™ software in order to view virtual machine session status. The virtual machine session status can be inaccurate if the polling cycle is too large.

Adding and managing a Microsoft Hyper-V server

For the DSView software to manage a Microsoft System Central Virtual Machine Manager (SCVMM), the following are required:

- SCVMM console must be installed on the same server as the DSView server.
- Hyper-V servers can only be managed by a DSView server running screens.
- Hyper-V servers and SCVMM have to be in the same domain as the DSView server.

To add a Hyper-V server:

1. Click *Units - Virtualization*.
2. Click *Add* to open the Add Unit Wizard.
3. Select *Microsoft Hyper-V Server* and click *Next*.
4. Enter the IPV4/IPV6 or DNS name of the Hyper-V server and click *Next*.
5. On the Server Credentials screen, enter the username, password and domain for the Hyper-V server and click *Next*.
6. Select the virtual machines to be managed by the DSView software and click *Add*.
7. Click *Next - Finish*.

To manage a Hyper-V server:

1. Click *Units - Virtualization - Microsoft Hyper-V server*.
2. Click the Hyper-V server name.
3. Modify the necessary access rights.
4. Click *Close*.

Accessing VMware Viewer sessions

From the DSView™ software, you can connect to the VMware Viewer for a VirtualCenter and an ESX server. The VMware Viewer is accessed by the IP address you entered in the Add Unit Wizard.

NOTE: This procedure is only applicable to VMWare.

To access the VMware Viewer:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter or ESX server.
3. Under Tools, click the *VMware Viewer* link.

Establishing SSH sessions to hypervisor servers

You can establish an SSH session to a hypervisor server, provided the server is configured with an SSH server and listening to SSH client requests. The SSH session service is automatically added when a hypervisor server reporting a POSIX operating system is added to the DSView software.

The following are prerequisites to establish an SSH session to a hypervisor server:

- The SSH service must first be configured on the virtual machine from the DSView software.
- The DSView SSH key (public key) must be exported and configured as a trusted public key for the SSH server.

To establish an SSH session to a hypervisor server:

1. Click *Units - Virtualization*.
2. Click the name of the hypervisor server.
3. Under Tools, click the *SSH Session* link.

Rebooting a hypervisor server

You can reboot a hypervisor server from the DSView software if you have access rights.

To reboot a hypervisor server:

1. Click *Units - Virtualization*.
2. Click the name of the hypervisor server to reboot.
3. Click the *Host Reboot* link in the Tools section to reboot the hypervisor server normally.

   -or-

   Click the *Forced Host Reboot* link in the Tools section to force the hypervisor server to reboot, even when in maintenance mode.

NOTE: A forced reboot is not supported in the virtual environment.

Synchronizing the virtual environment and DSView™ software

If you use the virtual environment to add or remove a virtual machine, one of two results occurs:

- If the corresponding events are logged in the DSView software, the virtual environment and DSView software are automatically synchronized.
- If the DSView™ server is unresponsive or if the connection is lost to the virtual environment, an event is not received by DSView software. In this case, automatic synchronization does not occur; you must run the Resync Unit Wizard or update topology task to synchronize the virtual environment and DSView software.

You must manually synchronize the hypervisor manager or server with the DSView software by using the Resync Wizard or the update topology task to resynchronize the systems and update the DSView software database.

An attached hypervisor server is automatically resynchronized when the hypervisor manager is resynchronized; you cannot resynchronize an attached hypervisor server separately.

Using the Resync Units Wizard

From the Units Overview screen, you can click *Resync* to launch the Resync Units Wizard for the hypervisor manager or server.

NOTE: Although not supported, Resync is displayed for attached hypervisor servers. In this case, clicking *Resync* displays a Resync Failed message.

Using the update topology task

The update topology task performs the same operations as the Resync Unit Wizard but can be scheduled to occur at regular intervals.

3.14.4 Operating a virtual machine

You can submit virtual machine operations to the virtual environment from the Operations menu in the DSView software. Operations include turn off or turn on, suspend or resume or reset virtual machines. The Operation Submitted screen allows you to view if the submission was successful. The events log records both a DSView event indicating that the operation was submitted and a virtual environment event stating the results of the operation.

You can also hide virtual machines from the DSView software screen or view virtual machine properties. These operations occur in the DSView software, not the virtual environment.

To turn off or on virtual machines:

1. Click the checkbox to select one or more virtual machines.
2. Click *Operations - Virtual Machine Power Off* from the menu to turn off the virtual machine.

   -or-

   Click *Operations - Virtual Machine Power On* from the menu to turn on the virtual machine.
3. Click the link to view the results of the submission.

To suspend or resume virtual machines:

1. Click the checkbox to select one or more virtual machines.

2. Click *Operations*.

   If the virtual machine is currently running, click *Virtual Machine Suspend* to pause the virtual machine.

   -or-

   If the virtual machine is currently suspended, click *Virtual Machine Resume* to return the virtual machine to its normal state.

3. Click the link to view the results of the submission.

To reset virtual machines:

1. Click the checkbox to select one or more virtual machines.
2. Click *Operations - Virtual Machine Reset* from the menu to turn off and turn on the virtual machine.
3. Click the link to view the results of the submission.

3.14.5 Managing virtual environments in the DSView™ software

Using the DSView software, you can manage properties, connections, session files and a variety of other functions for any unit, including units in the virtual environment.

NOTE: When the virtual environment units are selected, only the buttons and links for the supported operations are shown.

NOTE: The DSView Attach Device Wizard is not supported for virtual environment units.

Properties and settings specific to virtual environments are described in the following sections.

Configuring security settings

For some virtual environments, you can also define mapping relationships between virtual environment authorization roles and built-in DSView™ user groups.

With the exception of the Web Access Methods, security settings for attached ESX servers must be configured for the corresponding VirtualCenter. Otherwise, when an attached ESX server is connected, the Security screens display read-only information configured for the VirtualCenter.

To view and modify security settings:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor manager or server.
3. Click *Properties* and click *Security* in the side navigation bar.
4. Click *Certificate* to view and compare the recorded and actual certificates. If the certificates do not match, click *Update* to retrieve the latest certificate from the hypervisor manager or server.
5. Click *Credentials* and enter a new username and password in the corresponding fields.
6. To use DSView software user credentials for the hypervisor manager or independent hypervisor server operations, select the Use DSView User Credentials for Operations checkbox.

   -or-

   If the checkbox is not selected, the virtual environment credentials provided in the Add Unit Wizard will be used for all operations.

7. Click *Save*.
8. Click *Access Methods* to change the protocol or port information.
9. In the Environment Access Method area, change the protocol (HTTP or HTTPS) or port number that the DSView™ software uses to access the virtual environment.
10. (Optional - VMware only) In the Web Access Method area, change the protocol (HTTP or HTTPS) or port number that the DSView software uses to access the VMware Viewer. A unique Web Access Method can be changed for each VirtualCenter and ESX server.

NOTE: For successful connections, the protocol and port information entered in the DSView Access Methods screen must correspond to the port and protocol information configured in the virtual environment.

11. Click *Close*.

To view and modify authorization role settings (not supported in some virtual environments):

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor manager or server.
3. In the side navigation bar, click *Properties - Security - Authorization Roles*.
4. If you are accessing a hypervisor server that is managed by a hypervisor manager, you are prompted to log in to the hypervisor server.
5. Select the role from the list and click *View Privileges - Back* to view the privileges assigned to a hypervisor manager or server authorization role.
6. Select a hypervisor manager or server role from the list to map hypervisor manager or server roles to DSView™ built-in user groups.

NOTE: If a hypervisor manager or server role has the same name as an existing DSView™ group in the DSView software, an error message is shown and the virtual environment authorization role is not available for mapping.

   a. Select a DSView built-in user group from the list and click *Add*.
   b. Select a preemption level from the list.
   c. With both the role and user group highlighted, click *Map Role*.
   d. Click *Save Roles*.

After you save, the imported hypervisor manager or server roles become user-defined groups in the DSView database. Any modifications must be performed from the *Users - Groups* tab in the DSView software.

Configuring service address settings

For virtual machines that report multiple IP addresses, it can be necessary to designate the primary IP address. For example, a virtual machine connected to a DCHP server can report both a public and a private IP address. You can designate the public IP address as the primary to allow remote sessions to be launched from the DSView software.

To view and modify service address settings:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the virtual machine.
3. Click *Properties* and click *Services Address (Virtual)*.

4. Select the IP address from the list to designate an IP address as the primary.
5. If you do not want the selected IP address to be automatically replaced when an IP changed event occurs, deselect *Update Services Address on IP Changed Events*.

NOTE: By default, the Update Services Address on IP Changed Events option is selected. If selected, the primary IP address is overwritten when new IP addresses are reported, which disables remote sessions if the primary public IP address is overwritten by a private IP address.

6. Click *Save - Close*.

Viewing VirtualCenter server settings

The DSView™ software can access and display the following VMware VirtualCenter server settings; these settings are stored in the VirtualCenter and do not correspond to any DSView software settings.

NOTE: The following procedures are only applicable to VMWare.

To view VirtualCenter data centers:

NOTE: A VirtualCenter data center is an entity used to group VMware virtual machines and host entities.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter.
3. Click *Server Settings* in the side navigation.
4. Click the *Data Centers* tab and click *Close*.

To view VirtualCenter clusters:

NOTE: A VirtualCenter cluster is a collection of hosts available for backing virtual machines.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter.
3. Click *Server Settings* in the side navigation.
4. Click the *Clusters* tab and click *Close*.

To view attached ESX servers:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter.
3. Click *Server Settings* in the side navigation.
4. Click the *Hosted ESXs* tab and click *Close*.

To view VirtualCenter resource pools:

NOTE: A VirtualCenter resource pool is a division of resources used to manage allocations among virtual machines.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter.
3. Click *Server Settings* in the side navigation.
4. Click the *Resource Pools* tab and click *Close*.

To view hosted virtual machines:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter.
3. Click *Server Settings* in the side navigation.
4. Click the *Hosted VMs* tab and click *Close*.

To view VirtualCenter events:

NOTE: These events are stored in the VirtualCenter environment and do not correspond to DSView™ software events.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter.
3. Click *Server Settings* in the side navigation.
4. Click the *Events* tab and click *Close*.

To view VirtualCenter tasks:

NOTE: These tasks are stored in the VirtualCenter and do not correspond to DSView software tasks.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter.
3. Click *Server Settings* in the side navigation.
4. Click the *Tasks* tab and click *Close*.

To view VirtualCenter alarms:

NOTE: These alarms are stored in the VirtualCenter and do not correspond to DSView software alerts.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the VirtualCenter.
3. Click *Server Settings* in the side navigation.
4. Click the *Alarms* tab.
5. Click *Triggered* to view a list of any recently triggered alarms.

   -or-

   Click *Definitions* for a description of preset alarms.
6. Click *Close*.

Viewing hypervisor server settings

The DSView software can access and display hypervisor server general, hardware and software settings and hosted virtual machines, server events and pool members. With the exception of data logging, these settings are stored on the hypervisor server and do not correspond to any DSView software settings.

To view general settings for a hypervisor server:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor server.
3. Click *Server Settings* in the side navigation.

4. Click the *General* tab to view available information about the hypervisor server, including IP address, version, manufacturer and model information.

To view hardware settings for a hypervisor server:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor server.
3. Click the *Server Settings - Hardware* tab to view the hardware information for the hypervisor server. The following table lists the information that appears when a link is clicked.

Table 3.20 Hardware Information Link Descriptions

LINK NAME	LINK DESCRIPTION
Processors	General and system processor information
Memory	Physical memory information
Storage	Storage information, including identification, device, capacity, free space and type
Networking	Networking information, including virtual switch, total port groups, number of ports and total physical adaptors
Storage Adaptors	The name, device, type and Storage Area Network (SAN) identifier number for all storage adaptors
Network Adaptors	Device, speed, configured, vSwitch and network information for all network adaptors

To view software settings for a hypervisor server:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor server.
3. Click *Server Settings - Software* tab to view software information for the hypervisor server. The following table lists the information that appears when a link is clicked.

Table 3.21 Software Information Link Descriptions

LINK NAME	LINK DESCRIPTION
Licensed - Features	A list of licensed features and their status
Licensed - Add Ons	A list of licensed add-on components and their status
DNS and Routing	Host identification, DNS servers and default gateways
VM Startup/Shutdown	Startup and shutdown information for connected virtual machines
Security Profile	Firewall information
System Resource Allocation	System resource pool information

To view hosted virtual machines:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor server.
3. Click *Server Settings - Hosted VMs* tab.
4. Click the name of a virtual machine to view guest operating system, memory and storage capacity.
5. Click the name of a hosted virtual machine in the list to view more information about that virtual machine in the details panel.
6. Click *Close*.

To view events for a hypervisor server:

NOTE: This feature is not supported in all virtual environments. When the virtual environment units are selected, only the buttons and links for the supported operations are shown.

NOTE: These events are stored in the hypervisor server and do not correspond to DSView™ software events.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor server.
3. Click *Server Settings - Events tab*.
4. Click *Close*.

To view pool members:

NOTE: This feature is not supported in all virtual environments. When the virtual environment units are selected, only the buttons and links for the supported operations are shown.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor server.
3. Click *Server Settings - Pool Members* tab.
4. Click *Close*.

Viewing virtual machine properties

The DSView software can access and display the following virtual machine properties. With the exception of data logging, these settings are stored on the hypervisor server that hosts the virtual machine and do not correspond to any DSView software settings.

To view a summary of properties:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the arrow next to the hypervisor manager or server to display hosted virtual machines.

   -or-

   Click *Virtual Machine* in the side navigation bar to display all virtual machines.
3. Click the name of the virtual machine.
4. Click *VM Properties (Virtual) - Summary* to view a summary of the virtual machine properties.
5. Click *Close*.

To view resources:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the arrow next to the hypervisor manager or server to display hosted virtual machines.

   -or-

   Click *Virtual Machine* in the side navigation bar to display all virtual machines.
3. Click the name of the virtual machine.
4. Click *VM Properties (Virtual) - Resources*.
5. Click *Datastore* to view a list of datastore devices, corresponding capacity and free space.
6. Click *Disks* to view the location, capacity and free space for guest disks.

7. Click *Close*.

To view virtual machine events:

NOTE: This feature is not supported in all virtual environments; if not supported for the selected unit, the related interface elements are not displayed on screen.

NOTE: These events are stored in the virtual machine and do not correspond to DSView™ software events.

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the arrow next to the hypervisor manager or server to display hosted virtual machines.

   -or-

   Click *Virtual Machine* in the side navigation bar to display all virtual machines.
3. Click the name of the virtual machine.
4. Click *VM Properties (Virtual) - Events*.
5. Click *Close*.

3.14.6 Logging data

The DSView software supports logging of serial session console data from virtual environment units using the Syslog protocol. Data logging must be configured both in the DSView software and on each virtual machine. Licenses are required for data logging.

Configuring data logging in the DSView software

Data logging can be enabled on multiple virtual machines on one hypervisor server or on one virtual machine at a time.

To view and configure data logging on multiple virtual machines on a hypervisor server:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the name of the hypervisor server.
3. Click *Server Settings* and click *Data Logging*.
4. Select the row(s) and click *Enable* to enable data logging on virtual machines.

   -or-

   Select the row(s) and click *Disable* to disable data logging on virtual machines.
5. Click *Close*.

To view and configure data logging on a single virtual machine:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the arrow next to the hypervisor manager or server to display hosted virtual machines.

   -or-

   Click *Virtual Machine* in the side navigation bar to display all virtual machines.
3. Click the name of the virtual machine.
4. Click *VM Properties (Virtual) - Data Logging*.
5. Select the row(s) and click *Enable* to enable data logging on the virtual machine.

-or-

Select the row(s) and click *Disable* to disable data logging on the virtual machine.

6. Click *Close*.

Configuring data logging on a virtual machine

Data logging must be configured on each virtual machine to log data. The following system requirements must be implemented before you install and use the DSView™ software plug-in for Virtualization:

- A POSIX operating system (Linux or Solaris) with the Syslog enabled
- Sun Java™ VM J2SE 1.5 or later
- Secure Shell (SSH) (required to run SSH tunneling)

Exporting a virtual machine data logging key

For a virtual machine to be authenticated with the DSView™ SSH server, the virtual machine's unique certificate key must be submitted with the request.

To export a virtual machine data logging key:

1. Click *Units - Virtualization* in the side navigation bar.
2. Click the arrow next to the hypervisor manager or server to display hosted virtual machines.

   -or-

   Click *Virtual Machine* in the side navigation bar to display all virtual machines.
3. Click the name of the virtual machine.
4. Click *VM Properties (Virtual) - Summary* tab.
5. Click *Export Data Logging Key*.

   A message is displayed with the path and name of the exported key as follows:

   - The name of the file containing the key is id_rsa_[VMName].
   - The location of the exported key is the logged in user's temporary directory on the server where the DSView software is installed.

     For example, if the DSView™ server is installed on a screens server and the name of the virtual machine is myVM, the file location and name is C:\Documents and Settings\[username]\id_rsa_myVM, where [username] is the user login used by the DSView server.

Configuring the Syslog

The data logging client receives Syslog messages from a named pipe and forwards them to the DSView Syslog server.

To configure the Syslog:

1. From the virtual environment command line, log in as **administrator** or **root**.
2. Run the following **mkfifo** command to create a fifo device:

```
mkfifo -m 666 <fifo path and name>
```

For example: `mkfifo -m 666 /var/evt_pipe`

3. Edit the /etc/syslog.config file by adding the following line at the end:

```
<event filter> |<fifo path and name>
```

For example: `daemon.*;mail.*;*.=warn |/var/evt_pipe`

4. Restart the Syslog daemon using the following command:

```
/etc/init.d/sysklogd restart
```

-or-

```
/etc/init.d/syslog restart
```

Configuring the SSH

To configure the SSH:

1. Open the file */etc/ssh_config or /etc/ssh/ssh_config file* and add or modify the follow option:

```
StrictHostKeyChecking no
```

2. Import the DSView™ SSH key (public key) as a trusted public certificate.
3. Restart the SSH using the following command:

```
/etc/init.d/sshd restart
```

Installing the data logging client

To install the data logging client:

1. Download the *Datalogclient.zip* file from the Vertiv web site.
2. Copy and unzip the *Datalogclient.zip* file to an appropriate location on the virtual machine. It consists of three files:
   - DataLoggingClient.jar java executable jar
   - DataLoggingClient.properties properties file
   - DataLoggingClient.sh shell script
3. Copy the exported data logging key file to the appropriate location on the virtual machine.
   a. Set the data logging key file mode to 700 using the following command:

      chmod 700 filename

NOTE: The data logging key file is only readable by the owner.

b. If you also want to run the data logging key file with other users, provide ownership to other users using the following command:

chown username.username filename

4. Edit the DataLoggingClient.properties file.
5. Set the DataLoggingClient.sh to executable using the following command:

```
chmod +x DataLoggingClient.sh
```

6. Execute the bash file to run the client using the following command:

```
./DataLoggingClient.sh -p <path to the java/bin directory> -c <path to the DatatLoggingClient files>
```

7. Add the DataLoggingClient.sh file to run when the virtual machine starts.

The data logging client attempts to create the fifo device if it is not available. In this case, you must restart the Syslog daemon after the data logging client starts.

Properties file structure

The data logging client acts as a multiplexer by receiving data from the virtual machine Syslog and sending it back to one or more DSView™ servers or data log files. Input and output can be specified by defining different pipe entries. By default, the DataLoggingClient.properties file defines the input type as a fifo file to which the Syslog server writes, and the output type as the TCP port used to redirect data to the DSView server.

Table 3.22 Data Logging Client Properties

PROPERTY	DESCRIPTION
dls.localIp	Sets the IP address used by the DSView software to identify the virtual machine.
dls.queueSize	Sets the message queue size.
dls.bufferSize	Sets the size of the buffer (in bytes) used to receive and send data.
dls.packetSize	Sets the maximum number of messages included in a packet. By default, the data logging client attempts to get a number of messages before sending data to the DSView software. Setting this number to 1 decreases the performance and increases the network traffic.
dls.waitTimeout	Maximum wait time-out in milliseconds. The data logging client waits this amount of time to reach the maximum packet size and then sends the messages regardless of whether the packet size is reached.
dls.pipes	List of pipes. Only the names in these properties are created as input or output pipes.
dls.<pipe_name>	Type of pipe. Use dls.file for files, dls.pipe for named pipes or fifo devices or dls.tcp for TCP clients.
dls.<pipe_name>.type	Designates if the pipe is an input or output pipe.
dls.<pipe_name>.filepath	N/A
dls.<pipe_name>.ip	(For TCP only) The IP address where the data logging client creates a socket (always localhost).
dls.<pipe_name>.port	(For TCP only) Socket port.

PROPERTY	DESCRIPTION
dls.<pipe_name>.encoder	(For TCP only) Sets the tunneling encoder only if SSH is available.
dls.<pipe_name>.encoder.ip	IP address from the SSH server that runs tunneling (always localhost).
dls.<pipe_ name>.encoder.port	DSView Syslog Server port.
dls.<pipe_ name>.encoder.publicKeyFile	Path to the exported data logging key.
dls.<pipe_ name>.encoder.sshIp	DSView server IP address.
dls.<pipe_ name>.encoder.sshPort	DSview SSH server port.

Example: Properties file

```
dls.localIp = <virtual machine IP address>
dls.queueSize = 100
dls.bufferSize = 1000
dls.waitTimeout = 10000
dls.packetSize = 4
dls.pipes = pipe1,pipe2

dls.pipe1 = pipe
dls.pipe1.type = input
dls.pipe1.filepath = <path to the fifo device>

dls.pipe2 = tcp
dls.pipe2.type = output
dls.pipe2.ip = localhost
dls.pipe2.port = <port used in the Virtual Machine>
dls.pipe2.encoder = ssh
dls.pipe2.encoder.ip = localhost
dls.pipe2.encoder.port = <DSView Syslog server port>
dls.pipe2.encoder.publicKeyFile = <path to the DataLogging key>
dls.pipe2.encoder.sshIp = <DSView IP address>
dls.pipe2.encoder.sshPort = <DSView SSH server port>
```

3.14.7 Logging DSView™ software events

NOTE: This feature is not supported in all virtual environments. When the virtual environment units are selected, only the buttons and links for the supported operations are shown.

The following virtual environment events are logged under the Reports tab in the DSView software. The actions that cause these events can be initiated from the DSView software or from the virtual environment. For more information about events, see the Avocent® DSView™ 4.5 Management Software Installer/User Guide.

NOTE: The virtual environment also logs events. These events can be viewed from the DSView software Unit Overview screen for a virtual environment unit. However, events logged in the virtual environment do not correspond to DSView software events, which are shown under the Reports tab.

Table 3.23 DSView™ Software Events for a Virtual Environment

EVENTS	EVENTS
Host Forced Reboot Command Failed	Virtual Machine Name Changed
Host Forced Reboot Command Issued	Virtual Machine Name Change Failed
Host Reboot Command Failed	Virtual Machine Powered Off
Host Reboot Command Issued	Virtual Machine Powered On
Host Added	Virtual Machine Power Off Command Failed
Host Removed	Virtual Machine Power Off Command Issued
Virtual Machine Created*	Virtual Machine Power Off Failed
Virtual Machine Removed*	Virtual Machine Power On Command Failed
Virtual Machine Hot Migrating	Virtual Machine Power On Command Issued
Virtual Machine IP Address Changed	Virtual Machine Power On Failed
Virtual Machine IP Address Change Failed	Virtual Machine Reset Failed
Virtual Machine Migrated	Virtual Machine Resetting
Virtual Machine Migrating	Virtual Machine Suspend Command Failed
Virtual Machine Migration Failed	Virtual Machine Suspend Command Issued
Virtual Machine Reconfigured	Virtual Machine Suspended
Virtual Machine Reset Command Failed	Virtual Machine Suspend Failed
Virtual Machine Reset Command Issued	VMware Viewer Impersonation**

* If you use the virtual environment to add or remove a virtual machine, the corresponding events are logged and the virtual environment and DSView software are automatically synchronized.

** This event is initiated from the DSView software and does not have an equivalent in the virtual environment. This event is recorded if *Use DSView™ User Credentials for Operations* is not selected in the Add Unit Wizard or an event is initiated from a DSView™ server that does not own the virtual unit. In this case, the supplied virtual environment credentials are used to access the unit.

This page intentionally left blank.

VertivCo.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

590-1795-501A