Avocent® ACS6000 Advanced Console Server

Command Reference Guide

Technical Support Site

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

TABLE OF CONTENTS

1 Introduction, Navigation and Commands 1
1.1 Access Options and How to Log in to the CLI 1
1.2 Configuration Tasks Performed With the CLI 2
1.3 CLI Navigation 2
1.4 Autocompletion 4
1.5 Parameters 4
1.6 Command Line Syntax 4
2 CLI Command Set 7
2.1 Commands Used for the CLI 7
2.1.1 add 7
2.1.2 cd 7
2.1.3 commit 8
2.1.4 delete 8
2.1.5 exit/quit 8
2.1.6 ftp 9
2.1.7 help 9
2.1.8 list_configuration 9
2.1.9 ls 10
2.1.10 opiepasswd 11
2.1.11 pwd 11
2.1.12 passwd 11
2.1.13 revert 11
2.1.14 scp 12
2.1.15 set 12
2.1.16 show 12
2.1.17 wiz 13
2.1.18 connect 13
2.1.19 sniff 14
2.1.20 share 14
2.1.21 disconnect 15
2.1.22 cycle, on, off, lock and unlock 15
2.2 Special Multi-session Commands 16
2.2.1 list_shared_session 16
2.2.2 kill_shared_session 16
2.2.3 sendmsg 17
2.2.4 show_databuf and show_appliance_databuf 17
2.2.5 cleandbuf and clean_appliance_databuf 17
2.3 CLI Equivalent Actions to Web Manager Checkbox Selection 18
3 Port Access and Configuration Examples 21
3.1 View Information About the Console Server and Connected Devices 21

3.2 Connect to a Device Console Connected to a Serial Port 23
3.3 Accessing Serial Ports using ts_menu 24
3.4 Manage Power for a Device Connected to an Outlet on a PDU 24
3.5 Port Configuration Examples 24
4 CLI Overview for Administrators 27
4.1 System 27
4.2 System/Security 27
4.2.1 System/Date and Time 28
4.2.2 System/Help and Language 29
4.2.3 System/General 29
4.2.4 System/Boot Configuration 30
4.2.5 System/Information 30
4.2.6 System/Usage 31
4.3 Network 31
4.3.1 Network/Settings 31
4.3.2 Network/IPv4 and IPv6 32
4.3.3 Network/Devices 32
4.3.4 Network/Hosts 33
4.3.5 Network/Firewall 35
4.3.6 Network/IPSec(VPN) 35
4.4 Network/SNMP 35
4.4.1 Wiz command 35
4.5 Ports 36
4.5.1 Auxiliary ports 40
4.6 Pluggable Devices 40
4.7 Authentication 40
4.8 Users 42
4.9 Events_and_Logs 44
4.10 Power Management 45
4.11 Active Sessions Information 46
5 Appendices 49
Appendix A: Enabling Firmware Upgrades When the Boot Image is not in Flash 49
Appendix B: Migration CLI 50
5.0.1 Access rights 50
5.0.2 Exceptions 50
Appendix C: Su and Sudo Commands 53
5.0.3 Su command 53
5.0.4 Sudo command 54

1 INTRODUCTION, NAVIGATION AND COMMANDS

The Avocent® ACS6000 advanced console server is a 1U appliance that serves as a single point for access and administration of connected devices, such as target device consoles, modems and power devices. Console servers support secure remote data center management and out-of-band management of IT assets from any location worldwide.

On console servers, administration can be performed and connected devices can be accessed with the Command Line Interface (CLI) utility, with the web manager or with DSView™ 4 management software. Multiple users and administrators can be logged into the console server and connected to ports at the same time.

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

This guide describes how to access and navigate the CLI utility and how to use it after the console server has been installed and assigned an IP address. For information on how to install or operate your console server using the web manager, see the Avocent ACS6000 Installation/Administration/User Guide.

The console ports of servers, external modems or power distribution units (PDUs) can be connected to serial ports on the console server. Supported PDUs include Avocent® PM1000/2000/3000s, Vertiv™ MPH2 Rack PDUs and RPC2 cards, Cyclades™ PM IPDUs, Avocent SPC power devices and Server Technology CDUs. Either a PDU or an external modem can be connected to the AUX/Modem port if the port is not factory-configured for an internal modem.

1.1 Access Options and How to Log in to the CLI

The CLI utility can be accessed in the following ways:

- Through a local terminal or a computer that has a terminal emulation program connected to the console port of the console server with session settings of 9600, 8, N and 1, with no flow control.
- After the console server is connected to the network and has an IP address, it can be accessed by one of the following methods:
  - An SSH or Telnet client on a remote computer (if the SSH or Telnet protocol is enabled in the selected Security Profile)
  - With the *Web Manager - Access - Appliance Viewer* button
  - With DSView management software

NOTE: For details on the remote access methods and IP address configuration options, see the Avocent ACS6000 Installation/Administration/User Guide.

Administrators have full access to the CLI and to connected devices. An administrator can authorize regular users to access ports, manage power, manage data buffer storage and use one or more console server administration tools. Users can always change their own passwords.

To start the CLI:

1. Access the CLI through the console port, with Telnet, SSH or through the web manager.
2. Enter the username and password at the prompt. The cli-> prompt appears.

```
Welcome to ACS6000 <host name>.
Type help for more information
--:- / cli->
```

NOTE: The default password for admin is avocent **and for root is** linux**. The password for these users may have been changed during installation of the console server. If not, change the default root and admin passwords to avoid potential security breaches.**

1.2 Configuration Tasks Performed With the CLI

NOTE: This manual provides some configuration procedures as examples of how to use the CLI; an administrator who wants to use the CLI for configuration should reference the installation/administration/user guide for more information.

The navigation structure of the CLI mirrors that of the web manager. Options and parameters are also the same, except that spaces in web manager options and parameters are replaced with underscores (_), as in: system_tools. Examples that show how to select an option in the web manager use a dash surrounded by two spaces (-). In the CLI, two similar options in a path are separated by a forward slash (/).

For example, in the web manager, user configuration is done when an administrator selects - *Users* - *Local Accounts* - *User Names* to get to the User Names screen. To navigate to the equivalent configuration level in the CLI, an administrator would use the cd command followed by the path: **cd /users/local_accounts/user_names**.

Administrators should log into the CLI in one window and log into the web manager in another window to see how the menu options in the web manager map to the navigation options in the CLI. Configuration with the CLI also requires mastery of the following information on CLI navigation and of the CLI commands shown in Chapter 2.

1.3 CLI Navigation

The CLI navigation options are in a nested tree configuration.

NOTE: When a command line is shown in an example, and the step starts with "Enter," or when a syntax example is given, the user should type the command as shown and then press Enter**. The** Enter **key is not shown in command line examples unless needed for clarity.**

When a user logs in the CLI, the prompt indicates the user is at the / level.

```
--:- / cli->
```

No parameters can be set at this level of the navigation tree.

At any CLI prompt at any level, if you type **cd** and press **Tab Tab**, the navigation options (path elements) for that level are listed. Different options appear for administrators and for authorized users.

- When an administrator types the **cd** command and then presses **Tab Tab** at the / prompt, the following navigation options (path elements) appear.

```
--:- / cli-> cd<Tab><Tab>
```

access/	monitoring/	system/
active_sessions/	network/	
system_tools/		
authentication/	pluggable_devices/	users/
change_password/	ports/	
events_and_logs/	power_management/	

When a regular user types the **cd** command and then presses **Tab Tab** at the / prompt, the following navigation options appear.

```
--:- / cli-> cd<Tab><Tab>
access/ power_management/
```

Enter **cd** <one_or_more_path_elements> to move down one or more levels of the navigation tree:

```
--:- / cli-> cd system_tools
```

A prompt like the following appears at each level:

```
--:- system_tools cli->
```

NOTE: CLI commands are case sensitive.

At any level, you can press **Tab Tab** at the prompt to see the commands that can be entered at the current level.

```
---:- system_tools cli-><Tab><Tab>
batch_mode ls scp
cd opiepasswd shell
commit passwd show
echo pwd shutdown
exit quit upgrade_firmware
ftp reboot whoami
help restore_configuration wiz
hostname revert
list_configuration save_configuration
---:- system_tools cli->
```

If you know the path, you can enter multiple path elements in a single command separated with forward slashes (/).

```
--:- / cli-> cd ports/serial_ports/
--:- serial ports cli->
```

Enter **cd ..** to move up one level of the navigation tree. Enter **cd ../..[/..]** to move up multiple levels.

```
--:- serial ports cli-> cd ../..
--:- / cli->
```

1.4 Autocompletion

Autocompletion allows you to type the first few letters of a command or navigation option and then press **Tab**. The rest of the name is filled in automatically if the letters typed are unique to one command or to a navigation option at that level. If the letters match more than one of the commands or navigation options for that level, the matching options are listed.

For example, if you type **cd acc** and press **Tab** at the CLI prompt from the / level, the access option will be completed.

```
--:- / cli-> cd acc<Tab>
--:- / cli-> cd access
```

If you then press **Enter**, you are changed to the access level, and the access level prompt appears.

```
--:- access cli->
```

The following example illustrates a case when more than one command matches the letters typed.

```
--:- / cli-> sh<Tab>
shell show
```

1.5 Parameters

Some CLI commands take parameters. If you press **Tab Tab** after a command that requires a parameter, you are prompted to enter the parameter.

1.6 Command Line Syntax

NOTE: Square brackets ([ ]) denote an optional element. Each element is separated by a space. There are no spaces between sub-elements.

Command only (help, pwd):

```
--:- <current_level> cli-> <command>
```

Commands with paths only (cd, ls, add):

--:- <current_level> cli-> **<command> [Path]**

Commands with targets (del):

--:- <current_level> cli-> **<command> [Path] <Targets>**

Commands that require parameters (set):

--:- <current_level> cli-> **<command> [Path] <Params>**

Commands with values only (sendmsg, ftp…):

--:- <current_level> cli-> **<command> [Path] <Values>**
where:
Path := path_elem[/path_elem]*
path_elem := . | .. | Section_Label | ^/
Targets := Row_Label(,Row_Label)
Params := Param_Names=PValues
Param_Names := Param_Label(:Param_Label)*
PValues := Value_text(,Value_text)*
Values := Value_text Value_text
Section_Label
Param_Label
Value_text := labels or data from the UIC.

Syntax used:

^ : beginning of the element
* : 0 - many
| : or
() : group

This page intentionally left blank.

2 CLI COMMAND SET

2.1 Commands Used for the CLI

This chapter describes the general commands used when accessing the console server with the command line interface.

NOTE: Most of the commands work from any location when the path to the command parameter is included.

NOTE: The word "node" refers to an entity such as a route, host or user, which can be added, configured or deleted.

2.1.1 add

Add a node.

Syntax:

```
--:- / cli-> add <Path>
```

Example:

```
--:- / cli-> add network/hosts
--:#- [hosts] cli->
```

2.1.2 cd

Change directory (level).

Syntax:

```
--:- / cli-> cd <Path>
```

Example:

```
--:- / cli-> cd access
```

Displays the following:

```
--:- access cli->
```

Example:

```
--:- access cli-> cd ..
-or-
--:- access cli-> cd ../
```

Moves up one directory level and displays the following:

```
--:- / cli->
```

Example:

```
--:- access cli-> cd /
```

Moves to the top level and displays the following:

```
--:- / cli->
```

Example:

```
--:- access cli-> cd /information
```

Displays the following:

```
--:- information cli->
```

2.1.3 commit

Save settings.

Syntax:

```
**:- settings cli-> commit
```

2.1.4 delete

Delete a node.

Syntax:

```
--:- / cli-> delete <Path> <parameter>
```

2.1.5 exit/quit

Exit the CLI and return to the login prompt.

Syntax:

```
--:- / cli-> exit
```

-or-

```
--:- / cli-> quit
```

2.1.6 ftp

Connect to a remote FTP server.

Syntax:

```
--:- / cli-> ftp [<server_IP_address>|<hostname>]
```

NOTE: You must log into the CLI as root to have full control over the local directory path. All normal FTP commands apply.

2.1.7 help

Generate a help message about how to navigate the CLI.

Syntax:

```
--:- / cli-> help
```

```
- Thank you for using the cli -
This interface allows you to easily modify configurations
to customize and define the functionality of your unit.
Press <tab> <tab> to see the list of available commands.
Please refer to the Reference Guide for a description of
commands, special keys and additional information on how to
use this interface.
Some basic and useful keys are:
 up/down arrow - navigates up/down in the command history
 tab (once/twice) - shows the next possible option(s)
Other hints:
 Use backslash '\' to escape spaces, '\' and other control
 characters when assigning values to parameters.
```

2.1.8 list_configuration

List the configuration in a format that allows pasting the output directly on the appliance session (console, SSH or Telnet) in order to (re)configure the unit.

All configurable parameters are listed under the current node. When the parameter is not configured, the parameter name has the number sign character (#) as its prefix.

Syntax:

```
--:- / cli-> list_configuration
```

Example:

```
.list configuration of network device eth0:
--:- cli-> cd network/devices/eth0
--:- eth0 cli-> list_configuration
echo off
cd /network/devices/eth0
batch_mode
set status=enabled
set ipv4_method=dhcp
#set ipv4_method=static #ipv4_address=192.168.160.10 #ipv4_mask=255.255.255.0
#set ipv4_method=ipv4_address_unconfigured
#set ipv6_method=stateless
#set ipv6_method=dhcpv6
#set ipv6_method=static #ipv6_address= #ipv6_prefix_length=
set ipv6_method=ipv6_address_unconfigured
set mode=auto
submit
echo on
commit
--:- eth0 cli->
```

NOTE: Check the configuration of the program used to open a session against the appliance (SSH/Telnet, TeraTerm / HypertTerminal for console, and so on) to avoid the inclusion of a line feed character in lines that exceed terminal width, because this will affect the past operation.

2.1.9 ls

Show the available directories or subnodes at the current location.

Syntax:

```
--:- / cli-> ls
```

Example:

```
--:- / cli-> ls authentication
appliance_authentication/
authentication_servers/
--:- / cli->
```

2.1.10 opiepasswd

Configure a one time password (OTP) for the local user. After you type the command, you will be asked for the pass phrase to use for the OTP.

NOTE: Use this command to restart the sequence number.

Syntax:

```
--:- / cli-> opiepasswd -f -c <username>
```

Example:

```
opiepasswd -f -c teste
Adding teste:
Only use this method from the console; NEVER from remote. If you are using telnet, xterm, or a dial-
in, type ^C now or exit with no password.
Then run opiepasswd without the -c parameter.
Using MD5 to compute responses.
Enter new secret pass phrase:
Again new secret pass phrase:

ID teste OTP key is 499 AC0241
FOOD HUGH SKI ALMA LURK BRAD
```

2.1.11 pwd

Display the path to the current level (print working directory).

Syntax:

```
--:- / cli-> pwd
```

2.1.12 passwd

Configure the password for the current user. The terminal does not echo the password.

Syntax:

```
--:- / cli-> passwd
```

2.1.13 revert

Undo a previous parameter setting.

Syntax:

```
**:- / cli-> revert
```

2.1.14 scp

Perform a secure shell copy.

Syntax:

```
--:- / cli-> scp [[user@]host1:]file1 [...] [[user@]host2:]file2
```

2.1.15 set

Set a parameter.

Syntax:

```
--:- / cli-> set <Path> <Parameter>=<Value>
```

After a parameter has been changed using the set command, a pair of asterisks appear at the beginning of the CLI prompt.

```
**:- / cli->
```

Save the change:

```
**:- / cli-> commit
```

-or-

Undo the change:

```
**:- / cli-> revert
```

NOTE: After a commit or revert command, the asterisks at the beginning of the CLI prompt are replaced by hyphens. Asterisks will not appear after the execution of the set command if using wizard mode, which can be recognized by a prompt that has a pound sign after the colon and the current directory in square brackets (example, --:#- [hosts] cli->).

2.1.16 show

Show the content of the current location (shows tables and parameters with current values).

Syntax:

```
--:- / cli-> show
```

Example:

```
--:- language cli-> show
appliance_languate = english
--:- / cli->
```

2.1.17 wiz

Configures the IP parameters for the Eth0 interface. Shows the current configuration and asks for new values for the following parameters:

- Status of the interface (enabled or disabled)
- IPv4 method (dhcp or static)
- IPv6 method (dhcp or static)
- IP address, mask and gateway (if static is chosen for either of the previous parameters)
- DNS Primary Server, Secondary Server, Domain Name and Hostname
- Enable or disable IPv6 support

After setting all parameters, confirm that all parameters are correct to save them.

2.1.18 connect

Connect to a serial port.

Syntax:

```
--:- access cli-> connect <port_name>
```

Example:

```
--:- access cli-> connect 77-77-70-p-2
```

-or-

(Optional) From the default directory:

```
--:- / cli-> connect access/77-77-70-p-2
```

Displays the following:

```
Password:
```

-or-

Type the hotkey to suspend the connection:

Ctrl + z

NOTE: The connect, sniff and share commands allow you to connect to serial ports. These commands require authentication when single sign-on is disabled, so the password must be entered to authenticate the user in the authentication type configured for the serial port. If single sign-on is enabled or the user has already been authenticated, the session is opened.

2.1.19 sniff

Connect to a serial port as an additional, view-only user.

Syntax:

```
--:- access cli-> sniff <port_name>
```

Example:

```
--:- access cli-> sniff 77-77-70-p-2
```

Displays the following:

```
Password:
```

-or-

Type the hotkey to suspend the connection:

Ctrl + z

2.1.20 share

Connect to a serial port as an additional, read/write user.

Syntax:

```
--:- access cli-> share <port_name>
```

Example:

```
--:- access cli-> share 77-77-70-p-2
```

Displays the following:

```
Password:
```

-or-

Type the hotkey to suspend the connection:

Ctrl + z

2.1.21 disconnect

Use the text session hot key to suspend the target session and return to the CLI.

Syntax:

Ctrl+z

2.1.22 cycle, on, off, lock and unlock

Control power on outlets on a PDU that is either connected to a serial port or to the AUX/Modem port when the port is enabled and configured with the Power Profile.

NOTE: Lock and unlock commands are only supported on Cyclades and Avocent PDUs.

To power control (on, off, cycle) all outlets of PDUs or outlets merged to a target (serial port configured as CAS profile with merged outlets):

1. Go to the access level.

```
--:- / cli-> cd/access
```

2. Launch the power command with the argument being the target name or PDU ID.

```
--:- access cli-> [cycle|on|off][<PDU_ID>]|<target name>]
```

To power control (on, off, cycle) outlets of one specific PDU:

1. Go to the PDU level under access.

```
--:- / cli-> cd access/<PDU_ID>
```

2. Launch the power command with a specific outlet (number or name), range of outlets (use a hyphen to specify the range) or list of outlets (number or name separated by a comma).

```
--:- <PDU_ID> cli-> [cycle|on|off][<outlet name>|<outlet number>]
```

-or-

```
--:- <PDU_ID> cli-> [cycle|on|off]<outlet number>-<outlet number]
```

-or-

```
--:- <PDU_ID> cli-> [cycle|on|off]<outlet number>,<outlet number>
```

To power control (on, off, cycle, lock, unlock) outlets of one specific PDU under the power management level:

1. Go to the outlet level for the specific PDU.

--:- / cli-> cd power_management/pdus/<PDU_ID>/outlets

2. Launch the power command with a specific outlet number, range of outlets (use a hyphen to specify the range) or list of outlets (number or name separated by a comma).

--:- outlets cli-> [cycle|on|off] [<outlet number>]

-or-

--:- outlets cli-> [cycle|on|off] <outlet number>-<outlet number]

-or-

--:- outlets cli-> [cycle|on|off] <outlet number>,<outlet number>

2.2 Special Multi-session Commands

The following commands require navigation to an enabled and configured port to which one or more users are simultaneously connected. To get to the port, enter the following command.

--:- / cli-> cd access/<serial_port_ID>

2.2.1 list_shared_session

List the users connected to the shared serial port.

Syntax:

--:- <serial_port_ID> cli-> list_shared_session

2.2.2 kill_shared_session

Terminate the connection of a user on the port. The user is returned to the cli-> prompt.

Syntax:

--:- <serial_port_ID> cli-> kill_shared_session <username>

Example:

```
--:- <serial_port_ID> cli-> kill_shared_session admin@139
```

2.2.3 sendmsg

Send a message to a user connected to the port.

Syntax:

```
--:- <serial_port_ID> cli-> sendmsg <username> <message>
```

Example:

```
--:- <serial_port_ID> cli-> sendmsg admin@139 You are being terminated.
```

2.2.4 show_databuf and show_appliance_databuf

View the data buffer files for the port. Data buffering must be enabled in the CAS Profile for the port and the user must be authorized for data buffer management.

Syntax:

```
--:- <serial_port_ID> cli-> show_databuf
```

View the data logging for the appliance. Appliance Session Data logging must be enabled in Events and Logs/Appliance Logging

Syntax:

```
--:- / cli -> show_appliance_databuf
```

The following commands are available for show data buffering:

- Return - Scroll forward one line.
- Ctrl + F - Scroll forward one window.
- Ctrl + B - Scroll backward one window.
- /pattern - Search foward in the file for the first line containing the pattern.
- ?pattern - Search backward in the file for the first line containing the pattern.
- n - Repeat the search.
- q - Quit.

2.2.5 cleandbuf and clean_appliance_databuf

Clear the data buffer. Data buffering must be enabled in the CAS Profile or the port and the user must be authorized for data buffer management.

Syntax:

```
--:- <serial_port_ID> cli-> cleandbuf
```

Clear the data logging for the appliance. Appliance Session Data logging must be enabled in Events and Logs/Appliance Logging

Syntax:

```
--:- / cli -> clean_appliance_dbuf
```

2.3 CLI Equivalent Actions to Web Manager Checkbox Selection

NOTE: The following example procedure, which configures IPv6, illustrates the actions to use in the CLI to enable or disable an option when a checkbox would be selected or deselected in the web manager. The sub-parameters will be available after the option is enabled.

To configure IPv6 (example of how to perform the equivalent of web manager checkbox selection/deselection):

1. Log into the CLI and enter **cd network/settings.**

```
--:- / cli-> cd network/settings
```

2. Enter **show** to view the status of IPv6 configuration.

```
--:- settings cli-> show
hostname = ACS6048
primary_dns = 110.126.129.4
secondary_dns =
domain = corp.tst.com
enable_ipv6 = no
enable_bonding = no
enable_ipv4_multiple_routing_tables = no
```

3. Type **set enable_ipv6=** and press **Tab** to view the options for the parameter.

```
--:- ipv6 cli-> set enable_ipv6=<Tab>
no yes
```

4. Enter **set enable_ipv6=no** to disable IPv6.

```
--:- ipv6 cli-> set enable_ipv6=no
```

-or-

Enter **set enable_ipv6=yes** to enable IPv6.

```
--:- ipv6 cli-> set enable_ipv6=yes
```

5. (Optional) Enter either of the following commands to enable subparameters.

```
**:- ipv6 cli-> set get_dns_from_dhcpv6=yes
**:- ipv6 cli-> set get_domain_from_dhcpv6=yes
```

6. Enter **show** to verify the change.

```
**:- settings cli-> show
hostname = ACS6048
primary_dns = 110.126.129.4
secondary_dns =
domain = corp.tst.com
enable_ipv6 = yes
get_dns_from_dhcpv6 = no
get_domain_from_dhcpv6 = no
enable_bonding = no
```

7. Enter **commit**.

This page intentionally left blank.

3 PORT ACCESS AND CONFIGURATION EXAMPLES

By default, all serial ports and the AUX/Modem port are disabled. An administrator must enable and configure the ports before anyone can use them. Configuration of ports differs based on the type of connected device, which can be either a device console, a PDU or modem.

By default, all users can access all enabled and configured ports. The administrator must decide whether to restrict user access to ports by the assignment of authorizations to user groups. A user who is in an authorized group is referred to as an authorized user.

Some port configuration tasks are provided as examples of how to use the CLI. See the Avocent ACS6000 Installation/Administration/User Guide for an overview of the tasks the administrator must do to configure restricted access to ports. For more information about how to follow the web manager procedures in the CLI, see Configuration Tasks Performed With the CLI on page 2.

This section describes the following tasks related to port access, configuration, power management and where the tasks are performed in the CLI.

Table 3.1 Port Access and Configuration Tasks

TASK	WHERE PERFORMED
View information about the console server and the connected devices	access show
Authorized users access enabled on configured ports	access connect
Authorized users manage power on outlets	access/<PDU_ID>/outlets -or- power_management/PDUs/<PDU_ID>/outlet_table
Administrators configure ports connected to the consoles of devices	ports See Chapter 3 for all Ports options.

3.1 View Information About the Console Server and Connected Devices

When a regular user or an administrator enters **show** at the Access level, information about the following appears in the format shown in Access Parameters on page 22.

- The console server
- The AUX/Modem port (if it is enabled and configured with the Power Profile)
- The serial ports that user is authorized to access (if they are configured with the CAS or Power Profile)

Table 3.2 Access Parameters

FIELD	DESCRIPTION
For Appliance	
Name	Name assigned to the appliance (for example, ACS6048-1357908642)
Port	N/A
Type	N/A
Status	N/A
For Serial Port	
Name	Either the default name [*XX-XX-XX*-p-*n* (where *n*=port_number)], an administrator-assigned alias or an auto-discovered server name
Port	Number of the serial port
Type	Serial
Status	Idle / In-Use
For Power	
Name	PDU ID (either the default name in the format *XX-XX-XX*P*XX_n* or an administrator-assigned alias, such as myPDU)
Port	Number of the serial port/position on the chain
Type	PDU model
Status	Number of Outlets ON | Total outlets
For Outlets	Enter cd <PDU_ID>/outlets and enter show to see list of outlets and the actions that can be taken (commands that can be executed) for each outlet as shown below.
Name	Either the default *XX-XX-XX*P*XX_n_n* or an administrator-assigned name
Port	PDU outlet number
Type	Outlet
Status	ON / OFF
Action	None

To view information about the console server and connected devices:

1. Log into the CLI and enter **cd access** to change to the Access level.

```
--:- / cli-> cd access
```

2. Enter **show**. Information about the console server and the ports the current user is authorized to access appears.

```
--:- access cli-> show
Name Port Type Status
=====================================
ACS6016-0011223344
21-67-72-p-1 1 serial in-use
21-67-72-p-2 2 serial idle
21-67-72-p-4 4 serial idle
myPDU 3|1 PM8|15A 8|8
Type ls to see available sub-nodes
--:- access cli->ls
ACS6016-0011223344/
21-67-72-p-1/
21-67-72-p-2/
21-67-72-p-4/
```

```
myPDU/

Type show to see the content of the page
--:- access cli->
```

3.2 Connect to a Device Console Connected to a Serial Port

The following procedure is an example of how an administrator or an authorized user can connect to a device console when the device is connected to a port that is enabled and configured with the CAS Profile.

To connect to a device console connected to a serial port:

NOTE: The serial port must already be configured and enabled prior to this procedure. See Port Configuration Examples on page 24.

1. Log into the CLI and enter **cd access** to navigate to the Access level.

```
--:- / cli-> cd access
--:- access cli->
```

2. Enter **connect <**serial_port_name**>**. If authentication is configured for the port, the Password prompt appears when single sign-on is disabled.

```
--:- access cli-> connect 77-77-70-p-2
password:
```

NOTE: The connect command above shows a connection to a port that has an alias of 77-77-70-p-2.

3. If prompted, enter the password for the port. The following prompt appears.

```
Type the hot key to suspend the connection: <CTRL>z
```

4. Press **Enter** to continue. You are connected to the device that is connected to the port. The window shows the initial display for the device (usually a console banner and login prompt). An example is shown below.

```
Ubuntu 6.06.1 LTS fremont-techpubs ttyS2
fremont-techpubs login: fred
Password:
Last login: Tue Oct 2 13:09:04 2017 on :0
Linux fremont-techpubs 2.6.15-28-386 #1 PREEMPT Wed Jul 18 22:50:32 UTC 2007 i68
6 GNU/Linux
#
```

3.3 Accessing Serial Ports using ts_menu

The ts_menu is an application to facilitate connection to the serial ports. It displays a menu showing the server names connected to the serial ports of the console server. You must configure the login profile for the group that the users belong to as ts_menu.

ts_menu options

-u <user> [-l] [-ro] <console port>

Table 3.3 ts_menu Parameters

PARAMETER	DESCRIPTION
-u <user>	Invokes ts_menu as the user named by <user>. This requires a password to be entered. The user only has access to authorized serial ports.
-l	Generates a list of ports the user can access. Port aliases are shown if defined.
-ro	Invokes ts_menu in read-only mode. You may connect in read-only mode to any port you have access to.
<console port>	If issued, produces a direct connection to that port. If you have no access rights to the port or if the port does not exist, the application returns a console not found message and terminates. The console port may be the port alias or the port number.
-p	Display TCP port.
-i	Display Local IP assigned to the serial port.
-u <name>	Username to be used in SSH/Telnet or Raw command.
-e < [^]char>	Escape character used to close the target session. The default escape character is Ctrl-X.

To close the target session:

1. Enter the escape character shown when you connect to the port.
2. The menu with ports is displayed.
3. Select the exit option to return to the shell prompt.

3.4 Manage Power for a Device Connected to an Outlet on a PDU

See cycle, on, off, lock and unlock on page 15 for how an authorized user can manage power on PDU outlets when the PDU is connected to an enabled port configured with the Power Profile and the PDU is connected to the network and added to the appliance as Network PDU.

3.5 Port Configuration Examples

The following examples show how an administrator can configure a port when a device console is connected, assign the CAS profile, configure a port that is connected to a PDU and assign the Power Profile.

To set up a console access service (CAS) port:

1. Log onto the CLI as an administrator.

```
--:- / cli->
```

2. Enter **set_cas ports/serial_ports/** followed by a space and the number of the port you want to configure (port 1 is used as an example).

```
--:- / cli-> set_cas ports/serial_ports/ 1
```

3. Enter **show** to view the status of port 1.

```
Selected items: 1
Port: 1
enable_cisco_rj45_pin-out = no
status = enabled
speed = 9600
parity = none
data_bits = 8
stop_bits = 1
flow_control = none

Type ls to see available sub-nodes.
--:#- [serial_ports/physical] cli->ls
cas/
data_buffering/
alerts/
power/

Type show to see the content of the page.
--:#- [serial_ports/physical] cli->
```

4. Enter **set status=enabled**, then enter **show** and **save** as shown to enable the configured port and verify and save the configuration.

```
--:- serial_ports/physical cli-> set status=enabled
--:- serial_ports/physical cli-> show
--:- serial_ports/physical cli-> save
```

To enable a power management port:

1. Log onto the CLI as an administrator and enter **set_power ports/serial_ports/** <port number> to select a port with a PDU connected (port 3 is used as an example).

```
--:- / cli-> set_power ports/serial_ports/ 3
```

2. Enter **show** to view the configuration of port 3.

```
--:- serial_ports/physical cli-> show
Selected items: 3
Port: 3
enable_cisco_rj45_pin-out = no
status = enabled
```

```
speed = 9600
parity = none
data_bits = 8
stop_bits = 1
flow_control = none

Type ls to see available sub-nodes
--:- serial_ports/physical cli->
```

3. Enter **set status=enabled** then enter **save** to set the Serial_Profile to Power, enable the port and commit the changes.
4. Enter **show** to verify the configuration.

```
--:- serial_ports cli-> show
Port Device Name Profile Settings
==== ====== ================= ======= ========================
1 ttys1 ACS6016-0088664422 cas 9600_8N1_telnet-ssh_local
2 ttys2 21-67-72-p-2 cas 9600_8N1_telnet-ssh_local
3 ttys3 power cas 9600_8N1_telnet-ssh_local
4 ttys4 21-67-72-p-4 cas 9600_8N1_telnet-ssh_local
5 ttys5 21-67-72-p-5 cas 9600_8N1_telnet-ssh_local
6 ttys6 21-67-72-p-6 cas 9600_8N1_telnet-ssh_local
7 ttys7 21-67-72-p-7 cas 9600_8N1_telnet-ssh_local
8 ttys8 21-67-72-p-8 cas 9600_8N1_telnet-ssh_local
9 ttys9 21-67-72-p-9 cas 9600_8N1_telnet-ssh_local
10 ttys10 21-67-72-p-10 cas 9600_8N1_telnet-ssh_local
11 ttys11 21-67-72-p-11 cas 9600_8N1_telnet-ssh_local
12 ttys12 21-67-72-p-12 cas 9600_8N1_telnet-ssh_local
13 ttys13 21-67-72-p-13 cas 9600_8N1_telnet-ssh_local
14 ttys14 21-67-72-p-14 cas 9600_8N1_telnet-ssh_local
15 ttys15 21-67-72-p-15 cas 9600_8N1_telnet-ssh_local
16 ttys16 dial-in 38400

Type ls to see available sub-nodes
```

4 CLI OVERVIEW FOR ADMINISTRATORS

This chapter describes using the Command Line Interface (CLI) for administrators. Only administrators and authorized users can access the commands listed in this chapter. These procedures assume you have logged into the CLI as an administrator and are at the --:- / cli-> prompt.

NOTE: In the tables that show output from the show **command, when an option that is followed by an equal sign (=) is left blank, that option is not assigned a value by default.**

4.1 System

1. Enter **cd system** to navigate to the System level.

```
--:- / cli-> cd system
```

2. Enter **ls** to view the available options.

```
--:- system cli-> ls
security/
date_and_time/
help_and_language/
general/
boot_configuration/
information/
usage/
```

3. Enter **show** followed by an option name to view information about each option.

```
--:- security cli-> show security_profile
```

4.2 System/Security

Enter **cd security** to navigate to the security level.

```
--:- / cli-> cd system/security
```

Table 4.1 System Navigation Tree

security_profile		
	idle_timeout =	
	rpc =	
	port access =	
	session =	
	port_access_kill_multi_session =	
	port_access_send_message_multi_session =	
	port_access_power_control =	
	port_access_data_buffer_management = c	
	bootp_enabled=	
		bootp_interface=
		enable_live_configuration_retrieval=
	port_acess_per_user_group_authorization =	
	ssh_allows_authentication_via_username|password =	
	security_profile=	
		enable_telnet_service=
		enable_ftp_service= d
		enable_snmp_service=
		enable_ipsec=
		answer_icmp_message=
		ssh_version=
		ssh_tcp_port=
		ssh_allow_root_access=
		ssh_minimum_cipher_and_mac_suite_level =
		enable_http_session=
		http_port=
		enable_https_session
		https_ssl_version=
		https_port=
		https_minimum_cipher_suite_level=
		redirect_http|https=
dsview		
	all_appliance_to_be_managed_by_dsview=	
fips_140		
	enable_fips_140-2_module=	

4.2.1 System/Date and Time

Enter **cd system/date_and_time** to navigate to the date_and_time level.

```
--:- / cli-> cd system/date_and_time
```

Table 4.2 Date and Time Navigation Tree

date_and_time			
	date_and_time		
		settings=	
			day=
			hour=
			minute=
			month=
			second=
			year=
time_zone=			

4.2.2 System/Help and Language

Enter **cd system/help_and_language** to navigate to the online_help level.

```
--:- / cli-> cd system/help_and_language
```

To set the online help URL:

Perform this procedure if you have downloaded the online help files to a web server that is accessible to the console server.

1. Enter the following command.

```
--:- / cli> cd system/help_and_language/
```

2. Enter the following command.

```
--:- help_and_language cli> set url=<online_help_location>
```

A line similar to the following appears.

```
**:- help_and_language cli>
```

3. Save your settings.

```
**:- help_and_language cli> commit.
```

Table 4.3 Help and Language Navigation Tree

appliance_language=
url=

4.2.3 System/General

Enter **cd system/general** to navigate to the login_banner level.

```
--:- / cli-> cd system/general
```

To set the login banner:

1. Enter the following command.

```
--:- / cli> cd system/general/
```

2. Enter the following command.

```
--:- general cli-> set enable_login_banner=yes
**:- general cli> set login_banner=<login banner text>
```

NOTE: <login banner text> with new lines: Type the text between double quotes and enter the new line as \\n (double back slash and the character).

A line similar to the following appears.

```
**:- general cli>
```

3. Save your settings.

```
**:- general cli> commit.
```

4.2.4 System/Boot Configuration

Enter **cd system/boot_configuration** to navigate to the boot_configuration level.

```
--:- / cli-> cd system/boot_configurationcd
```

Table 4.4 Boot Configuration Navigation Tree

boot configuration	
	boot mode=
	image=
	watchdog_timer=
	console_speed=
	eth0_mode=
	eth1_mode=

4.2.5 System/Information

1. Enter **cd system/information** to navigate to the Information level.

```
--:- / cli> cd system/information/
```

2. Enter **show** to view the system information.

4.2.6 System/Usage

Enter **cd system/usage** to navigate to the Usage level.

```
--:- / cli> cd system/usage/
```

Table 4.5 Usage Navigation Tree

memory
flash usage

4.3 Network

1. Enter cd network to navigate to the Network level

   ```
   --:- / cli-> cd network/
   ```

2. Enter **ls** to view the list of available options.

```
settings/
devices/
ipv4_static_routes/
ipv6_static_routes/
hosts/
firewall/
ipsec(vpn)/
snmp/
```

4.3.1 Network/Settings

1. Enter **cd network/settings** to navigate to the Network settings level.

```
--:- / cli-> cd network/settings/
```

2. Enter **show** to view the list of available options.

Table 4.6 Network Settings Navigation Tree

Settings		
	hostname=	
	primary_dns=	
	secondary_dns=	
	domain=	
	search=	
	enable_ipv6=	
	get_dns_from_dhcpv6=	
	get_domain_from_dhcpv6=	
	enable_network_failover=	
	enable_bonding=	

4.3.2 Network/IPv4 and IPv6

IPv4 addresses are always enabled. An administrator can also enable IPv6 addresses at the appliance_ settings/network/ipv6 level. A procedure to enable IPv6 is used as an example in CLI Equivalent Actions to Web Manager Checkbox Selection on page 18.

Table 4.7 Network/IPv4 and IPv6 Options

ipv4_static_routes		
	default_3	
		gateway=
		interface=
		metric=
ipv6_static_routes		

4.3.3 Network/Devices

The procedure to configure a static IP address for the primary Ethernet interface is usually performed during installation so that administrators have a fixed IP address for access to the web manager and can finish configuration.

To configure a IPv4 or IPv6 static IP address:

NOTE: This procedure configures either an IPv4 or IPv6 static IP address for the ETH0 (eth0) or the ETH1 (eth1) port. You can configure an IPv6 static IP address only if IPv6 is enabled.

1. Enter **cd network/devices/**<eth0|eth1>**/settings** to navigate to the Settings level for the desired interface.

```
--:- / cli-> cd network/devices/eth0/
```

2. Enter **set ipv**<4|6>**_method=static** to set the method to static for IPv4 or IPv6.

```
**:- eth0 cli-> set ipv4_method=static
```

3. Enter **set ipv<4|6>_address=**<IP_Address> **ipv<4|6>_mask=**<netmask> to set the IP address and subnet mask, then enter **commit** to save the change.

```
--:- eth0 cli-> set ipv4_address=172.26.31.10 ipv4_mask=255.255.255.0
**:- eth0 cli-> commit
```

4. Enter **show** to view the changes.

```
--:- eth0 cli-> show
```

Table 4.8 Devices Navigation Tree

devices		
	eth0	
		set_as_primary_interface=
		status=
		ipv4_method=
		ipv6_method=
		mode=
	eth1	
		set_as_primary_interface=
		status=
		ipv4_method=
		ipv6_method=
		mode=

4.3.4 Network/Hosts

The following procedure describes how to add a host to the hosts table.

To add a host to the host table:

1. Enter **cd network/hosts** to navigate to the Hosts level.

```
--:- / cli-> cd network/hosts
```

2. Enter **show** to view the current host settings.

```
--:- hosts cli-> show
127.0.0.1
ip: 127.0.0.1
 hostname: localhost
 alias:
 127.0.0.1/
```

3. Type **add** then press **Return**.

```
--:- hosts cli-> add<Return>
--:#- [hosts] cli-> ls
ip =
hostname =
alias =
--:#- [hosts] cli->
```

4. Enter **set hostname=**<hostname> **ip=**<IP_address> to add the name of a host and the IP address for the host.

NOTE: Each parameter that follows the add command is separated by a space.

```
--:#- [hosts] cli-> set hostname=sharedacs6000 ip=172.26.31.164
```

5. Enter **commit**.

```
--:#- [hosts] cli-> save
```

6. Enter **show** to verify the changes took place and to view the new host entry.

```
--:- hosts cli-> show
```

```
127.0.0.1
ip: 127.0.0.1
 hostname: localhost
 alias:
172.26.31.164
ip: 172.26.31.164
 hostname: sharedacs6000
alias:
 127.0.0.1/add
172.26.31.164/
```

7. Enter **cd <IP_address>/settings** to navigate to the level where you can perform additional configuration of the host entry.

```
--:- hosts cli-> cd 172.26.31.164/settings
```

8. Enter **show** to view the additions to the host table and the Settings option.

```
--:- 172.26.31.164 cli-> show
ip: 172.26.31.164
hostname = sharedacs6000
alias =
```

Table 4.9 Hosts Navigation Tree

hosts		
	127.0.0.1	
		alias=
		hostname=

4.3.5 Network/Firewall

Enter **cd network/firewall** to navigate to the firewall level.

```
--:- / cli-> cd network/firewall
```

NOTE: To set a rule, you must enable the interface, set the rule for the interface and physically connect the interface to the network.

Table 4.10 Firewall Navigation Tree

firewall			
	ipv		
		ipv4_filter_table	
			FORWARD
			INPUT
			OUTPUT
		ipv6_filter_table	
			FORWARD
			INPUT
			OUTPUT

4.3.6 Network/IPSec(VPN)

Enter **cd network/ipsec(vpn)** to navigate to the ipsec(vpn) level.

```
--:- / cli-> cd network/ipsec(vpn)
```

4.4 Network/SNMP

Enter **cd network/snmp** to navigate to the snmp level.

```
--:- / cli-> cd network/snmp
```

4.4.1 Wiz command

The wiz command allows administrators to easily and quickly perform the initial network configuration of the eth0.

At the command prompt at the / level, enter **wiz** to view the current IP configuration. To change the IP configuration, press **Tab** to move through the parameters, and press **Esc + Tab** to edit the selected parameter. When you are finished, enter **yes** to confirm that all parameters are correct and to save the new parameters.

```
--:- / cli-> wiz
Current IPv4 address: 172.26.30.249
Current IPv6 address:
eth0:
device_status = enabled
ipv4_method = dhcp
ipv4_address = 192.168.160.10
ipv4_mask = 255.255.255.0
ipv4_default_gateway =
ipv6_method = ipv6_address_unconfigured
ipv6_address =
ipv6_prefix_length =
ipv6_default_gateway =
MAC Address: 00:e0:86:21:67:72
dns:
primary_dns = 172.26.29.4
secondary_dns =
domain = corp.avocent.com
hostname = ACS6016-0011223344
ipv6:
```

NOTE: Enabling or disabling IPv6 requires a reboot to be effective.

```
enable_ipv6 = yes
get_dns_from_dhcpv6 = no
get_domain_from_dhcpv6 = no

Some basic and useful keys are:
- tab (once/twice) - shows the next possible commands/option(s)
 - esc tab - gets the current parameter value for editting

Other hints:
 - Use backslash '\' to escape spaces, '\' and other control
 characters when assigning values to parameters.

Current IPv4 address: 172.26.30.249
Current IPv6 address:
eth0:
device_status (disabled, enabled) [enabled]:
```

4.5 Ports

Enter **cd ports** to navigate to the Ports level.

```
--:- / cli-> cd ports
```

Table 4.11 Ports Navigation Tree

serial ports			
	<port>		
		cas	
			port_name=
			enable_auto_discovery=
			enable_speed_auto_detection=
			protocol=
			authentication_type=
			text_session_hot_key=
			power_session_hot_key=
			restful_hot_key=
			telnet_port_alias=
			ssh_port_alias=
			raw_mode_port_alias=
			port_ipv4_alias=
			port_ipv4_alias_interface=
			port_ipv6_alias=
			port_ip6_alias_interface=
			dcd_sensitivity=
			enable_auto_answer=
			dtr_mode=
			dtf_off_interval=
			line_feed_suppression=
			null_after_cr_suspension=
			transmission_interval=
			break_sequence=
			break_interval=
			show_multi-session_menu=
			log_in|out_multi_session_notification=
			information_message_notification=
		physical	
			enable_cisco_rj45_pin-out=
			status=
			speed=
			parity=
			data_bits=
			stop_bits=
			flow_control=
		data_buffering	
			status=
			type=
			time_stamp=
			login|logout_message=
			serial_session_logging=
		alerts	
		power	
auxiliary ports			

	ttyM1			
		status=		
		speed=		
		init_chat=		
		ppp_address=		
		ppp_authentication=		
		chap-interval=		
		chap-max-challenge=		
		chap-restart=		
		ppp_idle_timeout=		
cas_profile				
	auto_discovery			
		settings		
			auto_discovery_timeout_(seconds)=	
			default_speed_on_auto_discovery_failure=	
			probe_speed_115200=	
			probe_speed_1200=	
			probe_speed_19200=	
			probe_speed_230400=	
			probe_speed_2400=	
			probe_speed_38400=	
			probe_speed_4800=	
			probe_speed_57600=	
			probe_speed_9600=	
			probe_timeout_(seconds)=	
	auto_answer			
		input string		
		output string		
	pool_of_ports			
		pool_name=		
		pool_telnet_port_alias=		
		pool_ssh_port_alias		
		pool_raw_mode_port_alias=		
		pool_ipv4_alias=		
		pool_ipv4_alias_interface=		
		pool_ipv6_alias=		
		pool_ipv6_alias_interface=		
		pool_members=		
	restful_settings			
		action_name_<#>=		
		http_method_<#>=		
		url_<#>=		
		post_data_<#>=		
		username_<#>=		
		password_<#>=		
dial-in_profile				
	secure_dial-in			
		callback_users		

	settings	
		log_in_to_appliance=
		otp_login_authentication=
		ppp_connection=
		ppp|pap_authentication=

Table 4.12 Serial Port Commands

COMMAND	SUMMARY
set_cas	Edits the command to configure a list of serial ports with the CAS profile. Syntax: set_cas<serial port number>, <serial port number> This command has five sub-nodes: physical, cas, data_buffering, alerts and power.
set_dial-in	Edits the command to configure one serial port with the Dial-In profile. Syntax: set_dial-in<serial port number>
set_dial-out	Edits the command to configure one serial port with Dial-out on demand profile. Syntax: set_dial-out <serial port number>
set_power	Edits the command to configure a list of serial ports with the Power profile. Syntax: set_power<serial port number>, [<serial port number>] This edit has two sub-nodes: physical and power.
set_socket-client	Edits the command to configure one serial port with Socket Client profile. Syntax: set_socket-client <serial port number>
clone_ports	Copies the configuration from one port to a list of serial ports. Syntax: clone_ports<serial port number>
reset_port_to_factory	Resets the serial ports to factory configuration. (This is disabled for CAS profile.) Syntax: reset_port_to_factory<serial port number>, [<serial port number>]
enable_ports	Enables serial ports. Syntax: enable_ports<serial port number>, [<serial port number>]
disable_ports	Disables serial ports. Syntax: disable_ports<serial port number>, [<serial port number>]

Example of how to set a list of serial ports 2,5 and 6 with the CAS Profile and enable the status:

```
--:- serial_ports cli-> cd /ports/serial_ports
--:- serial_ports cli-> set_cas 2,5,6
--:#- [serial_ports/physical] cli-> set status=enabled
--:#- [serial_ports/physical] cli-> show
Selected items: 2|5|6
Port: 2
enable_cisco_rj45_pin-out = no
status = enabled
speed = 9600
parity = none
data_bits = 8
stop_bits = 1
flow_control = none

Type ls to see availables sub-nodes.
--:#- [serial_ports/physical] cli-> ls
cas/
data_buffering/
alerts/
power/

Type show to see the content of the page.
--:#- [serial_ports/physical] cli->save
--:- serial_ports cli->
```

To copy the configuration from serial port 5 to ports 10 and 15:

```
--:- serial_ports cli-> clone_ports 5
--:#- [serial_ports] cli-> show
Copy configuration from: 5
copy_configuration_to =
--:#- [serial_ports] cli-> set copy_configuration_to=10,15
--:#- [serial_ports] cli-> save
--:- serial_ports cli->
```

4.5.1 Auxiliary ports

Enter **cd ports/auxiliary_ports** to navigate to the auxiliary ports level.

```
--:-cli-> cd /ports/auxiliary_ports/
```

If an internal modem is factory installed, the only available serial_profile option are Dial-in and Dial-out on demand. If an internal modem is not installed, either an external modem or a PDU can be connected to the port and a third serial_profile option, Power, is available.

If no internal modem is installed, the port name is ttyA1. If an internal modem is installed, the port name is ttyM1.

Enter the commands: **set_dial-in**, **set dial-out** or **set_power** to configure the auxiliary port.

NOTE: The set_power command will not be available when an internal modem is installed.

```
--:- / cli-> cd ports/auxiliary_ports/
--:- auxiliary_ports cli-> show

Port Device Status Profile
===== ====== ======== ============
ttyA1 ttyA1 disabled unconfigured

Type ls to see availables sub-nodes.
--:- auxiliary_ports cli->
```

4.6 Pluggable Devices

Type the command **enable_pluggable_device_detection** to permit detection of attached pluggable devices. Type **show** to display a list of all detected pluggable devices. Type **cd_<device name>** to configure the device.

4.7 Authentication

Enter **cd authentication** to navigate to the authentication level.

```
--:- / cli-> cd authentication
```

NOTE: Kerberos does not work unless the administrator copies the /etc/krb5.keytab file from the Kerberos server and overwrites the /etc/krb5.keytab file in the console server.

Table 4.13 Authentication Navigation Tree

authentication			
	appliance_authentication		
		authentication_type=	
		enable_fallback_to_local_type_for_root_user_in_appliance_console_port=	
		enable_single_sign-on=	
	authentication_servers		
		radius	
			first_authentication_server=
			first_accounting_server=
			second_authentication_server=
			second_accounting_server=
			secret=
			timeout=
			retries=
			enable_servicetype=
		tacacs+	
			first_authentication_server=
			first_accounting_server=
			second_authentication_server=
			second_accounting_server=
			service=
			secret=
			timeout=
			retries=
			tacacs+_version=
			enable_user-level=
		ldap(s)|ad	
			server=
			base=
			secure=
			database_user_name=
			database_password=
			login_attributes=
		kerberos	
			server=
			realm_domain_name=
			domain_name=
		nis	
			nis_domain_name=
			nis_server_address_or_"broadcast"=
		dsview	

			ip_address_1=
			ip_address_2=
			ip_address_3=
			ip_address_4=

4.8 Users

Enter **cd users** to navigate to the users level.

```
--:- / cli-> cd users
```

To add a user and password:

1. Enter **cd users/local_accounts/user_names** to navigate to the user_names level.

```
--:- / cli-> cd users/local_accounts/user_names
```

2. Enter **add.** Then enter **set** with the parameters all on one line separated by spaces as shown.

```
--:- user_names cli-> add
--:#- [user_name] cli-> set user_information/ user_name=fred password=smith123abc confirm_
password=smith123abc
--:#- [user_names] cli->
```

3. Enter **save**.

```
--:#- [user_names] cli-> save
```

4. Enter **show** to verify that the new user has been added.

```
--:#- [user_names] cli-> show
```

Table 4.14 Users Navigation Tree

users					
	authorization				
		groups			
			admin		
				members	
					admin
					root
				login_profile	
					session_timeout=
					enable_log-in_profile=cd
				access_rights	
					serial
					power
					appliance
			appliance-admin		
				members	
				login_profile	
					enable_log-in_profile=
				access_rights	
					serial
					power
					appliance
			shell-login-profile		
				members	
					root
				login_profile	
					session_timeout=
					enable_log-in_profile=
					profile=
					cli_cmd=
					exit_after_executing=
				access_rights	
					serial
					power
					appliance
			user		
				members	
				login_profile	
					session_timeout=
					enable_log-in_profile=
				access_rights	
					serial

					power
					appliance
		dsview_access_rights			
			map_to_=		
			multi_access_mode=		
			kill_multi_session=		
			send_message_multi-session=		
	local_accounts				
		user_names			
			admin root		
				password=	
				confirm_password=	
				password_change_at_next_login=	
				user_group=	
				password_minimum_days=	
				password_maximum_days=	
				password_inactive_days=	
				password_warnding_days=	
				account_expiration_date=	
		password_rules			
			check_password_complexity=		
			min_digits=		
			min_upper_case_characters=		
			min_special_characters=		
			minimum_size=		
			def_expiration_min_days=		
			def_experiation_max_days=		
			def_expiration_warning_days=		
			number_of_permitted_failed_attempts_ {0|disabled}=		
			account_lockout_duration_after_each_failed_ login_{min}=		
			unlock_account_after_{min}_{0|manual_unlock}=		

4.9 Events_and_Logs

Enter **cd events_and_logs** to navigate to the events_and_logs level.

```
--:- / cli-> cd events_and_logs
```

Table 4.15 Events and Logs Navigation Tree

event list		
event destinations		
	syslog	
	snmp trap	
	sms	
	email	
	dsview	
trap_forward		
data_buffering		
	local_data_buffering_settings	
		segment_size_(kbytes)=
		spare_segments=
	nfs_data_buffering_settings	
		nfs_server=
		nfs_path=
		segment_size_(kbytes)=
		spare_segments=
	local_nfs_data_buffering_settings	
		close_log_files_and_open_new_ones_at_time_(hh:mm)=
	syslog_data_buffering_settings	
		syslog_facility=
sensors		
	current_temperature:(deg_c, display only)	
	maximum_temperature_(deg_c)=	
	maximum_temperature_threshold_(deg_c)=(positive integer between 0 and 4)	
	minimum_temperature_(deg_c)=	
	minimum_temperature_threshold_(deg_c)=(positive integer between 0 and 4)	

4.10 Power Management

The Power Management Options are described in the table below.

Table 4.16 Power Management Options Descriptions

OPTION	DESCRIPTION
pdus	Allows an authorized user to reboot, restore factory default settings or to rename PDU(s). Also allows the authorized user to view information about each PDU, monitor sensors, clear sensor values, set up syslogging of events related to the PDU, configure an alarm and the LED display mode, and to manage outlets on the PDU.
login	Lists the username and password for each type of PDU connected to the console server.
outlet_ groups	Lists all configured outlet groups that the current user is authorized to manage (to manage outlet groups, the user must be in a user group that is authorized to manage all the outlets in the outlet group). An administrator can configure outlet groups.
network_ pdus	Allows an administrator to add, edit or delete PDUs connected to the network. These PDUs will show up in the PDUs node when they are discovered. Only power control opearation is supported by these PDUs.

To rename a PDU:

1. Log onto the CLI as an administrator and enter **cd power_management/pdus** to navigate to the pdus level.

```
--:- / cli-> cd power_management/pdus
```

2. Type **rename** and press **Tab Tab** to expand the parameters.

```
--:- pdus cli-> rename <PDU_ID> <Tab><Tab>
```

3. Enter **set newpdu_id=**<new_PDU_ID>.

```
--:#- [pdus] cli-> set new_pdu_id=mypdu
--:#- [pdus] save
```

NOTE: See the Avocent ACS6000 Installation/Administration/User guide for how to perform other authorized PDU configuration options.

To manage power for a selected outlet:

See cycle, on, off, lock and unlock on page 15 for how to manage power at the power_management level.

4.11 Active Sessions Information

The Active Session information fields are described in the table below. An authorized user can kill an active session with the Kill command.

Table 4.17 Active Sessions Field Descriptions

FIELD	DESCRIPTION
user	Logged in user
client_ip	Source of the connection
creation_time	Time of the session creation
session_type	Type of session (console, http)
connection_type	Type of connection (cli, wmi - that is, Web Manager)
target_name	Target name or alias if session is an access session
id	Session ID
parent id	Parent ID if session is a subsession

To view and kill Active_Sessions:

1. From the / level CLI prompt, enter **cd active_sessions**.

```
--:- / cli-> cd active_sessions
--:- active_sessions cli->
```

2. Enter **show**. Information displays as shown about all active sessions.

```
--:- active_sessions cli-> show
37
user: admin
client_ip: none
creation_time: Tue Dec 18 03:31:01 2007
session_type: console
connection_type: cli
target_name:
id: 37
parent_id:

--:- active_sessions cli->
```

3. To kill a session (if authorized), enter **kill** followed by the session number.

This page intentionally left blank.

5 APPENDICES

Appendix A: Enabling Firmware Upgrades When the Boot Image is not in Flash

To enable firmware upgrades when the boot image is not in Flash:

1. Connect to the console of the console server as root.

```
Welcome to ACS6000 <host name>.
Type help for more information.
--:- / cli->
```

2. Enter **shell**. A warning appears followed by the root prompt.

```
--:- cli-> shell
WARNING: Improper use of shell commands could lead to data loss,
the deletion of important system files or other unexpected result.
Please double-check your syntax when typing shell commands.
[root@ACS6048-3131313131 ~]#
```

3. Enter **recover-flash.sh --factory_default --doformat**.

```
[root@ACS6048-3131313131 ~]# recover-flash.sh --factory_default --doformat
[root@ACS6048-3131313131 ~]#
```

   The Flash memory is formatted, and the version of firmware in memory is stored in Flash. The command prompt reappears.

4. Enter **reboot**.

```
[root@ACS6048-3131313131 ~]# reboot
```

   When the system reboot completes, the web manager supports firmware upgrades.

Appendix B: Migration CLI

The Migration CLI is a tool that allows you to configure an ACS6000 console server that is running scripts based in the ACS advanced console server. For full configuration and management commands, it is recommended you use the ACS6000 console server's CLI.

NOTE: References to an ACS advanced console server in this section refer to any advanced console server other than the ACS6000 console server.

In the ACS6000 console server, the login profile for the user "root" goes directly to the shell prompt. This will allow the root user to run Migration CLI commands out of the ACS6000 console server. A new group, "login-profile-shell," is created with only root as a member. To run commands based from an ACS advanced console server, a root user should type **CLI** before the command.

5.0.1 Access rights

The access rights on the ACS6000 console server are based on authorization groups. The administrator configures the serial ports the group can access. To allow you to configure access rights, the following table displays authorization groups that will be created on the ACS6000 console server when using the Migration CLI.

Table A.1 Access Rights Groups

GROUP	MEMBERS	PERMISSIONS
cli_mus_ttySxx	Users who can open a second session to a serial port.	Access to a serial port in a muli-session (read/write or read only)
cli_power_ttySxx	Users who have power control in a serial port.	Power control (on/off/cycle) of outlets merged to a serial port.
cli_access_ttySxx	Users who can access a serial port in a single session.	Access to a serial port in a single read/write session.
cli_pmd_ <username>	<username>	Power control of the outlet.

5.0.2 Exceptions

This section will list all ACS advanced console server CLI commands not available in the Migration CLI for the ACS6000 console server. For a list of available commands, see the Avocent ACS Installation/Administration/User Guide.

The following commands or values are not supported by the Migration CLI:

Table A.2 Commands Not Supported by the Migration CLI

COMMAND	VALUE OR DESCRIPTIONS
administration	
backupconfig loadfrom sd	N/A
backupconfig saveto sd	N/A
upgradefw checkum	N/A
application	
connect	N/A
pm	N/A
view	N/A
config administration bootconf	
bootype	bootp/both/ftp
flashtest	full/skip
maxevents	<number>
ramtest	full/quick/skip
config administration notifications	
addemail	N/A
addpager	N/A
addsnmptrap	N/A
alarm	N/A
delete	N/A
edit	N/A
config application pmdconfig general	
add	N/A
delete	N/A
config application terminalmenu	
add	N/A
delete	N/A
menutitle	N/A
config network hostSettings	
secipaddress	<nnn.nnn.nnn.nnn>
secsubnetmask	<nnn.nnn.nnn.nnn>
mtu	N/A
config physicalports access	
users/groups	accepts only list of usernames
authtype	assume local
termshell	<shell command>
logintimeout	<login timeout in seconds>
config physicalports databuffering	
mode	cir/lin
showmenu	file/fileanderase/no/noerase/yes
syslogsize	<record length in bytes[40-255]>
config physicalports general	
pmsessions	none/ssh/ssh_telnet/telnet
protocol	bidirectionaltelnet, consoleraw, cslip, local, rawsocket, slip, sshv1, sshv2, telnet
config physicalports multiuser	
users	accepts only list of users

COMMAND	VALUE OR DESCRIPTIONS
sniffmode	in/inout/no/out
config physicalports other	
SSHexitkey	<SSH exit key>
banner	<login banner>
host	<host>
sttyoptions	<stty options>
tcpkeepalive	<number>
terminaltype	aixterm, att6386, linux-lat, vt100, vt320, xtermcolor, ansi, ibm3151, scoansi, vt102, vt52, at386, linux, sun, vt220, xterm
winems	no/yes
idletimeout	<number>
config physicalports power management	
enableIPMI	N/A
disableIPMI	N/A
key	N/A
server	N/A
config security	
addgroup/delgroup	N/A
config security adduser	
shell	<shell cmd but “ts_menu”>
comments	<comments>
config security profile custom	
ports auth2sport	no/yes
ports bidirect	no/yes
ports raw2sport	no/yes
ports ssh2sport	no/yes
ports telnet2sport	no/yes
ssh ssh_x509	no/yes
config virtualport	
config ipmi	<all or range/list[1-numberOfPorts]>
security authentication	
authtype	Otp, Otp/Local
pppauthtype	Otp, Otp/Local
timeout	
-t<time>	Time-out in minutes
-T	Disable the idle time-out. Same as -t0
config security loadkey	
url	N/A
username	N/A

Appendix C: Su and Sudo Commands

The su and sudo commands allow a user to execute commands as a different user.

5.0.3 Su command

Using the su (switch user) command, a user can switch to another user account to execute commands not authorized with their normal account. If used without a username, the su command defaults to root. Only users who are members of the wheel group can execute the su command to log in as root.

NOTE: The wheel group is a Linux group and is included in the firmware by default.

You will be prompted for the password of the account you're trying to switch to with the su command. You will remain logged into that account until you either press Ctrl-D or type exit.

NOTE: The su command will open a shell session instead of the restricted shell. The user will receive the shell prompt. Improper use of shell commands could lead to data loss. Double-check your syntax when using shell commands.

Syntax:

```
su [options][-][username[arguments]]
```

The following table describes options that can be used with the su command.

Table A.3 Su Command Options

OPTION	DESCRIPTION
-, -l, --login	Uses an environment similar to that had the user logged in directly. When - is used, it must be specified as the last su option.
-m, -p, --preserve-environment	Preserves the current environment.

Optional arguments may be provided after the username, in which case they are supplied to the shell (/bin/sh).

To add a member to the wheel group:

1. Create the user using the web manager or CLI.
2. Open a session in the appliance and log in as root.
3. In the shell prompt, run the usermod command to add the user to the wheel group.

```
# usermod -G wheel <username>
```

4. Run the groups command to verify.

```
# groups <username>
```

To delete a member from the wheel group:

1. Edit the file /etc/group.

2. Remove the username from the line with **wheel::XX:<user1>,<user2>,<user3>**.

5.0.4 Sudo command

Using the sudo (superuser do) command, a user can execute a command using the privileges of another user (often root), as specified in the /etc/sudoers file. The user is authenticated using his own password, not the root password. The /etc/sudoers file logs all commands and arguments.

Syntax:

```
sudo <command>
```

Configuring sudo

A system administrator configures the /etc/sudoers file to give groups or users access to some or all commands not authorized with their normal account. An administrator should log into the console server as a root user and edit the /etc/sudoers file by using the **/usr/sbin/visudo** command to configure sudo.

The sudoers file is composed of aliases and user specifications. When multiple entries match for a user, they are applied in order. Where there are conflicting values, the last match is used.

Since the sudoers file is parsed in a single pass, order is important. You should structure sudoers so that the Host_Alias, User_Alias, and Cmnd_Alias specifications come first, followed by any Default_Entry lines, and finally the Runas_Alias and user specifications.

An example of an /etc/sudoers file:

```
#User alias specification
User_Alias FULLTIMERS = millert, mikef, dowdy
User_Alias PARTTIMERS = bostley, jwfox, crawl

#Cmnd alias specification
Cmnd_Alias KILL = /bin/kill
Cmnd_Alias SHUTDOWN = /sbin/shutdown
Cmnd_Alias REBOOT = /sbin/reboot
Cmnd_Alias SU = /bin su

FULLTIMERS ALL = KILL, SHUTDOWN, REBOOT, SU
PARTTIMERS ALL = SHUTDOWN, REBOOT
```

In the preceding example, the users millert, mikef and dowdy can execute the kill, shutdown, reboot and su commands while the users bostley, jwfox and crawl can only shut down and reboot the console server.

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

590-1765-501A