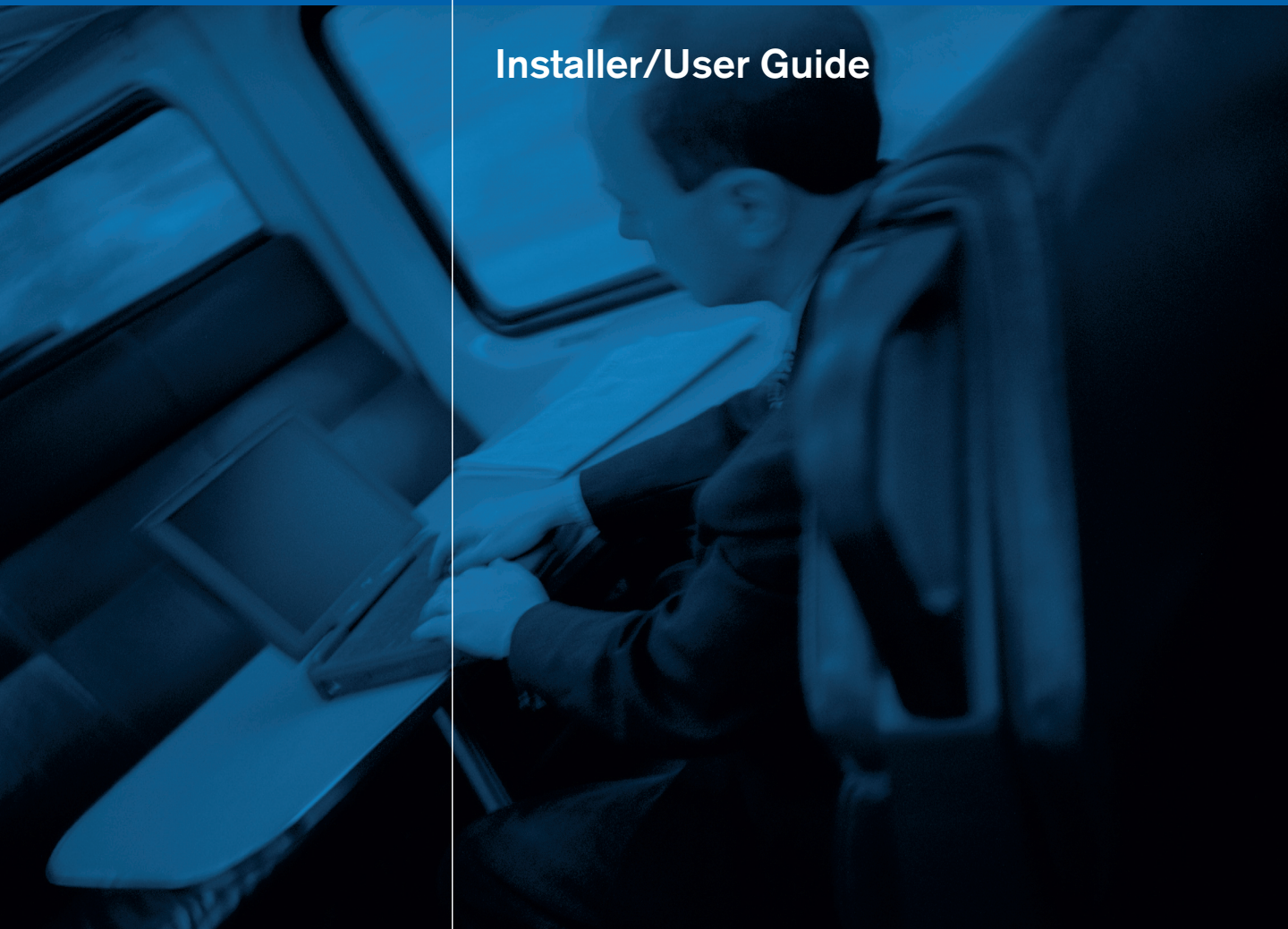
Avocent

DSView®

Installer/User Guide



INSTRUCTIONS

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

DANGEROUS VOLTAGE

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

POWER ON

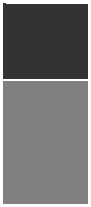
This symbol indicates the principal on/off switch is in the on position.

POWER OFF

This symbol indicates the principal on/off switch is in the off position.

PROTECTIVE GROUNDING TERMINAL

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.



DSView®

Management Software Installer/User Guide

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Product Overview

About the DSView Management Software

The DSView® software, part of the DS Management Software suite, is used to manage DS appliances, DSR™ switches, CPS serial over IP network appliances, EVR1500 environmental monitor and control appliances and SPC power control devices. Switches, network appliances and attached devices may be viewed and controlled using the DSView management software.

The DS Management Software suite includes secure, browser-based access to virtually any device in the data center, including access to all major server platforms and serial-based devices.

Use the DSAuth software and the DSView management software within the DS Management Software suite to specify DS users and their access levels. The DSView management software and DSWebview browser-based software components within the DS Management Software suite are used to manage your existing appliances or launch a session to a device with a single point of access. Views may contain appliances, devices and ports arranged in an ordered tree structure or a listing of servers for easy selection.

Features and Benefits

Network rebooting and troubleshooting

The DSView management software uses industry standard IP connections so that you can easily troubleshoot, or even reboot a server, from the Network Operations Center (NOC), from your desk or from any location in the world. With the DSView management software, you can access all of your data center devices from a single screen - making complex network access and control remarkably easy.

Web-based access and control

The DSWebview software provides secure, browser-based access to virtually any data center device via the Avocent DS series product suite. The Avocent DSView management software provides secure “point-and-click” control to any connected device, using IP connections.

The DSWebview software supports Microsoft® Internet Explorer version 5.5 and later, Netscape® version 6.2 and later, Mozilla™ and Internet Information Server (IIS)™ 5.0 on Windows® and Linux® operating systems and Safari™ 1.2 and later on the Apple Mac OS® X.

Creating and managing user permissions

The DSView management software and DSAuth software provide centralized network access, control and security for DS appliances. The DSView management software configures DS topology, permissions and per-device contact information. The DSAuth software stores the DS topology, permissions and per-device contact information and performs third party authentication during connection to the switch. DS users may be authenticated via the local database or by an external server using the Lightweight Directory Assistance Protocol (LDAP). Three kinds of encryption are available if you are using the DSView management software with a newer DSR switch.

NOTE: The DS1800 digital switch only supports DES encryption.

Software Components

The DS Management Software suite is comprised of three components.

DSView management software

The DSView management software is a Win32® application that allows DS users to manage target devices through Avocent network appliances. The DSView management software allows for IP-based video, serial and power management sessions. The DSView management software consists of a node manager, Telnet application viewer and Video Viewer.

The DSView management software is also used to graphically create and alter DS topology and permission information that is stored on a DSAuth Server.

Video Viewer window

The Video Viewer window allows you to control the keyboard, monitor and mouse functions of individual devices. You may also use predefined global macros to perform actions within the Video Viewer window, or create new macros within the window for the device. The Video Viewer window may be launched by double-clicking a device port in the DSView management software window or placing your cursor over a port and selecting *Connect* from the floating option menu in the DSWebview Client when using any of the following appliances:

- DS1800 switch
- DSR800 switch
- DSR1010 / 2010 / 4010 switch
- DSR1161 / 2161 / 4160 switch
- DSR1021 switch

DSAuth (DS Authentication) Server

The DSAuth software serves as a central repository for DS topology information, DS user permissions and centralized services such as authentication, access control, audit, DS appliance monitoring and DSView management software/DS appliance and DSWebview Client interface/DS appliance updates. DS users may specify a backup authentication server in addition to the primary server.

DSWebview browser-based software

The DSWebview software provides a web gateway that allows DS users to manage target devices through Avocent network appliances from an industry-standard browser. The gateway allows for IP-based video and serial management sessions. The DSWebview software consists of a DS appliance or DSR switch and the DSAuth software proxy. It also includes the DSWebview Client that provides DS Active Server Pages (ASPs) and video and Telnet application applets.

The following figure illustrates an example system configuration using the DS Management Software suite. For more information on how the components of the DS Management Software suite work together, see *Appendix B*.

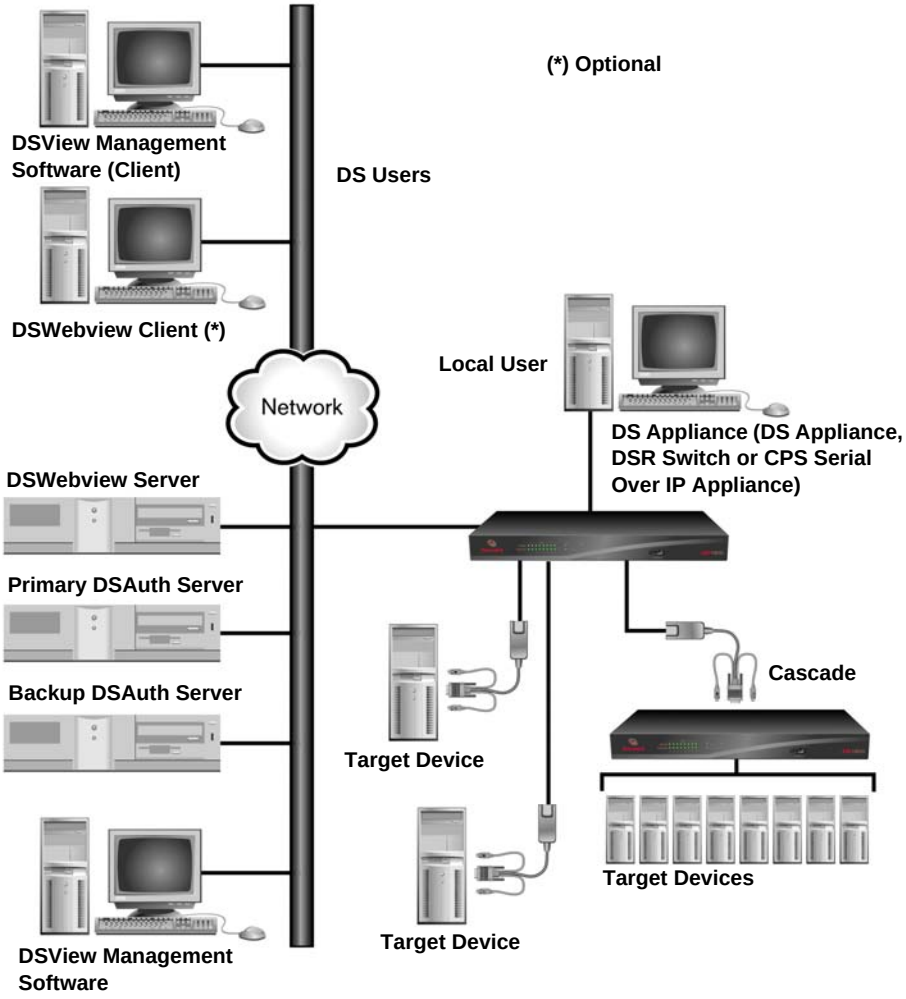


Figure 1.1: Example System Configuration Using the DS Management Software Suite

Overview: Working with the DS Management Software Suite

The DSView management software and DSWebview software consist of a Node Manager, a Video Viewer window and a Telnet application viewer. When you launch either the DSView management software or DSWebview software, the Node Manager appears. The Node Manager allows you to view, access, manage and create custom groupings for all of the supported DS appliances, DSR switches, CPS network appliances, EVR1500 environmental monitors and generic appliances in your data center.

Double-clicking an item or selecting *Connect* from the shortcut menu in the DSView management software window, selecting *Connect* from the floating option menu in the DSWebview Client Node Manager or clicking the *Connect* toolbar icon in the DSView management software window has the following effect:

- If using a DS appliance or DSR switch channel or port, a Video Viewer window launches
- If using a CPS appliance port, a Telnet application viewer launches
- If using an EVR1500 environmental monitor, a web browser launches
- If using a generic appliance, the command associated with the appliance executes

See *Appendix F* on page 146 for information on the DSView management software toolbar.

Double-clicking an SPC device outlet opens the Power State dialog box. See *Adding and Managing DS Users* on page 44 for more information.

NOTE: You must have Administrator privileges to launch a Telnet application viewer from a CPS appliance or port.

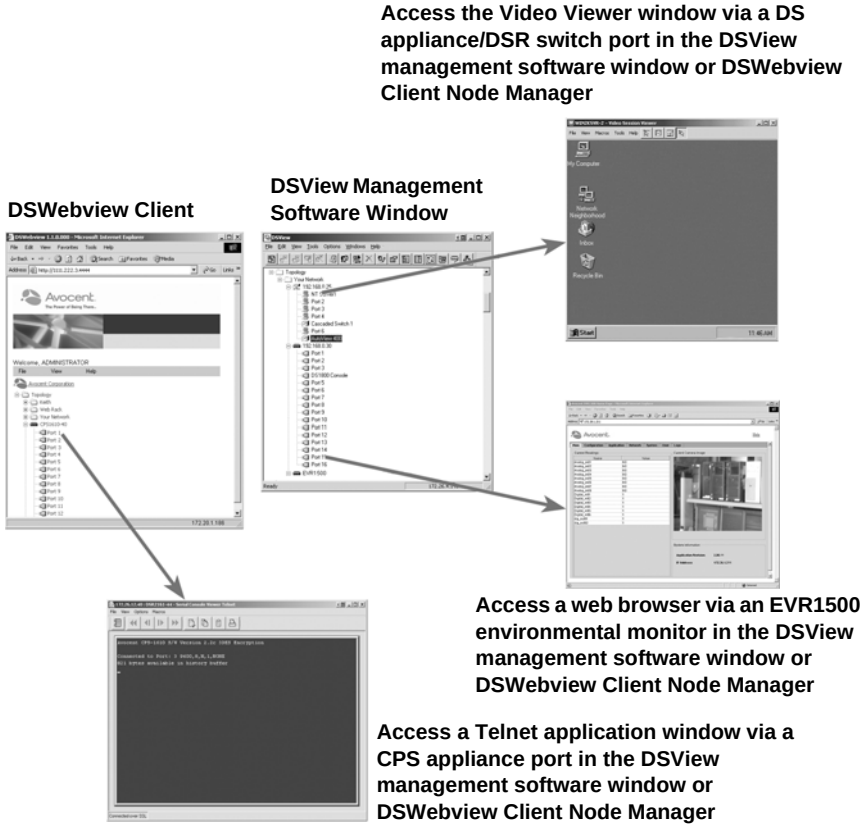


Figure 1.2: DS Management Software Suite Components

Appliances may be configured using the DSView management software, which also contains a Node Manager. When you select an appliance in the DSView management software Node Manager and then select the *Edit - Properties* command or click the *Properties* toolbar icon, the Properties dialog box is launched. The Properties dialog box contains tabs that enable you to configure your appliance.

See the *DSView management software, DSWebview browser-based software* and *Video Viewer window* sections in this chapter for more information on each of these windows.

Viewing Target Devices

Accessing devices with a DS series network appliance is accomplished through the DSView management software. When the DSView management software is opened, all host PCs and serial devices that may be accessed system-wide are displayed in a tree structure. This tree structure can be displayed in two ways: a DS topology view showing target devices and the appliances to which they're connected, or a server view that shows all available target devices. Both viewing methods can be selected under the View menu.

DS topology view

In the DS topology view, DS appliances and target devices are arranged in a tree structure. Available DS appliances and target devices are listed vertically by name or IP address. Each appliance can be expanded to display attached devices.

An SPC power control device will appear as a cascade device attached to a CPS network appliance or DSR1021 switch. Each outlet will appear with a power indicator cascaded below the port. To view an attached SPC device and its outlets, click on the expand (+) button beside a CPS network appliance or DSR1021 switch, then the SPC device's expand button.

NOTE: The topology view is not available when using the DSWebview software with a Netscape browser.

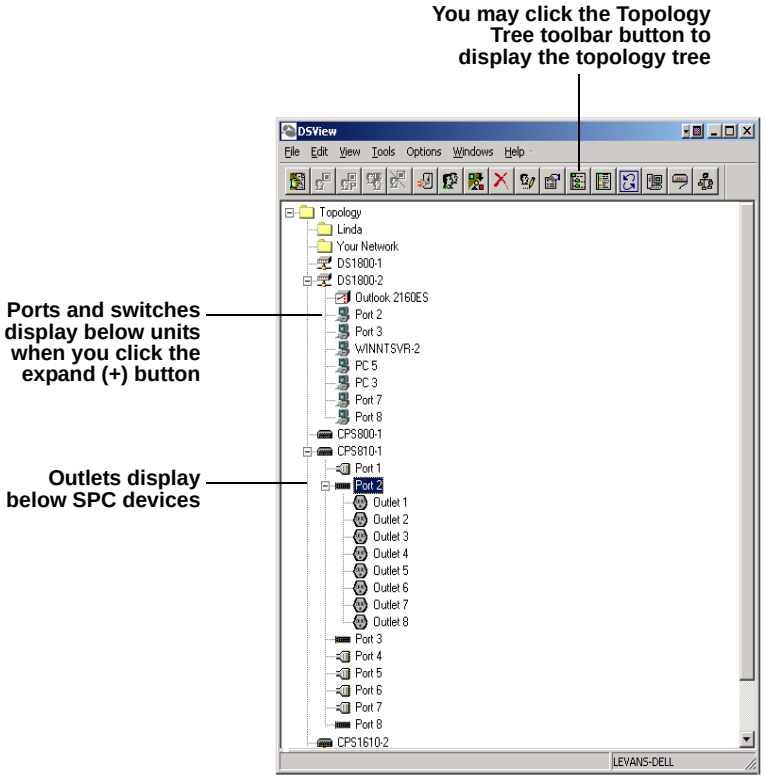


Figure 1.3: DS Topology Tree

To display the DS topology view:

1. In the DSView management software window, double-click on *Topology.*
2. Each name or IP address listed below Topology may be expanded by double-clicking on it.

This will display the ports for the DS appliance corresponding to that address. Each of these ports shares the DS appliance's IP address.

If a target device is attached to a port, the properties of that port will be the same as the properties of the target device.

If a Keyboard/Video/Mouse (KVM) switch is attached to one or more of these ports, double-clicking on the port name will display the channels on that KVM switch.

NOTE: You may also display the topology tree by clicking the *Topology Tree* toolbar icon.

Server view

In server view, available target devices are listed by name only.

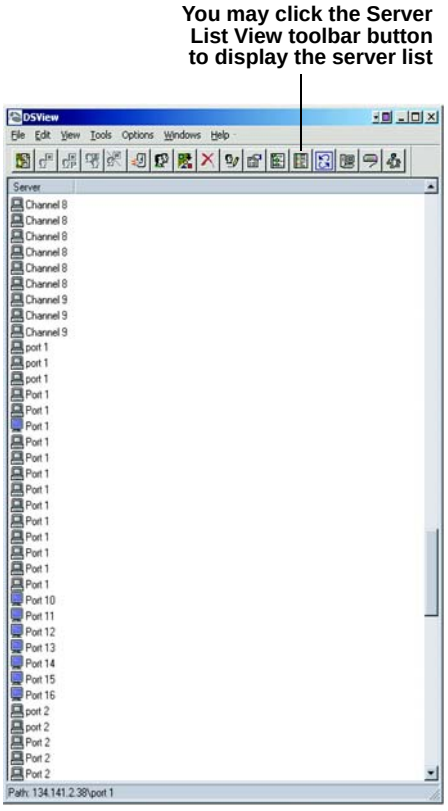


Figure 1.4: Server View

NOTE: You may also display the server list by clicking the *Server List View* toolbar icon.

The DSView management software and DSWebview software designate target device types with specific icons in the viewing panes. These icons are outlined in Table 1.1.

Table 1.1: Icons

Icon	Description
	DS appliance (DS topology view)
	A target device attached to a DS appliance or KVM switch
	CPS appliance (DS topology view)
	Generic web appliance
	Generic Telnet application appliance
	Generic appliance
	Generic command appliance
	An SPC power control device port (DS topology view)
	An SPC power control device outlet
	A port on a CPS appliance (DS topology view)
	A KVM switch attached to a DS appliance (DS topology view)
	A port on a CPS appliance or a port on a CPS appliance attached to an SPC power control device outlet (server view)
	EVR1500 environmental monitor

Port status indicators

NOTE: The display of unused CPS appliance, DS appliance and DSR switch ports, as well as SPC device outlets may be turned off. See *Viewing Ports, Outlets, Target Devices and Connected DS Users* on page 52 for more information.

Ports will normally appear as a grey icon in a DSView management software window. Configured SPC devices will appear using the icons listed in Table 1.1.

When port status polling is enabled, the DSView management software provides visual cues to indicate which ports and channels are in use, available, not powered or blocked, and the power state of SPC device outlets. For example, if SPC device outlets are not powered, they will appear with a black “X” over them when polling is enabled. See Chapter 4 for information on polling.

NOTE: Your CPS network appliance firmware must be up-to-date to view CPS appliance and SPC device poll status indicators.

Available

Available ports and SPC device outlets that are powered are highlighted in green. DS users may connect to ports in any mode desired.

In use

A port that is in use will be highlighted in yellow. The usage state of any CPS800 appliances or CPS1600 appliances is not available and will appear as Unknown.

When a DS appliance or DSR switch port is in use, DS users may only connect through sharing. More details on sharing are available later in this chapter.

NOTE: CPS810 appliance and CPS1610 appliance ports cannot be shared.

Blocked

Blocked ports will have a red icon covered by a red "X." No additional DS users may connect to this port or channel in any mode. DS users with Administrator privileges may terminate the session. For more information, see Chapter 5.

Not powered

Ports that are not powered will have a grey icon covered by a black "X." SPC device outlets that are not powered will have a shaded icon covered by a black "X." The usage state of any CPS800 appliance or CPS1600 appliance is not available and will appear as Unknown.

Port status reporting can be toggled if polling has been enabled in the DSView management software by selecting *File - Enable Port Status Polling* from the DSView management software window or selecting *File - Enable Port Status* from the DSWebview software window. If there is no check mark beside this menu option, the DSView management software will not request the port status information from the DSAuth Server. DS users may still get a snapshot of port status by selecting the *View - Refresh* command or clicking the *Refresh* toolbar icon. See Chapter 4 for information on enabling polling.

The OnBackup status bar indicator

When the DSView management software is communicating with its assigned primary DSAuth Server, that server name will appear in a status window. If the DSView management software is unable to communicate with the primary DSAuth Server, it will attempt to communicate with the backup DSAuth Server. If the DSView management software is communicating with a backup DSAuth Server, the server's name will appear highlighted in yellow.

NOTE: When the DSView management software is communicating with the backup DSAuth Server, it is working in a degraded mode. The backup DSAuth Server allows only View operations and does not allow any modifications to the tree, properties or permissions settings. When the DSView management software is using a backup DSAuth Server, the OnBackup status bar will turn yellow.

CHAPTER 2

Installation

Installing the DS Management Software Suite

Installation of the DS Management Software suite is comprised of three steps:

- Installing the DSAuth Server
- Installing the DSView management software
- Installing the DSWebview browser-based software

The DS Management Software suite can be installed from the CD or using a self-extracting .zip file downloaded from the Avocent web site.

The DSAuth Server and DSView management software must be present and configured before access can be gained.

NOTE: You will need to reboot your system as part of the installation process. This is necessary for Windows to properly register the new application.

Installing the DSAuth Server

NOTE: The DSAuth Server MUST be installed on a PC running Windows 2000 or Windows XP with Service Pack 1, or on a PC running Windows NT® 4.0 Service Pack 4 or later on an NTFS hard drive partition.

The DSAuth Server is a central repository for DS topology information, user permissions and centralized services such as authentication, access control, audit, appliance monitoring and DSView management software/appliance and DSWebview Client/appliance updates. DS users can define a primary and backup DSAuth Server.

The DSView management software can be installed on the same machine as the DSAuth Server, or on a separate machine. If the DSView management software is installed on a separate machine, it accesses the DSAuth Server using a network connection.

For more information on how the DS appliances (including CPS serial over IP network appliances and generic) and DS Management Software communicate with each other, see *Appendix B*.

To install from the CD:

1. Log on to the PC as Administrator.
2. Insert the DS Management Software CD. An autorun file will bring up a menu of installation options.
3. When prompted to select a program to install, select *Install DSAuthentication Server.* The software will check the Avocent web site to ensure you have the latest version of the DSAuth software. If a newer version is found, it will be automatically downloaded. The installation will then begin.
4. Follow the on-screen instructions. Windows will determine if the Microsoft Windows Installer Service is available. If it is not, Windows will install it and reboot the system. Setup will automatically continue after the reboot.
5. Continue following the on-screen instructions. The session time-out value will determine how long a DSView management software session can remain inactive before it is automatically logged out. The default time-out is 15 minutes. Selecting *Disable inactivity timeout feature* or entering a **0** will disable this feature.
6. The Installer service will determine if the Microsoft Data Access Components (MDAC) need to be installed. If so, they will be loaded and the system will reboot. Setup will automatically continue after the reboot.
7. When the DSAuth Server has finished installing, a system reboot is required.

To install using the DS Management Software suite downloaded from Avocent:

1. Log on to the PC as Administrator.
2. Using your DS appliance/DSR switch installer/user guide and quick installation guide, download the DS Management Software suite from the Avocent web site. (Go to www.avocent.com and click the *Support* link. On the Support page, click the *Product Upgrades and Options* link.)
3. Double-click on the executable downloaded from Avocent. The installation will begin.
4. Follow the on-screen instructions. Windows will determine if the Microsoft Windows Installer Service is available. If it is not, Windows will install it and reboot the system. Setup will automatically continue after the reboot.
5. Continue following the on-screen instructions. The session time-out value will determine how long a session can remain inactive before it is automatically logged out. The default time-out is 15 minutes. Selecting *Disable inactivity timeout feature* or entering a **0** will disable this feature.
6. The Installer service will determine if the MDAC components need to be installed. If so, they will be loaded and the system will reboot. Setup will automatically continue after the reboot.
7. When the DSAuth Server has finished installing, a system reboot is required.

Installing the DSView management software

The DSView management software is the administrative front end for the DSAuth Server that is used to configure user information and access levels. The DSView management software can be installed on the same machine as the DSAuth Server, or on a separate machine and then connected to the DSAuth Server through the network.

The DSView management software also provides a client interface that displays a listing of servers that an individual user can access. The DSAuth Server will check your NT domain cached credentials and provide a list of target devices available to you. There is a refresh option in the event that a new target device is added, changed or deleted. Once you have selected a target device from the list, the video of the selected target device will display in a Video Viewer window on the DS user's monitor. The DSView management software can be installed on any PC running a Win32 platform.

During the installation, a window will appear; enter the name or IP address of the PC where the DSAuth Server is installed. This will be your primary DSAuth Server. Also, if you are installing a non-English version of the DS Management Software, you will be prompted for the name of a default user setting.

To install from the CD:

1. Log on to the PC as Administrator.
2. Insert the DS Management Software CD. An autorun file will bring up a menu of installation options.
3. You will be prompted to select a program to install. Select *Install DSView.* The software will check the Avocent web site for a newer version of the DSView management software. If a newer version is found, it will be automatically downloaded. The installation will then begin.
4. Follow the on-screen instructions.

To install using the DS Management Software downloaded from Avocent:

1. Log on to the PC as Administrator.
2. Using your DS appliance/DSR switch installer/user guide and quick installation guide, download the DS Management Software suite from the Avocent web site. (Go to www.avocent.com and click the *Support* link. On the Support page, click the *Product Upgrades and Options* link.)
3. Double-click on the executable downloaded from Avocent. The installation will begin.
4. Follow the on-screen instructions.

Installing the DSWebview browser-based software

NOTE: Configuration may be necessary for outside access to servers using the DSWebview software. See Chapter 5 for configuration information.

The DSWebview software enables users to log in and manage target devices through DS appliances using an industry-standard browser.

NOTE: You must have Microsoft IIS installed to use DSWebview Central Services, which coordinate remote access to DS appliances and attached devices in a centralized manner.

Minimum requirements for DSWebview Central Services

The following are the minimum requirements for using the DSWebview Central Services:

- Windows NT Server, Windows 2000 Server or Windows XP with the latest service package
- IIS 5.5 or later

Minimum requirements for a DSWebview Client

The following are the minimum requirements for using the DSWebview Client on a Windows or Linux operating system:

- Java™ Runtime Environment (JRE) 1.4.1
- Internet Explorer 5.5 or later
- Netscape 6.2 or later
- Mozilla 1.2.1 or later
- Windows 95, 98, NT, 2000 or XP
- Linux 6.2 or later

The following are the minimum requirements for using the DSWebview Client on Apple Mac OS X:

- Safari 1.2 or later
- Java 1.4.2 or later plug-in

To install from the CD:

1. Log on to the PC as Administrator.
2. Insert the DS appliance software CD. An autorun file will bring up a menu of installation options.
3. You will be prompted to select a program to install. Select *Install DSWebview.* The software will check the Avocent web site for a newer version of the DSWebview software. If a newer version is found, it will be automatically downloaded. The installation will then begin.
4. Follow the on-screen instructions, noting the following.
   a. The default path c:\inetpub\wwwroot must be used when installing the DSWebview software.

b. Selecting *Install for all users* enables services to automatically start for all DS users. If you do not specify this option, the Administrator must log in and start services for all DS users.

To install using the DS appliance software downloaded from Avocent:

1. Log on to the PC as Administrator.
2. Using your DS appliance installer/user guide and quick installation guide, download the DSWebview software from the Avocent web site. (Go to www.avocent.com and click the *Support* link. On the Support page, click the *Product Upgrades and Options* link.)
3. Double-click on the executable downloaded from Avocent. The installation will begin.
4. Follow the on-screen instructions noting the following.
   a. The default path c:\inetpub\wwwroot must be used when installing the DSWebview software.
   b. Selecting *Install for all users* enables services to automatically start for all DS users. If you do not specify this option, the Administrator must log in and start services for all DS users.

After DSWebview browser-based software installation

After you have installed the DSWebview software, do the following.

To configure the DSWebview browser-based software:

1. Ensure that the default web site is configured in the IIS Administration Console.
   a. Start the IIS software.
   b. Right-click on *Default Web Page*.
   c. Click the *Documents* tab.
   d. On the Documents tab, check *Enable default document*.
   e. Ensure that dswebinterface.asp is in the list. If not, manually add it and move to the top of the list.

NOTE: The dswebviewinterface.asp file must not be renamed.

Once set up correctly, the login page may be accessed by starting a web browser and visiting the address of the web server (for example, http://webserver).

2. If you are not using the DSAuth Proxy Server, modify the Telnet application and Video settings.
   a. On the web server, change directories to c:\inetpub\wwwroot and open the Proxyports.asp file in an ASCII text editor. By default, the file settings are 8023 for the Telnet application and 8189 for Video.
   b. If you are not using the DSAuth Proxy Server, change the Video and Telnet application settings to zero (0).

c. Save and exit the Proxyports.asp file.

3. The DSWebview browser-based software may be assigned as a virtual directory using the IIS software's Create Virtual Directory Wizard to perform the following actions:
   a. In the Virtual Directory Alias window, type **any**.
   b. In the Web Site Directory window, select the directory in which the DSWebview browser-based software was installed.
   c. In the Access Permissions window, check *Read and Run Scripts* to allow access permissions to DSWebview Clients.

   See your IIS product documentation for more information.
4. If the DSWebview browser-based software will be used with a Mac client, the following line should be added to the Mac client's /Library/Java/Home/lib/security/java.policy file:

   "permission.java.util.PropertyPermission "*", "read";"

Displaying Firmware Version Information

You may display the version number of the firmware on DS appliances/DSR switches, CPS810 appliances or CPS1610 appliances. This information facilitates system troubleshooting and support. For optimum performance, keep your firmware current.

NOTE: Firmware versions also display in the [appliance] tab in the Properties dialog box.

To display firmware version information:

1. From the DSView management software window, right-click on a DS appliance/DSR switch, CPS810 appliance or CPS1610 appliance and select *Show Version Number.*

   - or -

   From the DSWebview Client Node Manager, place your cursor over a DS appliance/DSR switch, CPS810 appliance or CPS1610 appliance and select *Firmware Version* from the floating option menu.

   A message box will appear containing the version number of the appliance.
2. Click *OK* to dismiss the dialog box.

Updating Firmware

The firmware on attached DS appliances may be updated by selecting the *Tools - Update Firmware* command or clicking the *Update Appliance Firmware* toolbar icon. All DS appliances of the same model type may be updated at the same time. To update a different DS appliance model, you will need to perform the following process again when the current model update is completed.

NOTE: When updating the CPS810 appliances or CPS1610 appliances, application image updates must be performed prior to boot image updates.

To update firmware:

1. Select *Tools* - *Update Firmware* from the DSView management software menu.

   - or -

   Click the *Update Appliance Firmware* toolbar icon.

   The Appliance Firmware Update dialog box appears.
2. In the spaces provided, enter the filename of the update firmware and the IP address of the TFTP server where it is stored. Alternately, you may browse for the file by clicking the *Browse* button.
3. Select the DS appliance type that you wish to upgrade from the Select Appliance type drop-down menu. All available DS appliances will be listed in the Appliance Selection area of the dialog box.
4. Click on the appliances you wish to upgrade and use the add (>) button to move them to the list on the right.
5. If you are updating DS appliances/DSR switches or CPS network appliances, click the *Update* button to complete the upgrade.

   - or -

   If you are updating EVR1500 environmental monitor and control appliances, click the *Update* button. An instance of your web browser launches and opens an EVR1500 environmental monitor page for each EVR1500 environmental monitor selected for an upgrade. Continue to step 6.
6. Enter your Avocent-provided login and password in the web page of an EVR1500 environmental monitor you wish to upgrade.
7. Enter the upgrade information and perform the upgrade.
8. Repeat steps 6 and 7 for the remaining EVR1500 environmental monitors.

Exiting the DSView Management Software

To exit the DSView management software:

1. Select *File* - *Exit*.
2. If a Telnet application viewer and/or Video Viewer window is open, a message box will appear asking if you wish to close the viewer or window. Click *Yes* to close the viewer or window and exit the DSView management software.

To exit the DSWebview browser-based software:

1. Select *File* - *Log Out*.
2. If a Telnet application viewer and/or Video Viewer window is open, a message box will appear asking if you wish to close the viewer or window. Click *Yes* to close the viewer or window and exit the DSWebview software.

CHAPTER 3

DSAuth Server

About the DSAuth Server

The DSAuth Server works in conjunction with the DSView management software component of the DS Management Software suite to administer your site and authorize proper user access. You may set audit logs to record full details of user access and individual KVM switching activity. You may also specify a backup server for additional security.

Once the DSAuth Server and optional backup server are configured, use the DSView management software to create and configure the type of access levels you want to provide for DS users within your network environment.

Setting Up a DSAuth Server

The DSAuth software may be installed and configured on multiple computers to increase system flexibility. For maximum security, a backup computer running the DSAuth software may be added to an existing DS appliance or DSR switch installation.

The DS Management Software is designed to automatically determine the primary and backup DSAuth Server. However, you may choose to change these settings at a later date.

To add a new DSAuth Server:

1. Load the DSView management software and select *File - Select Authentication Server* to activate the Select Authentication Server dialog box.
2. Click the *Add* button on the right side of the dialog box.
3. You will be prompted for a name of the new server. You may enter it in the provided dialog box or browse for it by clicking the *Browse* button.
4. You may also enter a backup DSAuth Server for the new server using the same method in the provided field. If you do not wish to associate a backup, leave the field blank.
5. Click *OK* to exit and save changes.

To select an alternate DSAuth Server:

1. Load the DSView management software and select *File - Select Authentication Server* to activate the Select Authentication Server dialog box.
2. Click on the primary/backup server pair that you wish to use and click *OK*.

If you select the *Show on Startup* box, you will be prompted to select a server pair every time that you start the machine.

To add a backup DSAuth Server:

1. Install the DSAuth software on the PC that you have chosen as the new backup DSAuth Server.
2. From the Start menu, select *Settings - Control Panel* and double-click on the *DS Auth Configuration* icon. The DSAuth Configuration dialog box will appear.
3. Select *Backup Server* and enter the name of the primary DSAuth Server in the block provided.
4. When prompted, restart the Avocent Auth Server service.
5. From the Start menu, select *Settings - Control Panel* and double-click on the *DS Auth Configuration* icon for the PC running the DSAuth software that is also the primary DSAuth Server. The DSAuth Configuration dialog box will appear.
6. Select *Backup Server* and change the name of the backup DSAuth Server to the new name.
7. When prompted, restart the Avocent Auth Server service.
8. From the Start menu, select *Settings - Control Panel* and double-click on the *DS Auth Configuration* icon for the PC running the DSAuth software that is also the primary DSAuth Server. The DSAuth Configuration dialog box will appear.
9. Click the *Install Authentication Tokens* button. This will issue new authorization tokens to all attached systems running the DSView management software, identify any communications issues that the system is having and provide an opportunity to correct them.
10. Click the *Debug* button to create log files that may be used for debugging. See *Creating Debug Log Files* on page 21 for more information.
11. Finally, you will need to add the name of the backup DSAuth Server to each DSView management software or DSWebview browser-based software installation to which it pertains. This may be accomplished by selecting the *Select Authentication Server* menu choice.

To promote the backup DSAuth Server to primary:

1. From the Start menu, select *Settings - Control Panel* and double-click on the *DS Auth Configuration* icon on the PC running the DSAuth software that is also the primary DSAuth Server. The DSAuth Configuration dialog box will appear.
2. Within the dialog box, change the mode of operation to *Backup Server* and enter the name of the “new” PC that will run the DSAuth software as the primary DSAuth Server. When prompted, restart the service.

3. From the Start menu, select *Settings - Control Panel* and double-click on the *DS Auth Configuration* icon on the backup DSAuth Server. The DSAuth Configuration dialog box will appear.
4. Within the dialog box, change the mode of operation to *Primary Server* and enter the name of the "new" PC running the DSAuth software as the backup DSAuth Server. When prompted, restart the service.

To delete a DSAuth Server:

1. Load the DSView management software and select *File - Select Authentication Server* to activate the Select Authentication Server dialog box.
2. Click on the server name that you wish to delete, then click *Delete*. This will remove the primary/secondary pair.

Creating Debug Log Files

NOTE: You may also create files to log information about DSView sessions. See *Changing the System Settings* on page 58 for more information.

Log files may provide helpful information to assist in debugging your system. Administrators may choose to create the following log files:

- ConsoleAuthServer.log - Logs information about the active DSAuth Server. The ConsoleAuthServer.log file is created in the C: directory.
- DSBackup.log - Logs information about the system backup on the backup server. The DSBackup.log file is created in the C: directory.
- Trace.log - Logs messages between the DSAuth Server and DS appliances that are sent through the Avocent Secure Protocol Manager service. The Trace.log file is created in the <drive:>/Program Files/Avocent/DSAdmin directory when the Avocent Secure Protocol Manager service is started as part of starting the Avocent Auth Server service, remains open while the service is running and is overwritten each time the service is restarted.

The ConsoleAuthServer.log and DSBackup.log files may be deleted at any time during a DSView session by clicking *Clear Log*. You may also specify that ConsoleAuthServer.log and DSBackup.log files above a particular size will be deleted when a session is closed by clicking *Enable* in the Purge area and typing a file size in the Megabytes field.

To create a debug log file:

1. From the Start menu, select *Settings - Control Panel* and double-click on the *DS Auth Configuration* icon. The DSAuth Configuration dialog box will appear.
2. Click *Debug*. The Debug dialog box will appear.
3. Click the *Enable* checkbox for the log file you wish to create.
4. Click *OK* to dismiss the dialog box.

5. Restart the Avocent Auth Server service under *Settings - Control Panel - Services* if you wish to begin logging information in the ConsoleAuthServer.log or DSBackup.log file.

   - or -

   Stop and restart the Avocent Secure Protocol Manager if you wish to begin logging information in the Trace.log file.

To disable logging within a log file:

1. From the Start menu, select *Settings - Control Panel* and double-click on the *DS Auth Configuration* icon. The DSAuth Configuration dialog box will appear.
2. Click *Debug*. The Debug dialog box will appear.
3. Clear the *Enable* checkbox of the log file for which you wish to quit logging information.
4. Click *OK* to dismiss the dialog box.
5. Close the DSView software session.
6. Restart the Avocent Auth Server service under *Settings - Control Panel - Services* if you wish to disable the logging of information in the ConsoleAuthServer.log or DSBackup.log file.

   - or -

   Stop and restart the Avocent Secure Protocol Manager if you wish to disable the logging of information in the Trace.log file.

SNMP (Simple Network Management Protocol) Trap Logging (Windows NT/2000/XP Only)

The DSAuth software may be configured to log enterprise (SNMP) traps sent by DS appliances.

An SNMP trap is a notification sent by a DS appliance to a host system indicating that an event has occurred in the DS appliance that may require further attention.

SNMP is a protocol used to communicate management information between network management applications and DS appliances using TCP/IP and IPX protocols. Other SNMP managers (such as Tivoli® and HP OpenView) may communicate with your DS appliance by accessing MIB-II (Management Information Base) and the public portion of the enterprise MIB. MIB-II is a standard MIB that many SNMP target devices support. When you access a DS appliance for the first time, the DSAuth software will retrieve the SNMP parameters from the DS appliance.

DS appliances are defined on the host by criteria such as system information, which stations may manage the DS appliance, which stations may receive SNMP traps from the switch and the community to which they belong. If you select *Options - System Settings* from the DSAuth software window and then check *Enable SNMP trap log* in the Global Settings dialog box, the appliance will log SNMP received messages over UDP (User Datagram Protocol) port 162.

The traps must be configured on each DS appliance using the Command Line Interface (CLI). The address of the server running the DSAuth software must be configured as a trap recipient, the proper community must be set, and each desired trap must be enabled.

NOTE: SNMP trap logging cannot be enabled if SNMP services have not been installed.

All SNMP traps are logged in the DS[mm][yy][dd].csv audit log file, where [mm] is the month, [dd] is the day and [yy] is the year when log entries were last added.

The audit log file contains the following columns:

- DATE - Date of the log entry
- TIME - Time the log entry was made
- EVENT TYPE - Type of log entry, which is 9 SNMP_TRAP for SNMP traps
- USERNAME - Username of the user who created the trap, or “Unknown Username” if the username is not given
- DEVICE_PORT - Displays the following for SNMP traps:

  Appliance:[appliance name]::[appliance IP address]::[community of the trap]
- DESCRIPTION - Displays the following for SNMP traps:

  [generic trap code]:[specific trap code]::
  [generic trap name]::[specific description of trap]

To configure SNMP trap logging:

1. From the DSView management software menu, select *Options* - *System Settings*.

   - or -

   Click the *System Settings* toolbar icon.

   The Global Settings dialog box will appear.
2. Click the *Enable SNMP Trap Log* checkbox to log SNMP traps over UDP port 161.
3. Enter the community of the traps you wish to log in the SNMP Trap Community text field. The default community is public.
4. In the Delete logfiles older than text field, specify the number of days to keep the audit log file.
5. Specify the pathname for the audit log file in the File Location text field.
6. Click *OK* to save the settings and close the dialog box.

   - or -

   Click *Cancel* to exit the dialog box without saving.

To use SNMP trap logging:

1. Install and configure TCP/IP on the DSAuth Server.
2. Install the SNMP service on the DSAuth Server, configure the host as trap recipient and enable the traps.
3. Enable the SNMP service on the DSAuth Server.

Configuring the Event Log

The DS Management Software suite uses the DSAuth software's functionality to log event information in a text file that may be audited at a later time.

Events logged by the DSAuth software include:

- Failed DSAuth software authentication attempts. (For example, the error message *Channel Blocked, insufficient right access* may be output to the event log.)
- Server power state changes.
- Appliance reboot requests.
- Appliance reFLASH.
- SNMP alerts defined by the appliance's firmware.
- CPS serial over IP network appliance authentication.

When all software programs are installed, a modification to the event log of the computer running DSAuth software is required.

To configure the event log for use with Windows NT:

1. From the Start menu, select *Programs - Administrative Tools (Common) - Event Viewer.* The Event Viewer window displays.
2. From the Event Viewer window, select *Log - Log Settings* to display the Event Log Settings window.
3. Select *Overwrite Events as Needed* and click the *OK* button.

To configure the event log for use with Windows 2000:

1. From the Start menu, select *Settings - Control Panel* to open the Control Panel.
2. Double-click on the *Administrative Tools* icon, then the *Event Viewer* icon.
3. In the left viewer pane, click on *Application Log* and then choose *Action - Properties* from the menu at the top of the window. This will activate the Application Log Properties window.
4. Select *Overwrite Events as Needed* and click *OK*.

Updating DSAuth Server Appliance Information

When an appliance is added to the system, its port and channel names are automatically added to the DSAuth Server database with a default value. If you change port and/or channel names on the appliance, the information in the DSAuth Server database will not reflect the current names defined for the appliance.

An Administrator may update the port and channel names for DSR switches, CPS810 appliances and CPS1610 appliances within the DSAuth Server database by selecting the *Tools - Update with Appliance Names* command.

To update port and channel information in the DSAuth Server database:

1. From the DSView management software window, select a DSR switch, CPS810 appliance or CPS1610 appliance.
2. Select *Tools - Update with Appliance Names*. A dialog box will appear and prompt you to confirm updating the port and channel names for the appliance to those in the DSAuth Server database.
3. Click *Yes*. Another dialog box will appear prompting you to confirm the update. Continue to step 4.

   - or -

   Click *No* to exit the command.
4. Click *Yes* to confirm the update. The port and channel names in the DSAuth Server database are updated, based on the currently appliance values.

   - or -

   Click *No* to exit the command.

Forcing a Full Resynchronization

If the integrity of the DS topology view of the backup server should come into question or if a PC is moved to control a different DS topology view, a full resynchronization should be performed. This will force a check of all elements and should only be performed when necessary as it consumes a great deal of time and network bandwidth.

To force a full resynchronization:

1. From the Start menu, select *Settings - Control Panel* and double-click on the *DS Auth Configuration* icon. The DSAuth Configuration dialog box will appear.
2. Select your backup DSAuth Server and select the *Force Full Resynchronization* checkbox.
3. Click *OK* to begin the resynchronization.

Using a Backup Server for Authentication

By default, the DS management software and DSWebview software always attempt to use the primary DSAuth Server. If communication cannot be established with the primary server, the DS management software and DSWebview software will attempt to use a backup server if one has been configured in your system.

When an action is performed that requires communication with the primary server and communication cannot be established, a message box will appear and prompt you to decide if you wish for the system to use the backup authentication server. Click *Yes* to allow the system to use the backup server. If you click *No*, the action will not be performed.

NOTE: The backup server may not contain all functionality available on the primary server.

CHAPTER 4

DSView Management Software

About the DSView Management Software

The DSView software component of the DS Management Software suite works in conjunction with the DSAuth Server to administer your site and add, manage and authorize proper access to DS appliances and target devices by users.

An Administrator may modify system settings, manage Global Macros that may be used to perform actions on target devices and configure and select servers and users that may use LDAP authentication for an additional level of security. Topology data may also be exported into a comma separated file.

The DSView management software is also used to access connected servers. When you access a port, the desktop of the server will appear in a Video Viewer window and you may perform operations on the target server.

Within the Video Viewer window, a DS user may perform cursor operations, including changing how the local cursor displays and toggling it on or off. DS users may also create Local Macros for use on the system running the DSView management software.

Window Features

The DSView management software window consists of a Node Manager that may be used to access servers and devices attached to the DS appliance/DSR switch. When you launch the DSView management software, the Node Manager appears. The Node Manager allows you to view, access and manage all of the supported DS appliances, CPS serial over IP network appliances, EVR1500 environmental monitor and control appliances and generic appliances in your data center in a topology or server view.

Double-clicking an item in the Node Manager has the following effect:

- Selecting a DS appliance/DSR switch channel or port launches a Video Viewer window
- Selecting a CPS appliance port launches a Telnet application viewer
- Selecting an EVR1500 environmental monitor launches a web browser
- Selecting a generic appliance executes the command associated with the appliance

NOTE: You must have Administrator privileges to launch a Telnet application viewer from a CPS appliance.

Figure 4.1 shows the DSView management software window areas, and descriptions follow in Table 4.1.

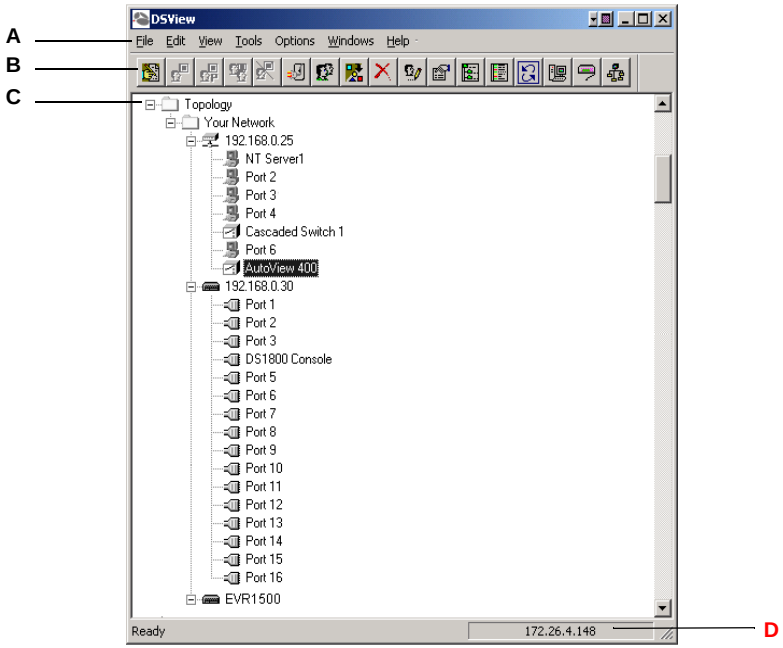


Figure 4.1: DSView Management Software Window

Table 4.1: DSView Management Software Window Descriptions

Letter	Description
A	Menu bar: Allows you to access many of the features in the DSView management software window.
B	Toolbar: Allows you to quickly access many of the features in the DSView management software window.
C	Root node: Each tree consists of a root node and branches if you are using topography view. If you are using server view, target devices are listed by name only.
D	Status bar: Displays the net address of the DSAuth Server.

Appliances may be configured using the DSView management software. You can launch the Properties dialog box by selecting an appliance in the Node Manager and then selecting *Edit - Properties*, right-clicking and selecting *Properties* from the pop-up menu or by clicking the *Properties* toolbar icon. The Properties dialog box contains tabs that enable you to configure your appliance.

Launching the DSView Management Software

This section describes how to launch the DSView management software so that you may begin using it to manage DS appliances and target devices.

NOTE: A warning message will appear and some software features may not be available if the version numbers of the DSView management software and DSAuth Server software are not compatible. This occurs when the DSView management software is launched. If the warning message appears, you may wish to upgrade either the DSView management software or DSAuth Server software. See Chapter 2 for information on software installation.

To launch the DSView management software:

Select *Start - Programs - Avocent - DSView*.

- or -

Double-click the *DSView* icon. The DSView management software will launch.

NOTE: A warning message displays if the software versions of the DSView management software and DSAuth Server do not match. The DSView management software will launch when you close the message box.

Configuring LDAP Authentication

In addition to authentication using the database on a DSAuth Server, an Administrator may also use Lightweight Directory Assistance Protocol (LDAP) authentication to provide DS users with a different type of authentication. LDAP is a vendor-independent protocol standard used for accessing, querying and updating a directory using TCP/IP. Based on the X.500 Directory Services model, LDAP is a global directory structure that supports strong security features including authentication, privacy, integrity and centralization.

To authenticate DS users, they must be stored on an LDAP-enabled directory server, such as Novell® e-Directory™. The Administrator defines and chooses the LDAP server that will be used for LDAP authentication, specifies LDAP service parameters and adds and deletes the LDAP service for DS users.

When a request is made to connect to an LDAP service, the DSView management software queries the DSAuth Server to determine if a DS user has access to the LDAP service. A user credentials dialog box will appear that prompts the DS user to supply a username, password and authentication type (Windows or LDAP). The DS user's login information is then sent to and verified in the LDAP database residing on the DSAuth Server and LDAP server, which enables the LDAP service for the DS user. Figure 4.2 illustrates this interaction.

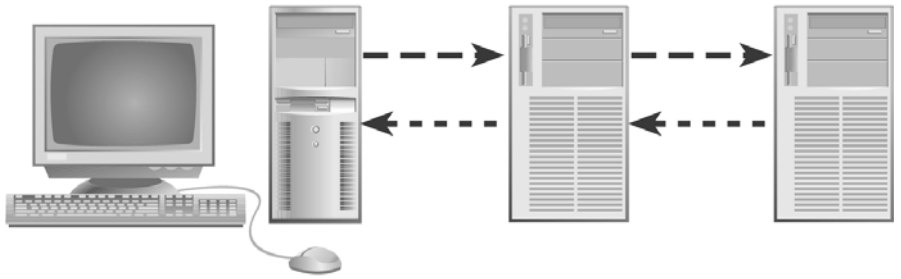


Figure 4.2: LDAP Authentication

The DSView management software performs the following functions:

- Requests LDAP Services/DSAuth software LDAP user list
- Requests Specific LDAP Services parameters
- Requests Selected LDAP Service user list (Adding Multiple LDAP Users)
- Sends Add/Delete LDAP service/DSAuth software LDAP users
- Sends Edit LDAP service

The DSAuth Server performs the following functions:

- Stores parameter in DSAuth software LDAP database
- Connects with defined parameters to validate LDAP service
- Requests list of users from LDAP service

To add or edit an LDAP service:

1. In the DSView management software window, select *Options - LDAP Database Maintenance - LDAP Services*. The Configure LDAP Services dialog box will appear.

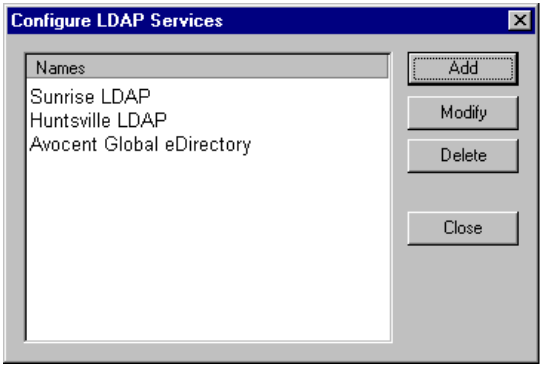


Figure 4.3: Configure LDAP Services Dialog Box

2. To add an LDAP service, click *Add*.

   - or -

   To edit an LDAP service, select a service and then click *Edit*.

The Add LDAP Service dialog box will appear.

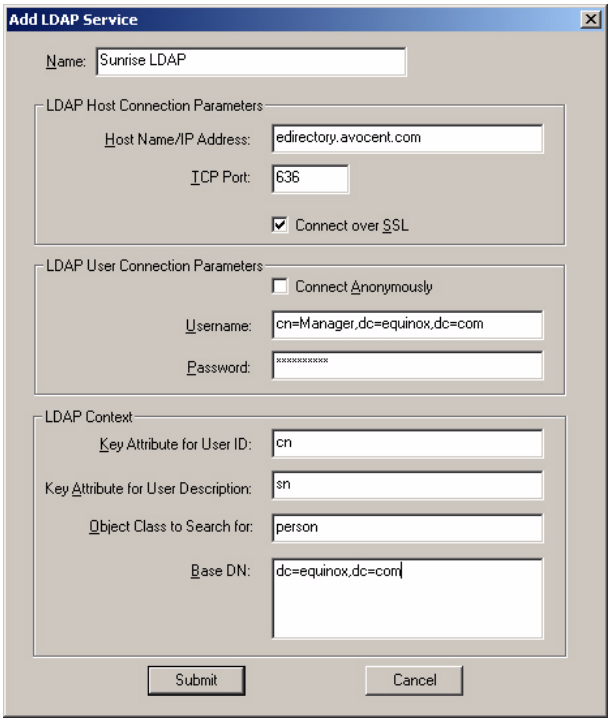


Figure 4.4: Add LDAP Service Dialog Box

3. Type the name of the LDAP service in the Name field.
4. Type the DNS name of the LDAP server in the format xx.xx.xx.xx in the Host Name/IP Address field.

   - or -

   Type the IP address of the LDAP server in the field.
5. Click *Connect over SSL* you want to use a Secure Socket Layer (SSL) connection. If this box is not checked, connections will be established using clear text (non-secure).
6. Type a username and password that will be used by the LDAP server for accepting queries in the LDAP User Connection Parameters area.

   - or -

Click *Connect Anonymously* to enable the LDAP server to accept queries without requiring a username and password.

7. Type the user ID key attribute to be used for searches.
8. Type the user description key attribute to be used for searches.
9. Type the object class to be used for searches.
10. Type the starting point from which LDAP searches will begin in the Base DN field. The default values are dc=<yourDomainName>, dc=com and may be modified. For example, to define a search base for test.com, type **dc=test, dc=com**.

NOTE: Each search base value must be separated by a comma.

11. Click *Submit*. The Add LDAP Service dialog box is dismissed. If you are adding an LDAP service, the Adding LDAP Service dialog box will appear and show the progress of the update. The data is saved in the LDAP service database on the DSAuth Server.

To delete an LDAP service:

1. In the DSView management software window, select *Options* - *LDAP Database Maintenance* - *LDAP Services*. The Configure LDAP Services dialog box will appear.

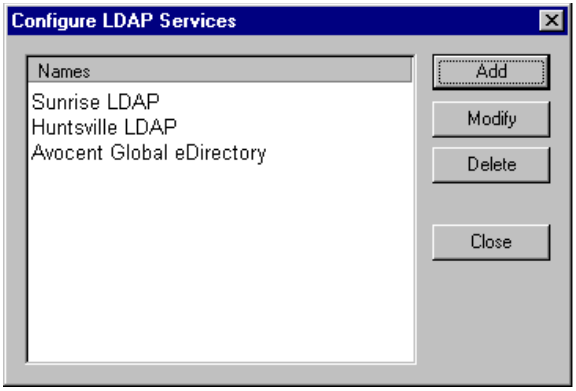


Figure 4.5: Configure LDAP Services Dialog Box

2. Select an LDAP service from the list.
3. Click *Delete*. A Delete LDAP Service dialog box will display prompting you to confirm the deletion.
4. Click *Yes*. The Deleting LDAP Service dialog box will appear and show the progress of the deletion. The LDAP service is deleted and the dialog box is dismissed.

To add a single LDAP user:

NOTE: The user must already exist in the LDAP service to add the DS user as an LDAP user.

1. In the DSView management software window, select *Options - LDAP Database Maintenance - LDAP Users*. The LDAP Users dialog box will appear.

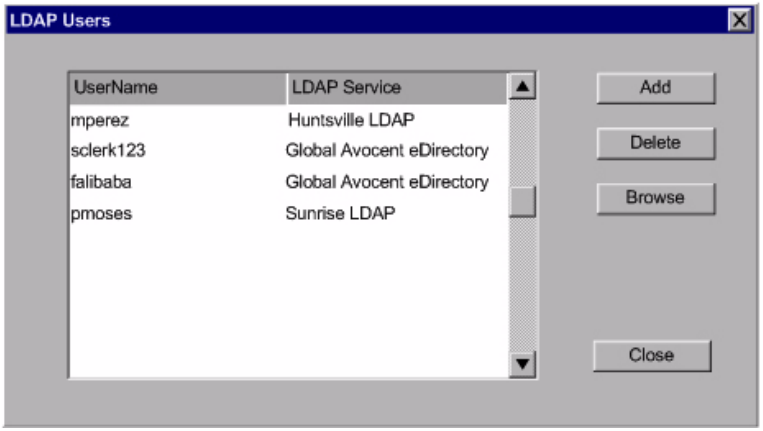


Figure 4.6: LDAP Users Dialog Box

2. Click *Add*. The Add LDAP Users dialog box will appear.

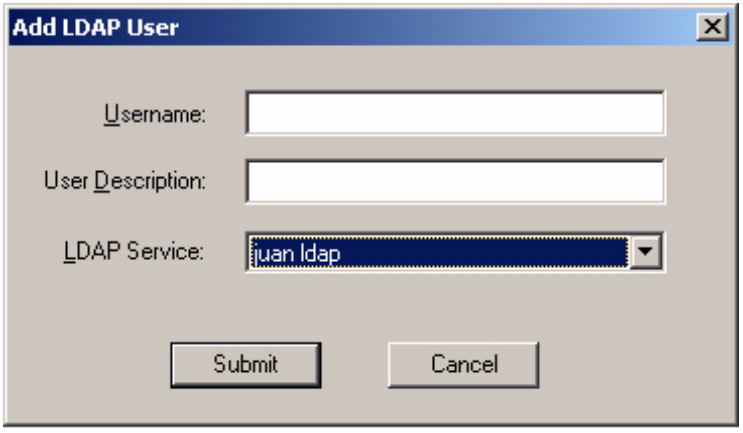


Figure 4.7: Add LDAP User Dialog Box

3. Type the name of the user in the Username field.
4. Select an LDAP service from the drop-down menu that will be used to authenticate the user. The User Description field is automatically filled with the value stored in the LDAP service.
5. Click *Submit*. The DS user is added to the LDAP user database on the DSAuth Server.

To add multiple LDAP users:

1. In the DSView management software window, select *Options - LDAP Database Maintenance - LDAP Users*. The LDAP Users dialog box will appear.
2. Click *Browse*. The Select LDAP Users dialog box will appear.

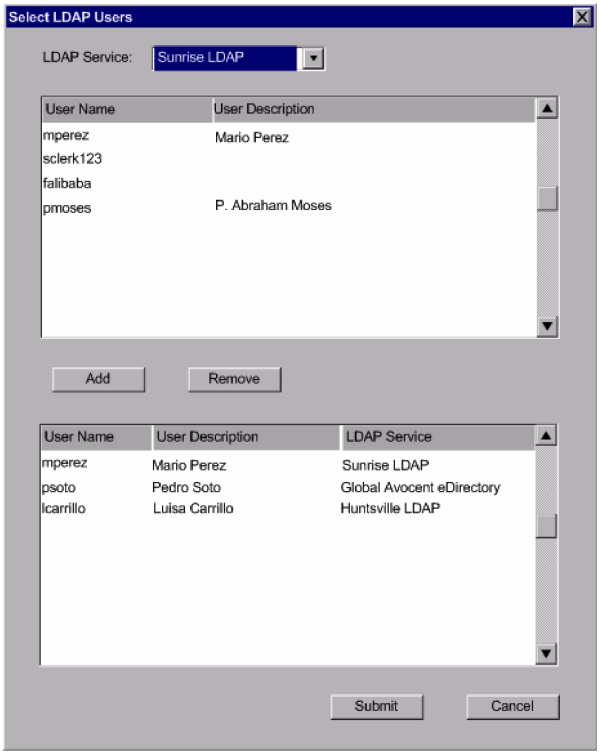


Figure 4.8: Select LDAP Users Dialog Box

3. Select an LDAP service from the drop-down menu that will be used to authenticate the users. A list of the users currently in the LDAP services database displays in the bottom list box.
4. Select one or more users from the top list box and then click *Add*. The selected users are added to the bottom list box.
5. Click *Submit*. An Adding LDAP users dialog box will appear and show the progress of the action. The DS users are added to the LDAP user database on the DSView management software server and the Select LDAP Users dialog box is dismissed.
6. Click *Close* to dismiss the LDAP Users dialog box.

To remove LDAP users:

1. In the DSView management software window, select *Options* - *LDAP Database Maintenance* - *LDAP Users*. The LDAP Users dialog box will appear, containing a list of DS users and the LDAP service to which they are associated.
2. Select one or more DS users from the Username list.
3. Click *Delete*. A Delete LDAP Users dialog box will display prompting you to confirm the deletion.
4. Click *Yes*. The Deleting LDAP Users dialog box will appear and show the progress of the deletion. The LDAP users are deleted and the dialog box is dismissed.

Logging onto LDAP servers

To use LDAP authentication, you must log in to the LDAP server. The following process occurs when you log in:

- The DS user starts the DSView management software.
- The Windows Network credentials for the DS user are compared with those on the DSAuth Server. If they do not match, the Enter Network Password dialog box displays and the user will need to log in to continue.
- The LDAP user database on the DSAuth Server is searched for the DS user and, if found, will be given access to the LDAP server for authentication. If the DS user is not found in the LDAP user database, the Enter Network Password dialog box will appear again and the DS user must log in again.

To log onto an LDAP server:

1. From the DSView management software window, select *File* - *Connect As*. The Enter Network Password dialog box will appear.

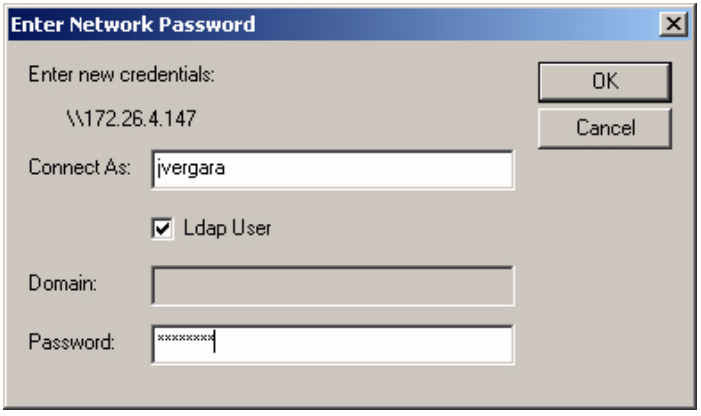


Figure 4.9: Enter Network Password Dialog Box

2. Type a username in the Connect As field and then type a password. Select the *Ldap User* checkbox and then click *OK*.

   The dialog box is dismissed and the DSAuth Server attempts to authenticate the DS user.

Specifying a Data Encryption Level

If an appliance has been upgraded to the appropriate firmware version, a DS user may set an encryption level to use for encoding keyboard and mouse data packets sent over a video session to the appliance. Port 2068 is used for sending the encoded keyboard and mouse data. Video data is sent over port 8192.

Table 4.2 lists the appliances and firmware versions that support the specifying of data encryption levels.

Table 4.2: Firmware Versions Supporting Multiple Encryption Levels

Appliance	Firmware Version
DSR800 switch	1.1.0.0 or later
DSR1161 switch/2161 switch/4160 switch	1.2.0.0 or later
DSR1161 switch/2161 switch/4160 switch	2.2.0.0 or later
DSR1010 switch/2010 switch/4010 switch	2.3.0.0

Three levels of encryption are available:

- DES (Data Encryption Standard) - This method encrypts and decrypts data in 64-bit blocks, using a 64-bit key
- 3DES (Triple Data Encryption Standard) - This method uses three stages of DES and provides additional security
- 128-bit - This method encrypts packet data using the Secure Socket Layer (SSL) protocol

The specified encryption level will be applied to all video sessions established on the appliance.

Encryption levels may not be set for older DS appliances/DSR switches or those switches not listed in Table 4.2. These DS appliances/DSR switches only use DES encryption and send video and encrypted keyboard and mouse data over port 8192.

See *Appendix B* for more information on ports.

To specify a data encryption level:

1. From the DSView management software window, select a DSR switch and select *Edit* - *Properties* from the drop-down menu.

   - or -

   Right-click and select *Properties* from the shortcut menu.

   - or -

   Click the *Properties* toolbar icon.

   The Properties dialog box will appear.
2. In the [*DSR Switch*] tab, select an encryption level.
3. Click *OK* to dismiss the dialog box.

Adding and Configuring DS Appliances and Target Devices

Once you have installed your hardware and software, you will need to configure the DS appliances. You may also need to configure KVM switches and associate SPC power control devices with an appliance port.

Adding DS appliances and DSR switches

You may add a DS appliance or DSR switch to your system by selecting the *File* - *New* - *[DS Appliance/DSR Switch]* command from the DSView management software window drop-down menu.

To add a new DS appliance or DSR switch to the system:

1. From the DSView management software window, click *View* - *Topology* to display the DS topology view.
2. Click *Topology* to add the new DS appliance or DS switch at the top level of the topology tree.

   - or -

   Expand the topology tree and click on the name of the group to which you wish to add the new DS appliance or DS switch.
3. From the DSView management software window, select *File* - *New* - *[DS Appliance/DSR Switch]*. The New dialog box appears.
4. In the [*DS Appliance/DSR Switch*] tab, enter the IP address for the appliance that you are adding. This is the IP address that you assigned in the Terminal Applications menu. See the installer/user guide for your DS appliance/DSR switch for more information.
5. Enter a name for the appliance that you are attaching. DS appliances/DSR switches can be identified by name or IP address.
6. Select the type of DS appliance or DSR switch you wish to add.
7. Click on the *Port* tab and configure each individual port.

Configuring host PCs

A computer attached directly to your DS appliance/DSR switch is called a “host PC.” If you are directly attaching a host PC, you may give it a descriptive name in the Port field. No further configuration is necessary.

Configuring attached KVM switches

NOTE: DS appliances support specific AutoView® switches and OutLook® switches. Contact Avocent Technical Support or your reseller for details.

Before the ports on an attached KVM switch can be accessed, the DSView management software must be configured to recognize the attached switch.

If a port is already associated with a KVM switch, you may modify or remove its association using either the Ports tab or the Properties tab in the [*DS Appliance/DSR Switch*] Properties dialog box.

To configure the DSView management software for an attached cascaded or non-cascaded switch:

1. Attach the switch as directed in your hardware installer/user guide.
2. Activate the DSView management software, and display the DS appliance/DSR switch to which the switch is attached.
3. Right-click on the DS appliance/DSR switch and select *Properties*. The Properties dialog box will appear.
4. Select the *Ports* tab.
5. You will see a list of ports and a corresponding drop-down menu beside it. Using the drop-down menu, select the number of channels supported by the KVM switch you are configuring.

Repeat this procedure for every KVM switch you plan to configure. Click *OK* when complete.

After all DS appliances/DSR switches are configured, you may add CPS serial over IP network appliances, EVR1500 environmental monitor and control appliances and generic appliances to the system.

Adding a CPS appliance

To add a new CPS appliance to the system:

1. From the DSView management software window, click *View* - *Topology* to display the DS topology view.
2. Click *Topology* to add the new CPS appliance at the top level of the topology tree.

   - or -

   Expand the topology tree and click on the name of the group to which you wish to add the new CPS appliance.

3. You must configure the CPS appliance for DS appliance management. Begin by establishing a Telnet application session to your CPS appliance. From the CPS appliance command line, enter the following command in a single line, with each parameter separated by spaces:

   server security authentication=ds
   encrypt=<DES>,<3DES>,<128>,<none>
   dsauth=<pri_ip>,<secondary_ip>,<any> dsclear lockout=<hours>

   Parameter usages for this command are described below:

   - Type **encrypt** to specify the type of authentication you wish to use. You may specify multiple values or **none** if you do not wish to authenticate users.
   - In place of <**pri_ip**> and <**secondary_ip**>, enter the IP address of the DSAuth Server(s) on which you wish to perform authentication. You may specify a primary only, a secondary only, a primary and secondary or **any** to use any DS authentication server.

NOTE: If **any** is specified, the first DSAuth Server adding the CPS appliance to its database will install credentials on the CPS appliance that place it in Secure mode. While in Secure mode, the CPS appliance may not be accessed by other DSAuth Servers.

If the first DSAuth Server adding the CPS appliance to its database is configured with a backup DSAuth Server, the credentials of both DSAuth Servers will be installed on the CPS appliance.

   - Type **dsclear** if you wish to clear any stored DS appliance/DSR switch credentials and authentication server credentials.
   - Type **lockout** to enable or disable Security Lock-out. In place of <**hours**>, enter the number of hours to lock out a DS user in the range 1-99. To disable, specify a 0 value.

   In the following example, any DSAuth Server may authenticate users, with the strongest encryption negotiated between triple DES and 128-bit:

   server security authentication=ds dsauth=any encrypt=3des,128

   In the following example, a primary and secondary server may authenticate users with 3DES encryption, clearing stored credentials and locking out a DS user for one hour after five unsuccessful login attempts:

   server security authentication=ds dsauth= 12.34.45.78,90.98.76.54 encrypt=3des dsclear lockout=1

   Press **Enter** to accept the configuration.

4. From the DSView management software, select *File - New - CPS*. The Properties dialog box will appear.
5. In the Device Identification tab, enter the IP address for the CPS appliance that you are adding. This is the IP address that you assigned in the Terminal Applications menu. See the CPS Installer/User Guide for more information.
6. Enter a name for the CPS appliance and select the type of CPS appliance that you are adding.

7. Click on the *Ports* tab. Give each port a descriptive name in the Port field. No further configuration is necessary. However, you may click on the *Properties* tab to list descriptive information for the CPS appliance that you are configuring.
8. Click *OK* to add the CPS appliance.

Adding an SPC device as a CPS appliance port

NOTE: A CPS network appliance must be configured to use an SPC device. See the CPS Installer/User Guide for more information.

When a CPS810 appliance or CPS1610 appliance is added to the system using the DSView management software, any SPC power control devices that have been configured on the CPS appliance are automatically added to the database on the DSAuth Server and display in all DS topology views.

An SPC device contains either 8 or 16 power outlets that may be used to control the power state of an attached device using the DSView management software. To do this, you must associate the port of the DS appliance with an SPC device. If the server has multiple power supplies, the appliance's port can be associated with multiple SPC device outlets.

NOTE: To use an SPC device, there must be at least one CPS810 appliance, CPS1610 appliance or DSR1021 switch on your network.

The integrated power management of the SPC device enables you to remotely power up, power down or reboot servers attached to the SPC device. The SPC device will appear as a series of outlets cascaded below the CPS appliance in the DS topology view. Each outlet will appear with a power indicator.

If the port configuration is changed on the CPS appliance, the DSAuth Server database may be updated to reflect the changes.

An SPC device outlet may be associated with your DS appliance port, EVR1500 environmental monitor or generic appliance in either of the following ways:

- From the DS appliance port, EVR1500 environmental monitor or generic appliance
- From the SPC device

To associate an SPC device outlet using a DS appliance port, EVR1500 environmental monitor or generic appliance:

NOTE: You must have Administrator privileges to associate a DS appliance port, EVR1500 environmental monitor or generic appliance with an SPC device outlet.

1. Ensure that the SPC device outlet display is viewable in the DSView management software window. See *Viewing Ports, Outlets, Target Devices and Connected DS Users* on page 52 for more information.
2. Right-click on a DS appliance/DSR switch port or channel, EVR1500 environmental monitor or generic appliance and then select the *Power State* menu item. The Power State dialog box will appear.

3. Click the *Link* button. The Server/SPC Outlet Links dialog box will appear, containing a list of all SPC device outlet names that are present on the DSAuth Server. Any SPC device outlets that were previously linked will appear with the server name next to the outlet name in the Current Server/SPC Outlets Links list.
4. To add an association, click on an SPC device outlet in the Outlets with No Server Association list that does not have an associated server name and then click *Add Link Association*. The SPC device outlet is associated with the DS appliance port or generic appliance and appears in the Modified Server/SPC Outlet Links list at the bottom of the dialog box.

   - or -

   To remove an association, click on an SPC device outlet/DS appliance port or SPC device outlet/generic appliance association in the Current Server/SPC Outlet Links list and then click *Remove Link Association*. The SPC device outlet association with the DS appliance port or generic appliance is removed and the change appears in the Modified Server/SPC Outlet Links list at the bottom of the dialog box.
5. Click *OK* to save your changes and close the dialog box, and then click *OK* on the Power State dialog box to close it.

To associate a DS appliance port, EVR1500 environmental monitor or generic appliance using an SPC device:

NOTE: You must have Administrator privileges to associate an SPC device outlet with a DS appliance port, EVR1500 environmental monitor or generic appliance using an SPC device.

1. Ensure that the SPC device outlet display is viewable in the DSView management software window. See *Viewing Ports, Outlets, Target Devices and Connected DS Users* on page 52 for more information.
2. Right-click on an SPC device outlet and click *Properties* from the pop-up menu. The *[SPC Device Outlet Name]* Properties dialog box will appear.
3. Select the DS appliance or DSR switch you wish to add from the *Associated Server Link* drop-down menu.

NOTE: A DS appliance port, EVR1500 environmental monitor or generic appliance may be associated with multiple SPC device outlets.

4. Click *OK* to associate the DS appliance port, EVR1500 environmental monitor or generic appliance and dismiss the dialog box.

To discover an SPC device added or removed from the CPS appliance or to update the DSAuth Server database with CPS appliance port configuration changes:

1. From the DSView management software window, select a CPS810 appliance or CPS1610 appliance.
2. From the DSView management software menu, select *Edit* - *Properties*.

   - or -

   Right-click and select *Properties* from the pop-up menu.

   - or -

   Click the *Properties* toolbar icon.
3. The [appliance name] Properties dialog box will appear and a message box will appear stating that the current configuration is being retrieved from the appliance.
4. If the configuration values are different than those stored in the DSAuth Server database, a dialog box containing the changes will appear.
5. Click *Yes* to automatically update the port settings.

   - or -

   Click *No* to reject the changes.
6. Click the *Properties* tab. A list of all ports will appear.
7. If desired, type a name in the Port field to the left of a port's drop-down menu to change its name.
8. Click *OK* to save the changes.

Adding a generic appliance

To add a new generic appliance to the system:

1. From the DSView management software window, click *View* - *Topology* to display the DS topology view.
2. Click *Topology* to add the new generic appliance at the top level of the topology tree.

   - or -

   Expand the topology tree and click on the name of the group to which you wish to add the new generic appliance.
3. Select *File* - *New* - *Generic Appliance*. The Generic Appliance dialog box appears.
4. Enter the IP address for the generic appliance that you are adding.
5. Enter the name for the generic appliance, which will display in the topology and server views.

6. Select the command to associate with the generic appliance.
   - None - Select this option if the generic appliance does not have an associated command.
   - Launch Telnet Session - If this option is selected, the generic appliance will use a Telnet application connection.
   - Launch Browser - If this option is selected, the generic appliance will use either the IP address of the appliance or a user-specified URL when the web connection is launched. Type the web address in the URL field.
   - Launch User Specified Application - If this option is selected, you must enter an associated executable in the Command field. If the $1 parameter is included with the executable, the IP address of the appliance will be automatically substituted when the command is executed.

   The command associated with the generic appliance will be executed when:
   - The appliance is double-clicked in the DSView management software window.
   - The generic appliance is right-clicked in the DSView management software or DSWebview Client and the *Command* menu option is selected.
7. Click the *OK* button to add the new generic appliance to the DSAuth Server and close the dialog box. The new generic appliance appears in the Topology and Server views.

NOTE: Once a generic appliance has been added, the specified connection option cannot be changed. You must delete the generic appliance and re-add it to specify a different connection method. However, you may choose a different URL if you are using the Launch Browser connection option or a different executable if you are using the Launch User Specified Application connection option.

Adding an EVR1500 environmental monitor

To add a new EVR1500 environmental monitor to the system:

1. From the DSView management software window, click *View* - *Topology* to display the DS topology view.
2. Click *Topology* to add the new EVR1500 environmental monitor at the top level of the topology tree.

   - or -

   Expand the topology tree and click on the name of the group to which you wish to add the new EVR1500 environmental monitor.
3. Select *File* - *New* - *EVR1500*. The New EVR1500 dialog box appears.
4. In the EVR1500 tab, enter the IP address for the EVR1500 environmental monitor that you are adding.
5. Enter the domain name for the EVR1500 environmental monitor, which will display in the Topology and Server views.
6. Click on the *Properties* tab and type in any information you wish to add.

7. Click *OK* to add the new EVR1500 environmental monitor to the DSAuth Server and close the dialog box. The new device appears in the topology and server views.

Adding and Managing DS Users

Adding DS users

You must add DS users within the DSView management software in order for them to have access to the system. Users are assigned a default access level when they are added. If you wish to assign DS users a different access level, you will need to change their permissions.

To add a user:

1. Within the DSView management software window, right-click on the DS appliance or port you wish to change and select *Permissions*. This will activate the Permissions dialog box.
2. Click *Add*. A type-in field will appear in the User or Group column. Type the name of a DS user and press **Enter** to add the DS user. Go to step 6.

   - or -

   Click *Browse*. The Select Users, Computers or Groups dialog box will appear including a listing of all DS users on the Windows domain. Continue to step 3.

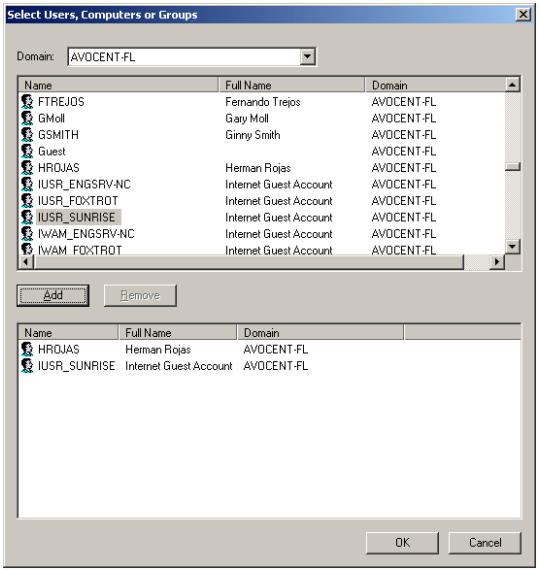


Figure 4.10: Selecting DS Users to Modify

3. Select a DS username to add from the upper list box.
4. Click *Add*. The DS user is added to the lower list box.

5. Click *OK* to dismiss the Select Users, Computers or Groups dialog box.
6. In the Permissions dialog box, check the access boxes appropriately for the new DS user.
7. Click *OK* to dismiss the Permissions dialog box and save your changes to the DSAuth Server database.
8. A dialog box will appear prompting you to apply permission changes to all "children." Click *Yes* to apply the changes.

   - or -

   Click *No* if you do not wish to accept the changes.

Changing DS user permissions

A DS appliance or DSR switch inherits the permissions of the group to which it is added in the DS topology view. For example, adding a DSR switch to the top level Topology node will cause the DSR switch to contain permissions identical to those defined for the Topology node.

When you wish to change default permissions for a DS appliance, it is recommended that the permissions of the group to which the DS appliance belongs be changed instead. This ensures that all DS appliances subsequently added to the group will contain identical default permissions.

To change default DS user permissions:

1. Select a DS appliance/port or generic appliance for which you wish to change DS user permissions.

   - or -

   Select the group containing the DS appliance or generic appliance to change the permissions of all group members.
2. Select *Edit - Permissions* from the drop-down menu.

   - or -

   Right-click and select the *Permissions* command from the shortcut menu.

   - or -

   Click the *Permissions* toolbar icon.
3. A DS user listing will appear. You will see a DS user listed as Everyone, which is configured with the default permissions. Any DS user you do not set up with individual permissions will use this default configuration.

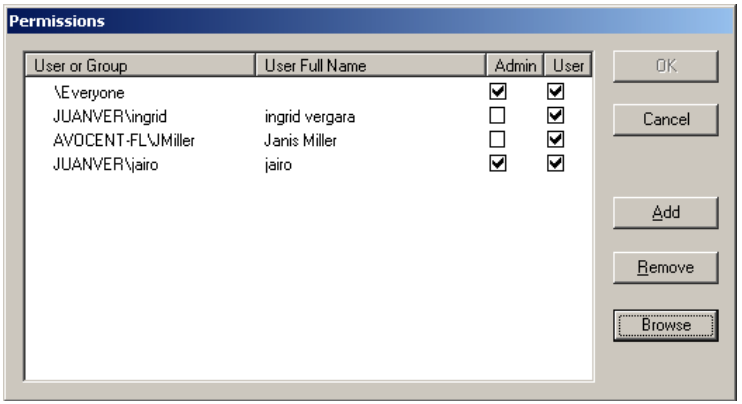


Figure 4.11: Permissions Dialog Box

4. Click *Everyone*. The default setting shows both boxes checked. Check or uncheck the *Admin* and *User* boxes to control access for all DS users without a specifically assigned configuration.

NOTE: Remember, Administrator access will allow the DS user to change permissions in the DSView management software for any DS user listed.

5. Click *OK*.

   If you selected a group or a DS appliance, a dialog box will appear prompting you to apply permission changes to all "children." Click *Yes* to apply the changes.

   - or -

   Click *No* if you do not wish to accept the changes.

To change specific user permissions:

1. Right-click on the entry you wish to change and select *Permissions*.
2. The Permissions dialog box will appear, listing all configured DS users. Change an individual DS user's access level by clicking on the username and selecting the access level you wish the user to have. If a DS user isn't listed, click the *Add* button. Refer to the previous section, *Adding DS users*.

NOTE: If you remove all permissions from a port or DS appliance, access to that port or DS appliance will be lost.

Adding, modifying and removing user access to multiple appliances or servers

Administrators may select the *Tools - Multi-User Operations* command to add, modify or remove user access to multiple appliances or servers. When you select the command, the Multi-User Operations dialog box displays.

Appliances and servers are arranged in a tree structure and may be viewed by either selecting *View - Show Users* or by double-clicking the *User Permissions* icon and then double-clicking each branch of the tree. Double-clicking each branch of the tree will first display users, then display the appliances assigned to a specific user and finally, show the port associations of an appliance. You may update the user, appliance, server and port listing at any time by selecting the *View - Refresh* command or clicking the *Refresh* toolbar icon.

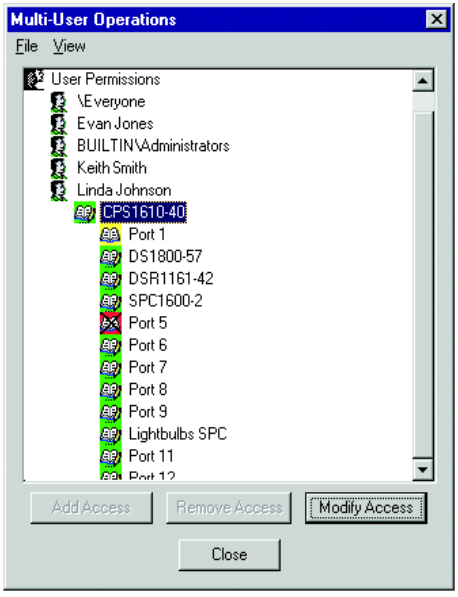


Figure 4.12: Multi-User Operations Dialog Box

To add user access to multiple appliances or servers:

1. From the Multi-User Operations dialog box, select *File - Add User Access*.

   - or -

   Click *Add Access*.

   The User Access dialog box displays.

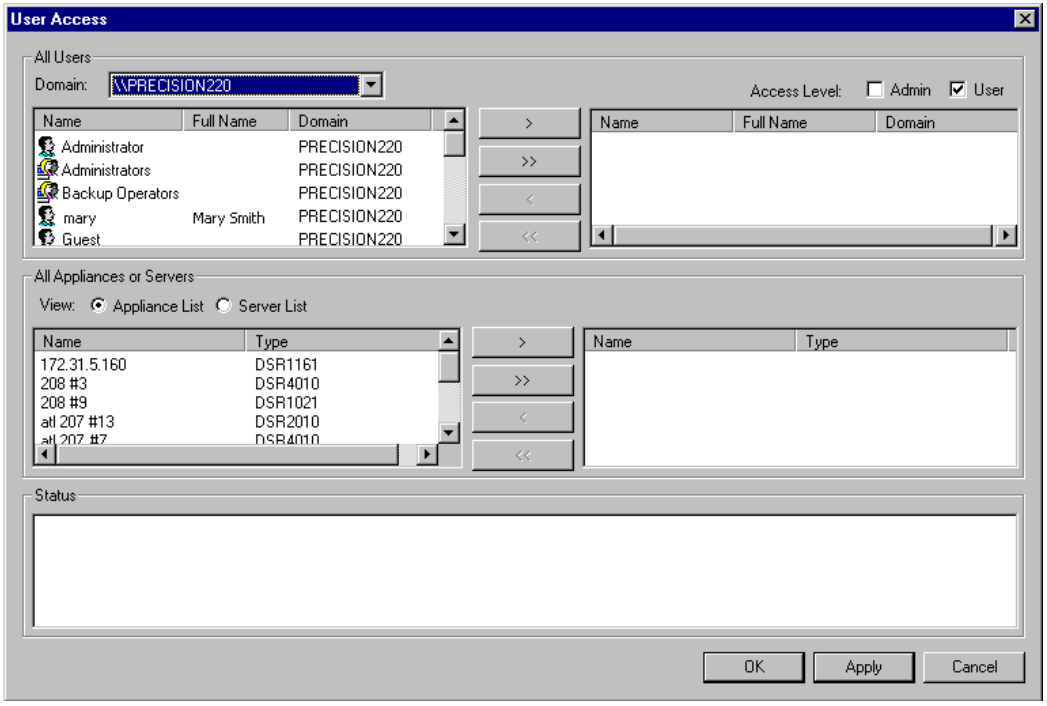


Figure 4.13: User Access Dialog Box

2. If necessary, select a domain containing the users in the All Users area.
3. Select one or more users in the All Users area and then click the Add button (>). The users display in the Selected Users area.
4. Select whether you wish to view a list of all available appliances or servers in the All Appliances or Servers area by clicking the corresponding radio button. A list of appliances or servers will display.
5. Select one or more appliances or servers in the All Appliances or Servers area and then click the Add button (>). The appliances or servers display in the Selected Appliances and Servers list.
6. Specify whether you wish to assign Administrator or User access to the users by selecting the corresponding Access Level checkbox.
7. Click *OK* to apply the changes.
8. A dialog box will appear prompting you to apply permission changes to all “children.” Click *Yes* to apply the changes.

   - or -

   Click *No* if you do not wish to propagate the changes.

9. The Status area displays the progress as each user is assigned the selected permissions to each appliance or server.
10. Click *Cancel* to close the User Access dialog box.
11. A dialog box will appear prompting you to refresh the user, appliance, server and port listing in the Global User Operations dialog box. Click *Yes* to update the listing.

To remove user access to an appliance:

1. From the Global User Operations dialog box, select a DS user in the User Permissions list.
2. Select *File - Remove Access*.

   - or -

   Click *Remove Access*.
3. A dialog box will appear prompting you to confirm the access removal. Click *Yes*.
4. Another dialog box will appear prompting you to verify the confirmation. Click *Yes*.
5. Repeat steps 1-4 to remove additional users.

To modify DS user access permissions:

The Permissions dialog box allows you to specify DS user or Administrator permissions for appliance users. To access the Permissions dialog box, select a DS user in the Global User Operations dialog box and then select *File-Modify Access* or click *Modify Access*. The Permissions dialog box appears.

See *Adding and Managing DS Users* on page 44 for information on using the Permissions dialog box.

Accessing Target Devices

You may access one or more target devices within a DS series appliance at the same time. To access multiple target devices, double-click on every port that you wish to display. Windows may be tiled or cascaded as you choose.

NOTE: A message box will display if an attempt is made to open a Video Viewer window while the DSRIQ module attached to the port is being FLASH upgraded.

To access a target device:

1. Load the DSView management software. This will display the Node Manager and provide you with a list of target devices that you may access.
2. Double-click on the target device that you wish to access. This will open a Video Viewer window and allow the DS user control of the target device.

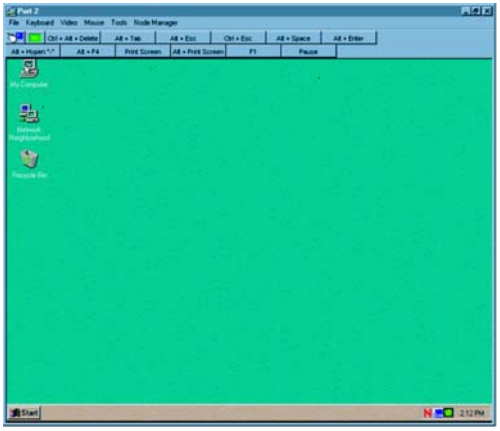


Figure 4.14: The Video Viewer Window

Accessing EVR1500 environmental monitors

An EVR1500 environmental monitor is a network-based appliance that monitors environmental conditions within the rack and/or data center and reports the data using the DSWebview software's browser. Environmental thresholds, such as alarm conditions, can be specified.

If the EVR1500 environmental monitor is attached to a CPS810 appliance or CPS1610 appliance, it can be remotely powered up, powered down or rebooted using an SPC power control device. See *Rebooting and Changing Power States* on page 56 for more information.

See *Configuring attached KVM switches* on page 38 for information on adding an EVR1500 environmental monitor. See the EVR1500 Installer/User Guide for more information on using an EVR1500 environmental monitor.

To launch an EVR1500 environmental monitor session:

1. Load the DSView management software. This will activate the DSView Node Manager and provide you with a list of servers and serial devices that you may access.
2. Double-click on an EVR1500 environmental monitor.

   - or -

   Right-click on an EVR1500 environmental monitor, then select *Connect* from the pop-up menu.

   - or -

   Select an EVR1500 environmental monitor, then select *Tools* - *Connect* from the drop-down menu.

   - or -

Select an EVR1500 environmental monitor, then click the *Connect* toolbar icon.

The system is connected to the EVR1500 environmental monitor and will open a web browser interface.

NOTE: Browser cookies must be enabled and the user must accept certificates for access. The Java runtime plug-in must be enabled for the browser being used for the EVR1500 environmental monitor interface.

3. When the login screen appears, enter your login name, password, DSAuth Server and domain name (when applicable). This information is available from your network Administrator.

Using Privacy mode

If a DS user needs to access a port while excluding all others, Privacy mode is used. When a port is selected in Privacy mode, no other DS user in the system may switch to that port. If another DS user initiates a connection to a port currently in Privacy mode, that user will receive a message indicating the port's status and will not be connected to the port.

To access a target device in Privacy mode:

1. Load the DSView management software. This will display the Node Manager and provide a list of target devices that you may access.
2. Highlight the target device that you wish to access and select *Tools - Privacy Mode Connect*.

   - or -

   Right-click on the target device's name and select *Privacy Mode Connect*.

   - or -

   Highlight the target device that you wish to access and click the *Privacy Mode Connect* toolbar icon.

Sharing a device session

When you attempt to access a port already in use, you will receive a notification message that the port is in use along with the name of the current DS user(s). At this point, you may request to share access to the port with the current DS user(s). The DS users that are currently active will receive a request to allow sharing. If they confirm, the new DS user will gain access to the port. When sharing access to a port, all DS users may monitor the port and may take control if no other DS user is currently active.

When you attempt to connect to a port using the DSView management software window, the DSView Connection Sharing dialog box displays. If you select the *Stealth Connection* checkbox and then click *Share*, you will be connected to a monitor-only session with no control of the port. The DS user that is currently active will not receive notification that access is being shared and no request to authorize sharing will be made. If you do not select Stealth Connection, the DS user will be notified that you wish to share the session.

NOTE: The only way to prevent a stealth connection to a port is by enabling Privacy mode.

Up to 12 DS users may share a single port at one time. If a 13th DS user attempts to connect, an error message will inform the DS user that no sessions are available. Administrators will be given the option of terminating a DS user session.

At any time, DS users may select *View - List of Shared Users* in a Video Viewer window to view a list of DS users sharing their port or channel. DS users in Stealth mode are excluded from this list.

Session time-out

A remote session will time-out if there has been no activity in a Video Viewer window for a specified time. The global session time-out value is configured by your Administrator and is the default value used by the DSView software. A DS user may override this value by selecting the *Local Options* tab on the Global Settings dialog box.

For detailed information on specifying a global or remote session time-out, see *Session time-out* on page 52.

Terminating sessions

Administrators using the DSView management software may terminate the local DS user currently viewing a target device so that you may access the target device.

When you attempt to connect to a port that is in use by the local DS user, a dialog box will appear. If you have Administrator privileges for the port, a selection will be available to enable you to disconnect the local DS user.

For detailed information on terminating a local device session, see *Terminating a target device session* on page 63.

Viewing Ports, Outlets, Target Devices and Connected DS Users

You may use commands in the DSView management software window to perform the following viewing operations:

- View target devices
- Toggle the display of unused CPS appliance, DS appliance, DSR switch and SPC device ports on or off
- View a list of DS users connected to a CPS appliance, DS appliance or DSR switch port with an open Telnet application viewer or Video Viewer window

To display the DS topology view:

1. From the DSView management software window, click *View - Topology* to display the DS topology view.
2. Double-click *Topology* to display the DS topology view.
3. Each name or IP address listed may be expanded by double-clicking on it.

This will display the ports for the DS appliance corresponding to that address. Each of these ports shares the DS appliance's IP address.

If a target device is attached to a port, the properties of that port will be the same as the properties of the target device.

If a KVM switch is attached to one or more of these ports, double-clicking on the port name will display the channels on that KVM switch.

To toggle the display of unused CPS appliance, DS appliance or DSR switch ports or SPC device outlets on or off:

NOTE: You may also toggle the display of unused CPS appliance, DS appliance or DSR switch ports on by right-clicking on a CPS appliance, DS appliance or DSR switch in the DSView management software window and selecting *Reset 'No System Present'* from the pop-up menu.

1. Select a CPS appliance, DS appliance, DSR switch port or SPC device outlet from the DSView management software window.
2. Select the *Edit - Properties* command.

   - or -

   Right-click on the port and select *Properties* from the pop-up menu.

   - or -

   Click the *Properties* toolbar icon.

   The [Port Name] Properties window will appear if an CPS appliance, DS appliance or DSR switch port was selected. The [SPC Device Outlet] Properties will appear if an SPC device outlet was selected.
3. To turn the display of the port or outlet off in the topology view, click *No System Present (Do not display)*.

   - or -

   Leave the checkbox empty to turn the display of the port on in the topology view.
4. Click *OK* to save your changes and dismiss the dialog box.

To view DS users connected to a CPS appliance, DS appliance or DSR switch port or channel:

1. Select a port in the topology view of the DSView management software window.
2. Select the *View - Connected Users* command.

   - or -

   Right-click on the port and select *Connected Users* from the pop-up menu.

   - or -

   Click the *Connected Users* toolbar icon.

A message box will appear containing the usernames of the DS users connected to the CPS appliance, DS appliance or DSR switch.

Managing Multiple Appliances and Devices

Administrators may select the *Tools - Group Operations* command or click the *Group Operations* toolbar icon to delete, disconnect, reboot, name synchronize and perform version control and power control on multiple DS appliances, DSR switches, CPS appliances or EVR1500 environmental monitors, SPC device outlets and target devices. When you select the command, the Group Operations dialog box displays.

Appliances and devices are processed in the same order as they appear in the topology or server view.

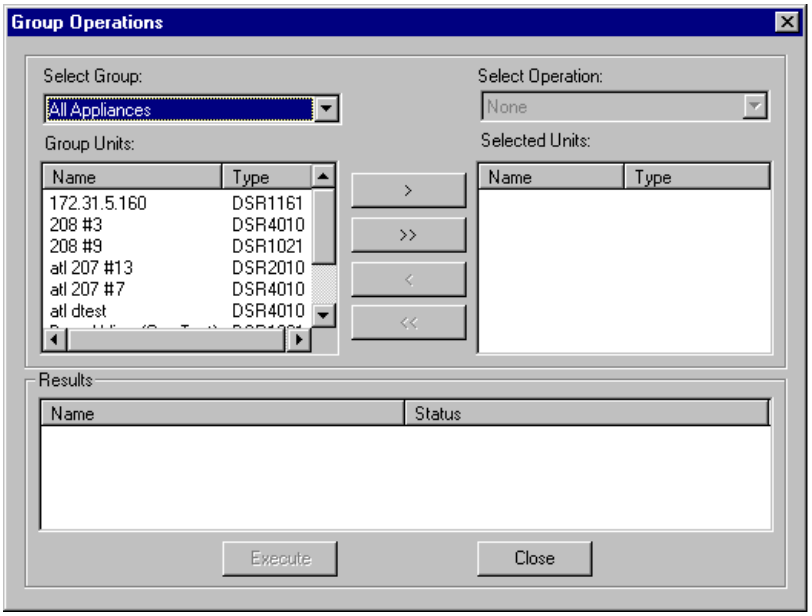


Figure 4.15: Group Operations Dialog Box

NOTE: Some operations may fail if the processed appliance's firmware does not support the operation.

To perform operations on multiple appliances or devices:

1. Select the DS appliance, DSR switch, CPS appliance or EVR1500 environmental monitor, SPC device or group of appliances or devices that you wish to modify from the Select Group drop-down menu. The units to which the operator has access display in the Group Units list.

2. Select one or more appliances or devices and then click the Add button (>). The selected appliances or devices appear in the Selected Units list.

   - or -

   Click the Add All button (>>) to add all appliances or devices.

3. Select an option to perform. If an option cannot be performed on an appliance or device, it will not be available. The options are:
   - Delete - Deletes all appliances, all DS appliances/DSR switches or specific types of DS appliances/DSR switches, all CPS810 appliances and CPS1610 appliances or specific types of CPS appliances, or EVR1500 environmental monitors
   - Reboot - Reboots all appliances, all DS appliances/DSR switches or specific types of DS appliances/DSR switches, or all or specific types of CPS810 appliances and CPS1610 appliances
   - Show Version - Shows the version of all appliances, all DS appliances/DSR switches or specific types of DS appliances/DSR switches, or all or specific types of CPS810 appliances and CPS1610 appliances
   - Disconnect - Disconnects all target devices
   - Power On - Powers up selected SPC device power outlets
   - Power Off - Powers down selected SPC device power outlets
   - Power Reboot - Reboots selected SPC device power outlets
   - Update the DSView Names from Appliance - Retrieves all port and channel names from CPS810 appliances, CPS1610 appliances and DS appliances/DSR switches containing updated firmware, and updates the DSAuth Server database with the port and channel names
4. Click *Execute*. A dialog box will appear and prompt you to confirm the action.
5. No dialog box will appear if you selected *Show Version* or *Power On* in the Select Operation drop-down menu.
6. Click *Yes* to perform the operation on the selected appliances or devices.

   - or -

   Click *No* to cancel the operation.
7. The In Progress dialog box appears and displays overall progress. The Results area of the Group Operations dialog box displays each appliance or device as it is processed. Clicking *Cancel* in the In Progress dialog box will terminate processing after the current appliance or device has been processed.
8. The In Progress dialog box will close when all appliances or devices have been processed and the *Operation Complete* message will appear in the Results area of the Group Operations dialog box.
9. Click *Close* to close the Group Operations dialog box.

Rebooting and Changing Power States

If you have Administrator privileges, you may perform a warm reboot on a DS appliance at a remote location.

To reboot a remote DS appliance:

1. Select the DS appliance in the DSView management software window.
2. Select *Tools - Reboot*.

   - or -

   Right-click and select *Reboot* from the shortcut menu.

   - or -

   Click the *Reboot* toolbar icon.

   A confirmation dialog box will appear.
3. Click *OK* to reboot the remote DS appliance.

Changing the SPC device power state

NOTE: To change the power state of a target device powered by an SPC device, the SPC device must be connected to a CPS810 appliance or CPS1610 appliance. For more information on connecting an SPC device to a CPS appliance, see the SPC Installer/User Guide.

The power state of any device powered by an SPC device outlet may be turned on or off. The SPC device outlet may also be used to reboot a server.

To change the SPC device power state:

1. Load the DSView management software. This will activate the Node Manager and display a list of DS appliances with ports linked to SPC devices that you may access.
2. From the DSView management software window, select a port or channel associated with an SPC device outlet or an unassociated SPC device outlet, then right-click on the item and select *Power State* from the shortcut menu. This will open the Power State dialog box with the current power state of the SPC device outlet selected.

The following items appear in the dialog box when the corresponding conditions occur:

- If the selected port or channel has an associated link to an SPC device outlet or if an unassociated SPC device outlet was selected, its current power state will appear in the dialog box.
- If there is an associated link for the selected port or channel, the name of the outlet(s) will appear in the dialog box.
- If there is an associated server for a selected outlet, the name of the server will appear in the dialog box.

3. Do one of the following:
   - Click *On* to turn the SPC device on.
   - Click *Off* to turn the SPC device off.
   - Click *Reboot* to reboot the SPC device and any attached servers. The SPC device's On or Off state will remain the same as the last time the Power State dialog box was accessed. Clicking *Reboot* on an SPC device outlet that is off will turn the SPC device outlet on immediately. Clicking *Reboot* on an SPC device outlet that is on will turn it off, delay, and then turn the SPC device outlet back on.
4. Click *OK* to perform the selected action and close the Power State dialog box.

NOTE: One DS appliance port may have multiple SPC device ports associated with it. Any on, off or reboot operation you choose to perform to one SPC device port associated to a specific DS port and target server occurs to every SPC device port associated to the DS port and target server.

Managing SPC device power states

Administrators may change the names of outlets on an SPC device, perform multiple operations on outlets of an SPC device and set a minimum and maximum AMP (amplitude) load for an entire SPC device.

NOTE: Changing the name of an SPC device outlet in the Power Management dialog box will also change the name of the SPC device outlet defined on the CPS appliance.

To change the name of an SPC device outlet:

1. In the DSView management software window, right-click on an SPC device and then select the *Power Management* menu item. The Power Management dialog box will appear.
2. Type a new name for each outlet you wish to rename.
3. Click *OK* to save your changes and close the dialog box. A confirmation dialog box displays.
4. Click *Yes* to save your changes.

   - or -

   Click *No* to cancel the operation.

To set AMP loads for an SPC device:

1. In the DSView management software window, right-click on an SPC device and then select the *Power Management* menu item. The Power Management dialog box will appear.
2. Type a minimum threshold load value for the entire SPC device.

   - or -

   Use the slider below the field to select a value.
3. Type a maximum threshold load value for the entire SPC device.

   - or -

   Use the slider below the field to select a value.

4. Click *OK* to save your changes and close the dialog box. A confirmation dialog box displays.
5. Click *Yes* to save your changes.

   - or -

   Click *No* to cancel the operation.

To set the state for outlets on an SPC device:

1. In the DSView management software window topology view, right-click on an SPC device and then select the *Power Management* menu item. The Power Management dialog box will appear.
2. For each SPC device outlet you wish to modify, do one of the following:
   - Click *On* under Status to turn the SPC device outlet on.
   - Click *Off* under Status to turn the SPC device outlet off.
   - Click *Reboot* to reboot the SPC device outlet. If a CPS appliance port is attached to the SPC device or a DS appliance port is attached to the CPS appliance, it will be rebooted also. The SPC device's On or Off state will remain the same as the last time the Power State dialog box was accessed. Clicking *Reboot* on an SPC device outlet that is off will turn the SPC device outlet on immediately. Clicking *Reboot* on an SPC device outlet that is on will turn it off, delay, and then turn the SPC device outlet back on.
   - Click *On* under Wake-up State to wake up the SPC device outlet from its sleep state when meaningful data is detected (such as an Administrator request, or network traffic targeted to a server).
   - Click *Off* under Wake-up State to disable the waking up of the SPC device outlet. The wake-up state indicates the state that the port will go into when the SPC device is powered up during normal operation or when power is restored after an outage. When power is first supplied to the SPC device, all outlets are initially off. The ports are then sequenced on in 2-second increments. Outlets set to a wake-up state of OFF will remain off, while outlets set to a wake-up state of ON will be turned on.
3. Click *OK* to save your changes and close the dialog box. A confirmation dialog box displays.
4. Click *Yes* to perform the specified SPC device operation.

   - or -

   Click *No* to cancel the operation.

Changing the System Settings

Depending on the level of security that you require, certain settings may be configured via the use of the DSView management software Global Settings dialog box. These options may be accessed by selecting the *Options - System Settings* command or clicking the *System Settings* toolbar icon, which displays a dialog box with seven tabs: Connections, Polling, Update, Audit Log, Local Options, Debug and User Names.

Connections tab settings

Changing the Video Viewer window time-out

The DSView management software may be configured to automatically log a DS user out after a specified inactivity period. Use this feature to heighten security or prevent a DS user from blocking access to a channel by forgetting to log out. To change the time-out, select the *Enable* checkbox, then enter the desired inactivity period within the provided field. You may also disable this feature by deselecting the *Enable* checkbox.

Limiting DS user port information

When a DS user attempts to select a channel that is in use, the DSView management software will report who is currently using that channel and offer DS users with administrative rights the option to log the current user out. If the *Administrators only* box is selected, this message will be limited to Administrators; DS users without Administrator access will only receive a message that the port is in use.

Connection sharing

By default, the DS Management Software is set to prompt connected users to allow sharing of their session. When the box marked *Allow Shared Connections Automatically* is checked, sharing will be initiated without a prompt.

Terminating a local port session

The DSView management software may be configured to allow a DS user with Administrator privileges to terminate a local port session. Click *Enable* in the DSR Local Port Session Termination area of the Connections tab to enable this functionality. See *Terminating a target device session* on page 63 for information on terminating a local port session.

Polling tab settings

Port status polling frequency

This option, when enabled, allows Administrators to configure how often the DSAuth Server polls appliances and how often the DSView management software polls the DSAuth Server. Entering a **0** in a field will disable polling on that field.

Update tab settings

DS Management Software suite update

In order to ensure that all DS users have the latest version of the DS Management Software suite, Administrators may specify a system wide software suite version number.

To specify a version number:

1. Enter the desired DSView management software update version in the Update version text box.

2. Enter the IP address of the TFTP server where the update resides.
3. If you wish to make updates mandatory, click the *Update is mandatory* checkbox. If Update is not selected, the DS user must upgrade the DSView management software manually. See Chapter 2 for more information.

   When a DS user with an older version of the DS Management Software suite logs into the system, the user will receive an upgrade prompt. Selecting *Yes* will begin the upgrade process. If the upgrade is mandatory, DS users with older versions of the DS Management Software suite will not be able to access the system until the upgrade is performed.

Audit log tab settings

Automatic creation and deletion of audit logs

Administrators may click *Enable SNMP Trap Log* in the Audit Log tab to allow the DSView system to create a log of SNMP trap information that may be reviewed at a later time.

Administrators may specify the following:

- How long the audit log file is stored before it is deleted. If you do not wish to have log files automatically deleted, enter a **0** in the provided field.
- The community containing the SNMP traps whose information will be written to the audit log.
- The directory where the audit log file is stored (default is root).

NOTE: Allowing log files to build for an extended period may consume a great deal of disk space. Routine deletion is recommended.

NOTE: When changing the location of the Audit log, the Administrator must make sure that the full path chosen exists, is accessible to both the primary and backup DSAuth Servers and is mapped to the same letter for both machines. If the log file is moved to a location other than the local system, both the primary and backup DSAuth Servers will use the same location for the files.

Local Options tab settings

Local Video Session Window Timeout

A local session will time-out if there has been no activity in a Video Viewer window for a specified time. An Administrator may set the session time-out value by selecting the *Connections* tab and specifying a global session time-out setting.

You may override this value within the DSView management software by using a remote session time-out value. If you specify a new time-out value, it will be used the next time the DSView management software is started.

To change the global session time-out setting:

NOTE: You must have Administrator privileges to change the global time-out setting.

1. From the DSView management software menu, select *Options - System Settings*.

   - or -

Click the *System Settings* toolbar icon.

The Global Settings dialog box will appear.

2. Click the *Connections* tab.
3. In the DSView Video Session Window Timeout area, select *Enable*.
4. Type the number of inactivity minutes to wait before the session times out.
5. Click *OK* to save the settings.

To change a remote session time-out value:

1. From the DSView management software menu, select *Options* - *System Settings*.

   - or -

   Click the *System Settings* toolbar icon.

   The Global Settings dialog box will appear.
2. Click the *Local Options* tab.
3. Select one of the following from the Local Options tab:
   - Default System Timeout Values - The global session time-out value set by an Administrator and stored on the DSAuth Server (default).
   - No Timeout - A remote session will never time-out due to inactivity.
   - Timeout Value - A remote session will time-out after the number of minutes of inactivity specified. Type a number from 1-60 in the Minutes field.
4. Click *OK* to save the settings.

Default Video Session Macro Group

The default global macro group used when a server is being viewed in a Video Viewer window may be specified using the Default Video Session Macro Group drop-down menu. See *Global Keyboard Macros* on page 64 for more information on global macros.

Default Local Cursor

The way that the local cursor will display when a server is initially being viewed in a Video Viewer window may be modified using the Local Options tab. You may choose a local cursor by clicking one of the buttons in the Default Local Cursor area, clicking *Default* to use the default DSView management software cursor or selecting *None* if you do not wish to display the local cursor when viewing a target device in a Video Viewer window.

Once a Video Viewer window has been displayed, you may change the local cursor within the Video Viewer window. See *Adjusting Mouse Options* on page 94 for more information.

Debug tab settings

Creating debug log files

NOTE: You may also create files to log information about the primary and secondary DSAuth Servers and ASMP Manager. See *Creating Debug Log Files* on page 21 for more information.

Log files may provide helpful information to assist in debugging your system. Administrators may choose to create the following log files:

- DSView.log - Logs Node Manager window information such as connections to and disconnections from the DSView 3.0 management software server during a DSView session. The DSView.log file is created in the C: directory.
- AcvvWin32Lib.log - Logs information passed through the AcvvWin32Lib.dll during a DSView session, such as typed keyboard inputs sent from the Node Manager window to a server displayed in a Video Viewer window. The AcvvWin32Lib.log file is created in the C: directory.
- Trace.log - Logs Video Viewer window information and is not updated during a DSView session. The Trace.log file is created in the <drive:>/Program Files/Avocent/DSView directory when a DSView session is opened, remains open throughout the DSView session and is overwritten each time the DSView software is restarted.

The DSView.log and AcvvWin32Lib.log files may be deleted at any time during a DSView session by clicking *Clear Log*. You may also specify that DSView.log and AcvvWin32Lib.log files above a particular size will be deleted when a session is closed by clicking *Enable* in the Purge area and typing a file size in the Megabytes field.

To create a debug log file:

1. Click the *Enable* checkbox for the log file you wish to create.
2. Click *OK* to dismiss the dialog box.
3. Close the DSView session.
4. Open a new DSView session. Logging will begin in the log file.

To disable logging within a log file:

1. Clear the *Enable* checkbox of the log file for which you wish to quit logging information.
2. Click *OK* to dismiss the dialog box.
3. Close the DSView session.
4. Open a new DSView session. No further information will be added in the log file.

User Names tab settings

By default, the full names of all DS users in the DSView software system are stored both on the DSAuth Server and in a cached list on the DSAuth Server. Caching provides quick retrieval of full names, which are used to display the names of DS users in the DSView software.

The caching of full names is controlled by selecting the *Use cached value for display of User Full Name* checkbox in the Names tab. You may clear the checkbox to disable caching. If caching is disabled, the DSView software must retrieve the full name for each DS user associated with a node in the DS topology view from the DSAuth Server. When caching is enabled, full names are retrieved from the list on the DSAuth Server.

Clicking *Refresh current User Name list* updates the cached list on the DSAuth Server if a change is made to the full name associated with a DS user's login name. For example, if an Administrator changes the full name of DS user Bill Smith to William Smith, using this option will update the cached list with the new full name information.

Terminating a target device session

If you have Administrator privileges and the target device you are attempting to access is currently being viewed by a local DS user, the DSView management software allows you to disconnect the local DS user so that you may access that target device. To terminate a local DS user's session, you must first specify the ability to do so by selecting the *Enable* checkbox in the Connections tab of the DSView management software Global Settings dialog box.

When you choose to terminate a local DS user's connection, a dialog box will display prompting you to confirm the termination. The local DS user will receive a notification message when you click *Yes* in the dialog box. Control of the port is then transferred to you.

Administrators may also disconnect a DS user or CPS appliance connected using the Telnet application by choosing the port that the user is accessing and selecting *Tools - Disconnect*, or by right-clicking on the port and selecting *Disconnect* in the DSAuth software window.

NOTE: You cannot preempt a local user that is in Broadcast mode. See the DSR Installer/User Guide for additional information.

To specify settings to terminate the local DS user session:

1. From the DSView management software menu, select *Options - System Settings*.

   - or -

   Click the *System Settings* toolbar icon.

   The Global Settings dialog box will appear.
2. Select the *Connections* tab.
3. Select the *DSR Local Port Session Termination Enable* checkbox in the area.
4. Click *OK* to save your settings and close the dialog box.

To terminate the current DS user session:

1. Select a port in the DSView management software window.
2. Select *Tools - Disconnect*.

   - or -

   Right-click and select *Disconnect* from the shortcut menu.

   - or -

   Click the *Disconnect* toolbar icon.
3. A dialog box will appear prompting you to confirm the termination of the current DS user connection.
4. Click *Disconnect.* A dialog box displays prompting you to confirm the termination of the DS user session. Click *OK*. The current DS user will then receive a notification message.

To terminate a CPS appliance Telnet application connection:

1. Select a port in the DSView management software window.
2. Select *Tools - Disconnect*.

   - or -

   Right-click and select *Disconnect* from the shortcut menu.

   - or -

   Click the *Disconnect* toolbar icon.
3. If the CPS appliance is connected using the Telnet application, a dialog box appears prompting you to terminate the current connection. Click *Yes*.
4. Another dialog box will appear prompting you to confirm the termination of the connection.
5. Click *Yes*. A dialog box displays prompting you to confirm the termination of the DS user session.
6. Click *OK*. You will receive a notification message. Click *OK* to dismiss the message.

Global Keyboard Macros

Since the DSView management software runs on a PC, certain commands must be sent to the controlled target device via keyboard macros. For example, pressing **Ctrl+Alt+Delete** on your keyboard would reset the PC running the DSView management software rather than resetting the target device. To reset the target device, a macro is needed. Two kinds of macros are available in the DS Management Software suite: Local Macros and Global Macros.

Local Macros may be created and accessed on the local computer using the Video Viewer window. Local Macros may be customized and grouped in any manner you wish. See Chapter 6 for more information on Local Macros.

Your DS Management Software suite is delivered with a number of pre-configured Global Macro sequences for ease of operation. New Global Macros may also be created and maintained by DS

users with Administrator privileges using the DSView management software. They are stored on the DSAuth Server and any specified backup servers and may be selected for use within the DSView management software. Global Macros cannot be modified by non-administrative DS users.

When a session is started in the DSView management software, Global Macros are retrieved from the DSAuth Server. Then, when a Video Viewer window session is started, the Global Macros are loaded as well as the local ones. A DS user may choose to use either Local Macros or Global Macros and switch between using them at any time during the session using the *Tools - Session Options* command in the Video Viewer window and then selecting the *Macros* tab in the Session Options dialog box. If Local Macros are chosen, the macros stored on the local computer will be used.

To access Global Macros:

From the DSView management software window, select the *Options - Keyboard Macros* command or click *Keyboard Macros* in the toolbar icon. The Keyboard Macro Configuration dialog box displays, containing a list of global programmed macros. Each programmed macro will have a checkbox by it.

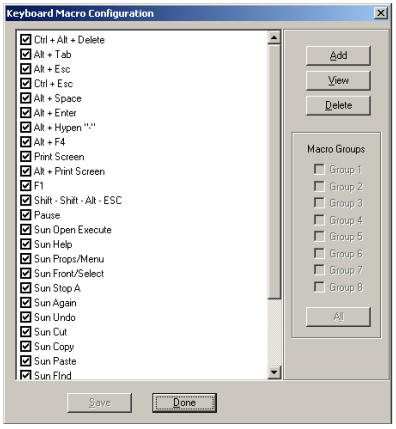


Figure 4.16: Keyboard Macro Configuration Dialog Box

Programming a global keyboard macro

If you require a key sequence that is not pre-programmed into the DS appliance/DSR switch, you may add a Global Macro by performing the following steps.

To add a Global Macro:

1. From the DSView management software window, select *Options* - *Keyboard Macros*.

   - or -

   Click the *Keyboard Macros* toolbar icon.
2. The Keyboard Macro Configuration dialog box will appear.
3. Click on the *Add* button in the upper right-hand corner.
4. The Add Keyboard Macro dialog box will appear.
5. Enter a unique description for the Global Macro in the Macro Description field.
6. In the Double-click for Key Press list, double-click the first keystroke of your macro. This will move the keystroke to the Double-click for Key Release list. Keystrokes may be removed from the list by clicking the *Remove* button below the list.
7. If this key needs to be released before the next keystroke is entered, double-click the keystroke in the Double-click for Key Release list to move it to the Macro Created list. If not, leave this key in the Double-click for Key Release list at this time. Repeat this step with your next keystroke. When you have no further keystrokes, proceed to step 7.
8. Now, double-click on the remaining commands, if any, under the Double-click for Key Release list in the order in which you'd like them released to move them to the Macro Created list. The Macro Created list will now show the key sequence in the exact order that it will be performed by the system. There should be no keys remaining in the Double-click for Key Release list. Macros may be removed from the list by clicking the *Remove* button below the list. The order of created macros may be changed by selecting a macro and clicking the *Up Arrow* to move the macro up one level or the *Down Arrow* to move the macro down one level.
9. Click the *OK* button to save the Global Macro to the DSAuth Server and any defined backup servers.

The macro will now appear in the macro list and also in the macro commands on every Node Manager window when *Tools* - *Keyboard* - *Global Macros* is selected in the DSView management software window.

Example: To create a macro where the Ctrl key is held while F1-F2-F3 are typed:

1. Enter a name for the macro. In this case, **Ctrl-F1-F2-F3**.

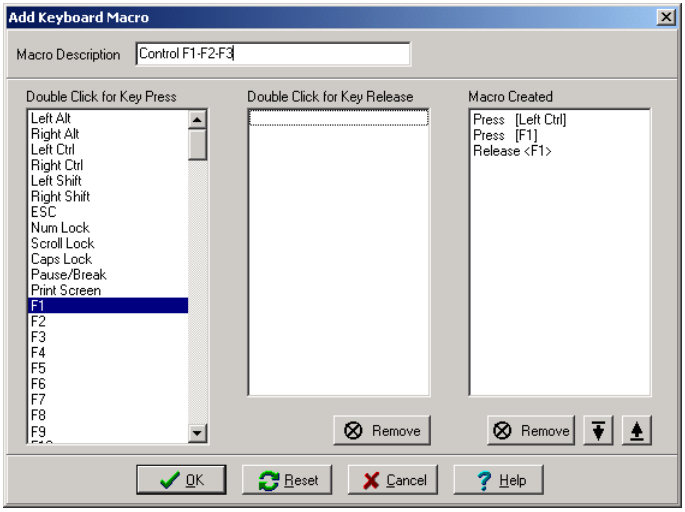


Figure 4.17: Entering the Macro Name

2. The **Ctrl** key is pressed first and held, so double-click on the *Left* or *Right Ctrl* key under Double-click for Key Press. It will move to the second list and the Press [Left Ctrl] command will appear in the third list.
3. **F1**, **F2** and **F3** are pressed and released in order. Locate *F1* in the Double-click for Key Press list and double-click it. It will move to the second list and the Press [F1] command will appear in the third list.
4. **F1** will be released before **F2** is pressed, so you will need to double-click on *F1* under the Double-click for Key Release list before proceeding. This will create a Release <F1> command in the Macro Created list and F1 will disappear from the second list.

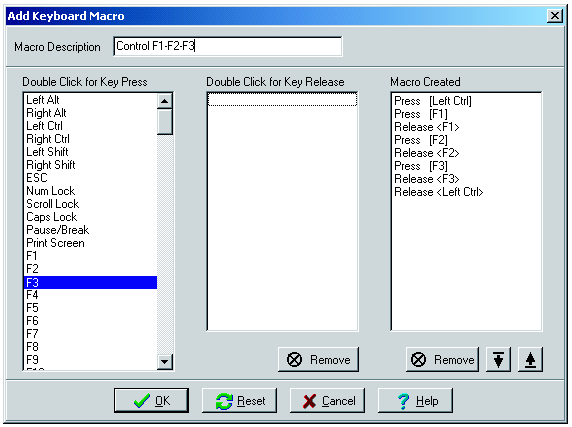


Figure 4.18: Macros Appearing in the Third List

5. Repeat steps 3 and 4 with **F2** and **F3**.
6. The last step is to release the **Ctrl** key. Double-click on *Left Ctrl* in the middle list. The Release [Left Ctrl] command will appear in the third list.

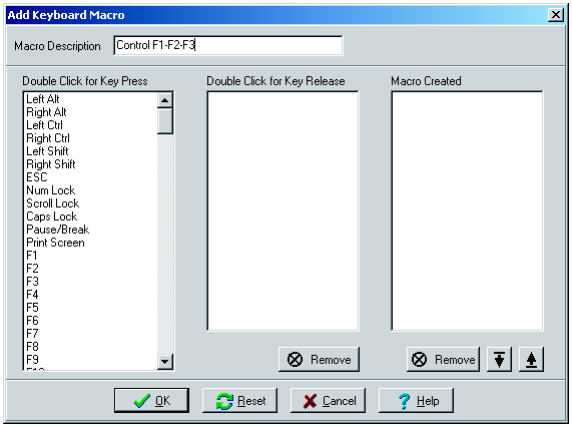


Figure 4.19: The Completed Macro

7. The keystrokes will be listed in correct order in the third list. Click *OK* to accept the macro if you are creating a Local Macro, or *Save* if you are creating a Global Macro.

To delete a global keyboard macro:

1. From the DSView management software window, select *Options* - *Keyboard Macros*. The Keyboard Macro Configuration dialog box will appear.
2. Select a macro from the list.

3. Click the *Delete* button.
4. Click *Done* to save your changes.

   - or -

   Click *Cancel* to reject deletion of the macro.

NOTE: You may also delete a global keyboard macro from the DSView management software window if Global Macros have been enabled using the DSView management software window *Tools - Keyboard - Global Macros* command.

Macro groups

Since the DSView management software may be used to access different computer platforms, users may find it helpful to assign distinct macro groups to Global Macros or Local Macros on individual systems. You may select the particular macro group that you wish to use from the Video Viewer window.

Once a macro group is created, it can be selected using the *Keyboard - Toolbar Macro Set* command in the Video Session window.

NOTE: Macros groups may also be created and macros may be grouped using the Video Viewer window. See Chapter 6 for information on Local Macros.

To create a Global Macro group:

NOTE: You may specify the default global macro group used when a server is being viewed in a Video Viewer window. See *Changing the System Settings* on page 58 for more information.

1. From a DSView management software window, select *Options - Keyboard Macros* to activate the Keyboard Macro Configuration dialog box to group Global Macros.
2. The dialog box's Macro Groups list contains eight macro groups available for configuration.

To assign a Global Macro to a group:

1. Click on the macro name.
2. In the box labeled Macro Groups, select the groups to which you'd like to have the macro assigned.

Exporting Topology Data

Topology data may be exported from the DSView management software into a comma separated value (.csv) file. Information on all appliances, ports and channels may be exported. The .csv file may be viewed in a text editor or spreadsheet application, such as Microsoft Excel.

The following fields, defined by selecting the *Edit - Properties* command, right-clicking and selecting *Properties* from the pop-up menu or clicking the *Properties* toolbar icon, are exported for each appliance:

- Appliance Name
- Appliance Type
- Appliance IP Address
- Appliance Version
- Accounting Information
- Description
- First Emergency Contact Name
- First Emergency Contact Phone
- Second Emergency Contact Name
- Second Emergency Contact Phone

The following fields may be optionally exported for all ports and channels on each appliance:

- Port/channel names for appliance
- Port/channel types for appliance
- Port/channel Name
- Port/channel Type
- Accounting Information
- Description
- First Emergency Contact Name
- First Emergency Contact Phone
- Second Emergency Contact Name
- Second Emergency Contact Phone

To export topology data:

1. From the DSView management software window, select *File - Export Data*. The Export Topology Data dialog box will appear.

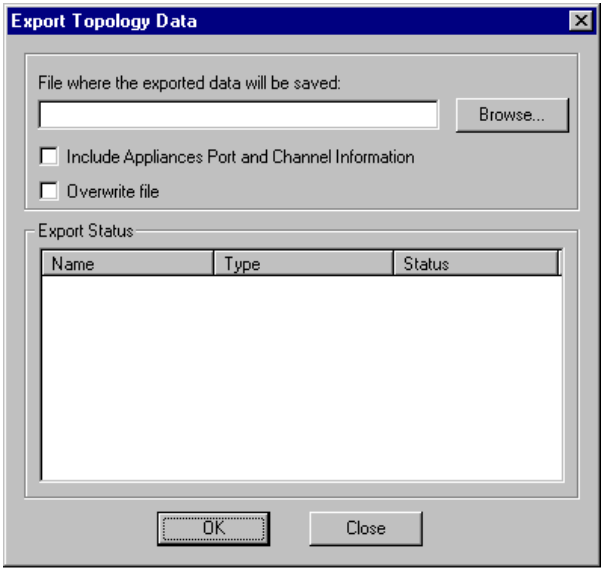


Figure 4.20: Export Topology Data Dialog Box

2. If you wish, specify a pathname and filename for the .csv file.

   - or -

   If you have previously created a .csv file, you may select *Overwrite file*.
3. Select the *Include Appliances Port and Channel Information* checkbox to add port/channel names and types to the .csv file.
4. Click *OK* to create the .csv file. The progress of the export will appear in the Export Status area and a message box will appear when the export is completed.
5. Click *OK* to dismiss the message box and click *Close* to dismiss the dialog box.

CHAPTER 5

DSWebview Browser-Based Software

About the DSWebview Software

Most of the DS Management Software suite functions can be performed through the World Wide Web using the DSWebview Server. The DSWebview Server allows DS users access from a web browser using a Video Session window running as a Java™ applet and provides secure, browser-based access to virtually any data center device.

The DSWebview brower-based software provides a HyperText Transfer Protocol, Secure (HTTPS) version of the DS Management Software Node Manager to a browser Client via Active Server Pages (ASPs). Remote KVM and serial Video Session windows may be launched from the ASP Node Manager via Java applets.

DSWebview Software Components

The DSWebview software is comprised of the following major components that reside on the IIS web server:

- Web Pages - ASPs are provided for functions such as user login, display of server lists and session launching.
- DSAuth Proxy Server - This component serves as a relay between the web browser and the DSAuth Server.
- DS appliance proxy (DSInterface component) - This component serves as a relay between the web browser and a DS appliance, such as a DS1800 switch, DSR switch or CPS serial over IP network appliance.
- Applets - Video and Telnet application viewer applets are installed on the web server so they can be uploaded to browser clients as needed.

Figure 5.1 illustrates the components of the DSWebview software. DS appliance configuration is accomplished through the DSView management software window; a web component is not provided for this purpose.

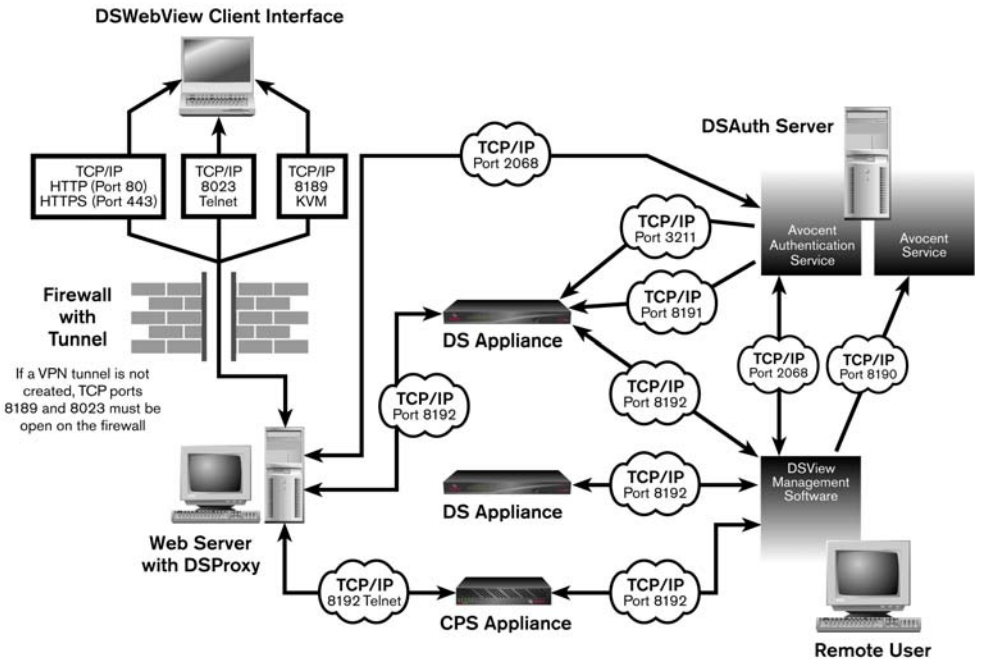


Figure 5.1: DSWebview Software Components

Active Server Pages (ASPs)

The DSWebview Client Node Manager runs within a web browser and provides both DS topology and server views. This functionality is provided by an ASP and uses the DSInterface component's COM component to communicate with the DSAuth Server.

The topology view is not available when using the DSWebview Client with a Netscape browser.

The Node Manager indicates in the DS topology view/server view which ports are active, idle, not powered or blocked. The DS user may instruct the Node Manager to refresh the DS topology view/server view with the latest connection status from the DSAuth Server. The Port Status will NOT be updated automatically as the current DSView management software window is.

DSAuth Proxy Server

A DSAuth Proxy Server is included to allow the Video Viewer window and Telnet application Client interface the ability to make the connection to a DS appliance over TCP port 8192. The messages received from the Video Viewer window applet are forwarded by the DSAuth Proxy Server to the DS appliance and vice versa. The DSAuth Proxy Server must run on the web server that is serving the DSWebview Client. The web server must have the Java runtime version 1.3.1 or later to perform the proxy function.

DS appliance proxy (DSInterface component)

The DSInterface component contains all necessary calls to allow communication between the ASPs and the DSAuth Server. This is a COM component, which must reside on the web server that is serving the DSWebview software ASPs.

The DSAuth Server may or may not be running on the web server.

If the DSAuth software is located on the internal private network, the web server will require access to both the public Internet and private corporate network.

Telnet application applet

The Telnet application component is incorporated into a Java applet providing DS users with the ability to launch a Telnet application session from a web browser. The Java applet, running in the web browser, will communicate through a DSAuth Proxy Server to the other DS appliances. Communicating through the proxy allows the appliance to be located on the internal private network.

As an alternative to the web proxy, it is possible to provide the DS appliances and DSAuth Server a static public IP address and the applet will communicate directly to the DS appliance.

The DSWebview Client requires a Java runtime version of 1.4.x or later. This applet is signed, giving it flexibility to support features like full screen, trace logging and so on.

Video Viewer window applet

The Video Viewer window component is incorporated into a Java applet providing DS users with the ability to launch a remote session from a web browser. The Java applet, running in the web browser, will communicate through a DSAuth Proxy Server to the appliance. Communicating through the proxy allows the appliance to be located on the internal private network.

DS appliances and the DSAuth Server must typically be on the same domain or same side of a firewall to communicate with each other. However, a DS appliance and the DSAuth Server may be given a static public IP address if the appliance and Client browser communicate with each other via their IP address. This method uses the applet to communicate directly to the DS appliance and is an alternative to using the web proxy.

The DSWebview Client requires a Java runtime version of 1.4.x or later. This applet is signed, giving it flexibility to support features like full screen, trace logging and so on.

The Java Video Viewer window component requires a Java runtime version of 1.4.x or later and supports connections to DS appliances using firmware version 1.0.0.105b or later.

DS Security

Depending on the web server configuration, the DSWebview software may either use HTTP (HyperText Transer Protocol) or HTTPS for communication between the browser and web interface component.

Communication between the web server and the DS Management Software environment follows the same security practices as the DSView management software window architecture. The Node Manager, running in the web browser, retrieves the node list from the DSAuth Server via the Security Support Provider Interface (SSPI). The Video Viewer window applet exchanges token information, via the DSAuth Server, identically to the DSView management software window security infrastructure.

TCP Ports

In addition to the HTTP port, the session viewer applets require TCP ports to communicate with a proxy that runs on the web server. There are two ports for this purpose. The first is 8189, which is used to access the KVM proxy. The second is 8023, which is used to access the Telnet application proxy. If the Telnet application is not required, then 8191 is the only port needed.

To minimize potential TCP port conflicts or security issues, it is possible to reconfigure the KVM and serial ports used by the proxy. In this manner, customers may choose the port with which they feel most comfortable.

Configuring the DSWebview software TCP ports for external access

If external access to the DSWebview software is desired, the following firewall ports must be opened.

Table 5.1: DSWebview Software TCP Ports

Port	Application
Port 80	HTTP (not necessary if you are using HTTPS)
Port 443	HTTPS (not necessary if you are using HTTP)
Port 8023	Telnet application proxy (only necessary if you are using the Telnet application)
Port 8189	KVM proxy
Port 8191	DSAuth Server (not necessary if DSAuth Server and the appliance are on the same side of the firewall)

NOTE: You will need to provide DSWebview software users with the server IP address where the DSWebview software is installed.

NOTE: The DSProxy component must be installed on the same computer as the web server.

Window Features

The DSWebview software consists of a Node Manager and a Video Viewer window. When you launch the DSWebview software, the Node Manager appears. The Node Manager allows you to view, access, manage and create custom groupings for all of the supported DS and CPS appliances, EVR1500 environmental monitor and control appliances, SPC power control devices and generic appliances in your data center.

You can place your cursor over a port and select *Connect* from the floating option menu in the Node Manager to launch a Video Viewer window. The Video Viewer window allows you to control the keyboard, monitor and mouse functions of individual servers.

The DSWebview software also contains drop-down menus and floating option menus. The drop-down menus contain many of the commands available in the DSView management software window. A floating option menu appears when the cursor is placed over an item in the DSWebview software window.

Figure 5.2 shows the DSWebview Client interface window areas, and descriptions are listed in Table 5.2.

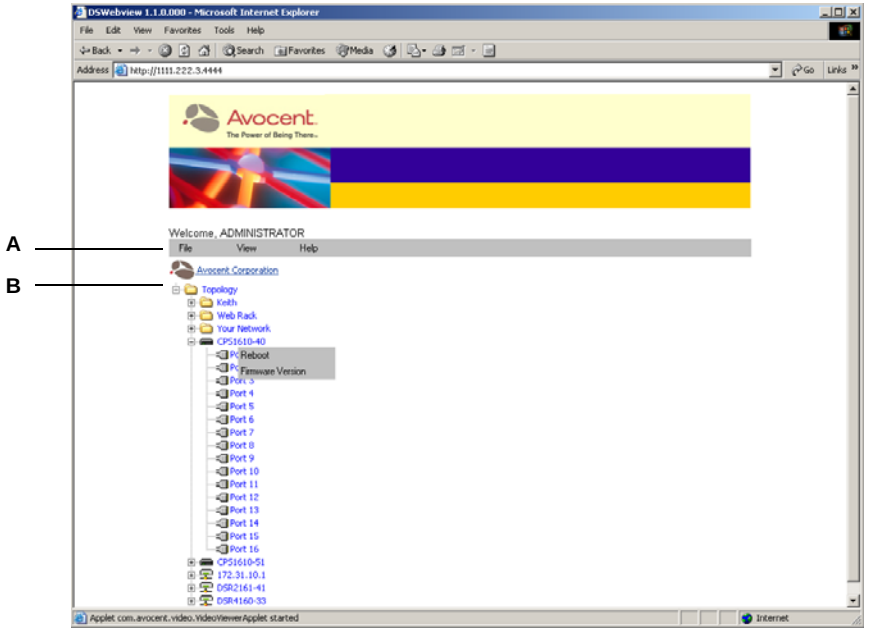


Figure 5.2: DSWebview Client Interface Window

Table 5.2: DSWebview Client Interface Window Descriptions

Letter	Description
A	Menu bar: Allows you to access many of the features in the Video Viewer window.
B	Root node: Each tree consists of a root node and branches.

Launching the DSWebview Software

This section describes how to launch the DSWebview software so that you may begin using it to manage DS appliances and target devices.

NOTE: A warning message will appear and some software features may not be available if the version numbers of the DSView management software and DSAuth Server software are not compatible. This occurs when the DSView management software is launched. If the warning message appears, you may wish to upgrade either the DSView management software or DSAuth Server software. See Chapter 2 for information on software installation.

To access a DSWebview Server via the web:

1. Within your web browser, enter the address for the DSWebview Server.
2. When the login screen appears, enter your login name, password, authentication server and domain name (when applicable). This information is available from your network Administrator.

NOTE: Browser cookies must be enabled and the user must accept certificates for access. The Java runtime plug-in must be enabled for the browser being used for the DSWebview software interface.

3. When you are logged in, the web page displays.

Accessing Target Devices

You may access one or more target devices within a DS series appliance at the same time. To access multiple target devices, place your cursor over a port and select *Connect* from the floating option menu for every port that you wish to display. Windows may be tiled or cascaded as you choose.

NOTE: A message box will display if an attempt is made to open a Video Viewer window while the DSRIQ module attached to the port is being FLASH upgraded.

NOTE: When tiling windows from the Node Manager, each remote session must be in Full Scale mode in order for windows to tile properly. By default, the scaling mode is specified as Auto Scale. To change the scaling mode, select *View - Scaling - Full Scale* in the Video Viewer window.

To access a target device:

1. Load the DSWebview software. This will display the Node Manager and provide you with a list of target devices that you may access.
2. Place your cursor over the target device that you wish to access and select *Connect* from the floating option menu. This will open a Video Viewer window and allow the DS user control of the target device.

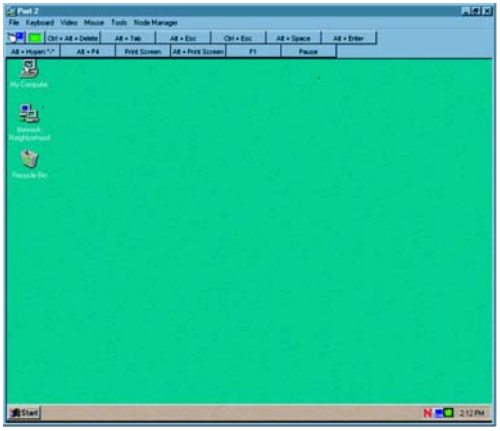


Figure 5.3: The Video Viewer Window

Accessing EVR1500 environmental monitors

An EVR1500 environmental monitor is a network-based appliance that monitors environmental conditions within the rack and/or data center and reports the data using the DSWebview software browser. Environmental thresholds, such as alarm conditions, can be specified.

If the EVR1500 environmental monitor is attached to a CPS810 appliance or CPS1610 appliance, it can be remotely powered up, powered down or rebooted using an SPC device. See Chapter 4 for more information. See the EVR1500 Installer/User Guide for more information on using an EVR1500 environmental monitor.

To launch an EVR1500 environmental monitor session:

1. Load the DSWebview software. This will activate the Node Manager and provide you with a list of servers and serial devices that you may access.
2. Place your cursor over the EVR1500 environmental monitor that you wish to access and select *Connect* from the floating option menu. The system is connected to the EVR1500 environmental monitor and will open a web browser interface.

NOTE: Browser cookies must be enabled and the user must accept certificates for access. The Java runtime plug-in must be enabled for the browser being used for the EVR1500 environmental monitor interface.

3. When the login screen appears, enter your login name, password, DSAuth Server and domain name (when applicable). This information is available from your network Administrator.

Using Privacy mode

If a DS user needs to access a port while excluding all others, Privacy mode is used. When a port is selected in Privacy mode, no other DS user in the system may switch to that port. If another DS user initiates a connection to a port currently in Privacy mode, that user will receive a message indicating the port's status and will not be connected to the port.

To access a target device in Privacy mode:

1. Load the DSWebview software. This will display the Node Manager and provide you with a list of target devices that you may access.
2. Place your cursor over the target device that you wish to access and select *Private Connect* from the floating option menu.

Sharing a Device Session

When you attempt to access a port already in use, you will receive a notification message that the port is in use along with the name of the current DS user(s). At this point, you may request to share access to the port with the current DS user(s). The DS users that are currently active will receive a request to allow sharing. If they confirm, the new DS user will gain access to the port. When sharing access to a port, all DS users may monitor the port and may take control if no other DS user is currently active.

When you attempt to connect to a port using the DSWebview software, the DSWebview Connection Sharing dialog box displays. If you click *Stealth Connection*, a video session is started but you will only be able to view what occurs on the server and be unable to control the keyboard or mouse. The DS user that is currently active will not receive notification that access is being shared and no request to authorize sharing will be made.

NOTE: The only way to prevent a stealth connection to a port is by enabling Privacy mode.

Up to 12 DS users may share a single port at one time. If a 13th DS user attempts to connect, an error message will inform the DS user that no sessions are available. Administrators will be given the option of terminating a DS user session.

At any time, a DS user may select *View - List of Shared Users* in a Video Viewer window to view a list of DS users sharing their port or channel. DS users in Stealth mode are excluded from this list.

Session time-out

A remote session will time-out if there has been no activity in a Session window for a specified time. The session time-out value is configured by your Administrator by selecting *Options - System Settings* in the DSView management software window or clicking the *System Settings* toolbar icon.

You may override this value within the DSView management software window. If you specify a new time-out value, it will be used the next time the DSView management software is started. See *Sharing a Device Session* on page 80 for more information.

Rebooting and Changing Power States

If you have Administrator privileges, you may perform a warm reboot on a DS appliance at a remote location.

To reboot a remote DS appliance:

1. Place your cursor over the DS appliance in the DSWebview software window and then select *Reboot* from the floating option menu.

   A confirmation dialog box will appear.
2. Click *OK* to reboot the remote DS appliance.

Changing the SPC device power state

NOTE: To change the power state of a target device powered by an SPC device, the SPC device must be connected to a CPS810 appliance or CPS1610 appliance. For more information on connecting an SPC device to a CPS appliance, see the SPC Installer/User Guide.

The power state of either a particular server, SPC device, CPS appliance, EVR1500 environmental monitor or generic appliance powered by an SPC device may be turned on or off. The SPC device may also be used to reboot a server.

To change the SPC device power state:

1. Load the DSWebview software. This will activate the Node Manager and display a list of DS appliances with ports linked to SPC devices that you may access.
2. From the DSWebview software window, place your cursor over an SPC device, then select *Power State* from the floating option menu. This will open up the Status: <current power state> dialog box.
3. Do one of the following:
   - Click *On* to turn the SPC device on.
   - Click *Off* to turn the SPC device off.
   - Click *Reboot* to reboot the SPC device and any attached servers. The SPC device On or Off state will remain the same as the last time the Power State dialog box was accessed.
4. A confirmation dialog box displays. Click *Yes* to perform the selected action.

NOTE: One DS port may have multiple SPC device ports associated with it. Any on, off or reboot operation you choose to perform to one SPC device port associated to a specific DS port and target server occurs to every SPC device port associated to the DS port and target server.

Terminating a Target Device Session

If you have Administrator privileges and the target device you are attempting to access is currently being viewed by a local DS user, the DSWebview software allows you to disconnect the local DS user so that you may access that target device. To terminate a local DS user's session, you must first specify the ability to do so in DSView management software Global Settings dialog box.

When you choose to terminate a local DS user's connection, a dialog box will display prompting you to confirm the termination. The local DS user will receive a notification message when you click *Yes* in the dialog box. Control of the port is then transferred to you.

Administrators may also disconnect a DS user or CPS appliance connected using the Telnet application.

NOTE: You cannot preempt a local user that is in Broadcast mode. See the DSR Installer/User Guide for additional information.

To terminate the current DS user session using the Disconnect command:

1. Place your cursor over a port in the DSWebview window and select *Disconnect* from the floating option menu. A dialog box will appear prompting you to confirm the termination of the current DS user connection.
2. Click *Disconnect*. A dialog box displays prompting you to confirm the termination of the DS user session. Click *OK*. The current DS user will then receive a notification message.

To terminate a CPS appliance Telnet application connection using the Disconnect command:

1. Place your cursor over a port in the DSWebview window and select *Disconnect* from the floating option menu. If the CPS appliance port is not connected using the Telnet application, the port cannot be disconnected and a message box appears. Click *OK*.

   - or -

   If the CPS appliance is connected using the Telnet application, a dialog box appears prompting you to terminate the current connection. Click *Yes*.
2. Another dialog box will appear prompting you to confirm the termination of the connection.
3. Click *Yes*. A dialog box displays prompting you to confirm the termination of the DS user session.
4. Click *OK*. You will receive a notification message. Click *OK* to dismiss the message.

To terminate a DSR switch local port session:

NOTE: To terminate a local port session, the Enable checkbox must have been selected in the DSView management software System Settings and the user terminating the session must have Administrator privileges.

1. Select a port on a DSR switch.
2. From the DSView management software window, select *Tools - Disconnect*.

   - or -

   Right-click and select *Disconnect* from the shortcut menu.
3. Place your cursor over a port in the DSWebview software window and select *Disconnect* from the floating option menu.

   A dialog box will appear prompting you to disconnect the local port session.
4. Click *Disconnect.* Another dialog box will appear prompting for verification that the current connection should be terminated.
5. Click *Yes* to terminate the local port session.

Displaying Firmware Version Information

You may display the version number of the firmware on DS appliance/DSR switches, CPS810 appliances or CPS1610 appliances. This information facilitates system troubleshooting and support. For optimum performance, keep your firmware current.

To display firmware version information:

1. From the DSWebview software window, place your cursor over a DS appliance/DSR switch, CPS810 appliance or CPS1610 appliance and select *Firmware Version* from the floating option menu.

   A message box will appear containing the version number of the appliance.
2. Click *OK* to dismiss the dialog box.

CHAPTER 6

Video Viewer Window

About the Video Viewer Window

The Video Viewer window is a Java-based program that may be run in any of the following ways:

- By double-clicking an appliance port within the DSView management software window
- By selecting and right-clicking a port and then selecting *Connect* from the shortcut menu within the DSView management software window
- By clicking an appliance port hyperlink within a DSWebview software window
- By placing your cursor over a port and selecting *Connect* from the floating option menu within a DSWebview software window

When you connect to a device using the Video Viewer window, the device's desktop appears in a separate Video Viewer window. You will see both the local and the device's cursor. The Video Viewer window supports either a 3- or 5-button mouse.

NOTE: The DS Management Software suite uses system memory to store and display images within Video Viewer windows. Each opened Video Viewer window requires additional system memory. An 8-bit color setting on the Client PC requires 1.4 MB of memory per Video Viewer window, a 16-bit color setting requires 2.4 MB and a 32-bit color setting requires 6.8 MB. Opening more than four simultaneous Video Viewer windows may affect system performance and is not recommended. If you attempt to open more Video Viewer windows than your system memory allows, you will receive an out of memory error and the requested Video Viewer window will not open.

From this window, you will be able to operate a device as if you were sitting in front of it. You may also perform viewer-specific tasks such as sending macro commands to the device.

The Video Viewer window may be launched to devices from any DS appliance/DSR switch. The Video Viewer window session will be established using the encryption level specified by the Administrator in the Properties dialog box. See Chapter 4 for more information.

If the device you are attempting to access is currently being viewed by the local user and you have Administrator privileges, you may disconnect the local user so that you may access that device.

NOTE: You cannot preempt a local user who is in Broadcast mode. See the DSR Installer/User Guide for additional information.

Video Viewer window minimum requirements

The Video Viewer window requires one of the following:

- Windows 2000 Workstation or Server with Service Pack 2
- Window NT 4.0 Workstation or Server with Service Pack 6a
- Windows XP Home Edition or Professional
- Red Hat® Linux® 7.2, 7.3, 8.0 or 9.0 with 2.4 Kernel (supported in the DSWebview software only)

To access the Video Viewer window:

In the DSView management software window, double-click on a port.

- or -

Click an appliance port hyperlink.

- or -

Select a port and then right-click and select *Connect* from the shortcut menu.

- or -

In the DSWebView software, place your cursor over a port and select *Connect* from the floating option menu.

The Viewer launches in a new window.

To preempt the local user:

1. In the DSView management software window, select a port and then right-click and select *Disconnect* from the shortcut menu.

   - or -

   In a DSWebview software window, place your cursor over a port and select *Disconnect* from the floating option menu.
2. A message will prompt you to terminate the local user's session (if you have appropriate access rights) when the local user is viewing this device.
3. Click *Yes* to terminate the local user's connection. The local user will receive a notification message. The Video Viewer window launches.

   - or -

   Click *No* to allow the local user to retain the connection.

To close a Video Viewer window session:

Select *File - Exit* from the Video Viewer window.

Window Features

Figure 6.1 shows the Video Viewer window areas, and descriptions follow in Table 6.1.

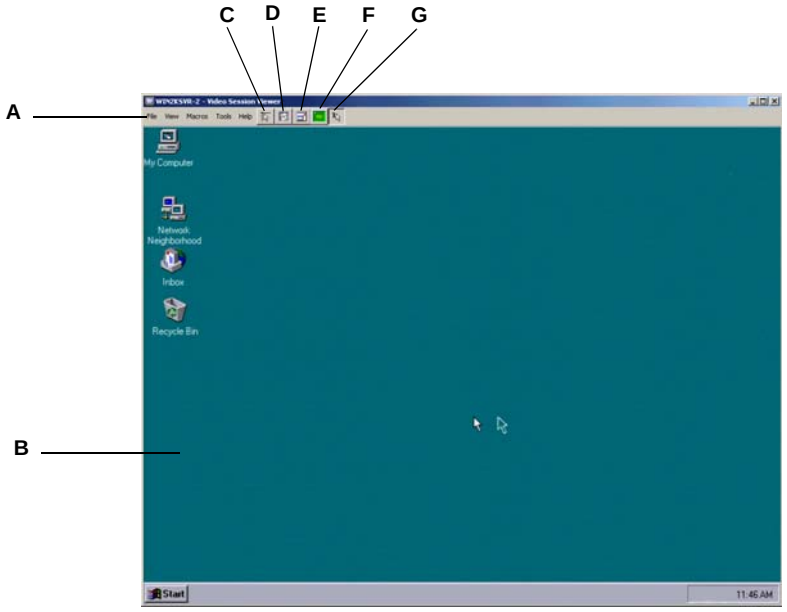


Figure 6.1: Video Viewer Window

Table 6.1: Video Viewer Window Descriptions

Letter	Description
A	Menu and toolbar: Allows you to access many of the features in the Video Viewer window.
B	Accessed device desktop: Interacts with your device through this window.
C	Align Local Cursor button: Re-establishes proper tracking of the local cursor to the remote device cursor.
D	Refresh Image button: Regenerates the digitized video image of the device desktop.
E	Full Screen Mode button: Expands the accessed device desktop to fill the entire screen. When you expand the window, the menu bar is replaced with a floating palette containing four buttons (Align Local Cursor, Refresh Video, Full Screen Mode and Single Cursor Mode), the Macros menu and the device name.
F	Automatic Video Adjustment button: Optimizes the display of the Video Viewer window.
G	Single Cursor Mode button: Toggles Single Cursor mode on or off.

See the DSR Installer/User Guide for information about how the keys on a standard Type 5 Sun keyboard are emulated on a PS/2 keyboard.

Setting the Window Size

When the DSView management software is used for the first time, any Video Viewer windows that are opened from a DS appliance/DSR switch port or channel in any DSView management software sessions will display at a resolution of 1024 x 768 until the value is changed by a DS user. Each Video Viewer window may be set to a different resolution.

The DSView management software will automatically adjust the display if the window size changes during a session as long as autoscaling is enabled. When a DS user accesses a channel via sharing, the display will be adjusted to match the input resolution of the first DS user to access that channel. This will prevent the first DS user's display from being affected. If the target device's resolution changes any time during a session, the display will be adjusted automatically.

To change the Video Viewer window resolution:

Select the *View - Scaling* command and then click on the desired resolution.

Adjusting the View

Using menus or Task buttons in the Video Viewer window, you may:

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable Full Screen mode.
- Enable automatic or manual scaling of the session image. With automatic scaling, the desktop window remains fixed and the device image is scaled to fit the window. With manual scaling, a drop-down menu of supported image scaling resolutions is displayed.
- Specify the connection speed to the appliance. This value is used to throttle the video stream based on the available bandwidth, which allows the system to optimize its operation.
- Changing the color of depth compression of the session image (DSR switches with Dambrackas Video Compression™ (DVC) algorithm upgrade only).

NOTE: The DVC algorithm upgrade is standard on all newer DS appliances/DSR switches. Older DS appliances/DSR switches use standard video compression with 8-bit color depth (256 colors). For DVC algorithm upgrade purchase information, contact Avocent Technical Support or your Avocent reseller.

To align the mouse cursors:

Click the *Align Local Cursor* button in the Video Viewer window toolbar. The local cursor will align with the cursor on the remote device.

If cursors drift out of alignment, turn off mouse acceleration in the device.

To refresh the screen:

Click the *Refresh Image* button in the Video Viewer window toolbar.

- or -

Select *View - Refresh* from the Video Viewer window menu. The digitized video image will be completely regenerated.

To enable or disable Full Screen mode:

1. To enable Full Screen mode, click the *Full Screen Mode* button.

   - or -

   Select *View - Full Screen* from the Video Viewer window menu.

   The desktop window will disappear and only the accessed device desktop will be visible. The screen will be resized up to a maximum of 1024 x 768. If the desktop has a higher resolution, then a black background will surround the full screen image. The floating toolbar will appear.
2. To disable Full Screen mode, click the *Full Screen Mode* button on the floating toolbar to return to the desktop window.

NOTE: Full Screen mode cannot be enabled if the Video Viewer window is being accessed during a shared session.

To enable automatic or manual scaling:

To enable automatic scaling, select *View - Scaling* from the Video Viewer window menu. The device image will be scaled automatically.

- or -

To enable manual scaling, select *View - Scaling* from the Video Viewer window menu, then choose the dimension to scale the window. Available manual scaling sizes are:

- 1024 x 768
- 960 x 720
- 896 x 672
- 832 x 624
- 768 x 576
- 704 x 528
- 640 x 480

NOTE: Scaling cannot be changed if the Video Viewer window is being accessed during a shared session.

To specify the connection speed:

1. Select *Tools - Options* from the Video Viewer window menu. The Session Options dialog box appears.
2. Click the *Connection Speed* tab.

3. Click the radio button for the desired connection speed. Available connection speeds are:
   - Lan (10/100BaseT)
   - Full T1 (1.544 Mbps)
   - Fractional T1 (512 Kbps)
   - Fractional T1 (256 Kbps)
4. Click *OK*.

Adjusting color depth (DSR switch DVC algorithm upgraded only)

The DSR switch DVC algorithm upgrade enables DSView management software users to adjust the number of viewable colors in a remote session window. You may choose to display more colors for the best fidelity, or fewer colors to reduce the data transferred on the network.

NOTE: The DVC algorithm upgrade is standard on all newer DS appliances/DSR switches. Older DS appliances/DSR switches use standard video compression with 8-bit color depth (256 colors). For DVC algorithm upgrade purchase information, contact Avocent Technical Support or your Avocent reseller.

Video Viewer windows can be viewed using the best color available (slower updates), the best compression (fastest updates), a combination of best color and best compression or in greyscale.

The color depths of individual ports and channels can be specified by selecting the *View - Color* command in a remote session window. These settings are saved individually per port and channel and override the global color depth setting.

NOTE: A color depth cannot be applied to a remote session window during a shared device session. See Chapter 4 and Chapter 5 for more information.

Additional video adjustment

In some cases, DS users may wish to view several target devices at the same time on the same screen. Generally, the Video Viewer window's automatic adjustment features will optimize the video for the best possible view. However, DS users may fine tune the video with the help of Avocent Technical Support by using the *Tools - Manual Video Adjust* command in the Video Viewer window menu. This displays the Manual Video Adjust dialog box.

Video adjustment is a per target setting and applies to each target device you access.

Modified video settings are written to the target device. Settings are also stored per port/channel session on a system when they are made and saved so they may be used during a non-shared session as follows:

- If sharing is not enabled, the video settings made on the local DS appliance/DSR switch during the session are used.
- If sharing is enabled, video settings are read from the target device.

See Chapter 4 and Chapter 5 for more information on session sharing.

Users may verify the level of packets per second required to support a static screen by observing the packet rate which is located in the lower left-hand corner of the dialog box.

To manually adjust the video quality of the window:

NOTE: The following video adjustments should be made only on the advice and with the help of Avocent Technical Support.

1. Select *Tools - Manual Video Adjust* from the Video Viewer window menu. The Manual Video Adjust dialog box appears. See the following figure; descriptions follow the figure.
2. Click the icon corresponding to the feature you wish to adjust.
3. Move the slider bar and then fine tune the setting by clicking the *Min* (-) or *Max* (+) buttons to adjust the parameter for each icon pressed. The adjustments will display immediately in the Video Viewer window.
4. When finished, click *Close* to exit the Manual Video Adjust dialog box.

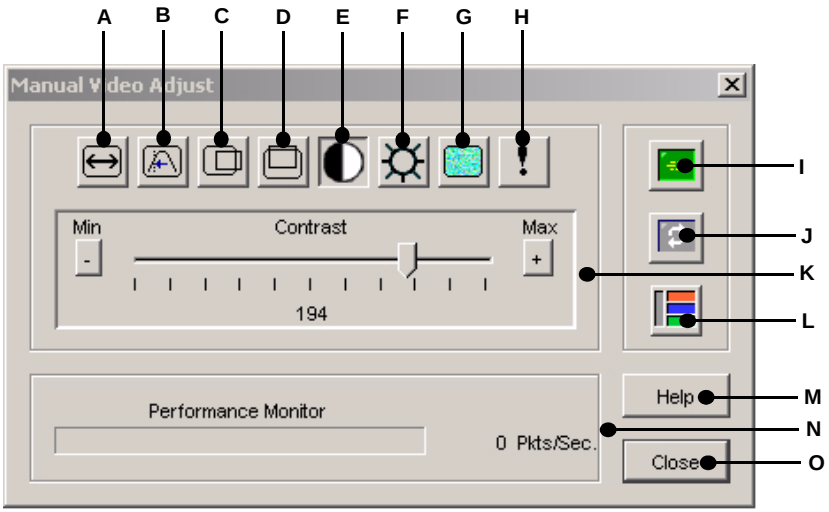


Figure 6.2: Manual Video Adjust Dialog Box

Table 6.2: Manual Video Adjust Dialog Box Descriptions

Letter	Description	Letter	Description
A	Image Capture Width	**I**	Automatic Video Adjustment
B	Image Capture Height	**J**	Refresh Image
C	Image Capture Horizontal Position	**K**	Adjustment bar
D	Image Capture Vertical Position	**L**	Video Test Pattern
E	Contrast	**M**	Help button
F	Brightness	**N**	Performance Monitor

Table 6.2: Manual Video Adjust Dialog Box Descriptions (Continued)

Letter	Description	Letter	Description
G	Noise Threshold or Block Noise Threshold	**O**	Close box
H	Priority Threshold or Pixel Noise Threshold		

NOTE: Noise Threshold and Priority Threshold settings are available if you are using standard video compression. Block Noise Threshold and Pixel Noise Threshold settings are available if you are using the DSR switch DVC algorithm upgrade. The DVC algorithm upgrade is standard on all newer DS appliances/DSR switches. Older DS appliances/DSR switches use standard video compression. For DVC algorithm upgrade purchase information, contact Avocent Technical Support or your Avocent reseller.

The following sections describe the effects of the video adjustments.

Image Capture Width, Image Capture Height, Image Capture Horizontal Position and Image Capture Vertical Position

The Image Capture Width, Image Capture Height, Image Capture Horizontal Position and Image Capture Vertical Position adjustments affect how the target video is captured and digitized and are seldom changed.

The image capture parameters are automatically changed by the Automatic Adjustment function. A special image is required on the target in order to make accurate adjustments independently.

Contrast and brightness

If the image in the Video Viewer window is not clear, select *Tools - Automatic Video Adjust* first. This command is also available in the Video Adjustments dialog box. In most cases, this will correct video problems. In those cases where clicking on Auto Adjust several times does not clear up a mottled screen, adjusting the contrast and brightness may help.

First increase the brightness. Do not go more that 10 increments before moving the contrast. Generally the contrast should be moved very little.

When the packet count gets close to zero (0), refresh the screen. If the packet count stays at 0, the video adjustment is completed.

Detection thresholds

In some cases, noise in the video transmission keeps the packets/sec count up. This may be seen when little dots change in the area of the cursor when it is moved. Varying the threshold values may result in “quieter” screens and improved cursor tracking.

Noise Threshold and Priority Threshold values may be modified if you are using standard video compression. Block Noise Threshold and Pixel Noise Threshold values may be modified if you are using the DSR switch DVC algorithm upgrade. Default threshold values can be restored by clicking *Auto Adjust Video*.

NOTE: The DVC algorithm upgrade is standard on all newer DS appliances/DSR switches. Older DS appliances/DSR switches use standard video compression. For DVC algorithm upgrade purchase information, contact Avocent Technical Support or your Avocent reseller.

Noise Threshold and Priority Threshold (Standard Video Compression)

The Noise Threshold and Priority Threshold values set the minimum levels in terms of changed pixels per thousand that are allowed without updating the video block. The thresholds are described below:

- Raising the Noise Threshold will usually make the packets/sec count decrease. The result will be larger cursor image artifacts remaining on the screen. Decreasing the value will make the size of these artifacts smaller.
- The Priority Threshold sets the level where a significant change is noted, such as a new cursor position. Increasing the value will make the mouse movements more sluggish. The Priority Threshold setting should always be greater than the Noise Threshold setting, and usually two to three times its value. Setting these thresholds to zero (0) will cause a constant refresh of the screen, which will make cursor tracking very difficult and may make it difficult for other network users. The goal is to reduce the packet rate to 0.

Block Noise Threshold and Pixel Noise Threshold (DSR switch DVC Algorithm Upgrade)

The Block Noise Threshold and Pixel Noise Threshold values set the minimum color levels in terms of changed video blocks and pixels per thousand that are allowed. See *Adjusting the View* for information on changing the color depth of a Video Viewer window. The thresholds are described below:

- The Block Noise Threshold sets the minimum color change that will occur in a single video block. Increasing the value will reduce the network bandwidth. Decreasing the value will make the size of these artifacts smaller.
- The Pixel Noise Threshold sets the minimum color change in a single pixel. Decreasing the value will reduce the number of low-contrast artifacts, but will increase network bandwidth.

Automatic video adjustment

NOTE: You may also select *Tools - Automatic Video Adjust* from the Video Viewer window menu to automatically adjust the video.

In most cases, you will not need to alter the Video Settings from the default. The system will automatically adjust and use the optimal video parameters. The DSView management software performs best when the video parameters are set such that no (0) video packets are transmitted for a static screen.

You may easily adjust your video parameters by clicking on the *Auto Adjust Video* button in the Manual Video Adjust dialog box, which instructs the DS appliance/DSR switch to optimize the video to ideal settings.

NOTE: A green screen with yellow lettering may appear during auto-adjustment.

Refresh Image

NOTE: You may also select *View - Refresh* from the Video Viewer window menu to refresh the image.

Clicking the *Refresh Image* button in the Manual Video Adjust dialog box will completely regenerate the digitized video image.

Video Test Pattern

Clicking the *Video Test Pattern* button in the Manual Video Adjust dialog box will toggle a display a video test pattern. Click the *Video Test Pattern* button again to toggle back to a normal video image.

Adjusting Mouse Options

The Video Viewer window mouse options affect cursor type, cursor mode, scaling, alignment and resetting. Mouse settings are device-specific; that is, they may be set differently for each device.

NOTE: If the device does not support the ability to disconnect and reconnect the mouse (almost all newer PCs do), then the mouse will become disabled and the device will have to be rebooted.

Cursor type

The Video Viewer window offers five appearance choices for the local mouse cursor. You may also choose no cursor or the default cursor.

NOTE: You may define the default cursor type that will appear when a Video Viewer window is opened. See *Changing the System Settings* on page 58 for more information.

Single Cursor mode (Windows operating system only)

In Single Cursor mode, the display of the local (second) cursor in the Video Viewer window is turned off and only the target device's mouse pointer will be visible. The only mouse movements that will appear are those of the target device's remote cursor. When Single Cursor mode is active, relative mouse movements are sent to the target device instead of the absolute mouse cursor locations sent in regular desktop (two-cursor) mode.

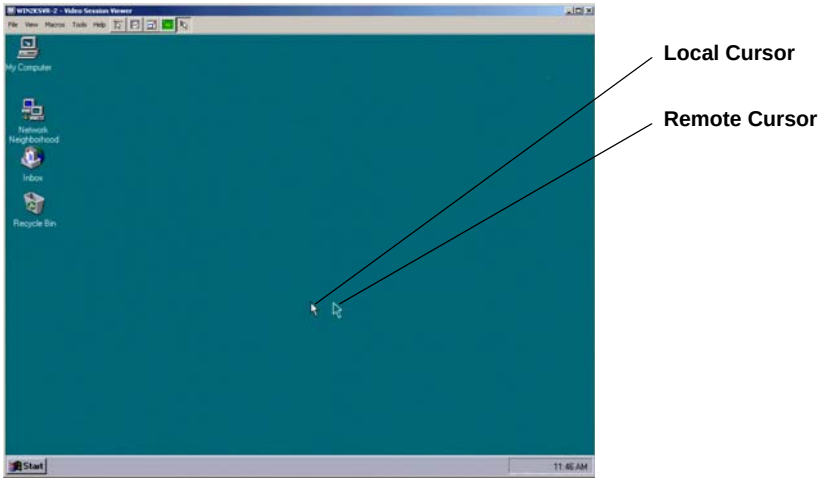


Figure 6.3: Video Viewer Window with Local and Remote Cursors Displayed

The cursor mode status of the Video Viewer window displays in the title bar, including the keystroke that will exit Single Cursor mode. You may define the keystroke that will exit Single Cursor mode in the Session Options dialog box.

NOTE: When using a device that captures keystrokes before they reach the operating system, you should avoid using the keys that restore the mouse pointer.

To enter Single Cursor mode:

Select *Tools - Single Cursor Mode*. The local cursor will not appear and all movements will be relative to the target device.

- or -

Click the *Single Cursor Mode* button.

To select a key for exiting Single Cursor mode:

1. Select *Tools - Session Options* from the Video Viewer window menu. The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. Select a terminating keystroke from the drop-down menu in the Single Cursor mode area.
4. Click *OK*. When you enable Single Cursor mode, the specified key may be pressed to return to regular desktop mode.

To exit Single Cursor mode:

Press the key on the keyboard that appears in the title bar.

To eliminate the local mouse pointer:

From the Video Viewer window, select *Tools - Single Cursor Mode*.

Cursor settings

When using the DS Management Software, your mouse pointer will change shape when over a Video Viewer window. You may change the appearance of this second local cursor or eliminate it from within the DSView management software. See *Changing the System Settings* on page 58 for more information.

Scaling

You may choose among three preconfigured mouse scaling options or set your own custom scaling. The preconfigured settings are: Default (1:1), High (2:1) or Low (1:2), as follows:

- In a 1:1 scaling ratio, every mouse movement on the desktop window will send an equivalent mouse movement to the server.
- In a 2:1 scaling ratio, the same mouse movement will send a 2X mouse movement.
- In a 1:2 scaling ratio, the value will be 1/2X.

Alignment

Because the DSView management software cannot get constant feedback from the mouse, there are times when the mouse on the DS appliance system may lose sync with the mouse on the host system. If your mouse or keyboard no longer responds properly, you may align the mouse to re-establish proper tracking or reset the PS/2 connection.

Alignment causes the local cursor to be aligned with the cursor on the remote server. Resetting causes the appliance to simulate a mouse and keyboard reconnect at the device as if you had disconnected and then reconnected them.

To change the mouse cursor setting:

1. Select *Tools - Session Options* from the Video Viewer window menu. The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. Select a mouse cursor type in the Local Cursor panel.
4. Click *OK*.

To set mouse scaling:

1. Select *Tools - Session Options* from the Video Viewer window menu. The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. To use one of the preconfigured settings, check the appropriate radio button.

4. To set custom scaling, click the *Custom* radio button. The X and Y fields become enabled. Type a mouse scaling value in the X and Y fields. For every mouse input, the mouse movements are multiplied by the respective X and Y scaling factors. Valid input ranges are 0.25-3.00.

To realign the mouse:

Click the *Align Local Cursor* button in the Video Viewer window toolbar.

To reset the PS/2 connection:

1. Select *Tools - Session Options* from the Video Viewer window menu. The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. Click the *Reset PS/2* button. A dialog box prompts you to confirm.
4. Enable the Reset PS/2 Connection at the Device checkbox and click *OK*.

Using keyboard pass-through

Keystrokes that a DS appliance user enters when using a Video Viewer window may be interpreted in two ways, depending on the screen mode of the Video Viewer window.

- If a Video Viewer window is using Full Screen mode, keystrokes and keyboard combinations are sent to the remote server being viewed.
- If a Video Viewer window is using regular desktop mode, Keyboard Pass-through mode may be used to control whether the remote server or local computer will recognize keystrokes or keystroke combinations.

When enabled, Keyboard Pass-through mode will send keystrokes and keystroke combinations to the remote server being viewed when the Video Viewer window is active. When the local desktop is active, keystrokes and keystroke combinations entered by the DS user affect the local computer.

If you wish to use Keyboard Pass-through mode, it must be specified using the Session Options dialog box.

NOTE: The **Ctrl-Alt-Delete** keyboard combination can only be sent to a remote server by using a macro. See *Global Keyboard Macros* on page 64 and *Using Local Macros* in the following section for more information.

NOTE: The Japanese keyboard **ALT-Han/Zen** keystroke combination is always sent to a remote server, regardless of the screen mode or keyboard pass-through setting.

To specify keyboard pass-through:

1. Select *Tools - Options* from the Video Viewer window menu. The Session Options dialog box appears.
2. Click the *Keyboard* tab.

3. Select *Pass-through all keystrokes in regular window mode*.
4. Click *OK*.

Using Local Macros

Two kinds of macros are available in the DS Management Software suite: Global Macros and Local Macros.

Global Macros are created and maintained by DS users with Administrative privileges and are stored on the DSAuth Server and any specified backup servers. See *Global Keyboard Macros* on page 64 for more information on Global Macros.

Local Macros are created and accessed on the local computer using the Video Viewer window. Local Macros may be customized and grouped in any manner you wish.

When a session is started in the DSView management software, Global Macros are retrieved from the DSAuth Server. Then, when a Video Viewer window session is started, the Global Macros are loaded as well as the local ones. A DS user may choose to use either Local Macros or Global Macros and switch between using them at any time during the session by selecting the *Tools* - *Session Options* command in the Video Viewer window and then selecting the Macros tab in the Session Options dialog box. If Local Macros are chosen, the macros stored on the local computer will be used.

The Video Viewer window macro function allows you to:

- Send multiple keystrokes to a device, including keystrokes that you cannot generate without affecting your local system, such as **Ctrl-Alt-Delete**.
- Send a macro from a predefined macro group. Macro groups for Windows, Sun and Groups 1-10 are already defined.
- Create, edit and delete your own macros. When you create or edit a macro, you may type the desired keystrokes or you may select from among several available categories of keystrokes. Each category contains a set of keystroke combinations. Selecting from the available categories and keystrokes saves time and eliminates the risk of typographical errors.
- Create, edit and delete your own macro groups. You may also modify the predefined macro groups.
- Change the macro group that displays by default. This causes the macros in the specified group to be available in that menu.

Macro group settings are device-specific; that is, they may be set differently for each device.

To send a macro:

Select *Macros* - <*desired macro*> from the Video Viewer window menu.

- or -

Select *Macros* - *Configure* from the Video Viewer window menu. The Macros dialog box appears. Select the desired macro from the Defined Macros list and then click *Run*.

To create or edit a macro:

1. Select *Macros* - *Configure* from the Video Viewer window menu. The Macros dialog box appears.
2. To create a macro, click *Create*.

   - or -

   To edit a macro, click *Edit*.
3. The Create Macro or Edit Macro dialog box appears.
4. If you are creating a macro, type a 1-32 character name in the Macro Name field.
5. To build the macro, you may select keystrokes from a set of categories, or type the keystroke definitions. The categories contain many commonly-used keystrokes, and provide an easy alternative to typing the keystroke definitions.

   To build the macro from the categories, select a category in the Available Keystrokes pulldown menu and then select keystrokes from the adjacent pulldown menu, clicking *Add* after each keystroke selection. The selected keystrokes appear in the Keystrokes field.

   To build the macro by typing the keystroke definitions, enter the text in the Keystrokes field, as follows:

   - Letters and numbers may be entered without additional symbols.
   - To specify a keystroke such as **Enter** or **Home**, type the name of the keystroke and surround that text with a less than (<) and greater than (>) symbol (for example, **<Enter>**).
   - To specify auxiliary keystrokes such as **Ctrl**, **Shift** or **Alt**, where the command requires a press, hold and release, type the initial press keystroke (for example, **<Ctrl-Press>**), then type the name of the keystroke, letter or number of the command, followed by the closing release (for example, **<Ctrl-Release>**).
6. Click *OK* to accept the changes and return to the Macros dialog box.

   - or -

   Click *Reset* to erase all the keystrokes entered in the Keystrokes field.
7. Click *Close* to exit the Macros dialog box.

To delete a macro:

1. Select *Macros* - *Configure* from the Video Viewer window menu. The Macros dialog box appears.
2. Select a macro in the Defined Macros list, then click the *Delete* button. You are prompted to confirm the deletion.
3. Click *Yes* to confirm the deletion.

   - or -

   Click *No* to cancel the deletion.
4. Click *Close* to exit the Macros dialog box.

To create a macro group:

1. Select *Macros* - *Configure* from the Video Viewer window menu. The Macros dialog box appears.
2. Click the *Group* button. The Macro Groups dialog box appears. The Macros Available field lists macros that are not currently assigned to this group.
3. Click the *Create* button. The Create Macro Group dialog box appears.
4. In the Macro Group Name field, enter a 1-32 character unique macro group name.
5. Click *OK* to save the name and return to the Macro Groups dialog box. A tab with the new macro group name appears.

   - or -

   Click *Cancel* to leave the dialog box without saving changes.
6. Click *Apply* to confirm the change and remain in the Macro Groups dialog box.

   - or -

   Click *OK* to confirm the change and return to the Macros dialog box.
7. Click *Close* to exit the Macros dialog box.

To add or delete macros in an existing macro group:

1. Select *Macros* - *Configure* from the Video Viewer window menu. The Macros dialog box appears.
2. Click the *Group* button. The Macro Groups dialog box appears.
3. Click the tab for the macro group to be altered. Windows, Sun and Groups 1-10 are the default tabs. If you have created new groups, there will also be tabs for each of them.
4. To add macros to the group, select the macro to add from the Macros Available list. Click the *Add* button. The macro moves to the Macros in Group list. Use the *Move Up* and *Move Down* buttons to move the macro up or down in relation to the other macros.
5. To remove macros from the group, select the macro to delete from the Macros in Group list. Click the *Remove* button. The macro moves to the Macros Available list.
6. Repeat steps 4 and 5 until the Macros in Group list contains all the desired macros.
7. Click *Apply* to accept the macro group and stay in the Macro Groups dialog box.

   - or -

   Click *OK* to accept the macro group and return to the Macros dialog box.

   - or -

   Click *Cancel* to leave the dialog box without saving changes.
8. Click *Close* to exit the Macros dialog box.

To rename a macro group:

1. Select *Macros - Configure* from the Video Viewer window menu. The Macros dialog box appears.
2. Click the *Group* button. The Macro Groups dialog box appears.
3. Click the tab for the macro group to be renamed. Windows and Sun are the default tabs. If you have created new groups, there will also be tabs for each of them.
4. Click the *Rename* button. The Rename Macro Group dialog box appears.
5. In the Macro Group Name field, enter a 1-32 character unique macro group name.
6. Click *OK* to save the name and return to the Macro Groups dialog box.

   - or -

   Click *Cancel* to leave the dialog box without saving changes.
7. Click *Close* to exit the Macros dialog box.

To delete a macro group:

1. Select *Macros - Configure* from the Video Viewer window menu. The Macros dialog box appears.
2. Click the *Group* button. The Macro Groups dialog box appears.
3. Click the tab for the macro group to be deleted.
4. Click the *Delete* button. You are prompted to confirm the deletion.
5. Click *Yes* to confirm the deletion.

   - or -

   Click *No* to cancel the deletion.
6. Click *OK* to return to the Macros dialog box.
7. Click *Close* to exit the Macros dialog box.

To change the macro group to be displayed in the Macros menu:

1. Select *Tools - Session Options* from the Video Viewer window menu. The Session Options dialog box appears.
2. Click the *Macros* tab.
3. Select a macro group from the pulldown menu.
4. Click *OK* to save the change.

   - or -

   Click *Cancel* to exit without saving any change.

Macros in the selected group will appear in the Video Viewer window Macros menu.

Displaying Video Viewer Window Users

You may use the *View - Connected Users* command to view the current users connected to a Video Viewer window session.

To view current Video Viewer window users:

1. Select *View - Connected Users* from the Video Viewer window menu.
2. The Users Connected to <device - Video Session number> dialog box appears, containing a list of all users connected to the Video Viewer window session.
3. Click *OK* to close the dialog box.

Saving the View

The display of a Video Viewer window may be saved to either a file or to the clipboard for pasting into a word processing or other program.

To capture the Video Viewer window to a file:

1. Select *File - Capture to File* from the Video Viewer window menu. The Save dialog box appears.
2. Enter a filename and choose a location to save the file.
3. Click *Save*.

To capture the Video Viewer window to your clipboard:

Select *File - Capture to Clipboard* from the Video Viewer window menu. The image data is saved to the clipboard.

APPENDICES

Appendix A: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service:

1. Check the pertinent section of the manual to see if the issue may be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the on-line service request.
3. Call Avocent Technical Support for assistance at (888) 793-8763. Visit the Avocent web site at http://www.avocent.com/support and click on *Support Phone Numbers* for current phone support hours.

Appendix B: TCP Ports

When the DSView management software window is launched, the Node Manager will become active. Node Manager will attempt to establish a Security Support Provider Interface (SSPI) Messenger Class session using TCP/IP over port 2068 to the DSAuth Server (Authentication Service). First, Node Manager will use the current NT/2000 cached credentials to establish the session. If the cached credentials have the proper permissions, the browse list is returned from the DSAuth Server over TCP/IP port 2068. Note that the DSView management software window caches this list. Using the refresh option will update the list from the DSAuth Server. If the session is refused using the cached credentials, a pop-up dialog box will prompt for the proper username and password.

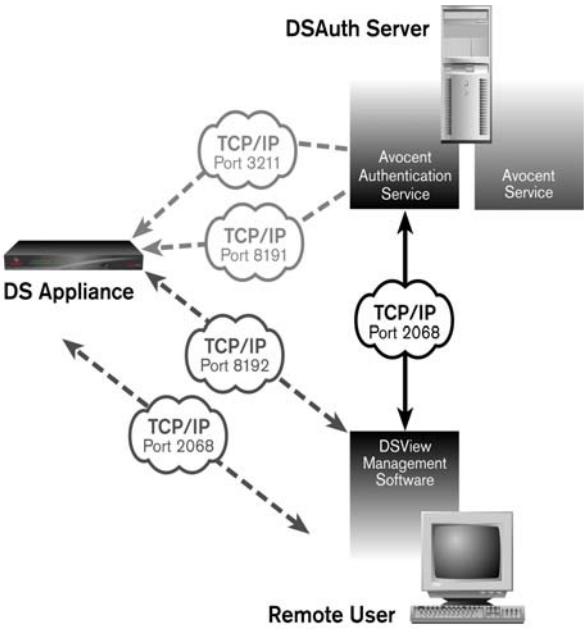


Figure B.1: SSPI Messenger Class Session Establishment

After the browse list is returned to Node Manager, the user may double-click on a specific port to initiate a KVM session with that port on the DS appliance. The DSView management software contacts the DSAuth Server, which checks the permissions on the port again. If the logged in user has permissions to the port selected, the DSAuth Server will establish a connection to the DS appliance using TCP/IP port 8191. The DSAuth Server then tells the appliance to “listen” to port 8192 for a DSView management software connection if DES encryption is specified in the DSView management software properties. If 3DES or 128-bit encryption is specified, port 2068 is used.

For debugging purposes, the details of this connection may be seen by using the console port to place the DS appliance into Debug mode.

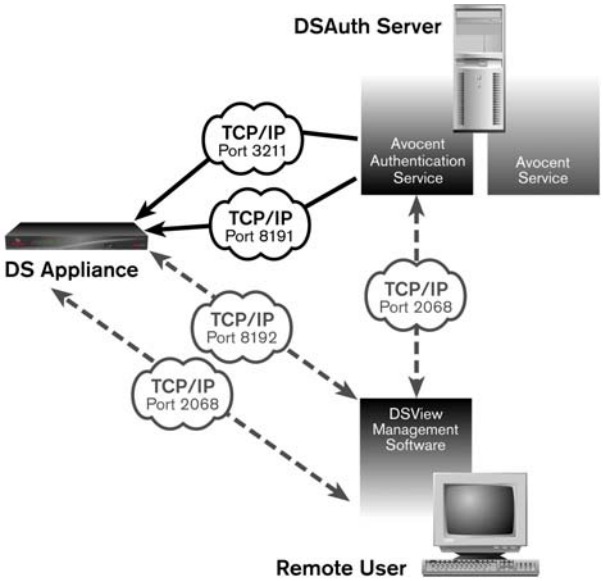


Figure B.2: Establishing Connection to a DS Appliance

The DSView management software establishes a TCP/IP session with the appliance over the TCP/IP port 8192 (DES encryption) or 2068 (3DES or 128-bit encryption). The DSAuth Server will establish a connection to the DS appliance using TCP/IP port 8191. The DSAuth Server then communicates to the appliance to listen to port 8192 (DES encryption) or port 2068 (3DES or 128-bit encryption) for a DSView management software connection. All communication between the DS appliance and the DSView management software takes place over TCP/IP port 8192 until the DSView management software closes the session.

If the system configuration includes a CPS810/CPS1610 appliance or DSR1021 switch, port 3211 is used to retrieve configuration information and perform status polling and power control commands. Information is sent between the DSAuth Server and CPS810/CPS1610 appliance or DSR1021 switch over port 3211 using the Avocent Secure Management Protocol (ASMP).

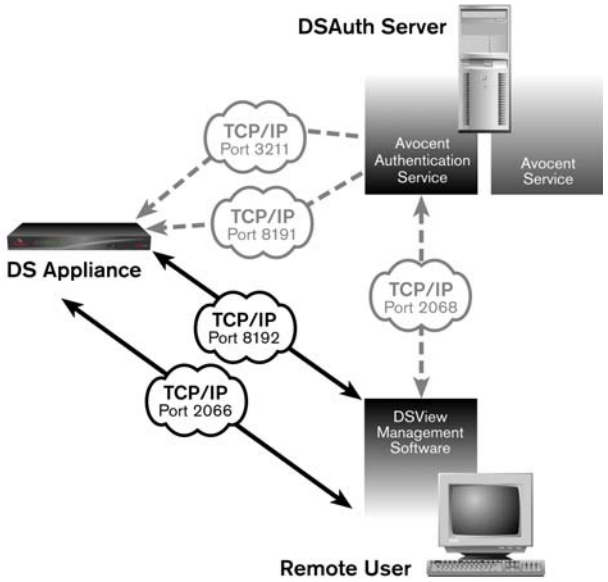


Figure B.3: DSView Management Software Establishing a Session with a DS Appliance

If the DS user wishes to establish a session with another port on the DS appliance, the same process is used.

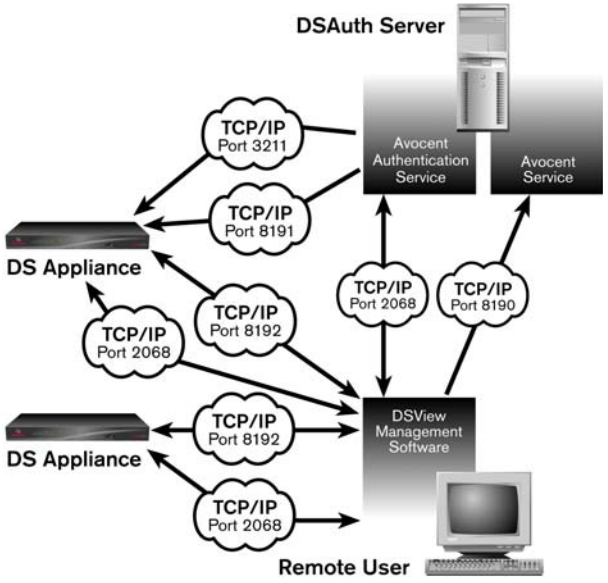


Figure B.4: Establishing a Session with an Additional DS Appliance Port

The DSView management software establishes a connection using TCP/IP port 2068, and uses the same process for authentication and return of the browse list.

Whenever a DS appliance is added or removed or the properties of a DS appliance are changed, the changes are communicated from the DSView management software to the DSAuth Server database using TCP/IP port 8190. This port is also used by the DSView management software to retrieve information from the DSAuth Server database.

The adding or removing of appliances will cause the browse list to change. Once the changes made in the DSView management software are communicated back to the DSAuth Server database using port 8190, the DSView management software refreshes its browse list view over the TCP/IP port 2068 connection.

When the backup Authentication Service is active, it communicates with the Primary Authentication Service via TCP port 8193. Changes to the topology are copied to and from the Primary over this port.

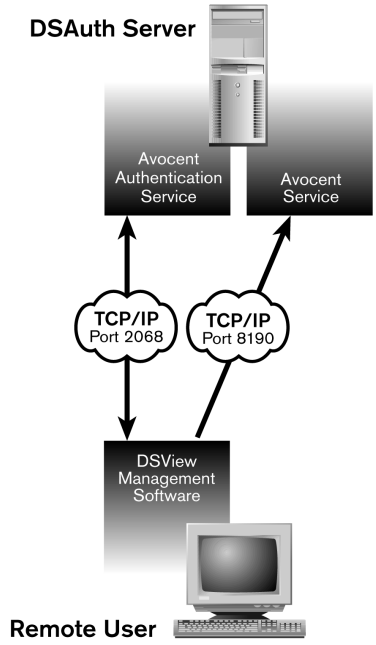


Figure B.5: DSView Management Software Functionality

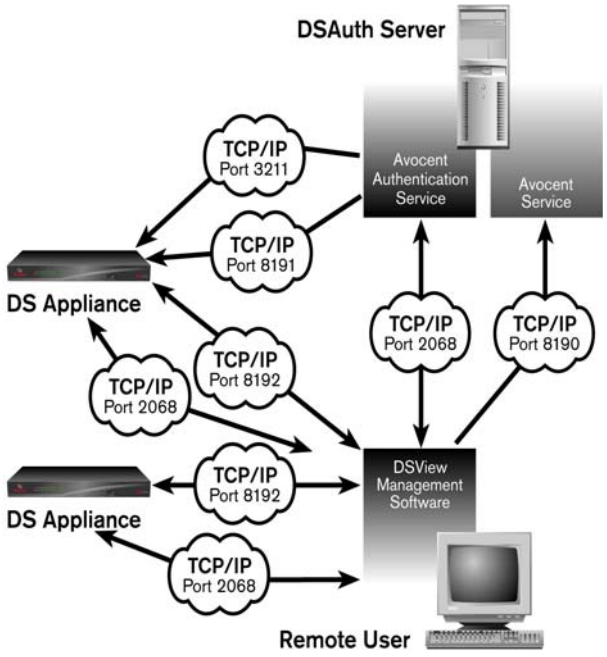


Figure B.6: Full Diagram with DSView Management Software Configuration

A DSWebview Client interface may also be used to access the system and perform commands via a web browser. The DSWebview software utilizes a web server that provides communication with a DSWebview Client interface. TCP/IP port 80 is used for HTTP or TCP/IP port 443 is used for HTTPS connections. The DSWebview Client interface may communicate with the web server on a Virtual Private Network (VPN) or remotely using TCP/IP port 8189. If you wish to communicate using the Telnet application, TCP/IP port 8023 must be used in addition to TCP/IP port 8189. If a VPN tunnel has not been created, TCP ports 8189 and 8023 must be configured as open on your firewall.

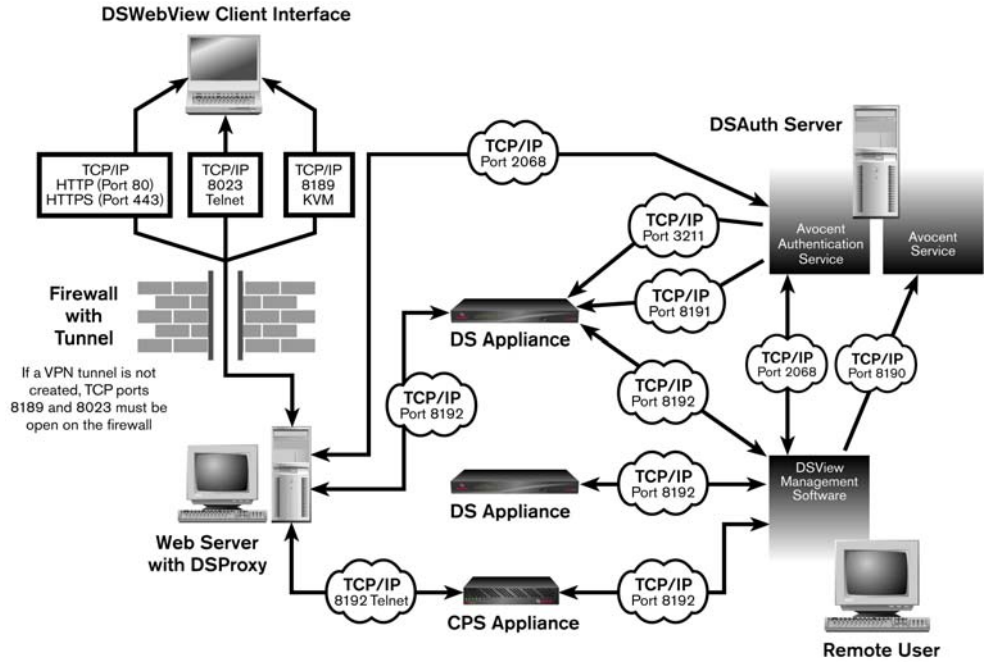


Figure B.7: Full Diagram with DSWebview Client Interface Configuration

Appendix C: Telnet Application Operations

The DSView management software ships bundled with a built-in proprietary Telnet application that provides features unavailable in many other Telnet application programs. These features include configurable session properties tailored for each device, and configurable user preferences for all sessions.

Additionally, the DSView management software Telnet application offers a separate History mode to review session data, a choice of connection modes to a DS appliance, a scripting function for automatic device login and a logging function for saving session data to a file.

You may use the DSView management software Telnet application to access any DS appliance that supports Telnet application connections, as well as DS appliance ports.

If you do not specify a communications application for a device, the DSView management software uses its Telnet application by default. See the installer/user guide for your DS appliance for information about setting and changing the default application.

DSView management software Telnet application screen

The title bar at the top of the screen displays the name of the device to which you are connected. If you are connected to a port on a device, the title bar displays the device name followed by the port number and port name.

The status bar at the lower left corner of the screen indicates *Connected* when you are operating in normal Terminal Emulation mode during a Telnet application session. When you are in the History mode, the status bar indicates *ESC to return to terminal mode*. When you are logging, the status bar indicates *Logging* or *Logging Paused* as appropriate.

The lower right corner of the status bar contains an icon that, when clicked, activates the console application, bringing it to the foreground. With this feature, you may access the console tree view without having to close the Telnet application session.

Each toolbar icon has a tooltip that appears when you rest the mouse pointer on the icon without clicking.

Viewing port users

You may view the current users connected to a CPS810 serial over IP network appliance or CPS1610 serial over IP network appliance port via the Telnet application in a DSView management software window, or you may view the current users connected to a DS appliance/ DSR switch or CPS appliance port in a DSWebview software window.

To view current port users:

1. In the DSView management software window tree view, select a CPS810 appliance or CPS1610 appliance port and then select *View - Connected Users* from the menu bar.

   - or -

   From the DSWebview software window, place your cursor over a DS appliance/DSR switch or CPS appliance port and then select *View Connected Users* from the floating option menu.

2. The Connected Users dialog box appears, containing a list of all users connected to the CPS810 appliance or CPS1610 appliance port using the Telnet application. Click *OK* to close the dialog box.

   - or -

   If no users are connected to the CPS810 appliance or CPS1610 appliance port using the Telnet application, a message box appears. Click *OK* to close the message box.

Security property

The Telnet application's security property specifies whether Telnet application sessions to a DS appliance will be in Plain Text mode or SSL mode.

In Plain Text mode, all data is sent unencrypted to the DS appliance. When Plain Text mode is used, any Telnet application that supports VT52, VT100, VT100+, VT102, VT220, VT320 or ASCII Terminal Emulation mode may be used to access the DS appliance.

In SSL mode, all data sent to the device during the DSView management software Telnet application session is DES encrypted. The DS appliance supports anonymous Diffie-Hellman key exchange. The exchange of certificates for authentication is not supported. When SSL mode is used, only the built-in DSView management software Telnet application may be used to access the DS appliance. The ports on a DS appliance have the same security property as the device.

The security property is set in the DSView management software and in the DS appliance from the Command Line Interface (CLI). When you initiate access to a DS appliance or port using the Telnet application from the DSView management software, the DSView management software attempts to read the security property directly from the DS appliance.

If the SSL property has not been enabled on the DS appliance, and the DSView management software receives confirmation from the DS appliance, the DSView management software will automatically open its built-in Telnet application and you will be prompted for a DS appliance username and password.

After that information has been entered, an SSL connection to the DS appliance is established over TCP port 8192. When that connection is established, the DS appliance validates the user's access privileges and port availability. In this case, the Telnet application's property screen in the DSView management software for that DS appliance will automatically be set to SSL values, even if they previously held Plain Text mode values. The property screen will be disabled, and you will not be allowed to change any of its values. The DSView management software database will be updated with the information read from the DS appliance/DSR switch.

If the DSView management software does not receive a reply from the DS appliance, it will use the Security mode settings in the DSView management software database. In this case, the Telnet application's property screen in the DSView management software for that DS appliance will show the database values, and you will be able to change them.

Setting the security property

The security property that is set when a DS appliance is added to the DSView management software database depends on the method being used to add the device.

If the Run New Device Install wizard method is used, you are prompted to select the Security mode. It should match the DS appliance Server Security mode value that was set via the DS appliance CLI.

- or -

If the Discover Configured Devices method is used, the security value that is reported by the DS appliance is used.

- or -

When the Manually Add a Device method is used, a default value of Plain Text is used.

If a discrepancy occurs between the configuration of the DS appliance and DSView management software, the determining factor will be whether the DSView management software is able to communicate with the DS appliance. If possible, the DS appliance settings will overrule any security settings in the DSView management software database. However, if the DSView management software cannot communicate with the DS appliance, the DSView management software will use the current information from its own database.

To configure the DSView management software Telnet application for SSL mode:

1. In the DSView management software window tree view, select a DS appliance.
2. Select *Edit* - *Properties* from the menu bar.
3. Click the *Telnet* tab. The DSView management software will attempt to access the DS appliance.
4. The Properties dialog box appears. If the SSL security mode has been set on the DS appliance, and the DSView management software successfully accesses that device, the DSView management software Telnet application properties are automatically updated with SSL mode information, and then disabled.

Opening and closing a session

A DSView management software Telnet application session is opened from the DSView management software.

To open a DSView management software Telnet application session with a DS appliance:

1. In the DSView software window tree view, select a DS appliance.
2. Select *Tools* - *Configure* from the menu bar.

   - or -

   Click the *Launch Telnet to configure ...* icon in the toolbar.

To open a DSView management software Telnet application session with a DS appliance port:

1. In the DSView management software window tree view, select a DS appliance.
2. Select *Tools* - *Connect* in the menu bar.

- or -

Double-click on a port.

- or -

Press **Enter** after selecting a port.

- or -

Click the *Connect to the ... attached device* icon in the toolbar.

To open a DSView management software Telnet application session with a generic appliance:

1. In the DSView management software window topography view or server list, select a generic appliance.
2. Right-click and select *Connect* from the shortcut menu.

   - or -

   Select *Device - Telnet* from the menu bar.

   - or -

   Click the *Launch Telnet to the selected device* icon in the toolbar.

To close a DSView management software Telnet application session:

Select *Telnet - Exit* from the menu bar.

To activate the DSView software from the DSView software Telnet application:

Click the *DSView* icon in the lower right corner of the display.

Customizing the application

You may specify preferences for the DSView management software Telnet application that will be used for every session, regardless of the device to which you connect. These application preferences are entered from the DSView management software Telnet application display when you are connected to a device or port. After the preferences are entered, they are applied to devices/ports during subsequent DSView management software Telnet application sessions.

Changing colors

You may change the background color and text color on the DSView management software Telnet application screen at any time.

To change the DSView software Telnet application window background color:

1. Select *Options - Preferences* from the menu bar.
2. In the Colors panel, click the *Background/Normal Mode* box, and choose a color. The default value is blue.

To change the DSView software Telnet application text color:

1. Select *Options* - *Preferences* from the menu bar.
2. In the Colors panel, click the *Text/Normal Mode* box, and choose a color. The default value is white.

Changing the cursor

You may specify whether the cursor (caret) on the DSView management software Telnet application screen appears as an underline or as a block.

To change the DSView software Telnet application cursor appearance:

1. Select *Options* - *Preferences* from the menu bar.
2. In the Caret list, choose *Block* to display the cursor as a block or choose *Underline* to display the cursor as an underline. The default value is Underline.

Enabling and disabling the exit warning prompt

When the exit warning prompt is enabled, a message appears when you select *Telnet* - *Exit*. You may then choose to exit or continue the session. When disabled, the session closes without further prompting.

To enable/disable an exit warning prompt for DSView software Telnet application sessions:

1. Select *Options* - *Preferences* from the menu bar.
2. Enable or disable the *Prompt on Exit* checkbox. The default value is enabled.

Customizing session properties

When you are connected to a device or port using the DSView management software Telnet application, you may specify session properties that will be stored and reused every time you connect to the selected device or port. When you select *Options* - *Session Properties* in the DSView software Telnet application, the Terminal, Login Scripts and Logging tabs appear.

Changing the terminal window size

The Terminal Size lists specify the number of rows and columns to display in the virtual terminal window. These values determine the window's height and width.

To change the DSView Telnet terminal window size:

1. Select *Options* - *Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.

3. In the Rows list, choose a value of *24* or *48*. The default value is 24.
4. In the Columns list, choose a value of *80* or *132*. The default value is 80.

Changing the Terminal Emulation mode

You may set the DSView management software Telnet application to emulate ASCII, VT100, VT100+, VT102, VT52, VT220 or VT320 terminals, depending on the connected device. *Appendix E* contains encoding and decoding information for each of the Terminal Emulation mode types.

To change the DSView software Telnet application Terminal Emulation mode:

1. Select *Options - Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.
3. From the Terminal Emulation list, choose one option: ASCII, VT100, VT100+, VT102, VT52, VT220 or VT320. The default value is VT100.

NOTE: When connecting to a DS appliance, the terminal type setting must match the Terminal Emulation mode type.

Changing Arrow key sequences

When the Terminal Emulation mode is VT100, VT100+, VT102, VT52, VT220 or VT320, you may specify either VT100 or ANSI **Arrow** key sequences. The following table lists the **Arrow** keys and the sequences transmitted for each.

Table C.1: Arrow Key Sequences

Key	VT100	ANSI	VT52 *
Up Arrow	<Esc> [A	<Esc> OA	<Esc> A
Down Arrow	<Esc> [B	<Esc> OB	<Esc> B
Right Arrow	<Esc> [C	<Esc> OC	<Esc> C
Left Arrow	<Esc> [D	<Esc> OD	<Esc> D

* When the Terminal Emulation mode is VT52, the **Arrow** keys are interpreted as indicated in this column, regardless of the value in the Arrow Keys list.

To change the DSView software Telnet application Arrow key sequences:

1. Select *Options - Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.

3. In the Arrow Keys list, choose either *VT100* or *ANSI*. The default value is VT100.

Changing the terminal type

The terminal type is used during Telnet session negotiation. You may change this value at any time.

To change the terminal type:

1. Select *Options* - *Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.
3. In the Terminal Type box, enter a value of up to 40 characters, beginning with a letter and ending with a letter or digit. Valid characters are the letters A-Z, digits 0-9, forward slash, dash, left parenthesis and right parenthesis.

NOTE: When you are connected to a DS appliance, the terminal type must be entered in the Terminal Type field exactly as shown in the following table for each Terminal Emulation mode.

Table C.2: Terminal Emulation Mode and Type

Terminal Emulation Mode	Terminal Type
VT52	DEC-VT52
VT100	DEC-VT100
VT100+	DEC-VT100
VT102	DEC-VT102
VT220	DEC-VT220
VT320	DEC-VT320

Changing the linefeed settings

When connecting to devices that do not insert a carriage return in incoming or outgoing data, you may instruct the DSView management software to automatically insert a line after each line of data. This prevents overwriting data when a new line is received.

To change the linefeed settings:

1. Select *Options* - *Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.

3. If the *New Line Mode - Inbound* box is checked, an inbound carriage return from the device will be treated as if both a carriage return and a linefeed were received. If not checked, a linefeed is not added to an inbound carriage return.

If the *New Line Mode - Outbound* box is checked, an outbound carriage return to the device will always be followed by a linefeed character. If not checked, a linefeed is not sent with a carriage return. The default value is disabled for inbound and outbound.

Enabling and disabling line wrap

When line wrap is enabled, characters wrap onto the next line when a new character is received and the cursor is at the end of the line. When disabled, new characters will overwrite the last character on the current line when the cursor is at the end of the line.

To enable/disable line wrap:

1. Select *Options - Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.
3. Enable or disable the *Auto Wrap Line* checkbox. The default value is enabled.

Enabling and disabling local echo

When you are connected to a device that does not repeat or echo the data that you type, you may enable Local Echo mode. Otherwise, the DSView management software Telnet application will not display the text you type. However, if you are connected to a device that echoes data, and you are in Local Echo mode, all of the data you type will appear on your terminal twice.

To enable/disable local echo:

1. Select *Options - Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.
3. Enable or disable the *Local Echo* checkbox. The default value is disabled.

Enabling and disabling 7-bit ASCII

When you are connected to a device that requires transmission of 7-bit ASCII, you may instruct the DSView management software Telnet application to strip the eighth bit of every character that is sent and received.

To enable/disable 7-bit ASCII:

1. Select *Options - Session Properties* from the menu bar.

   - or -

Click the *Session Settings* icon in the toolbar.

2. Click the *Terminal* tab.
3. Enable or disable the *Strip 8th Bit* checkbox. The default value is disabled.

Login scripts

The DSView management software Telnet application has a login scripting function that enables you to automatically log in to a device. A login script is built with a sequence of expect and send strings, and initial transmission characters that work with them. To use a login script, you must enable automatic login in a checkbox.

The first Initial character (that is, the first entry in the Initial character column) specifies what is sent to the device as soon as the Telnet application session is established. This is selected from a list containing the choices: None, CR (carriage return), CR+LF (carriage return and linefeed), ESC (Escape) and CTRL+P (Control and P).

The first Expect string indicates what the device will send as its first prompt.

The first Send string indicates what the login script will send to the device after it receives the first Expect string.

You may then build additional Expect and Send strings according to what the particular device will prompt for and what will be sent in response.

To build a login script and enable/disable automatic login:

1. Select *Options - Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Login Scripts* tab.
3. Enable or disable the *Automate Login* checkbox. The default value is disabled.
4. In the Initial Character list, select one option: CR (carriage return), CR+LF (carriage return and linefeed), ESC (Escape), CTRL+P (Control+P sequence, 0 x 10 in hex) or None (no initial transmission character).
5. In the Expect box, type the 1-32 alphanumeric character string that you expect from the device. Spaces are allowed.
6. In the Send box, type the 0-32 alphanumeric character string that you wish to send in response to the Expect string. Spaces are allowed, and a blank field is valid. A CR or CR+LF is appended to the string, based on the New Line Mode - Outbound setting.
7. Repeat the Expect and Send entries as needed, to a maximum of four each.

Telnet application History mode

The DSView management software Telnet application's History mode enables you to view the history of a current DSView software Telnet application session. You may navigate to various parts of the history buffer by clicking menu selections or tools, or by pressing **Arrow** keys. You may

configure the maximum size of the history buffer, and customize the background and text colors of the History mode display.

While you are in History mode, new incoming data is buffered, but it will not be displayed until you exit History mode. You may not enter outgoing data. The status bar in the lower left area of the display will show *ESC to return to terminal mode*.

To enter the DSView management software Telnet application's History mode:

Select *View* - *History* from the menu bar.

- or -

Click the *History* icon in the toolbar.

To exit the DSView management software Telnet application's History mode:

Press the **Esc** key.

- or -

Click the *History* icon in the toolbar.

To go to the beginning of the DSView management software Telnet application's history:

Select *View* - *Goto Beginning* from the menu bar.

- or -

Click the *double-left-arrow* icon in the toolbar.

To go to the end of the DSView management software Telnet application's history:

Select *View* - *Goto End* from the menu bar.

- or -

Click the *double-right-arrow* icon in the toolbar.

To move up (back) one page in the DSView management software Telnet application's history:

Select *View* - *Previous Page* from the menu bar.

- or -

Click the *left-arrow-and-bar* icon in the toolbar.

To move down (forward) one page in the DSView management software Telnet application's history:

Select *View* - *Next Page* from the menu bar.

- or -

Click the *right-arrow-and-bar* icon in the toolbar.

To move back or forward one line in the DSView management software Telnet application's history:

Press the **Left Arrow** (for back) or **Right Arrow** (for forward) on your keyboard.

To change the maximum number of lines in the DSView management software Telnet application's history buffer:

1. Select *Options* - *Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.
3. In the History Buffer Size box, type a value from 1-1000. The default value is 250.

To change the background color for the DSView management software Telnet application's History mode:

1. Select *Options* - *Preferences* from the menu bar.
2. In the Colors panel, click the *Background/History Mode* box and select a color. The default color is dark cyan.

To change the text color for the DSView management software Telnet application's History mode:

1. Select *Options* - *Preferences* from the menu bar.
2. In the Colors section, click the *Text/History Mode* box and select a color. The default color is white.

Macros

The DSView management software Telnet application has a macro function that allows you to create and use macros during Telnet application sessions. A macro comprises a series of keystrokes that you define. Additionally, you may specify a hotkey in the macro's definition. When you define a macro and enable its inclusion in the Macros menu, you may execute the macro during a Telnet application session either by selecting it from the Macros menu or by pressing the defined hotkey on your keyboard.

You may also define one or more macro groups, then add macros to the groups. A macro may belong to more than one macro group; however, a macro does not have to belong to a macro group. Selecting *Session Properties -Terminal* takes you to a screen that contains a list of defined macro groups from which you may select one group or all defined groups. The macros in the selected group(s) are then available for use during subsequent Telnet application sessions with that device/port.

After defining a macro or a macro group, you may edit or delete it at any time. When you delete a macro or macro group, you are prompted for confirmation. When you change a macro group name, each macro belonging to the changed macro group is updated, but the change is not visible until the

next Telnet application session is established. When you delete a macro group, you delete only its name - the individual macros in the group are not affected.

To create a macro:

1. Select *Macros* - *Configure* from the menu bar. The Macros dialog box appears.
2. Click the *Create* button. The Create Macro/Edit Macro dialog box appears.
3. Type a 1-32 character name in the Name field.
4. To define a hotkey for the macro, choose one from the Key list. To add a modifier to the hotkey, check the *Control*, *Shift* or *Alt* boxes.
5. By default, the Include in Macro Menu box is checked, indicating the macro will appear in the Macros menu. If you do not wish to include the macro in the Macros menu, uncheck this box. In this case, if the macro definition includes a hotkey, you will still be able to use the hotkey to run the macro, even if the macro's name does not appear in the Macros menu.
6. Type the macro string in the Enter Keystrokes box. For non-printing and special character code sequences, use the following escape sequences:

   Carriage return: \n

   Tab: \t

   Hexadecimal code sequence: \0x<NN>, where <NN> is the hexadecimal byte Delay character (500 ms): \d
7. To add the macro to an existing macro group, click the *Include Macro* checkbox next to the macro group name in the Macro Groups table.
8. Click the *OK* button. This returns you to the Macros dialog box, and the newly created macro appears in the Defined Macros table.
9. Click the *Close* button.

To edit an existing macro:

1. Select *Macros* - *Configure* from the menu bar. The Macros dialog box appears.
2. Select a macro. Click the *Edit* button. The Create Macro/Edit Macro dialog box appears.
3. Edit the macro properties as needed and then click the *OK* button.

To delete a macro:

1. Select *Macros* - *Configure* from the menu bar. The Macros dialog box appears.
2. Select the macro in the Defined Macros table and then click the *Delete* button. A dialog box appears, prompting you to confirm the deletion.

To execute a macro:

Select the macro from the Macros menu.

- or -

If the macro's definition includes a hotkey, press the hotkey or hotkey sequence.

- or -

Select *Macros* - *Configure* from the menu bar. The Macros dialog box appears. Then select the macro in the Defined Macros table and click the *Run* button.

To create a macro group:

1. Select *Macros* - *Configure* from the menu bar. The Macros dialog box appears.
2. Click the *Create* button. The Create Macro/Edit Macro dialog box appears.
3. Click the *Create* button in the Macro Groups tab. A new row in the Macro Groups list appears.
4. Position the cursor in the Group Name column of the new row and enter the new group name. Duplicate macro group names are not allowed. Press **Enter**.

To enable a macro group for use during Telnet application sessions:

1. Select *Options* - *Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Terminal* tab.
3. Select a macro group name from the Macro Groups list, or select *All*, which will make all macros in all groups available for use.

To delete a macro group:

1. Select *Macros* - *Configure* from the menu bar. The Macros dialog box appears.
2. Click the *Create* button. The Create Macro/Edit Macro dialog box appears.
3. Select the macro group name. To select multiple macro group names, press the **Shift** key while clicking.
4. Click the *Delete* button in the Macro Groups tab. When the dialog box appears, confirm the deletion.

Logging

The DSView management software Telnet application has a logging function that saves the contents of a Telnet application session to a file. You may enable automatic logging or dynamically start logging at any time. Additionally, you may pause, resume and stop logging, regardless of whether it was started automatically or dynamically.

While logging is occurring or when it is paused, a Logging Status label appears in the status panel at the bottom of the DSView management software Telnet application window.

NOTE: When you enable or disable automatic logging, the logging will begin or end at the start of the next DSView management software Telnet application session to that device. If you change the default log file directory used for automatic logging, the change does not take effect until the next session to that device.

Log files

The format of log filenames is shown below, where <mmddyy> represents the month, day and year, and <hhmmss> represents the current hour, minute and second in military time:

avtelnet<mmddyy>_<hhmmss>.log

The default log directory is session-specific, that is, each Telnet application session may have its own location for storing log files. You may change the name of the file and the location of the directory that stores the log files. If you do not change the default directory, log files are stored in your home directory.

You may view a log file at any time, using a standard text editor. The screen buffer is written to the log file when the buffer is full, or when logging is paused or stopped. To ensure the log file is up-to-date, either pause or stop the logging.

To change the default log file directory:

1. Select *Options - Session Properties* from the menu bar.

   - or -

   Select the *Session Settings* icon in the toolbar.
2. Click the *Logging* tab. The Default Directory field displays the current default location for log files.
3. Click the *Browse* button. The Set Directory dialog box appears.
4. Select a directory from the Look in list.

   - or -

   Create a new directory:

   a. Click the *Create New Folder* button. A new directory named New Folder appears in the directory list.

   b. Click the *New Folder* entry in the directory list to highlight it. Then, click the entry again to edit its name. Type in a new name. Press **Enter**. The directory appears in alphabetical order in the directory list.

   c. Select the newly-created directory in the directory list. The File name field will now contain the name of the new directory.
5. Click the *Set Directory* button to select the newly-created or selected directory as the default log file directory. The Set Directory dialog box will close.
6. The Default Directory field now contains the name of the newly-created or selected directory. Click *OK* to save the new information.

   - or -

   Click *Cancel* to exit the dialog box without saving any new information.

To enable automatic logging:

1. Select *Options* - *Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Logging* tab.
3. Enable the *Logging* checkbox.
4. The Default Directory field displays the current default location for log files. If that is the desired directory, click *OK*. If you wish to change the default log file directory, see *To change the default log file directory.*

Automatic logging will begin when you initiate the next DSView management software Telnet application session to that device. At that time, the Logging Status label will indicate *Logging*.

To disable automatic logging:

1. Select *Options* - *Session Properties* from the menu bar.

   - or -

   Click the *Session Settings* icon in the toolbar.
2. Click the *Logging* tab.
3. Disable the *Logging* checkbox.
4. Click *OK*.

Automatic logging will stop when you initiate the next DSView management software Telnet application session to that device. When logging stops, the Logging Status label disappears.

To start dynamic logging:

1. Select *Options* - *Logging* - *Start* from the menu bar. The Log dialog box appears.
2. The Look in list contains the default log file directory and the File name field contains the default log filename. Using this filename format is recommended; however, you may change it for the duration of this DSView management software Telnet application session. If you choose to use the default log filename, skip to step 4.
3. To change the default log filename for the duration of the dynamic logging session, you may select a directory from the Look in list. The directory list may contain directories and files. To create a new directory:
   a. Click the *Create New Folder* button. A new directory named New Folder appears in the directory list.
   b. Click the *New Folder* entry in the directory list to highlight it. Then click the entry again to edit its name. Type in a new name. Press **Enter**. The directory appears in alphabetical order in the directory list.
   c. Double-click the newly-created directory in the directory list. The File name field will now contain the name of the new directory.

d. Type a new filename in the File name field. If you enter a filename that already exists, the new file will overwrite the old file.

4. Click *Log* to confirm the directory selection and begin logging.

   - or -

   Click *Cancel* to exit the dialog box and cancel the request to start logging.

When logging begins, the Logging Status label will indicate *Logging*.

To pause logging:

Select *Options* - *Logging* - *Pause* from the menu bar. The Logging Status label will change to *Logging Paused*.

To resume logging:

Select *Options* - *Logging* - *Resume* from the menu bar. The Logging Status label will change to *Logging*.

To stop logging:

Select *Options* - *Logging* - *Stop* from the menu bar. The Logging Status label will disappear.

Copying, pasting and printing session data

In the DSView management software Telnet application you may:

- Copy a screen of the DSView software Telnet application session data to the system clipboard
- Copy the DSView software Telnet application history buffer contents to the system clipboard
- Paste the contents of the system clipboard into a DSView software Telnet application session
- Print a screen of the DSView software Telnet application session data
- Print a screen of the DSView software Telnet application session history data

Information that is copied from a DSView software Telnet application session may be pasted in other applications. Similarly, information copied from other applications may be pasted into a DSView management software Telnet application session.

NOTE: Only textual data may be copied and pasted in the DSView management software Telnet application.

To copy a DSView management software Telnet application screen:

Select *Options* - *Copy Screen* from the menu bar.

- or -

Click the *Copy Screen* icon in the toolbar.

The screen contents are saved to the system clipboard. You may then paste the clipboard contents into this or another application.

To copy DSView management software Telnet application session history data:

1. Select *View* - *History* from the menu bar.

   - or -

   Click the *History* icon in the toolbar.
2. Select *Options* - *Copy Screen* from the menu bar.

   - or -

   Click the *Copy Screen* icon in the toolbar.

The entire contents of the history buffer are copied to the system clipboard. You may then paste the clipboard contents into this or another application.

NOTE: The entire history buffer is copied to the system clipboard, regardless of the amount of data in it.

To paste system clipboard contents:

1. Place textual data on the system clipboard, using a text editor or other application.
2. Initiate a DSView management software Telnet application session.
3. At the point where you wish to paste the clipboard contents, select *Options* - *Paste* from the menu bar.

   - or -

   Click the *Paste* icon in the toolbar.

To print a DSView management software Telnet application screen:

1. Select *Options* - *Print Screen* from the menu bar.

   - or -

   Click the *Print Screen* icon in the toolbar.
2. The operating system's print dialog box appears. Make the appropriate settings. The screen contents will then be sent to the printer.

To print a screen of DSView management software Telnet application session history data:

1. Select *View* - *History* from the menu bar.

   - or -

   Click the *History* icon in the toolbar.
2. Select *Options* - *Print Screen* from the menu bar.

   - or -

   Click the *Print Screen* icon in the toolbar.
3. The operating system's print dialog box appears. Choose the appropriate settings. The screen contents will then be sent to the printer.

Appendix D: Establishing a Modem Connection (DSR1021 Switches Only)

An external modem may be attached to the DSR1021 switch. The modem may be used to access the appliance when an Ethernet connection is not available.

A modem/PPP dial-up connection must be established before the remote operation is enabled. The dial-up connection options should be set to 115200 baud, 8 bits, 1 stop bit, no parity and enabled hardware flow control. The remote operations must then be enabled within the authentication time-out specified in the Terminal Applications menu or the PPP link will be disconnected. See Chapter 4 for more information about setting the authentication time-out.

Once a modem dial-up connection is established, you select the DSView management software window *Options - Remote Operations - Enable* command to establish a DSView management software session with the DSR1021 switch over the modem link.

When a remote operation is enabled, the DSView management software window will contain a topology tree with the single DSR1021 switch.

The following DSView management software options are not available when using a modem connection:

- Specification of an authentication server
- Enabling of port status polling
- Displaying server views
- Global Macros
- Privacy mode connections to the Video Viewer window
- Viewing connected users to a Video Viewer window

Before you begin

The following actions should be performed before using the DSView management software over a modem connection:

- Ensure that the DSR1021 switch is configured. See the DSR1021 Installer/User Guide for more information.
- Ensure that DS users have been added to the DSR1021 switch internal database. If the DSAuth Server is not available, the appliance database is used for appliance authentication. If neither are available, authentication cannot be performed for the DSR1021 switch, an error will display and the appliance will not be available in the DSView management software window topology tree. See the DSR1021 Installer/User Guide for more information.
- Ensure that an external modem is attached to the DSR1021 switch modem port. The modem port should have auto-answer turned off (typically a modem's default setting).
- Ensure that the PC containing the DSView management software has dial-up software and that the software is configured properly. See your operating system documentation for more information.

To establish a remote DSView management software session over a modem connection:

1. Establish a dial-up connection to the DSR1021 switch from the PC containing the DSView management software. The IP address 10.0.0.2 will be assigned to the DSR1021 switch and the IP address 10.0.0.3 will be assigned to the PC containing the DSView management software.

NOTE: Windows displays a dialog box that prompts the DS user for a username and password when a dial-up connection is established. It is not necessary to enter a username or password in the dialog box. When this dialog box appears, click *OK* to dismiss the dialog box.

2. When a connection is established, start the PC containing the DSView management software.
3. Select *Options* - *Remote Operations* - *Enable*. The Remote Login Authentication dialog box displays.

Figure D.1: Remote Login Authentication Dialog Box

NOTE: The DSR1021 switch will disconnect the modem connection if a DS user does not log in within the time period specified by the authentication time-out value. The default authentication time-out value (120 seconds) may be changed using the Terminal Applications menu. See the DSR1021 Installer/User Guide for more information.

The DSR1021 switch will attempt to contact the DSAuth Server to authenticate the DS user. If the DSAuth Server is unavailable, the DSR1021 switch will use its internal database to authenticate the DS user.

4. Type the username, password and domain to which you wish to connect and then click *OK*. If authentication is successful, the DSR1021 switch, its ports and the outlets of any attached SPC devices will appear in the DSView management software window topology view.

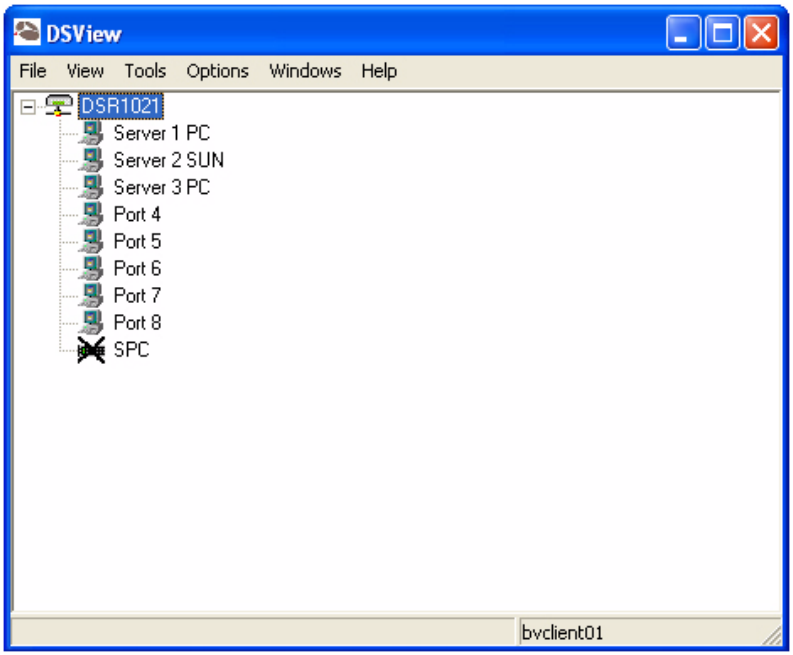


Figure D.2: DSR1021 Switch Modem Connection

NOTE: The DSR1021 switch will disconnect the modem connection if there is no activity on the modem connection for the time period specified by the inactivity time-out value. The default inactivity time-out value (15 minutes) may be changed using the Terminal Applications menu. See the DSR1021 Installer/User Guide for more information.

Appendix E: Terminal Emulation

This appendix contains information about the keys, sequences, encoding and decoding for the DS Management Software Terminal Emulation modes. Encode refers to how the Client interface processes typed keys. Decode refers to how the Client interface processes data coming from the target device.

VT terminal emulation

The following table lists the VT key and keypad numeric codes. Avocent encodes all applicable keys as numeric; decoding is not supported.

Table E.1: VT Key and Keypad Numeric Codes

Key	Keypad Numeric Code
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
- (dash)	- (dash)
, (comma)	, (comma)
. (period)	. (period)
Enter	Same as Return key

VT100+ terminal emulation

The VT100+ Terminal Emulation mode provides compatibility with the Microsoft headless server EMS serial port interface. The DSView management software Telnet application's VT100+ Terminal Emulation mode works identically to VT100, with the exception of support for the function keys listed in the following table.

Table E.2: VT100+ Function Key Support

Function	Sequence	Function	Sequence
Home	<Esc> h	F4 **	<Esc> 4
End	<Esc> k	F5	<Esc> 5
Insert	<Esc> +	F6	<Esc> 6
Delete *	<Esc> -	F7	<Esc> 7
Page Up	<Esc> ?	F8	<Esc> 8
Page Down	<Esc> /	F9	<Esc> 9
F1 **	<Esc> 1	F10	<Esc> 0
F2 **	<Esc> 2	F11	<Esc> !
F3 **	<Esc> 3	F12	<Esc> @

* ASCII, VT100 and VT102 modes send hex 7F when the **Delete** key is pressed.

** VT100 and VT102 modes map the **F1**-**F4** keys to the **PF1**-**PF4** keys.

VT102 terminal emulation

VT102 Terminal Emulation mode works identically to VT100 with additional support for decoding receive codes as described in the following table.

Table E.3: VT102 Receive Codes

VT102 Receive Code	Action
Delete Character (DHC)	Deletes n characters starting with the character at the current cursor position, and moves all remaining characters left n positions. n spaces are inserted at the right margin.
Insert Line (IL)	Inserts n lines at the line where the cursor is currently positioned. Lines displayed below the cursor position move down. Lines moved past the bottom margin are lost.
Delete Line (DL)	Deletes n lines starting with the line where the cursor is currently positioned. As lines are deleted, lines below the cursor position move up.

VT100 terminal emulation

The following table lists the VT100 special key and control (**Ctrl**) key combinations and indicates Avocent encoding/decoding support, where Yes = supported and No = not supported.

Table E.4: VT100 Special Keys and Ctrl Keys

Keys	Hex Code	Function Mnemonic	Encode/Decode
Return	0D	CR	Yes/Yes
Linefeed	0A	LF	Yes/Yes
Backspace	08	BS	Yes/Yes
Tab	09	HT	Yes/Yes
Spacebar	20	(SP)	Yes/Yes
ESC	1B	ESC	Yes/No
Ctrl+Spacebar	00	NUL	Yes/No
Ctrl+A	01	SOH	Yes/No
Ctrl+B	02	STX	Yes/No
Ctrl+C	03	ETX	Yes/No
Ctrl+D	04	EOT	Yes/No
Ctrl+E	05	ENO	Yes/No
Ctrl+F	06	ACK	Yes/No
Ctrl+G	07	BELL	Yes/Yes
Ctrl+H	08	BS	Yes/Yes
Ctrl+I	09	HT	Yes/Yes
Ctrl+J	0A	LF	Yes/Yes
Ctrl+K	0B	VT	Yes/No
Ctrl+L	0C	FF	Yes/No
Ctrl+M	0D	CR	Yes/No
Ctrl+N	0E	SO	Yes/No
Ctrl+O	0F	SI	Yes/No
Ctrl+P	10	DLE	Yes/No

Table E.4: VT100 Special Keys and Ctrl Keys (Continued)

Keys	Hex Code	Function Mnemonic	Encode/Decode
Ctrl+Q	11	DC1 or XON	Yes/No
Ctrl+R	12	DC2	Yes/No
Ctrl+S	13	DC3 or XOFF	Yes/No
Ctrl+T	14	DO4	Yes/No
Ctrl+U	15	NAK	Yes/No
Ctrl+V	16	SYN	Yes/No
Ctrl+W	17	ETB	Yes/No
Ctrl+X	18	CAN	Yes/No
Ctrl+Y	19	EM	Yes/No
Ctrl+Z	1A	SUB	Yes/No
Ctrl+[	1B	ESC	Yes/No
Ctrl+\	1C	FS	Yes/No
Ctrl+]	1D	GS	Yes/No
Ctrl+~	1E	RS	Yes/No
Ctrl+?	1F	US	Yes/No

The following table lists the VT100 ANSI mode and cursor keys for set and reset modes. Encoding and decoding is supported for all the cursor keys listed.

Table E.5: VT100 ANSI Set and Reset Mode Cursor Keys

Cursor Key	Mode Reset	Mode Set
Up	Esc [A	Esc O A
Down	Esc [B	Esc O B
Right	Esc [C	Esc O C
Left	Esc [D	Esc O D

The following table lists the VT100 PF1-PF4 key definitions. Encoding of each listed key is supported; decoding is not applicable.

Table E.6: VT100 PF1-PF4 Key Definitions

Key	Code Sequence
F1	Esc [O P
F2	Esc [O Q
F3	Esc [O R
F4	Esc [O S

The following table lists the ANSI mode control sequences for VT100 Terminal Emulation mode and indicates Avocent encoding/decoding support, where Yes = supported and No = not supported.

Table E.7: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
Esc # 4	Double Height Line - Bottom Half	No/No
Esc # 6	Double Width Line	No/No
Esc Z	Identify Terminal	No/No
Esc =	Keypad Application Mode	No/No
Esc >	Keypad Numeric Mode	No/No
Esc [Ps q	Load LEDs	No/No
Esc 8	Restore Cursor	No/Yes

Table E.7: VT100 ANSI Mode Control Sequences (Continued)

Control Sequence	Definition	Encode/Decode
Esc [<sol>; <par>;	Report Terminal Parameters <nbits>; <xspeed>; <rspeed>; <clkmul>; <flags>x	No/No
Esc [<sol> x	Request Terminal Parameters	No/No
Esc 7	Save Cursor	No/Yes
Esc [Pn; Pn r	Set Top and Bottom Margins	No/No
Esc # 5	Single Width Line	No/No
Esc [2; Ps y	Invoke Confidence Test	No/No
Esc [Ps n	Device Status Report	No/Yes
Esc [Ps J	Erase in Display	No/Yes
Esc [Ps K	Erase in Line	No/Yes
Esc H	Horizontal Tabulation Set	No/No
Esc [Pn; Pn f	Horizontal and Vertical Position	No/Yes
Esc D	Index	No/Yes
Esc E	Next Line	No/Yes
Esc M	Reverse Index	No/Yes
Esc c	Reset to Initial State	No/No
Esc [Ps; Ps;..;Ps 1	Reset Mode	No/No
Esc (A	Select Character Set G0 U.K.	No/No
Esc) A	Select Character Set G1 U.K	No/No
Esc (B	Select Character Set G0 ASCII	No/No
Esc) B	Select Character Set G1 ASCII	No/No
Esc (0	Select Character Set G0 Spec. Graphics	No/No
Esc) 0	Select Character Set G1 Spec. Graphics	No/No
Esc (1	Select Character Set G0 Alt. Character ROM Standard Character Set	No/No

Table E.7: VT100 ANSI Mode Control Sequences (Continued)

Control Sequence	Definition	Encode/Decode
Esc) 1	Select Character Set G1 Alt. Character ROM Standard Character Set	No/No
Esc (2	Select Character Set G0 Alt. Character ROM Special Graphics	No/No
Esc) 2	Select Character Set G1 Alt. Character ROM Special Graphics	No/No
Esc [Ps;..; Ps m	Select Graphic Rendition	No/No
Esc Ps;..;Ps h	Set Mode	No/No
Esc [Ps g	Tabulation Clear	No/No
Esc [Ps;Ps;..; Ps m	Character Attributes 7 - Reverse Video On	No/Reverse Video only
Esc [K or Esc [0 K	Erase from cursor to end of line	No/Yes
Esc [1 K	Erase from beginning of line to cursor	No/No
Esc [2 K	Erase entire line containing cursor	No/No
Esc [J or Esc [0 J	Erase from cursor to end of screen	No/Yes
Esc [1 J	Erase from beginning of screen to cursor	No/No
Esc [2 J	Erase entire screen	No/No
Esc [Ps;Ps;..Ps q	Programmable LEDs	No/No
Esc [Pt; Pb r	Scrolling Region	No/No
Esc H	Set tab at current column	No/No
Esc [g or Esc [0 g	Clear tab at current column	No/No
Esc [3 g	Clear all tabs	No/No
Esc [2 0 h	Modes to Set - New Line Only supports linefeed/new line column mode wraparound	No/Yes->-
Esc [2 0 l	Modes to Reset - Linefeed Only supports Linefeed/New Line Column mode wraparound	No/Yes->

Table E.7: VT100 ANSI Mode Control Sequences (Continued)

Control Sequence	Definition	Encode/Decode
Esc [? 1 h	Modes to Set - Cursor Key Mode Appl.	No/No
Esc [? 1 l	Modes to Reset - Cursor Key Mode Cursor	No/No
Esc [? 2 l	Modes to Reset VT52	No/No
Esc [? 3 h	Modes to Set - 132 columns	No/No
Esc [? 3 l	Modes to Reset - 80 columns	No/No
Esc [? 4 h	Modes to Set - Smooth Scroll	No/No
Esc [? 4 l	Modes to Reset - Jump Scroll	No/No
Esc [? 5 h	Modes to Set - Reverse Screen Mode	No/No
Esc [? 5 l	Modes to Reset - Normal Screen Mode	No/No
Esc [? 6 h	Modes to Set - Relative Origin Mode	No/No
Esc [? 6 l	Modes to Reset - Absolute Origin Mode	No/No
Esc [? 7 h	Modes to Set - Wraparound On	No/No
Esc [? 7 l	Modes to Reset - Wraparound Off	No/No
Esc [? 8 h	Modes to Set - Auto Repeat On	No/No
Esc [? 8 l	Modes to Reset - Auto Repeat Off	No/No
Esc [? 9 h	Modes to Set - Interlace On	No/No
Esc [? 9 l	Modes to Reset - Interlace Off	No/No
Esc [6 n	Report Cursor Position - Invoked by	No/No
Esc [P1; Pc R	Report Cursor Position - Response is	No/No
Esc [5 n	Status Report - Invoked by	No/No
Esc [0 n	Status Report - Response is terminal OK	No/No
Esc [3 n	Status Rpt - Response is terminal not OK	No/No

Table E.7: VT100 ANSI Mode Control Sequences (Continued)

Control Sequence	Definition	Encode/Decode
Esc [x or Esc [0 c	What are you? Invoked by	No/No
Esc [? 1; Ps c	What are you? Response is	No/No
Esc c	Reset	No/No
Esc # 8	Fill screen with Es	No/Yes
Esc [2; Ps y	Invoke Test(s)	No/No

VT220 terminal emulation

The following table lists the keystroke mapping (encoding) for VT220 emulation.

Table E.8: VT220 Encoding

VT220 Keyboard	PC Keyboard	VT200 Keyboard Byte Sequence
Delete	Delete	0x7F
Left Arrow	Left Arrow	Esc [D
Right Arrow	Right Arrow	Esc [C
Up Arrow	Up Arrow	Esc [A
Down Arrow	Down Arrow	Esc [B
Keypad /	Keypad /	/
Keypad *	Keypad *	*
Keypad -	Keypad -	-
Keypad +	Keypad +	+
Keypad .	Keypad .	.
Keypad 0..9	Keypad 0..9	0..9
F1	F1	Esc O P
F2	F2	Esc O Q
F3	F3	Esc O R
F4	F4	Esc O S
F6	F6	Esc [1 7 ~

Table E.8: VT220 Encoding (Continued)

VT220 Keyboard	PC Keyboard	VT200 Keyboard Byte Sequence
F7	F7	Esc [1 8 ~
F8	F8	Esc [1 9 ~
F9	F9	Esc [2 0 ~
F10	F10	Esc [2 1 ~
F11	F11	Esc [2 3 ~
F12	F12	Esc [2 4 ~
F13	Ctrl - F5	Esc [2 5 ~
F14	Ctrl - F6	Esc [2 6 ~
F15	Ctrl - F7	Esc [2 8 ~
F16	Ctrl - F8	Esc [2 9 ~
F17	Ctrl - F9	Esc [3 1 ~
F18	Ctrl - F10	Esc [3 2 ~
F19	Ctrl - F11	Esc [3 3 ~
F20	Ctrl - F12	Esc [3 4 ~

The following table lists the DSView management software decoding for VT220 Terminal Emulation mode.

Table E.9: VT220 Decoding

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Index	Esc D
New Line	Esc E
Reverse Index	Esc M
Escape	Esc O
Save cursor and attributes	Esc 7
Restore cursor and attributes	Esc 8
Up Arrow	Esc [A
Down Arrow	Esc [B

Table E.9: VT220 Decoding (Continued)

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Right Arrow	Esc [C
Left Arrow	Esc [D
Set cursor to home position	Esc [H
Set cursor to home position	Esc [f
Character attributes	Esc [m
Erase from cursor to end of line	Esc [K
Erase from cursor to end of screen	Esc [j
Programmable LEDs	Esc [q
What are You?	Esc [c
Set Mode	Esc [?
Delete 1 Character	Esc [P
Insert 1 Line	Esc [L
Delete 1 Line	Esc [M
Up Arrow	Esc [O A
Down Arrow	Esc [O B
Right Arrow	Esc [O C
Left Arrow	Esc [O D
Fill Screen with Es	Esc # 8
Up Arrow amount specified by Pn	Esc [Pn A
Down Arrow amount specified by Pn	Esc [Pn B
Right Arrow amount specified by Pn	Esc [Pn C
Left Arrow amount specified by Pn	Esc [Pn D
Erase parts of current line	Esc [Pn K
Erase parts of current screen	Esc [Pn J
Direct Cursor Addressing	Esc [Pn H
Direct Cursor Addressing	Esc [Pn f
Programmable LEDs	Esc [Pn q

Table E.9: VT220 Decoding (Continued)

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Scrolling Region	Esc [Pn r
Clear tabs	Esc [Pn g
Device status report	Esc [Pn n
What are you?	Esc [Pn c
Sat Mode	Esc [Pn h
Delete Pn Characters	Esc [Pn P
Insert Pn Characters	Esc [Pn L
Delete Pn Lines	Esc [Pn M
Insert Character	Esc [Pn @
Erase Pn Characters	Esc [Pn X

VT52 terminal emulation

The following table lists the DSView management software keystroke mapping (encoding) for VT52 Terminal Emulation mode.

Table E.10: VT52 Encoding

VT52 Keyboard	PC Character Sequence	VT152 Keyboard Byte Sequence
Delete	Delete	0x7F
Up Arrow	Up Arrow	Esc A
Down Arrow	Down Arrow	Esc B
Right Arrow	Right Arrow	Esc C
Left Arrow	Left Arrow	Esc D
Shift-F1	PF1	Esc P
Shift-F2	PF2	Esc Q
Shift-F3	PF3	Esc R
Shift-F4	PF4	Esc S

The following table lists the DS Management Software decoding for VT52 Terminal Emulation mode.

Table E.11: VT52 Decoding

VT52 Keyboard Function	VT52 Keyboard Byte Sequence
Cursor Up	Esc A
Cursor Down	Esc B
Cursor Right	Esc C
Cursor Left	Esc D
Cursor Home	Esc H
Reverse Linefeed	Esc I
Erase to end of screen	Esc J
Erase to end of line	Esc K

VT320 terminal emulation

The following table lists the DS Management Software keystroke mapping (encoding) for VT320 Terminal Emulation mode.

Table E.12: VT320 Encoding

VT320 Keyboard	PC Character Sequence	VT320 Keyboard Byte Sequence
Escape Key (ESC)	Esc	0x1B
F1	F1	Esc O P
F2	F2	Esc O Q
F3	F3	Esc O R
F4	F4	Esc O S
F5	F5	Esc O T
F6	F6	Esc [1 7 ~
F7	F7	Esc [1 8 ~
F8	F8	Esc [1 9 ~
F9	F9	Esc [2 0 ~
F10	F10	Esc [2 1 ~

Table E.12: VT320 Encoding (Continued)

VT320 Keyboard	PC Character Sequence	VT320 Keyboard Byte Sequence
F11	F11	Esc [2 3 ~
F12	F12	Esc [2 4 ~
F13	Ctrl - F5	Esc [2 5 ~
F14	Ctrl - F6	Esc [2 6 ~
F15	Ctrl - F7	Esc [2 8 ~
F16	Ctrl - F8	Esc [2 9 ~
F17	Ctrl - F9	Esc [3 1 ~
F18	Ctrl - F10	Esc [3 2 ~
F19	Ctrl - F11	Esc [3 3 ~
F20	Ctrl - F12	Esc [3 4 ~
Insert	Insert	Esc [1 ~
Home	Home	Esc [2 ~
Delete	Delete	Esc [4 ~
End	End	Esc [5 ~
Up Arrow	Up Arrow	Esc [A
Down Arrow	Down Arrow	Esc [B
Left Arrow	Left Arrow	Esc [D
Right Arrow	Right Arrow	Esc [C

The following table lists the DS Management Software decoding for VT320 Terminal Emulation mode.

Table E.13: VT320 Decoding

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Index	Esc D
New Line	Esc E
Reverse Index	Esc M
Escape O	Esc O

Table E.13: VT320 Decoding (Continued)

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Save cursor and attributes	Esc 7
Restore cursor and attributes	Esc 8
Up Arrow	Esc [A
Down Arrow	Esc [B
Right Arrow	Esc [C
Left Arrow	Esc [D
Set cursor to home position	Esc [H
Set cursor to home position	Esc [f
Character Attributes	Esc [m
Erase from cursor to end of line	Esc [K
Erase from cursor to end of screen	Esc [J
Programmable LEDs	Esc [q
What are You?	Esc [c
Set Mode	Esc [?
Delete 1 Character	Esc [P
Insert 1 Line	Esc [L
Delete 1 Line	Esc [M
Up Arrow	Esc O A
Down Arrow	Esc O B
Right Arrow	Esc O C
Left Arrow	Esc O D
Fill Screen with Es	Esc # 8
Up Arrow amount specified by Pn	Esc [Pn A
Down Arrow amount specified by Pn	Esc [Pn B
Right Arrow amount specified by Pn	Esc [Pn C

Table E.13: VT320 Decoding (Continued)

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Left Down Arrow amount specified by Pn	Esc [Pn D
Erase parts of current line	Esc [Pn K
Erase parts of current screen	Esc [Pn J
Direct Cursor Addressing	Esc [Pn H
Direct Cursor Addressing	Esc [Pn f
Programmable LEDs	Esc [Pn q
Scrolling Region	Esc [Pn r
Clear tabs	Esc [Pn g
Device status report	Esc [Pn n
What are you?	Esc [Pn c
Sat Mode	Esc [Pn h
Delete Pn Characters	Esc [Pn P
Insert Pn Lines	Esc [Pn L
Delete Pn Lines	Esc [Pn M
Insert Character	Esc [Pn @
Erase Pn Characters	Esc [Pn X

Appendix F: Menus, Toolbars and Commands

Drop-down menus

The DSView management software, DSWebview software and Video Viewer windows each contain a number of commands that may be accessed using the drop-down menus located along the top of the windows.

Shortcut menus and commands

You may access shortcut menus within the DSView management software and DSWebview software windows by selecting a DS appliance, target device or port and right-clicking to display a shortcut menu.

DSView management software shortcut menus and commands

In the DS topology view, you may right-click on any DS appliance's name or IP address in the DSView management software window to display a shortcut menu containing ten commands:

- Collapse - Clicking on this command will hide the port information associated with the selected name or IP address
- Expand - Clicking on this command will display the port information associated with the selected name or IP address
- Properties
- Update DSView Management Software Names from Appliance (DS appliances, DSR switches and CPS810/1610 serial over IP network appliances only)
- Rename
- Delete
- Permissions
- Reboot
- Show Version Number
- Update with Appliance Names

In the DS topology view, you may right-click on any DS appliance port to display a shortcut menu containing six commands:

- Connect (if the port is not connected) or Disconnect (if the port is connected)
- Properties
- Rename
- Permissions
- Privacy Mode
- View Connected Users

In the DS topology view, you may right-click on any EVR1500 device or generic appliance to display a shortcut menu containing four (generic appliance) or six (EVR1500 device) commands:

- Properties
- Delete
- Rename
- Permissions
- Configure (EVR1500 devices only)
- Connect or Disconnect (EVR1500 devices only)

DSWebview software window shortcut menus and commands

In the DS topology view, you may right-click on any DS appliance name or IP address in the DSWebview software window to display a shortcut menu containing four commands:

- Reboot
- Collapse
- Expand
- Firmware Version

In the DS topology view, you may right-click on any port to display a shortcut menu containing three commands:

- Connect (if the port is not connected) or Disconnect (if the port is connected)
- Private Connect
- View Connected Users

Video Viewer window thumbnail shortcut menus and commands

In the Video Viewer window, you may right-click on a thumbnail to display a shortcut menu containing three commands:

- View Interactive Session
- Enable
- Credentials

DSView management software window toolbar

The DSView management software window toolbar may be used to quickly access common commands used during a DSView session. Select *View* - *Tool Bar* from the menu to display the DSView management software window toolbar. Table F.1 lists the commands available from the DSView management software window toolbar.

Table F.1: DSView Management Software Window Toolbar Icons

Icon	Description
	Configure - Connects an EVR1500 environmental monitor.
	Connect - Connects a CPS appliance, DS appliance or DSR switch port, EVR1500 environmental monitor or generic appliance.
	Privacy Mode Connect - Connects a CPS appliance, DS appliance or DSR switch port using Privacy mode. See *Using Privacy mode* on page 51 for more information.
	Connected Users - Displays the DS users connected to a CPS appliance, DS appliance or DSR switch port or channel. See *Viewing Ports, Outlets, Target Devices and Connected DS Users* on page 52 for more information.
	Terminate Current Connection - Disconnects a CPS appliance, DS appliance or DSR switch port, EVR1500 environmental monitor or generic appliance.
	Reboot - Reboots a CPS appliance, DS appliance or DSR switch port, EVR1500 environmental monitor, generic appliance, SPC device or SPC device outlet.
	User Permissions - Displays the Multi-User Operations dialog box. See *Adding, modifying and removing user access to multiple appliances or servers* on page 47 for more information.
	Group Operations - Displays the Group Operations dialog box. See *Managing Multiple Appliances and Devices* on page 54 for more information.
	Delete - Removes a CPS appliance, DS appliance, DSR switch, EVR1500 environmental monitor, generic appliance or SPC device from your system.
	Permissions - Displays the Permissions dialog box, which allows you to change the permissions of a DS appliance or port. See *Adding and Managing DS Users* on page 44 for more information.
	Properties - Displays the properties dialog box for a selected CPS appliance, DS appliance, DSR appliance or port, EVR1500 environmental monitor, generic appliance, SPC device or SPC device outlet.
	Topology View - Displays the DS Topology view in the DSView management software window. See *DS topology view* on page 6 for more information.
	Server List View - Displays the Server view in the DSView management software window. See *Server view* on page 8 for more information.
	Refresh - Refreshes the DSView management software window.

Table F.1: DSView Management Software Window Toolbar Icons (Continued)

Icon	Description
	System Settings - Displays the Global Settings dialog box, which enables you to specify settings related to your system, such as connections, polling and the creation of debug files. See *Changing the System Settings* on page 58 for more information.
	Keyboard Macros - Displays the Keyboard Macro Configuration dialog box, which allows you to configure global keyboard macros. See *Global Keyboard Macros* on page 64 for more information.
	Update Appliance Firmware - Displays the Firmware Update dialog box. See *Updating Firmware* on page 16 for information on updating DS appliance firmware.

Telnet application window menus and commands

Serial DS appliances and target devices are operated through a Telnet application window. When you are operating a DS appliance or target device using the DS appliance, you will be provided with several optional commands.

Telnet application menu

Exit

This command will exit the Telnet application Client interface and return users to the DSView management software window. If the option to *Prompt on Exit* (see the *Preferences* section of this appendix) is enabled and a connection is active, the DS user will be prompted to confirm the exit. If no connection is active, the DSView management software window will exit without a prompt.

View menu

History

When this menu option is checked, the DS user will be switched to History mode. Here the DS user may scroll through a history of the Telnet application session up to the current point. While the DS user is in History mode, all new data is buffered and may be viewed by scrolling to the end of the history. DS users may exit History mode at any time by pressing the **Esc** key.

Go to Beginning

This command moves the cursor to the beginning of the history file.

Previous Page

This command moves the cursor back one page in the history file.

Next Page

This command moves the cursor forward one page in the history file.

Go to End

This command moves the cursor to the end of the history file.

Options menu

Preferences

When this menu option is selected, a dialog box that displays application preferences will appear. Here DS users may change options that pertain to the appearance of the Telnet application.

Session Properties

This option activates the Property Sheet dialog box where node session properties for the port that is currently active. The dialog box has two tabs, Terminal and Login Scripts.

Terminal

This tab allows you to alter the settings that determine how text in the Telnet application Client interface is formatted.

Login Scripts

This tab allows you to create scripts that answer simple login questions. These scripts allow DS users to completely automate the login process.

View commands are also accessible through menu icons in the Terminal window.

Appendix G: Glossary

DS appliance

A network appliance, such as a DS appliance, DSR switch or CPS serial over IP network appliance which is managed by DS Management Software.

Target device

A server, router or other device that is attached to a DS appliance.

DS topology

A hierarchy of DS appliances, cascade devices and target devices.

DSAuth Server

A central repository for DS topology information, DS user permissions and centralized services such as authentication, access control, audit, appliance monitoring and DSView management software/appliance updates. DS users may define a primary and backup DSAuth Server.

DS permissions

Defines the set of DS appliances and target devices to which a DS user has access within the DS topology.

DSView management software

A Win32 application that allows DS users to manage target devices through DS appliances. The DSView management software window may be used for IP-based video, serial and power management sessions. You may also create and alter DS topology and permission information that is stored on a DSAuth Server using the DSView management software.

DSWebview Server

A web gateway that allows DS users to manage target devices through DS appliances from an industry-standard browser. The gateway allows for IP-based video and serial management sessions.

DS user

An authenticated user of the DSView management software or DSWebview software.

Local user

A user of a DS appliance local port.

INDEX

Numerics

A

B

C

E

F

M

N

O

P

R

S

T

U

W

X

LIMITED WARRANTY

Avocent Corporation warrants to the original retail purchaser that this product is and will be free from defects in materials and workmanship for a period of 24 months from the date of purchase.

Additionally, all Avocent products carry an unconditional thirty-day satisfaction guarantee. If, for any reason, you are dissatisfied with the performance of this product, you may return it to the point of purchase for a refund of the purchase price (excluding shipping charges). This guarantee does not apply to special order products, and may not be available through all resellers. During the warranty period, purchaser must promptly call Avocent for a RETURN MATERIALS AUTHORIZATION (RMA) number. Make sure that the RMA number appears on the packing slip, proof of purchase, AND ON THE OUTSIDE OF EACH SHIPPING CARTON. Unauthorized returns or collect shipments will be refused.

Ship prepaid to: Avocent Corporation
4991 Corporate Drive
Huntsville, AL 35805 U.S.A.
Telephone: (256) 430-4000

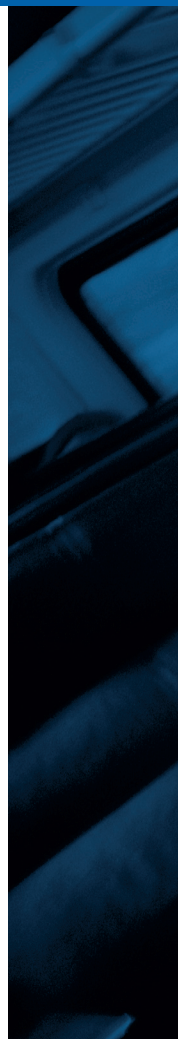
The above limited warranty is voided by occurrence of any of the following events, upon which the product is provided as is, with all faults, and with all disclaimers of warranty identified below:

1. If defect or malfunction was caused by abuse, mishandling, unauthorized repair, or use other than intended.
2. If unauthorized modifications were made to product.
3. If unreported damages occurred in any shipment of the product.
4. If damages were due to or caused by equipment or software not provided by Avocent.
5. If the product is used with non-grounded or incorrectly polarized AC power.
6. If the product is used in contradiction to any instruction provided by any User Guide or Instruction Sheet provided to you or with the product.
7. If the product is damaged due to power surges, water exposure or act of God including lightning.

EXCEPT AS SPECIFICALLY PROVIDED ABOVE AND TO THE MAXIMUM EXTENT ALLOWED BY LAW, AVOCENT CORPORATION DISCLAIMS ALL WARRANTIES AND CONDITIONS WHETHER EXPRESS, IMPLIED, OR STATUTORY AS TO ANY MATTER WHATSOEVER INCLUDING, WITHOUT LIMITATION, TITLE, NON-INFRINGEMENT, CONDITION, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR OR INTENDED PURPOSE.

EXCEPT AS EXPRESSLY PROVIDED ABOVE AND TO THE MAXIMUM EXTENT ALLOWED BY LAW, AVOCENT CORPORATION SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION, LOSS OF PROFIT, LOSS OF BUSINESS, LOSS OF INFORMATION, FINANCIAL LOSS, PERSONAL INJURY, LOSS OF PRIVACY OR NEGLIGENCE) WHICH MAY BE CAUSED BY OR RELATED TO, DIRECTLY OR INDIRECTLY, THE USE OF A PRODUCT OR SERVICE, THE INABILITY TO USE A PRODUCT OR SERVICE, INADEQUACY OF A PRODUCT OR SERVICE FOR ANY PURPOSE OR USE THEREOF OR BY ANY DEFECT OR DEFICIENCY THEREIN EVEN IF AVOCENT CORPORATION OR AN AUTHORIZED AVOCENT DEALER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES.

Avocent
The Power of Being There®



For Technical Support:

Email: support@avocent.com
www.avocent.com

Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama 35805-6201 USA
Tel: +1 256 430 4000
Fax: +1 256 430 4031

Avocent International Ltd.
Avocent House, Shannon Free Zone
Shannon, County Clare, Ireland
Tel: +353 61 715 292
Fax: +353 61 471 871

Avocent Asia Pacific
Singapore Branch Office
100 Tras Street, #15-01
Amara Corporate Tower
Singapore 079027
Tel: +656 227 3773
Fax: +656 223 9155

Avocent Germany
Gottlieb-Daimler-Straße 2-4
D-33803 Steinhagen
Germany
Tel: +49 5204 9134 0
Fax: +49 5204 9134 99

Avocent Canada
50 Mural Street, Unit 5
Richmond Hill, Ontario
L4B 1E4 Canada
Tel: +1 877 992 9239
Fax: +1 877 524 2985

590-410-001B