VERTIV™

Avocent® ACS800/8000 Advanced Console System

Installer/User Guide

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

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.vertiv.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

1 Introduction

The Avocent® ACS800/8000 advanced console system serves as a single point for access and administration of connected devices, such as serial consoles, modems and power devices. The console system supports secure remote data center management and out-of-band management of IT assets from any location worldwide.

NOTE: Unless noted, references to a console system refer to all models in the 800/8000 series.

The console system provides secure local (console port) and remote (IP and dial-up) access. The console system runs the Linux® operating system with a persistent file system in Flash memory that can be upgraded with a local file on a computer connected to the console system.

Multiple administrators can be logged into the console system at the same time and can use the web user interface (web UI), the Command Line Interface (CLI utility) or DSView™ 4 management software to access and configure the console system.

NOTE: Unless otherwise noted, all references to DSView software in this document refer to version 4 or greater.

Depending on the model, the console system has either four or eight USB ports to support modems, storage devices, network adapters, USB hubs and USB console devices. Some models have an SD card slot to support an additional storage device.

Two network ports support connections to more than one network, or can be configured for Ethernet bonding for redundancy and greater reliability or network failover support.

For dial-in and secure dial-back with Point-to-Point Protocol (PPP), an optional internal modem can be factory installed or you can use an external modem connected to either a serial or USB port.

Some models also come equipped with an antenna for cellular connectivity.

1.1 Features and Benefits

1.1.1 Access options

Secure access is available through the following local (analog console port) and remote (digital IP and dial-up) options:

- LAN/WAN IP network connection.
- Dial-up to a factory-configured internal modem (optional) or a modem connected to one of the serial or USB ports.
- Some models also have an antenna for cellular connectivity.
- Target device connection. An authorized user can make a Telnet, SSH v2 or Raw connection to a target device. For Telnet or SSH to be used for target device connections, the Telnet or SSH service must be configured in the Security Profile that is in effect.
- Console system console connection. An administrator can log in either from a local terminal or from a computer with a terminal emulation program that is connected to the console port and can use the CLI utility. The CLI utility prompt (--:- cli->) displays at login.

More than one administrator can log into the console system and have an active CLI or web UI session. All sessions receive the following warning message when the configuration is changed by another administrator or by the system: *The appliance configuration has been altered from outside of your session*. Upon receipt of this message, each administrator needs to verify that changes made during the session were saved.

1.1.2 Web user interface (web UI)

Users and administrators can perform most tasks through the web user interface (web UI), which can be accessed with HTTP or HTTPS. The web UI runs in Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome and Apple Safari on any supported computer that has network access to the console system. The list of supported client browsers and their versions are available in the release notes.

NOTE: When accessing the console system via the web UI, do not disable additional dialogs if prompted by your browser. Disabling dialogs will disable some functionality of the web UI.

1.1.3 IPv4 and IPv6 support

The console system supports dual stack IPv4 and IPv6 protocols. The administrator can use the web UI or CLI to configure support for IPv4 addresses only or for both IPv4 and IPv6 addresses. The following list describes the IPv6 support provided in the console system:

- DHCP
- Dial-in and dial-out sessions (PPP links)
- DSView software integration
- eth0 and eth1 Ethernet interfaces
- Firewall (IP tables)
- HTTP/HTTPs
- Linux kernel
- Remote authentication: Radius, Tacacs+, LDAP and Kerberos servers
- SNMP
- SSH and Telnet access
- Syslog server

NOTE: IPSec is not supported with IPv6.

1.1.4 Flexible users and groups

An account can be defined for each user on the console system or on an authentication server. The admin and root users have accounts by default, and either can add and configure other user accounts. Access to ports can be optionally restricted based on authorizations an administrator can assign to custom user groups or individual users. For more information, see Users accounts and user groups on page 60.

1.1.5 Security

Security profiles determine which network services are enabled on the console system. Administrators can either allow all users to access enabled ports or allow the configuration of group and user authorizations to restrict access. You can also select a security profile, which defines which services (FTP, TFTP, ICMP, IPSec and Telnet) are enabled and SSH and HTTP/HTTPS access. The administrator can select either a preconfigured security profile or create a custom profile. For more information, see Security on page 20.

1.1.6 Authentication

Authentication can be performed locally, with One Time Passwords (OTP), a remote Kerberos, LDAP, RADIUS, TACACS+ authentication server or a DSView server. The console system also supports remote group authorizations for the LDAP, RADIUS and TACACS+ authentication methods. Fallback mechanisms are also available.

Any authentication method configured for the console system or the ports is used for authentication of any user who attempts to log in through Telnet, SSH or the web UI. For more information, see Authentication on page 58.

iCOM.pdf

1.1.7 VPN based on IPSec with NAT traversal

If IPSec is enabled in the selected security profile, an administrator can use the VPN feature to enable secure connections. For more information, see IPSec(VPN) on page 28.

1.1.8 Packet filtering

An administrator can configure a console system to filter packets like a firewall. Packet filtering is controlled by chains, which are named profiles with user-defined rules. The console system filter table contains a number of built-in chains that can be modified but not deleted. An administrator can also create and configure new chains.

1.1.9 SNMP

If SNMP is enabled in the selected security profile, an administrator can configure the Simple Network Management Protocol (SNMP) agent on the console system to answer requests sent by an SNMP management application.

The console system SNMP agent supports SNMP v1/v2 and v3, MIB-II and Enterprise MIB. For more information, see SNMP configuration on page 35.

NOTE: The text files with the Enterprise MIB (ACS8000-MIB.asn) and the TRAP MIB (ACS8000-TRAP-MIB.asn) are available in the appliance under the /usr/local/mibs directory.

1.1.10 Data logging, notifications, alarms and data buffering

An administrator can set up data logging, notifications and alarms to alert administrators of problems with email, SMS, SNMP trap or DSView software notifications. An administrator can also store buffered data locally, remotely or with DSView management software. Messages about the console system and connected servers or devices can also be sent to syslog servers.

1.1.11 Power management

The console system enables users who are authorized for power management to turn power on, turn power off and reset devices plugged into a connected power distribution unit (PDU). The power devices can be connected to any serial port. Authorized users can also monitor and control a connected uninterruptible power supply (UPS) device. For more information, see Power management on page 70.

1.1.12 Auto discovery

An administrator can enable auto discovery to find the hostname of a target connected to a serial port. Auto discovery's default probe and answer strings have a broad range. An administrator can configure site-specific probe and answer strings. Auto discovery can also be configured through the DSView software.

1.1.13 FIPS module

The 140 series of Federal Information Processing Standards (FIPS) are U.S. government computer security standards that specify requirements for cryptography modules.

The console system uses an embedded cryptographic module that is based on the FIPS 140-2 validated cryptographic module (certificate number 1747) running on a Linux ARM platform. For more information, see FIPS module on page 21.

1.2 Configuration Examples

The following graphic and table illustrate a Avocent® ACS800/8000 advanced console system configuration with all possible options. Options vary by model and no model has all the options shown.

Figure 1.1 ACS8000 Advanced Console System Configuration With All Options Shown

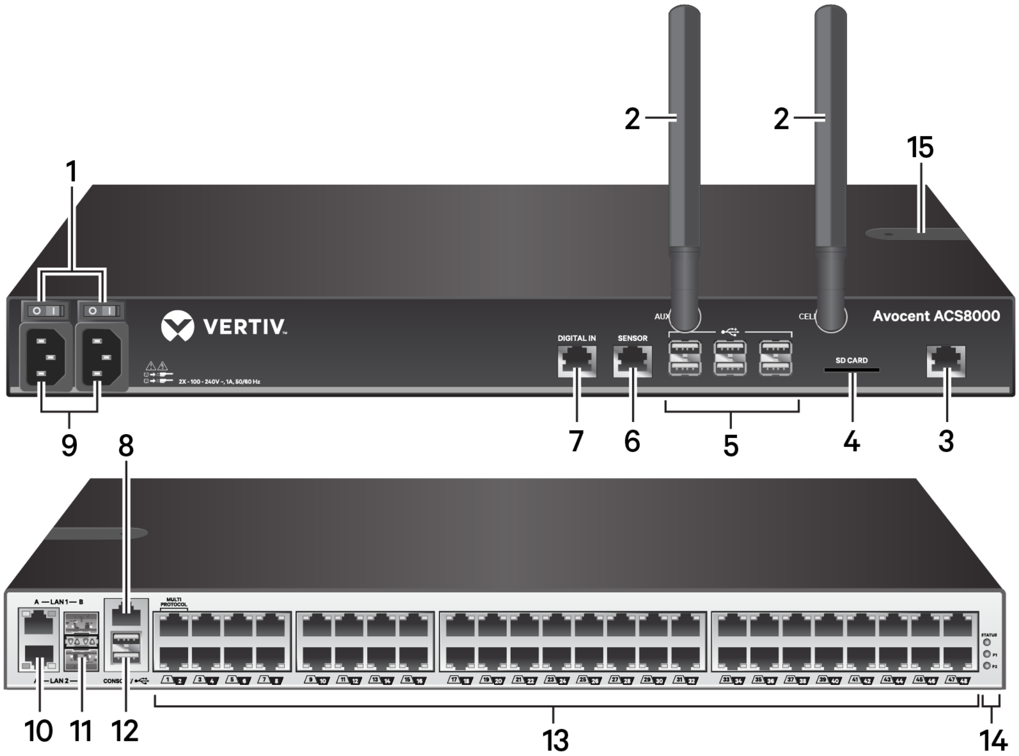


Table 1.1 ACS8000 Advanced Console System Configuration Descriptions

Number	Description
1	Power buttons (dual power supply shown).
2	Cellular antennas for the cellular modem (not available on some models).
3	Connect a phone line to the Modem port for the internal modem.
4	SD card slot (not available on some models).
5	USB ports for supported USB devices (not available on some models).
6	Sensor port for a 1-Wire environmental sensor (not available on some models).
7	Digital In port for smoke, leak, pressure or dry contact sensors (not available on some models).
8	Console port for connecting a terminal or workstation. The console system is configured using a terminal or terminal emulator with session settings of: 9600, 8, N and 1, with no flow control.
9	Power supply (dual power supply shown).
10/11	LAN ports. The ports on the left are for copper interface connections. The ports on the right are for fiber interface connections. You may connect to either or both network ports for redundancy, however only one LAN1 and one LAN2 port may be used at the same time. If both LAN1 or LAN2 ports are connected, the fiber connection has priority.
12	Two USB ports on the rear of the console system for additional USB devices.
13	Serial ports. Using CAT 5e or CAT 6 cables and DB9 or DB25 console adaptors, connect the appropriate serial and power devices to the serial ports on the console system.
14	Status LEDs.
15	SIM card slot

The following graphic and table illustrate the multi-protocol ports and LEDs.

Figure 1.2 Avocent® ACS8000 Advanced Console System Multi-Protocol Ports and LEDs

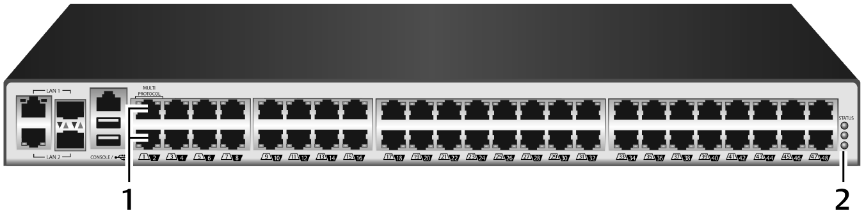


Table 1.2 Multi-Protocol Ports and LED Descriptions

Number	Description
1	Multi-protocol ports. These two ports can accept RS422 and RS485 pin-outs in addition to Cyclades and Cisco pin-outs.
2	LEDs. The STATUS LED is green when the console system is fully booted up and initialized. The P1 and P2 LEDs indicate an active power supply. P1 is green when Power Supply 1 is on. P2 is green when Power Supply 2 is on.

Figure 1.3 Inserting the SIM card

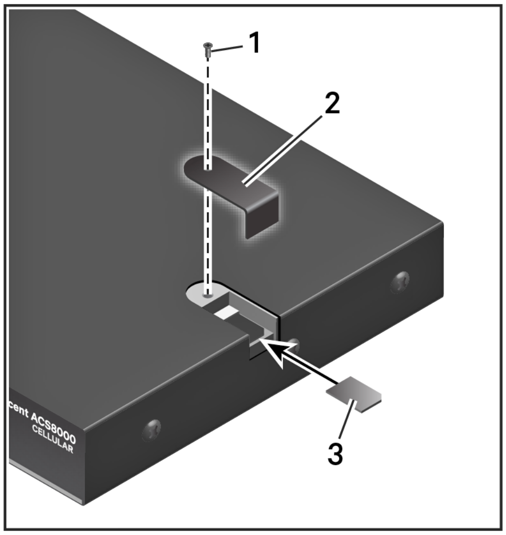


Table 1.3 Inserting the SIM Card Descriptions

item	description
1	Remove the screw to release the cover. Once the card is inserted, replace the cover and reinsert the screw.
2	Remove the cover to expose the SIM card slot. Replace the cover once the card has been inserted.
3	Insert the card.

Figure 1.4 Typical ACS800 Advanced Console System Configuration

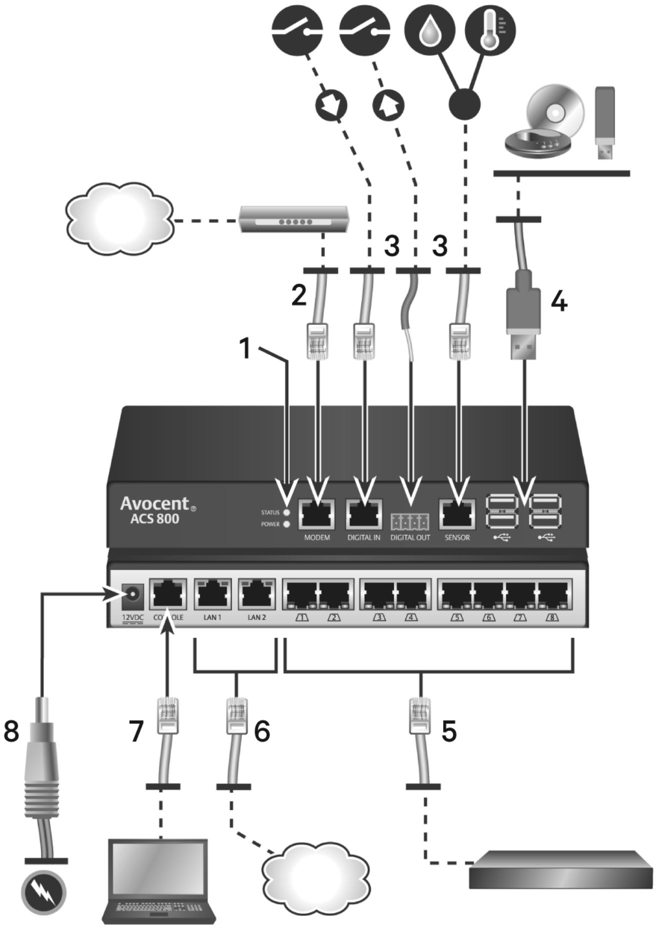


Table 1.4 Typical ACS800 Advanced Console System Descriptions

Number	description
1	LEDs. The STATUS LED is green when the console system is fully booted up and initialized. The Power LED is green when power is being supplied to the console system.
2	Connect a phone line to the Modem port for the internal modem.
3	Sensor ports for 1-Wire environmental, smoke, leak, pressure or dry contact sensors.
4	USB ports for supported USB devices.
5	Serial ports. Using CAT 5e or CAT 6 cables and DB9 or DB25 console adaptors, connect the appropriate serial and power devices to the serial ports on the console system. All of the serial ports are multi-protocol and user selectable with RS485, RS422 and RS232 pinouts.
6	Copper LAN ports. You may connect to either or both network ports for redundancy.
7	Console port.
8	Power supply.

1.2.1 Serial port LED status

Each serial port has two LEDs that illuminate either green or yellow. Green LEDs indicate the status for physical connection with a serial port, remote connectivity (when applicable) and data transfer. Yellow LEDs indicate whether a serial port is being monitored along with the alert level (emergency, alert or none) of a monitored target. The following table describes the meaning of each LED status.

Table 1.5 LED Status Descriptions

State	Description for Green LEDs	Description for Yellow LEDs
Off (not illuminated)	No physical connection	No data buffering
On (solid green or yellow)	Device is physically connected to the serial port	Data buffering is enabled for the serial port
Slow blink	Telnet, SSH or Raw session is active	Alert is active
Fast blink	TX or RX data activity	Emergency

2 Getting Started

2.1 Installation

For information on installing your console system, see the ACS800 or ACS8000 Quick Installation Guide that shipped with your product.

2.2 Turning On the Console System

Depending on the model, the console system is supplied with single or dual AC or DC power supplies.

⚠ **WARNING! Always execute the shutdown command through the web UI, CLI or DSView software under the Overview/Tools node before turning the console system off, then on again. This will ensure the reset doesn't occur while the file system in Flash is being accessed, and it helps avoiding Flash memory corruptions.**

2.2.1 AC power

To turn on a console system with AC power:

1. Make sure the console system is turned off.
2. Plug the power cable into the console system and into a power source.
3. Turn the console system on.
4. Turn on the power switches of the connected devices.

2.2.2 DC power

DC power is connected to a DC-powered console system by way of three wires: Return (RTN), Ground (GND) and -48 VDC. For redundancy, there are two sets of wires that can be connected to two separate power sources.

⚠ **WARNING! It is critical that the power source supports the DC power requirements of your console system. Make sure that your power source is the correct type and that your DC power cables are in good condition before proceeding. Failure to do so could result in personal injury or damage to the equipment.**

The following diagram shows the connector configuration for DC power.

NOTE: DC Power is only available on the ACS8000 console system.

Figure 2.1 DC Power Connection Terminal Block

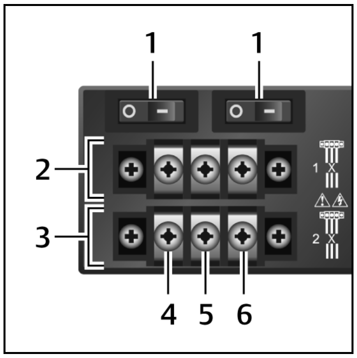


Table 2.1 DC Power Connection Details

Number	Description	Number	Description
1	Power switch, one for each power source	4	RTN (Return)
2	Connections for the first power source	5	GND (Ground)
3	Connections for the second power source	6	-48 VDC

To turn on a console system with DC power:

1. Make sure the console system is turned off.
2. Make sure DC power cables are not connected to a power source.
3. Remove the protective cover from the DC power block by sliding it to the left or right.
4. Loosen all three DC power connection terminal screws.
5. Connect your return lead to the RTN terminal, your ground lead to the GND terminal and your -48 VDC lead to the -48 VDC terminal and tighten the screws.
6. Slide the protective cover back into place over the DC terminal block.
7. If your console system has dual-input DC terminals, repeat steps 3-6 for the second terminal.
8. Connect the DC power cables to the DC power source and turn on the DC power source.
9. Turn on the console system.
10. Turn on the power switches of the connected devices.

2.3 Configuring a Console System

A console system may be configured at the appliance level through the command line interface accessed through the CONSOLE or Ethernet port. All terminal commands are accessed through a terminal or PC running terminal emulation software.

NOTE: To configure the console system using DSView software, see the Avocent® DSView 4.5 Management Software Installer/User Guide. To configure the console system using the web UI, see Web User Interface Overview for Administrators on page 15. To configure the console system using Telnet or SSH, see the Avocent® ACS 800/8000 Advanced Console System Command Reference Guide.

To connect a terminal to the console system:

1. Using a null modem cable, connect a terminal or a PC that is running terminal emulation software (such as HyperTerminal) to the CONSOLE port on the back panel of the console system. An RJ-45 to DB9 (female) cross adaptor is provided.

The terminal settings are 9600 bits per second (bps), 8 bits, 1 stop bit, no parity and no flow control.

2. Turn on the console system. When the console system completes initialization, the terminal will display the login banner plus the login prompt.

2.3.1 Using Telnet or SSH

An authorized user can use a Telnet or SSH client to make a connection directly to the console of a device if all of the following are true:

The Telnet or SSH:

- protocol is enabled in the selected security profile
- client is available, and it is enabled on the computer from which the connection is made

To use Telnet to connect to a device through a serial port:

For this procedure, you need the username configured to access the serial port, the port name (for example, 14-35-60-p-1), device name (for example, ttyS1), TCP port alias (for example, 7001) or IP port alias (for example, 100.0.0.100) and the hostname of the console system or its IP address.

To use a Telnet client, enter the information in the dialog boxes of the client.

-or-

To use Telnet in a shell, enter the following command:

```
#telnet [hostname | IP address]
login: username:[portname | device name | TCP Port Alias]
-or-
#telnet [hostname | IP address] TCP Port Alias
login: username
-or-
#telnet IP Port Alias
login: username
```

To close a Telnet session:

Enter the Telnet hotkey defined for the client. The default is **Ctrl] + q** to quit

-or-

enter the text session hotkey for the CLI prompt and then enter **exit**.

To use SSH to connect to a device through a serial port:

For this procedure, you need the username configured to access the serial port, the port name (for example, 14-35-60-p-1), TCP port alias (for example, 7001), device name (for example, ttyS1), and the hostname of the console system, IP address or IP Port alias (for example, 100.0.0.100).

To use an SSH client,

Enter the information in the dialog boxes of the client.

-or-

To use SSH in a shell, enter the following command:

```
ssh -l username:port_name [hostname | IP_address]
-or-
ssh -l username:device_name [hostname | IP_address]
-or-
ssh -l username:TCP_Port_Alias [hostname | IP_address]
-or-
ssh -l username IP_Port_Alias
```

To close an SSH session:

At the beginning of a line, enter the hotkey defined for the SSH client followed by a period. The default is **~**.

-or-

enter the text session hotkey for the CLI prompt and then enter **exit**.

3 Accessing the Console System via the Web UI

Once you've connected your Avocent® ACS800/8000 advanced console system to a network, you can access the console system with its web user interface (web UI). The web UI provides direct access to the console system via a graphical user interface instead of a command-based interface.

NOTE: For a new console system using factory defaults, LAN1 attempts to obtain an IP address using DHCP, and LAN2 has a static IP address of 192.168.161.10. Use LAN2 for initial configuration or use the Console port to discover the IPv4 DHCP-assigned address for LAN1.

NOTE: For instructions on accessing the console system via the CLI or DSView software, see the Avocent® ACS800/8000 advanced console system Command Reference Guide or the Avocent® DSView 4.5 Management Software Installer/User Guide.

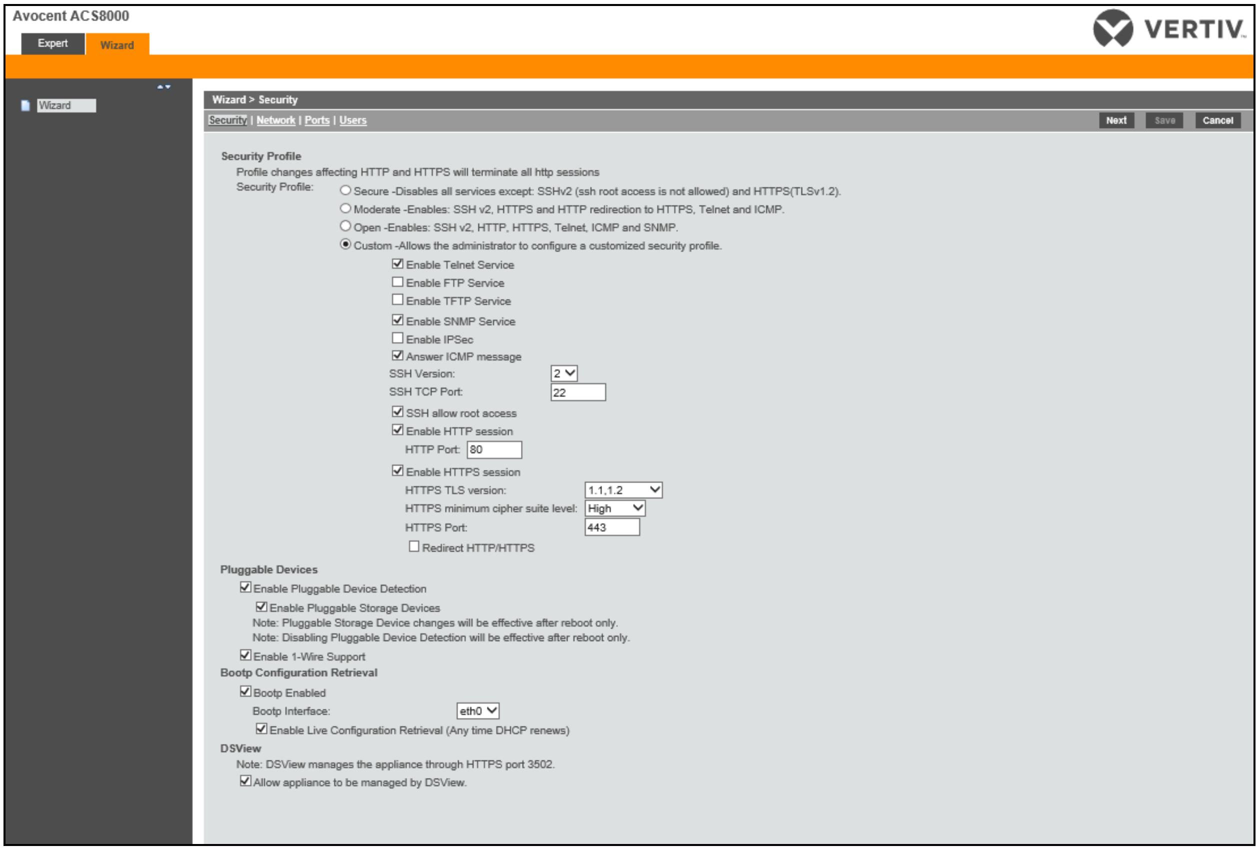
3.1 Wizard Mode

The Wizard mode is designed to simplify the setup and configuration process by guiding an administrator through the configuration steps. An administrator can configure all ports in the CAS Profile and set the Security Profile, Network and Users Settings using the Wizard.

By default, the first time an administrator accesses the console system through the web UI, the Wizard displays. Subsequent log-ins open in Expert mode, and once the console system has been configured, Expert mode becomes the default mode. An administrator can toggle between Expert and Wizard modes by clicking the tab bar on the web UI administrator screen.

The following image shows a typical screen when an administrator is in Wizard mode.

Figure 3.1 Wizard Screen



Security Profile

Profile changes affecting HTTP and HTTPS will terminate all http sessions

Security Profile:
○ Secure -Disables all services except: SSHv2 (ssh root access is not allowed) and HTTPS(TLSv1.2).
○ Moderate -Enables: SSH v2, HTTPS and HTTP redirection to HTTPS, Telnet and ICMP.
○ Open -Enables: SSH v2, HTTP, HTTPS, Telnet, ICMP and SNMP.
● Custom -Allows the administrator to configure a customized security profile.

☑ Enable Telnet Service
□ Enable FTP Service
□ Enable TFTP Service
☑ Enable SNMP Service
□ Enable IPSec
☑ Answer ICMP message
SSH Version: 2
SSH TCP Port: 22
☑ SSH allow root access
☑ Enable HTTP session
HTTP Port: 80
☑ Enable HTTPS session
HTTPS TLS version: 1.1,1.2
HTTPS minimum cipher suite level: High
HTTPS Port: 443
□ Redirect HTTP/HTTPS

Pluggable Devices

☑ Enable Pluggable Device Detection
☑ Enable Pluggable Storage Devices
Note: Pluggable Storage Device changes will be effective after reboot only.
Note: Disabling Pluggable Device Detection will be effective after reboot only.
☑ Enable 1-Wire Support

Bootp Configuration Retrieval

☑ Bootp Enabled
Bootp Interface: eth0
☑ Enable Live Configuration Retrieval (Any time DHCP renews)

DSView

Note: DSView manages the appliance through HTTPS port 3502.
☑ Allow appliance to be managed by DSView.

The following procedures describe how to configure the console system from the Wizard.

To configure security parameters and select a Security Profile:

1. Select the *Security* link in the content area.
2. Select the desired Security Profile. If using a Custom Security Profile, click the checkboxes and enter values as needed to configure the services, SSH and HTTP and HTTPS options to conform with your site security policy.
3. Pluggable devices, which include devices connected to SD card slot and USB ports, are disabled by default. To enable them, check the Enable Pluggable Device Detection box. Storage devices (SD card and USB storage) are enabled by default when Pluggable Device Detection is enabled. To disable this subset of pluggable devices, clear the Enable Pluggable Storage Devices box. Pluggable devices also include the 1-Wire Sensor port which is enabled by default. To disable the 1-Wire Sensor port, uncheck the Enable 1-Wire Support box.

NOTE: These options appear for all console system models, even though some models do not have SD card or 1-Wire sensor ports. If your model does not have these ports, leave these options disabled.

4. Under the Bootp Configuration Retrieval heading, uncheck the box(es) to disable Bootp configuration retrieval and/or live configuration retrieval.
5. If you are not using DSView software to manage the appliance, uncheck the *Allow Appliance to be Managed by DSView* box.
6. Click *Next* to configure the Network or click the *Network*, *Ports* or *Users* link to open the appropriate screen.

To configure network parameters:

1. Select the *Network* link in the content area.

2. Enter the Hostname, Primary DNS and Domain in the appropriate fields.
3. Select the IPv4 or IPv6 method for the ETH0 interface. If using Static, enter the Address, Mask and Gateway in the appropriate fields.
4. Enable or disable LLDP (Link Layer Discovery Protocol).
5. Enable or disable IPv6 support.
6. Click *Next* to configure ports or click on the *Security*, *Ports* or *Users* link to open the appropriate screen.

To configure Ports:

1. Select the *Ports* link in the content area.
2. Check the box to enable all ports.
3. Use the appropriate drop-down menus to select the values for the RJ45 Pin-Out, Speed, Parity, Data Bits, Stop Bits, Flow Control, Protocol, Authentication Type and Data Buffering Status and Data Buffering Time Stamp.
4. Select the Data Buffering Type. If using NFS, enter the NFS Server and NFS Path information in the appropriate fields.
5. Click *Next* to configure users or click on the *Network*, *Security* or *Users* link to open the appropriate screen.

To configure users and change passwords:

1. Select the *Users* link in the content area.
2. Click a username (*admin* or *root*) and enter the new password in the Password and Confirm Password fields.

   -or-

3. Click *Add* to add a user. Enter the new username and password in the appropriate fields.
4. (Optional) To force the user to change their password the next time they log in, select the *User must change password at next login* checkbox.
5. Assign the user to one or more groups.
6. (Optional) Configure account expiration and password expiration.
7. Click *Next*.
8. Repeat steps 3-7 as needed to configure new user accounts and assign them to default groups.

NOTE: By default, all configured users can access all enabled ports. Additional configuration is needed if your site security policy requires you to restrict user access to ports.

9. Click *Save,* then click *Finish*.

3.2 Web User Interface Overview for Administrators

NOTE: For an overview of the web user interface (UI) for regular users, see Web UI Overview for Regular Users on page 77.

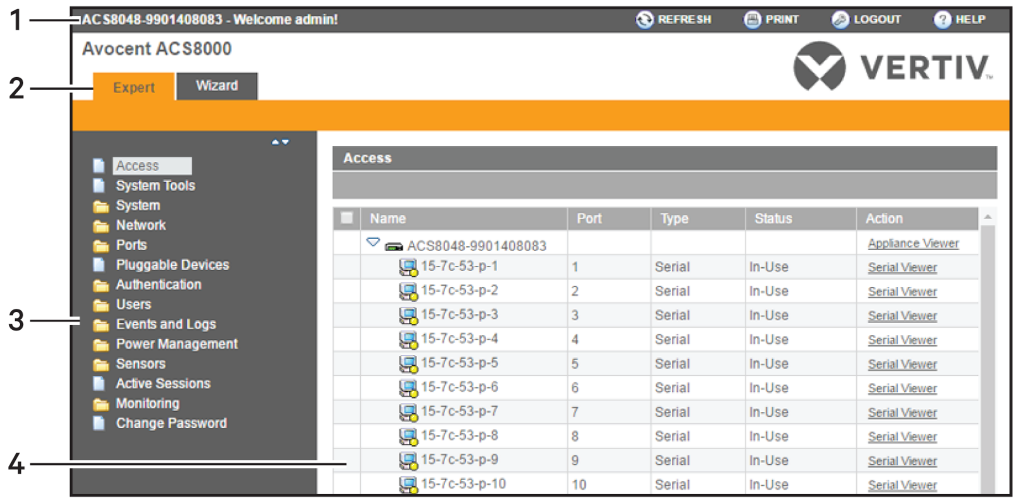
To log into the web UI:

1. Open a web browser and enter the console system IP address in the address field.
2. Log in with your username and password. The default username is admin. The first time you log in as admin, leave the password field blank. You are prompted to create a new password.

NOTE: By default, the root user is disabled. An admin can enable the root user from the Users - Local Accounts - User Names page.

The following figure shows a typical web UI screen for an administrator.

Figure 3.2 Administrator Web UI Screen



Name	Port	Type	Status	Action
ACS8048-9901408083				Appliance Viewer
15-7c-53-p-1	1	Serial	In-Use	Serial Viewer
15-7c-53-p-2	2	Serial	In-Use	Serial Viewer
15-7c-53-p-3	3	Serial	In-Use	Serial Viewer
15-7c-53-p-4	4	Serial	In-Use	Serial Viewer
15-7c-53-p-5	5	Serial	In-Use	Serial Viewer
15-7c-53-p-6	6	Serial	In-Use	Serial Viewer
15-7c-53-p-7	7	Serial	In-Use	Serial Viewer
15-7c-53-p-8	8	Serial	In-Use	Serial Viewer
15-7c-53-p-9	9	Serial	In-Use	Serial Viewer
15-7c-53-p-10	10	Serial	In-Use	Serial Viewer

Table 3.1 Web UI Screen Areas

Number	Description
1	Top option bar. The name of the appliance and of the logged in user appear on the left side. Refresh, Print, Logout and Help buttons appear on the right.
2	Tab bar. Displays whether the admin is in Expert or Wizard mode.
3	Side navigation bar. Menu options for configuration, viewing of system information and access to devices. The options change based on user rights.
4	Content area. Contents change based on the options selected in the side navigation bar.

3.3 Expert Mode

The following tabs are available in the side navigation bar of the web UI when an administrator is in Expert mode.

3.3.1 Access

All the devices connected to the console system can be viewed from the Access icon.

To view and connect to devices using the web UI:

1. Select *Access* in the side navigation bar. The content area displays the name of the console system and a list of names or aliases for all installed and configured devices the user is authorized to access.
2. Select *Serial Viewer* from the Action column to open a connection to the selected serial port.

   -or-

   Select *Appliance Viewer* from the Action column to open a connection to the console system.

NOTE: The HTML5 viewer is the default viewer to open; however, if an administrator has selected the JNLP viewer, the Java applet viewer appears.

3. If you are not automatically logged in, log in when prompted.

3.3.2 System Tools

Click *System Tools* to display icons which can be clicked to reboot or shut down the console system, upgrade the console system's firmware, save or restore its configuration or open a terminal session with the console system.

Upgrading firmware

The console system supports the storage of two firmware images. As the firmware is upgraded, the image not currently running will be overwritten with the new firmware. The latest firmware can be downloaded from the Vertiv website and accessed by the console system using a File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP) server. Firmware can also be downloaded via a web browser from the user's local machine.

To view the console system's current firmware version, from the sidebar of the Expert tab, click *System-Information*.

To upgrade a console system's firmware:

1. From http://www.VertivCo.com, browse to the product updates section and find the firmware for your console system.
2. Save the new firmware to a server accessible via FTP, SFTP or SCP, or to your desktop.
3. From the sidebar of the console system's web UI, click *System Tools*, then click *Upgrade Firmware*.
4. Download the file from the server you selected in step 2.
    a. Click the radio button next to Remote Server, then use the drop-down menu to select the protocol of the server where you saved the file.
    b. Enter the IP address for the server where the firmware is saved in the appropriate field.
    c. Enter the username and password for the server in the appropriate fields.
    d. Enter the file directory where the firmware is saved and the filename for the firmware in the appropriate fields.

   -or-

   Download the file from your desktop by selecting *My Computer*.

    a. Type the filename for the new firmware or click *Browse* to open a window and browse to the file.
5. Click *Download*. The console system will download the firmware from the specified site and will display a message when the download is complete.
6. Click *Install*.
7. Once the new firmware is installed, reboot the console system.

Configuration files

An administrator can create a backup image of the console system's configuration. During creation, no changes should be made to the configuration. The backup configuration file may be uploaded to a remote server, stored on a console system local file or saved to the web user's computer. Configuration files can be saved as a compressed file, CLI script or XML file.

To save the current configuration file:

1. From the sidebar of the Expert tab, click *System Tools*.
2. Click *Save Configuration*.
3. Use the drop-down menu to select the file format.
4. Upload the file to a remote server.

a. Click the Remote Server radio button, then use the drop-down menu to select the protocol of the server where you want to save the file.

b. Enter the IP address for the server where the file will be saved in the appropriate field.

c. Enter the username and password for the server in the appropriate fields.

d. Enter the file directory where the configuration file will be saved and the filename in the appropriate fields.

-or-

Save the file locally by clicking the Local File radio button, then enter the filename.

NOTE: The filename can include the full path to where the file will be saved. Specifying the full path permits the file to be saved to a USB storage device that is mounted, for example /media/sda1/filename. If the full path is not specified, the file is written to /mnt/hdUser/backup/<filename>.

-or-

Save the file to your computer by clicking the My Computer radio button. The file will be saved in your Downloads folder.

5. Click *Save*.

To restore a previous configuration:

1. From the sidebar of the Expert tab, click *System Tools*.
2. Click *Restore Configuration*.
3. Restore the file from a remote server.

a. Click the Remote Server radio button, then use the drop-down menu to select the protocol of the server where the configuration file is saved.

b. Enter the IP address of the server where the file is saved in the appropriate field.

c. Enter the username and password for the server in the appropriate fields.

d. Enter the path and filename for the configuration file.

-or-

Restore from a local file by clicking the Local radio button and entering the filename.

-or-

Restore the file from your computer by clicking the My Computer radio button, then browse to where the file is saved on your computer and click *Open*.

4. Click *Restore*.

Configuration integrity

In order to ensure configuration integrity, the console system permits an administrator to generate and verify a digital signature (MD5) of the console system's configuration. The console system compares its MD5 checksum value against a known MD5 checksum value to verify its configuration and keep it protected from corruption.

An administrator can specify a running configuration as trusted and instruct the console system to generate an MD5 tag for the trusted configuration. An administrator can also verify the configuration by comparing it to another known or trusted configuration. The console system will declare the configuration to either be Unchanged or Modified after the verification is complete.

Configuration integrity works with and relies on the console system's saved and restored configuration files. It's also dependent on the zero-touch provisioning feature.

NOTE: In order to use configuration integrity, you must save the configuration using the compressed file option. The compressed file format captures more configuration data to ensure the accuracy of the configuration integrity results. Saving the configuration in either the CLI script or XML file formats will produce invalid configuration integrity results.

The console system generates an event notification each time an MD5 tag is generated. For more information about events, see Event list on page 68.

To generate an MD5 tag:

1. From the sidebar of the console system's web UI, click *System Tools* and then click *Configuration Integrity*.
2. Click the Generate MD5 tag for the Running Configuration radio button and click *Execute*.
3. The generated MD5 tag displays on the screen as a 32-character hexadecimal value and is also saved on the console system as the value to compare against later. An administrator can cut and paste this string to use on other systems.

To verify an MD5 tag:

1. From the sidebar of the console system's web UI, click *System Tools* and then click *Configuration Integrity*.
2. Click the Verify Running Configuration radio button.
3. Leave the MD5 field blank to verify the running configuration.

   -or-

   Enter an MD5 checksum string to verify a known configuration.

4. Click *Execute*.

HTTPS certificate

You can generate a new self-signed certificate or download a signed certificate to the appliance from an FTP server or from your desktop.

To generate a new self-signed certificate:

1. From the sidebar of the Expert tab, click *System Tools*.
2. Click *Generate / Download Certificate*.
3. To generate a new certificate, click the radio button next to Generate Self-Signed Certificate and enter the desired information in the self-signed certificate fields: Country, State/Province, City/Locality, Organization, Organization Unit, Common Name, Email Address and Netscape Comment.

   -or-

   To download a signed certificate from an FTP, SFTP or SCP server, click the radio button next to Remote Server and enter all information about the server: IP Address, Username, Password, File Directory and File Name.

   -or-

   To download a certificate from your desktop, click the radio button next to Download Certificate From My Computer, click *Choose File* or *Browse* to browse to where the file is saved and click *Open*.

4. Click *Generate/Download*. The certificate's information will be displayed.

5. Click *Apply*. The message shows *Applying the new certificate will terminate all HTTP/HTTPS sessions. The restart of your browser is required. Are you sure you want to continue?*
6. Click *OK* to continue. The certificate will be saved and the browser will restart to use the new certificate.

NOTE: All http/https sessions will close, and the user will need to re-establish the connection.

3.3.3 System

Click *System* to display information about the console system and allow an administrator to configure the console system's system parameters. The following tabs are listed under System in the side navigation bar.

Security

Security Profile

A Security Profile determines which services are enabled on the console system.

During initial configuration, the console system administrator must configure security parameters to conform with the site security policy. The following security features can be configured either in the web UI, CLI or the DSView software:

- Configure the session idle time-out
- Enable or disable RPC
- Enable or disable pluggable device detection, storage devices and 1-Wire sensors
- Ability to configure serial port access for all users, or allow the configuration of group and user-specific authorizations to restrict access
- Select a Security Profile, which defines:
  - Enabled services (FTP, TFTP, ICMP, IPSec, SNMP and Telnet)
  - SSH and HTTP/HTTPS access
  - Enable or disable Bootp Configuration retrieval, Bootp interface and enable or disable Live Configuration Retrieval

The administrator can select either a preconfigured Security Profile or create a custom profile.

All the services and the SSH and HTTP/HTTPS configuration options that are enabled and disabled for each Security Profile are shown in the Wizard - Security and the System - Security - Security Profile pages.

To configure a Security Profile:

1. Select *System - Security - Security Profile.*
2. In the Idle Timeout field, enter the number of seconds before the console system times out open sessions.

NOTE: This value applies to any user session to the appliance via HTTP, HTTPS, SSH, Telnet or CONSOLE port. It will not overwrite the value configured for the user's authorization group. The new idle time-out will be applied to new sessions only.

3. Under the Enabled Services section, enable or disable the *RPC* checkbox.
4. Under the Pluggable Devices section, enable or disable pluggable device detection for USB and SD devices. If enabled, the USB storage and SD card can be disabled to restrict the type of pluggable devices for security reasons. The 1-wire sensors can also be disabled in this section.

NOTE: These options appear for all console system models, even though some models do not have SD card or 1-Wire sensor ports. If your model does not have these ports, leave these options disabled.

NOTE: Disabling Pluggable Device Detection or changing the Storage Device setting will only be effective after a reboot.

5. Under the Serial Devices heading, select whether port access is controlled by user and group authorization or whether port access settings to apply to all users.
6. Under Bootp Configuration retrieval, enable or disable the service.
7. Enable/disable SSH authentication via username/password.
8. Select the checkbox for *Custom*, *Moderate*, *Open* or *Secure* under the Security Profile heading.
9. Click *Save*.

FIPS module

The console system uses an embedded cryptographic module that is based on the FIPS 140-2 validated cryptographic module (certificate number 1747) running on a Linux ARM platform.

If an administrator enables the FIPS module, the console system will use the FIPS Object Module to perform encryption operations. The FIPS module is disabled by default.

When the FIPS module is enabled, the Monitoring - FIPS mode page will show what service (SSHv2, HTTPS, SNMPv3 and ADSAP2) is in FIPS mode. All security functions and cryptographic algorithms used by the service are performed in FIPS 140-2 Approved mode.

To enable the FIPS module:

1. Select *System - Security - FIPS 140*.
2. Check the box to Enable the FIPS 140-2 Module and click *Save*.

The console system will automatically reboot. During the reboot, the console system will erase SSH keys, update the configuration of HTTPD, SSHD, ADSAP2d and SNMPD files and test the integrity of the FIPS Object Module. Once the reboot is complete, the console system will accept SSH and HTTPS connections using only FIPS-approved ciphers.

When FIPS is enabled the following restrictions apply:

For SSH sessions:

- Triple-DES CBS and AES 128/192/256 are the only encryption ciphers that will be accepted.
- HMAC-SHA1 and HMAC-SHA1-96 are the only message integrity algorithms that will be accepted.
- Only RSA keys 1024 to 16384 bits will be accepted.

HTTPS sessions will accept only the SSL v 3.1(TLSv1) protocol to establish the SSL tunnel with one of the following encryption ciphers:

- AES-256-SHA
- AES-128-SHA
- Triple DES SHA (DES-CBC3-SHA)

SNMP version 3 requests will be accepted when authentication is SHA and the encryption cipher is AES.

DSView software security

You can also configure DSView software security settings. When the console system is managed by the DSView software, the DSView server will supply the certificate to the console system. Under normal conditions, the DSView software will manage the certificate to clear and replace it with a new certificate as needed. If communication with the DSView software is lost, the DSView server will be unable to clear the certificate and the console system cannot be used. Click the *Clear DSView Certificate* button to configure the console system in Trust All mode.

To configure DSView software security settings:

1. Select *System - Security - DSView*.
2. Click the *Allow appliance to be managed by DSView* checkbox and click *Save*.

Date and Time

The console system provides two options for setting the date and time. It can retrieve the date and time from a network time protocol (NTP) server, or you can set the date and time manually so that the console system's internal clock is used to provide time and date information.

NOTE: The Current Time displayed in the Date & Time screen shows only the time when the screen was opened. It does not continue to update in real time.

To set the time and date using NTP:

1. Click *System - Date And Time*.
2. Select *Enable network time protocol*.
3. Enter the NTP server site of your choice and click *Save*.

To set the time and date manually:

1. Click *System - Date And Time*.
2. Select *Set manually*.
3. Using the drop-down menus, select the required date and time and click *Save*.

To set the time zone using a predefined time zone:

1. Click *System - Date And Time - Time Zone*.
2. Select *Predefined*.
3. Select the required time zone from the drop-down menu and click *Save*.

To define custom time zone settings:

1. Click *System- Date And Time - Time Zone*.
2. Select *Define Time Zone*.
3. Enter the Time Zone Name and Standard Time Acronym of your choice.
4. Enter the GMT Offset.
5. Select *Enable daylight savings time* if needed.
6. Select or enter the required values for daylight savings time settings and click *Save*.

Help and Language

Click *System - Help And Language* and use the drop-down menu to select the console system's language.

NOTE: Language applies to SSH, Telnet and Console Port sessions to the console system. Browser language is determined by the browser.

Online help

When the online help feature is configured for your console system, clicking the *Help* button from any form on the web UI opens a new window and redirects its content to the configured path for the online help product documentation.

Enter the full URL of the online help, ending in /index.html, on the local web server in the Online Help URL field. Click *Save*.

NOTE: Using the online help feature from the Vertiv server is not always possible due to firewall configurations, nor is it recommended. It is generally advisable for you to use the online help system provided with the product or download the online help .zip file and run it from a local server.

The system administrator can download the online help from Vertiv™. For more information on downloading the online help, contact Technical Support.

Once the online help file is obtained (in zip format), the files must be extracted and put into a user-selected directory under the web server's root directory. The web server must be publicly accessible.

General

Click *System-General* to create a login banner or select the viewer type.

Login banner:

An administrator can configure a login banner to display when a user begins a SSHv2, Telnet, Console or web UI session.

To create a login banner:

1. *Click System* - *General* in the side navigation bar.
2. Check the box to enable the login banner.
3. Enter the text you want displayed upon login in the Login Banner field and click *Save*.

Serial viewer

By default, the console system uses a basic HTML5 serial viewer. It also supports a more robust Java-based serial viewer. An administrator can configure which serial viewer is used for the serial ports and console system.

NOTE: The HTML5 serial viewer supports a maximum of 10 sessions per port with a limit of 48 total sessions.

To configure the serial viewer:

1. Click *System* - *General* in the side navigation bar.
2. Select either HTML5 Viewer or JNLP Viewer, then click *Save*.

Java-based serial viewer

NOTE: Java 1.8.0.91 or later is recommended. You must have the 32-bit version installed in order to run the serial viewer.

The following table describes the available buttons in the Java applet.

Table 3.2 Java Applet Buttons for Connecting to the Console System

Button	Purpose
SendBreak	To send a break to the terminal
Disconnect	To disconnect from the Java applet

NOTE: Using the serial or appliance viewers may require disabling the client browser's popup blocker.

NOTE: When the viewer is run, the browser may ask for permission to run the Mindterm application. Granting this permission is required for the viewer applet to run.

Boot Configuration

Boot Configuration defines the location from which the console system loads the operating system. The console system can boot from its internal firmware or from the network. By default, the console system boots from internal firmware in Flash memory. Clicking *System- Boot Configuration* displays the Boot Configuration screen.

If you need to boot from the network, make sure the following prerequisites are met:

- A TFTP server must be available on the network
- A firmware file must be downloaded from Vertiv and made available on the TFTP server
- The boot filename and the IP address of the TFTP server is known

To configure boot configuration:

1. Click *System - Boot Configuration.*
2. Under Boot Mode, select *From Flash*, and select *Image 1* or *Image 2*.

   -or-

   Select *From Network* and enter the following information:

   - Appliance IP Address: Enter the fixed IP address or a DHCP assigned IP address to the console system.
   - TFTP Server IP: Enter the IP address of the TFTP boot server.
   - Filename: Enter the filename of the boot firmware.
3. Using the drop-down menu, select whether the Watchdog Timer is enabled. If the Watchdog Timer is enabled, the console system reboots if the software crashes.
4. Using the drop-down menu, select the console port speed and click *Save*.

Information

Click *System - Information* to view the console system's identity, versions, power and CPU information.

Usage

Click *System - Usage* to view memory and Flash usage.

3.3.4 Network

Click *Network* to view and configure the Hostname, DNS, IPv6, Bonding, IPv4 and IPv6 static routes, Hosts, Firewall, IPSec (VPN) and SNMP network options.

Settings

Click *Network - Settings* to make changes to the configured network settings.

From this page, an administrator can configure the console system's hostname and DNS settings, which includes the primary and secondary DNS, domain and search addresses. An administrator can also enable IPv6 and configure it to get the DNS and/or domain from DHCPv6.

For a fault tolerant network configuration, the Bonding option may be selected to combine eth0 and eth1 into a single high-availability network interface using the active-backup bonding mode. Interface eth0 is the normal active interface with eth1 as the backup; if the carrier signal is lost on eth0, eth1 becomes the active interface. The eth0 MAC address is always used in bonding mode, no matter which interface is active.

NOTE: After enabling or disabling bonding, you must reboot the console system for the change to take effect.

Routing type

The console system supports multiple routing tables for flexible policy routing. Multiple routing tables can not be enabled at the same time network failover or bonding is enabled.

To enable multiple routing tables:

1. Click *Network - Settings*.
2. Under Multiple Routing , click the Enable IPv4 Multiple Routing Tables radio button.

Network failover

To ensure a console system can be relied upon to provide access to critical devices during a network outage, it should be configured for network failover. Failover can occur when a primary interface goes down or when a certain IP/gateway becomes inaccessible. Failover can be enabled using a secondary network or PPP (dialout) connection. If dialout is configured, PPP0 will be available as a secondary interface but can not be used as the primary interface.

Using DSView software with a console system will ensure the console system can always be accessible when in a failover situation, because the console system will "phone home" and update its IP address within the DSView software.

From the Network-Settings page, an administrator can configure a secondary network interface to be used for failover. The primary interface sets the system default gateway while the secondary interface is used when the primary interface is not available. An administrator can also select one of four triggers that enable the failover:

- Primary Interface Down
- Unreachable Primary Default Gateway
- Unreachable DSView
- Unreachable IP Address

If the IPSec tunnel has been configured (see IPSec(VPN) on page 28), an administrator can configure the IPSec tunnel to be established over the secondary interface when it is up.

To enable Network Failover:

1. From the sidebar of the Expert tab, click *Network-Settings*.
2. Under the Routing heading, click the radio button to Enable Network Failover.
3. Use the drop-down menus to select the primary and secondary interfaces as well as the VPN connection name.
4. Click the radio button next to the trigger you want to use to initiate the failover.
5. Click *Save*.

You can also configure failover using the cellular modem, for models that come with one. For more information, see Using the cellular modem in failover on page 54.

NOTE: Cellular can be used for failover if it is not already being used as the primary interface.

Devices

An administrator can select, enable and configure the IP addresses assigned to the network interfaces and view the MAC address. Besides the two standard Ethernet interfaces, the list of network interfaces includes an entry for any USB Ethernet device that may be installed.

To configure a network device:

1. Select *Network - Devices*. The Devices screen appears with a list of network interfaces and their status (enabled or disabled).

2. Click the name of the network device to configure.
3. Check the box if you want to set the network device as the primary interface. By default, eth0 is set as the primary interface.
4. Select the status (either *Enabled* or *Disabled*) from the drop-down menu.
5. Select one of the following IPv4 method options:
    - Select *DHCP* to have the IPv4 IP address set by the DHCP server.
    - Select *Static* to enter the IPv4 IP address, subnet mask and gateway address manually.
    - Select *IPv4 address unconfigured* to disable IPv4.
6. Select one of the following IPv6 method options:
    - Select *Stateless* if the link is restricted to the local IP address.
    - Select *DHCPv6* to have the IPv6 IP address set by the DHCP server.
    - Select *Static* to enter the IPv6 IP address and prefix length manually.
    - Select *IPv6 address unconfigured* to disable IPv6.

NOTE: The MAC Address for the device will be displayed after this option.

IPv4 and IPv6 static routes

To add static routes:

1. Select *Network - IPv4 Static Routes* or *IPv6 Static Routes.* Any existing static routes are listed with their Destination IP/Mask, Gateway, Interface and Metric values shown.
2. Click *Add.*
3. Select *Default* to configure the default route.

    -or-

    Select *Host IP Or Network* to enter custom settings for Destination IP/Mask.

    Enter the required Destination IP/Mask Bits with the syntax <destination IP>/<CIDR> in the Destination IP/Mask Bits field.
4. Enter the IP address of the gateway in the Gateway field.
5. Enter the interface name (Eth0, Eth1 or PPPx) in the Interface field when the route is by interface.
6. Enter the number of hops to the destination in the Metric field, then click *Save.*

Hosts

An administrator can configure a table of host names, IP addresses and host aliases for the local network.

To add a host:

1. Select *Network - Hosts.*
2. Click *Add* to add a new host.
3. Enter the IP address, hostname and alias of the host you want to add, then click *Save.*

To edit a host:

1. Select *Network - Hosts.*
2. Click on the IP address of the hostname you want to edit.
3. Enter a new hostname and alias, if applicable, then click *Save.*

Firewall

Administrators can configure the console system to act as a firewall. By default, three built-in chains accept all INPUT, FORWARD and OUTPUT packets. Select the *Add*, *Delete* or *Change Policy* buttons to add a user chain, delete user-added chains and to change the built-in chains policy. Default chains can have their policy changed (Change Policy) to accept or drop, but cannot be deleted. Clicking on the *Chain Name* allows you to configure rules for chains.

Firewall configuration is available by clicking on *Network - Firewall*. Separate but identical configuration screens are available from either the *IPv4 Filter Table* or *IPv6 Filter Table* menu options.

Only the policy can be edited for a default chain; default chain policy options are ACCEPT and DROP.

When a chain is added, only a named entry for the chain is created. One or more rules must be configured for a chain after it is added.

Configuring the firewall

For each rule, an action (either *ACCEPT*, *DROP*, *LOG, REJECT or RETURN*) must be selected from the Target pull-down menu. The selected action is performed on an IP packet that matches all the criteria specified in the rule.

If *LOG* is selected from the Target pull-down menu, the administrator can configure a Log Level and a Log Prefix.

If *REJECT* is selected from the Target pull-down menu, the administrator can select an option from the Reject with pull-down menu; the packet is dropped and a reply packet of the selected type is sent.

Protocol options

Different fields are activated for each option in the Protocol pull-down menu.

If *Numeric* is selected from the Protocol menu, enter a Protocol Number in the text field.

If *TCP* is selected from the Protocol menu, a TCP Options Section is activated for entering source and destination ports and TCP flags.

If *UDP* is selected from the Protocol menu, the UDP section is activated for entering source and destination ports.

Table 3.3 Firewall Configuration - TCP and UDP Options Fields

Field/Menu Option	Definition
Source Port - or - Destination Port	A single IP address or a range of IP addresses.
TCP Flags	[TCP only] SYN (synchronize), ACK (acknowledge), FIN (finish), RST (reset), URG (urgent) and PSH (push). The conditions in the pull-down menu for each flag are: Any, Set or Unset.

If ICMP is selected from the Protocol menu, the ICMP Type pull-down menu is activated.

If an administrator enters the Ethernet interface (eth0 or eth1) in the input or output interface fields and selects an option (*2nd and further packets, All packets and fragments* or *Unfragmented packets and 1st packets*) from the Fragments pull-down menu, the target action is performed on packets from or to the specified interface if they meet the criteria in the selected Fragments menu option.

To add a chain:

1. Select *Network - Firewall*.
2. Select either *IPv4 Filter Table* or *IPv6 Filter Table* as needed.
3. Click *Add*.
4. Enter the name of the chain to be added.

5. Click *Save*.

NOTE: Spaces are not allowed in the chain name.

6. Add one or more rules to complete the chain configuration.

To change the policy for a default chain:

NOTE: User-defined chains cannot be edited. To rename a user-added chain, delete it and create a new one.

1. Select *Network - Firewall*.
2. Select either *IPv4 Filter Table* or *IPv6 Filter Table* as needed.
3. Select the checkbox next to the name of the chain you want to change (*FORWARD*, *INPUT*, *OUTPUT*).
4. Click *Change Policy* and select *Accept* or *Drop* from the drop-down menu.
5. Click *Save*.

To add a rule:

1. Select *Network - Firewall*.
2. Select either *IPv4 Filter Table* or *IPv6 Filter Table* as needed.
3. From the chain list, click the name of the chain you want to add a rule to.
4. Click *Add* and configure the rule as needed, then click *Save*.

To edit a rule:

1. Select *Network - Firewall*.
2. Select either *IPv4 Filter Table* or *IPv6 Filter Table* as needed.
3. From the chain list, click the name of the chain with the rule you want to edit.
4. Select the rule you want to edit and click *Edit*.
5. Modify the rule as needed and click *Save*.

IPSec(VPN)

Virtual Private Network (VPN) enables a secure communication between the console system and a remote network by utilizing a gateway and creating a secure connection between the console system and the gateway. The IPSec protocol is used to construct the secure tunnel and provides encryption and authentication services at the IP level of the protocol stack.

With a console system located on a separate network behind a router, it establishes an IPSec tunnel using a x.509 certificate to a firewall. Certificates and keys are distributed to the firewall and the console system by a Certificate Authority (CA).

NOTE: The console system supports one certificate per tunnel. Multiple certificates are not supported. IPv6 tunnels are not supported. Certificates (in PKCS12 format) can be loaded from the System Tools menu.

NOTE: To run IPSec (VPN), you must enable IPSec under the custom security profile.

The remote gateway is referred to as the remote or right host and the console system is referred to as the local or left host.

Creating a Certificate of Authority

To configure the Fortinet Fortigate firewall, you need to create an internal Certificate of Authority (CA) server that generates RSA certificates the console system uses for authentication.

For information on creating a CA on an Ubuntu server, see Creating a CA.

Creating a tunnel on the server

To create a tunnel on the server:

1. From the *System* tab of the Fortigate web UI, click *Certificates* and import the CA certificate and the SERVER certificate that was generated from the easy-rsa server.
2. From the *User & Device* tab, click *PKI* and create a new user named user1 with a CA named CA_Cert_1. Then create a user group named user_group1 and put user1 in that group.
3. From the *VPN* tab, click *IPSec - Tunnels* and create a new custom VPN tunnel with the following configuration, then click *OK*.

Table 3.4 VPN Tunnel Configuration Parameters

Parameter	Value
Network	
Remote Gateway	Dial-up User
Interface	wan1
Mode Config	Enabled
IP Version	IPv4
Client Address Range	10.77.20.100-10.77.20.110
Subnet Mask	255.255.255.0
Use System DNS	Enabled
Enable IPv4 Split Tunnel	Enabled
Accessible Networks	local_lan
NAT Traversal	Enabled
Keepalive Frequency	300
Dead Peer Detection	Enabled
Authentication	
Method	Signature
Certificate Name	server
IKE Version	2
Peer Options Accept Types	Peer Certificate Group
Peer Certificate Group	user_group1
Phase 1 Proposal	
Encryption	AES128
Authentication	SHA1
Diffie-Hellman Group	14
Key Lifetime (Seconds)	86400
Local ID	C=<country> S=<state> L=<city> O=<organization>
Edit Phase 2	
Name	<name>
Comments	<comments>
Local Address Subnet	0.0.0.0/0.0.0.0
Remote Address Subnet	0.0.0.0/0.0.0.0
Phase 2 Proposal	
Encyption	AES128
Authentication	SHA1
Enable Replay Detection	Enabled
Enable Perfect Forward Secrecy (PFS)	Enabled

Table 3.4 VPN Tunnel Configuration Parameters (continued)

Parameter	Value
Diffie-Hillman Group	14
Local Port All	Enabled
Remote Port All	Enabled
Protocol All	Enabled
Autokey Keep Alive	Enabled
Key Lifetime	Seconds
Seconds	43200

4. From the *Policy & Objects* tab, click *Objects - Addresses* to create a VPN range with the following settings, then click *OK*.

Table 3.5 VPN Range Configuration

Parameter	Value
Name	ipsec_vpn_range
Type	IP Range
Subnet / IP Range	10.77.20.100 - 10.77.20.110
Interface	Any
Show in Address List	Enabled
Comments	The IP address given to VPN clients that are connecting

5. From the *Policy & Objects* tab, click *Objects - Addresses* to create a Local LAN range with the following settings, then click *OK*.

Table 3.6 Local LAN Range Configuration

Parameter	Value
Name	local_lan
Type	IP / Netmask
Subnet / IP Range	192.168.1.0 / 255.255.255.0
Interface	internal
Show in Address List	Enabled
Comments	Local Lan - inside network

6. From the *Policy & Objects* tab, click *Policy - IPv4* to create Firewall Policy 1 with the following settings, then click *OK*.

Table 3.7 Firewall Policy 1 Configuration

Parameter	Value
Incoming Interface	forti2acs
Source Address	ipsec_vpn_range
Outgoing Interface	internal
Destination Address	local_lan
Schedule	always
Service	ALL
Action	ACCEPT
Firewall / Network Options	
NAT	ON
Use Outgoing Interface Address	Enabled
Security Profiles	
Antivirus, Web Filter, Application Control, SSL Inspection	All OFF
Traffic Shaping	
Shared Shaper, Reverse Shaper, Per-IP Shaper	All OFF
Logging Options	
Log Allowed Traffic	ON
Security Events	Enabled
Comments	<Comments>
Enable this policy	Enabled

7. From the *Policy & Objects* tab, click *Policy - IPv4* to create Firewall Policy 2 with the following settings, then click *OK*.

Table 3.8 Firewall Policy 2 Configuration

Parameter	Value
Incoming Interface	internal
Source Address	local_lan
Outgoing Interface	forti2acs
Destination Address	ipsec_vpn_range
Schedule	always
Service	ALL
Action	ACCEPT
Firewall / Network Options	
NAT	ON
Use Outgoing Interface Address	Enabled
Security Profiles	
Antivirus, Web Filter, Application Control, SSL Inspection	All OFF
Traffic Shaping	
Shared Shaper, Reverse Shaper, Per-IP Shaper	All OFF
Logging Options	
Log Allowed Traffic	ON
Security Events	Enabled
Comments	<Comments>
Enable this policy	Enabled

8. From the *Policy & Objects* tab, click *Policy - IPv4* to create Firewall Policy 3 with the following settings, then click *OK*.

Table 3.9 Firewall Policy 3 Configuration

Parameter	Value
Incoming Interface	any
Source Address	all
Outgoing Interface	any
Destination Address	all
Action	DENY
Logging Options	
Log Violation Traffic	OFF

Creating a tunnel on the console system

To create a tunnel on the console system:

1. From the sidebar of the *Expert* tab, click *Network - IPSec(VPN)*, then click *Add*.
2. Enter a name for the connection.

3. Use the drop-down menus to select *IKEv2* for the IKE version and either *Start*, *Add* or *Ignore* for the Boot Action.
    a. Start - loads a connection and brings it up immediately (boot up, or after saving the configuration).
    b. Add - loads a connection without starting it. For example, the VPN can be conditionally started with a script.
    c. Ignore - ignores the connection
4. For the Remote (Right) Side, enter the following parameters:
    a. Leave the ID field blank.
    b. Enter the IP address of the remote VPN in the IP Address field.
    c. Enter the subnet the console system will use to connect through in the SubNet field.
5. For the Local (Left) Side, enter the following parameters:
    a. Leave the ID field blank.
    b. Enter the IP address of the primary interface in the IP Address field.

NOTE: The primary interface is the interface (etho or eth1) used to connect to the remote firewall. By default, the setting is eth0 and Bootp Configuration Retrieval is enabled. If your primary interface is eth1, make sure the Bootp Configuration Retrieval on the Security Profile page is disabled.

6. Click the RSA Certificate radio button, click the Local PKCS12 Files drop-down arrow and select the PKCS12 file.

To enable IPSec on the console system:

1. From the sidebar of the *Expert* tab, click *System - Security - Security Profile*.
2. Click the Custom radio button under Security Profile.
3. Check the Enable IPSec box, then click *Save*.

NOTE: After the Save button is clicked, the VPN connection starts automatically if the Boot Action is Start. The information is saved and the VPN starts (or restarts).

Verification

Verification tests can be performed to ensure the IPSec configuration was successful. The ping command is used to test communication.

To verify the IPSec status and test communication:

1. Log in to the console system as **root**.
2. Check the status of the IPSec by entering the command *ipsec status* at the Shell prompt. Note the VPN DHCP IP address.
3. Enter **ping** at the command prompt, press the Space bar, enter the address you'd like to ping and then press the Enter key on your keyboard and wait for the ping results..Test the communication from the console system to the remote subnet's target client.
4. Test the communication from the remote subnet's target client to the VPN DHCP IP address of the console system.

NOTE: To test communication, enter ping from the target client to the VPN DHCP IP address the console system and from the console system to the subnet's target client.

3.3.5 IPSec(VPN) Advanced Settings

The IPSec(VPN) configuration page includes the Advanced Settings for the ipsec.conf file. These settings, described in the following table, are displayed when the Show Advanced Settings checkbox is enabled.

Table 3.10 Advanced Settings Descriptions

Name	Description
IKE (Internet Key Exchange) Cipher Suite	Protocols used to exchange cryptographic keys. The suite includes algorithms for Encryption (confidentiality), Hash (message authentication) and DH group (key exchange) protocols when setting up the VPN.
ESP (Encapsulating Security Payload) Cipher Suite	Protocols used to exchange cryptographic keys. The suite includes algorithms for Encryption (confidentiality), Hash (message authentication) and DH group (key exchange) protocols when setting up the VPN. if DH group is used, the higher group numbers are more secure, but take a longer time to compute the key.
Security Association (SA)	
Reauthentication	Specifies whether the device should reauthenticate when an IKE Security Association (SA) changes. (An SA describes how two or more devices will communicate securely.)
IKE Lifetime	Specifies how long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated.
Key Lifetime	Specifies how long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry.
Rekey	Specifies whether a connection should be renegotiated when it is about to expire.
Keying Tries	Specifies how many attempts (a positive integer or %forever) should be made to negotiate a connection, or a replacement for one, before giving up. The default is 3.
Rekey Margin	Specifies how long before connection expiry or keying-channel expiry, should attempts to negotiate a replacement begin.
DPD Delay	Specifies the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer.

3.3.6 SNMP configuration

An administrator can configure SNMP, which is needed if notifications are to be sent to an SNMP management application.

NOTE: The Avocent® ACS800/8000 advanced console system Enterprise MIB text file is available in the appliance at: /usr/local/mibs/ACS8000-MIB.asn. The Avocent® ACS800/8000 advanced console system Enterprise TRAP MIB text file is available in the appliance at: /usr/local/mibs/ACS8000-TRAP-MIB.asn. Both files are also available at www.VertivCo.com.

To configure SNMP:

1. Click *Network - SNMP*.
2. Click the *System* button.
    a. Enter the SysContact information (email address of the console system's administrator, for example, acs8000_admin@vertivco.com).
    b. Enter the SysLocation information (physical location of the console system, for example, Avocent_ACS8000), then click *Save* to go back to the SNMP screen.
3. Click *Add* to add a new community or v3 user.
4. Enter the community name for SNMP v1/v2 or the user name for SNMP v3 in the Name field and enter the OID.
5. Select the desired permission from the pull-down menu. Choices are *Read and Write* or *Read Only*.

6. If the required SNMP version is v1 or v2, click the *Version v1, v2* button, then enter the source (valid entry is the subnet address).

   -or-

   If the required SNMP version is v1 or v2 using an IPv6 network, click the *Version v1,v2 for IPv6 network* button, then enter the source (valid entry is the subnet address).

   -or-

   If the required SNMP version is v3, click the *Version v3* button, then select the Authentication Type (*MD5* or *SHA*), enter the authentication passphrase or password, select the Encryption Method (DES or AES), enter the privacy passphrase and select the Minimum Authentication Level (*NoAuthNoPriv*, *AuthNoPriv*, *AuthPriv*).
7. Click *Save*.

NOTE: For SNMP v1/v2c, the console system will allow an administrator to configure the same community name with different sources (filters) to have access to specific object identifiers (OIDs).

3.3.7 Ports

An administrator can enable and configure serial ports, auxiliary ports, the CAS Profile and the Dial-in Profile from the Ports tab in the side navigation bar. On the auxiliary ports screen, you can enable and configure the internal modem.

The console system's serial ports may work in several different roles, depending on the profile configured for a port.

Serial ports

On the Serial Ports table, you can specify the connection profile (CAS, Dial-In, Power, Dial-Out or Socket Client) based on the type of connected device and you can clone the port, reset to factory defaults, enable/disable ports or open a serial session.

The table displays the port number, device ID, status, name, profile, signals and settings. The Settings column contains the pin-out being used for the port with the following abbreviations:

- CYC - Cyclades
- CIS - Cisco
- 422 - RS422
- 485 - RS485

NOTE: The pin-out may not display if no device is connected to the port.

To enable or disable one or more serial ports:

1. Select *Ports - Serial Ports*.
2. Click the checkbox for each port you want to enable or disable.
3. Click the *Enable* or *Disable* button.

To configure or edit one or more serial ports with the CAS profile:

1. Select *Ports - Serial Ports*.
2. Click the checkbox for each port you want to configure.
3. Click the *Set CAS* button. Use the drop-down menus to enable or disable the port and set the RJ-45 pin-out, speed, parity, data bits, stop bits and flow control.

NOTE: Selecting AUTO for the RJ-45 pin-out enables automatic detection for either Cyclades or Cisco pin-outs for RS-232 devices.

4. Click *Next* or click the *CAS* link.
    a. Enter the port name (when only one port was selected) or the port name prefix (when more than one port were selected). The port name will be <port name prefix>-p-<port number>.
    b. Check the box to enable auto discovery. In this case, the port name will be used when auto discovery fails to discover the server name.
    c. Check the box to enable speed auto detection.

NOTE: Auto speed detection requires additional configuration in the CAS Profile-Auto Discovery Settings screen.

    d. Use the appropriate drop-down menus to set the protocol and authentication type.
    e. Enter the text session, power session and RESTful hotkeys in the appropriate fields.
    f. Enter the TCP port alias for each protocol type (Telnet, SSH and Raw Mode) in the appropriate field.
    g. Enter the IPv4 or IPv6 alias and its interface in the appropriate field.
    h. To allow a session only if DCD is on and to enable auto answer, check the appropriate boxes.
    i. Use the drop-down menu to select the DTR mode and enter the DTR off interval.
    j. Use the drop-down menus to enable or disable line feed suppression and NULL after CR suppression.
    k. Enter the transmission interval, break sequence and break interval in the appropriate fields.

NOTE: The transmission interval defines the delay (in milliseconds) before the transmission of data to the Ethernet is received through a serial port. The default is 20ms.

    l. Use the drop-down menu to enable or disable the Multi-Session Menu. For more information, see Multi-Session Menu on page 43.
    m. Use the drop-down menus to enable or disable log in/out multisession notification and informational message notification.

5. Click *Next* or click the *Data Buffering* link and use the drop-down menus to enable and configure data buffering.
6. Click *Next* or click the *Alerts* link.
    a. Click *Enable Alerts* to enable detection of alerts.
    b. Click *Add* to add an alert string. In the Alerts String field, enter the string. In the Script field, enter the shell script that will run when the match happens. Check the Emergency box to cause the serial port LED to quickly blink amber whenever this alert occurs. A non-emergency alert slowly blinks. Click *Next* to return to the Alerts screen.

NOTE: The console system allows an administrator to associate one shell script to the alert string. When there is a match with the alert string, the console system will call the script passing the port number and the line where the match occurs as arguments.

    c. Check the box next to an existing alert and click *Delete* to delete the string.
    d. Click *Delete Any* to delete all strings whether selected or not.

NOTE: Clicking *Delete Any* will delete all alert strings. Selecting all the alert strings and clicking *Delete* is not the same functon as it will not delete alert strings not shown in the table.

7. Click *Next* or click the *Power* link.
    a. Click *Add* to add a new outlet. Click *Selected PDU* and select a PDU from the list of detected PDUs. Enter the outlet(s) in the Outlets field, and click *Next*.
    b. Check the box next to an existing merged outlet and click *Delete* to delete it.

NOTE: Power is only available when a single serial port is selected.

8. Click *Save*.

Table 3.11 CAS Profile Parameters

Parameter	Description
Physical	
Status	Defines the status of the serial port as either enabled or disabled. Default: Disabled.
RJ-45 Pin-Out	Defines the serial port pin-out as Auto, Cyclades or Cisco. Ports 1 and 2 also support RS-422 and RS-485 pin-outs. Default: Auto.
Speed	Defines the speed as 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 or 230400. Default: 9600.
Parity	Defines the parity as either Even, Odd or None. Default: None.
Data Bits	Defines the data bits as either 5, 6, 7 or 8. Default: 8.
Stop Bits	Defines the stop bits as either 1 or 2. Default: 1.
Flow Control	Defines the flow control as none, hardware, software, RxON software or TxON software. Default: None.
CAS	
Port Name	Name associated with the serial port (as an alias). Default: <appliance mac address>-p-<port number>.
Enable Auto Discovery	The target name will be discovered and will be associated with this serial port. If it fails, the Port Name will be used. Default: Disabled.
Enable Speed Auto Detection	Tries to discover the speed of the serial port. This feature requires additional configuration under the CAS Profile / Auto Discovery / Settings page. Default: Disabled.
Protocol	The protocol that will be used by authorized users to access the serial port/target. The console system accepts three protocols for connection to the target: Telnet for telnet connection, SSH for secure connection and Raw Mode for raw socket connection. An administrator can configure the port to accept one, two or all three types. NOTE: Raw protocol requires the configuration of the Raw Mode Port Alias. Default value: SSH.
Authentication Type	Authentication type that will be used to authenticate the user during target session. Default: Local.
Text Session Hot Key	Hotkey to suspend the target session and go to the CLI prompt. Not available for Raw. Default: Ctrl-Z. Note: The default escape character for ts_menu is Ctrl-X.
Power Session Hot Key	Hotkey to suspend the target session and display Power Management Menu to control the outlets merged to the target. Not available for Raw. Default: Ctrl-P. Note: The default escape character for ts_menu is Ctrl-X.
RESTful Hot Key	Hotkey to suspend the target session and display the RESTful menu, which is used to perform user-defined RESTful actions. Default: not configured (blank).
TCP Port Alias	Telnet Port Alias: TCP port to connect directly to a serial port using Telnet protocol for the connection. SSH Port Alias: TCP port to connect directly to a serial port using SSH protocol for the connection. Raw Mode Port Alias: TCP port to connect directly to a serial port using raw socket for the connection.
Port IPv4/IPv6 Alias	IPv4/IPv6 address used to connect directly to a serial port. Default: not configured (blank).
Port IPv4/IPv6 Alias Interface	Interface (ETH0/ETH1) associated with the IPv4/IPv6 alias. Default: ETH0.
Allow Session Only if DCD is On	When the DCD is OFF, the appliance will deny access for this serial port. Default: Disabled (allow access if DCD is OFF).
Enable Auto Answer	When the input data matches one input string configured in Auto Answer, the output string will be transmitted to the serial port. Default: Disabled.
DTR Mode	DTR Mode can be set to the following: Always On. Normal - the DTR status will depend on the existence of a CAS session. Off Interval - when the a CAS session is closed, the DTR will stay down during this interval. Default: Normal.
DTR Off Interval	Interval in seconds used by DTR Mode Off Interval in milliseconds. Default: 100.
Line Feed Suppression	Enables the suppression of the LF character after the CR character. Default: Disabled.

Table 3.11 CAS Profile Parameters (continued)

Parameter	Description
Null After CR Suppression	Enables the suppression of the NULL character after the CR character. Default: Disabled.
Transmission Interval	The interval the port waits to send data to a remote client in milliseconds. Default: 20.
Break Sequence	An administrator can configure the control key as the break sequence, entering ^ before the letter. Not available for Raw. Default: ~break.
Break Interval	Interval for the break signal in milliseconds. Not available for Raw. Default: 500.
Show Multi-Session Menu	Enables the multi-session menu when connecting to a port that is already being accessed by another user. Default: Disabled.
Log In/Out Multi Session Notification	Enables the notification to multi-session users when a new user logs in or a user logs out. Not available for Raw. Default: Disabled.
Informational Message Notification	Displays an information message when a target session is opened. Not available for Raw. Default: Enabled.
Data Buffering	
Status	Enables or disables data buffering. Default: Disabled.
Type	Displays the type of data buffering: Local - stores the data buffering file in the local file system. NFS - stores the data buffering file in the NFS server. Syslog - sends the data to the syslog server. DSView - sends the data to the DSView software. Default: Local.
Local Type	When the type is set to local, specifies where on the local system the data buffering files are stored. Options are the built-in memory (mmcblk0) or connected USB storage and SD card storage locations. Default: mmcblk0.
Time Stamp	When enabled, adds the time stamp to the data buffering line for a Local or NFS database. Default: Disabled.
Log-in/out Message	Includes special notification for logins and logouts in data buffering. Default: Disabled.
Serial Session Logging	Enabled - stores data at all times. Disabled - stores data when a CAS session is not opened. Default: Enabled.
Alerts	
Status	A special event notification will be generated when input data matches one of the alert strings. Default: Disabled.
Alert Strings	Strings used to generate event notifications. Default: Empty.
Scripts	Name of shell script that will be called when there is match of the alert string in the line. The script will be called with two arguments: the port number and the line where the match happened.
Emergency	Marking an alert as an Emergency causes the serial port's LED to quickly blink amber when this alert occurs rather than slowly blinking for a non-emergency.

To configure the Dial-in Profile for a serial port with a connected modem:

1. Select *Ports - Serial Ports*.
2. Click the checkbox for a serial port with a connected modem.
3. Click the *Set Dial-In* button and use the drop-down menus to configure the dial-in settings.
4. Configure the PPP parameters (address, authentication and so on) and click *Save*.

Table 3.12 Dial-in Parameters

Parameter	Description
Status	Enables or disables the port. Default: Disabled.
Speed	The speed that will be used by mgetty to configure the serial device. Default: 38400 bps.
Init Chat	Chat for modem initialization. Default: "" \d\d\d+++\d\d\dATZ OK.
PPP Address	Configures the local and the remote IP address for the the PPP link. If *Accept Configuration from Remote Peer* is selected, the remote peer should send both IP addresses (local and remote) during negotiation. Default: No Address.
Local IPv4/IPv6 Address	Configures the local IPv4/IPv6 address for this PPP connection.
Remote IPv4/IPv6 Address	Configures the remote IPv4/IPv6 address for this PPP connection.
PPP Authentication Protocol	Uses the radio button to select: none, PAP, CHAP or EAP. None - no authentication. • PAP - use PAP protocol and the authentication type configured in the PPP authentication type (it is configured in the Authentication / Unit Authentication page). • CHAP - use CHAP protocol. The configuration of the CHAP secrets should be done while editing the file /etc/ppp/chap-secrets. • EAP - use EAP protocol. Available authentications: CHAP, SRP-SHA1 and TLS. The configuration of the secrets for CHAP should be done while editing the file /etc/ppp/chap-secrets. The configuration of the secrets for SRP-SHA1 should be done while editing the file /etc/ppp/srp-secrets. Note: EAP authentication is only available with Windows XP operating systems. Default: None.
CHAP	Configure the CHAP-interval, CHAP-max-challenge and CHAP-restart. Default values: • CHAP Interval = 0. • CHAP Max Challenge = 10. • CHAP Restart = 3.
PPP Idle Timeout	Number of seconds being idle before PPP times out. Default: 0 (no time-out).

To configure or to edit one or more serial ports with a connected PDU:

1. Select *Ports - Serial Ports*.
2. Click the checkbox for one or more serial ports with a connected PDU.
3. Click the *Set Power* button and use the drop-down menus to configure the physical settings.
4. Click *Next* or click the *Power* link.
    a. Use the drop-down menu to select the PDU type.
    b. Check the box to enable speed auto detection.
    c. Configure the polling rate.
    d. For Avocent/Cyclades PDUs, enter the power cycle interval and then use the drop-down menus to enable or disable Syslog, Buzzer and SW Overcurrent Protection.
5. Click *Save*.

Table 3.13 Power Parameters

Parameter	Description
Physical	
RJ-45 Pin-Out	Defines the serial port pinout as Auto, Cyclades or Cisco. Default: Auto.
Status	Defines the status of the serial port as either enabled or disabled. Default: Disabled.
Speed	Defines the speed as 1200, 2400, 4800, 9600, 19200, 38400, 57600,115200 or 230400. Default: 9600.
Parity	Defines the parity as either Even, Odd or None. Default: None.
Data Bits	Defines the data bits as either 5, 6, 7 or 8. Default: 8.
Stop Bits	Defines the stop bits as either 1 or 2. Default: 1.
Flow Control	Defines the flow control as none, hardware, software, RxON software or TxON software. Default: None.
Power	
UPS Type	Defines the type or vendor of the UPS connected to the serial port. Liebert GXT4 and Liebert GXT5 UPSs are supported. Default: Liebert GXT4.
PDU Type	Defines the type or vendor of the PDU connected to the serial port. Default: Auto. • Auto - the vendor is detected. • Avocent-Cyclades - Avocent-Cyclades PM PDU family. • Vertiv - Vertiv PDUs • SPC - SPC power control device family. • ServerTech/Server Tech PRO2 - Server Tech family. • Raritan - Raritan PX G2 PDU family. • APC - APC rPDU2 family. • Eaton - Eaton ePDU G3 PDUs. • Geist - Geist PDU family.
Enable Speed Auto Detection	When enabled, detects the speed of the port. Default: Disabled.
Polling Rate	The interval in seconds to update information from the PDU. Default: 20.
For Avocent/Cyclades PDUs	
Power Cycle Interval	The interval in seconds between Off and On actions for the power cycle command. Default: 15.
Syslog	When enabled, the PDU will send syslog messages to the appliance. Default: Enabled.
Buzzer	Enables or disables the PDU's buzzer. Default: Enabled.
SW Overcurrent Protection	When enabled, the software's overcurrent protection is on. Default: Disabled.

To copy/clone the configuration of one port to other ports:

1. Select *Ports - Serial Ports*.
2. Click the checkbox for the serial port you want to clone.
3. Click the *Clone* button.
4. Enter the serial port(s) to be configured in the Copy Configuration To field and click *Save*.

NOTE: If the selected port is configured as a CAS Profile, the following parameters will not be copied: Port Name, TCP Port Alias, IPv4 Port Alias, IPv6 Port Alias and Power (merged outlets).

To reset one or more serial ports to their factory configuration:

1. Select *Ports - Serial Ports*.

2. Click the checkbox for one or more serial ports you want to reset to their factory configuration, then click the *Reset To Factory* button.

NOTE: Serial ports are set to the CAS Profile and disabled in the factory configuration.

Multi-Session Menu

An administrator can enable or disable the Multi-Session Menu. When enabled, users can access the menu from the web UI, CLI or the DSView software, and multiple users can connect simultaneously to a serial port. To connect to a port or start a shared session, the user must have permission to access the port. If more than one session to a serial port is being established, the console system displays the Multi-Session Menu. If the session being established is the first with the serial port, a normal session with the target opens. A first-session user can still access the Multi-Session Menu by typing the text hotkey (Ctrl-Z by default).

To enable the Multi-Session Menu:

1. From the sidebar of the *Expert* tab, click *Ports-Serial Ports*.
2. Click the port for which you want to enable the Multi-Session Menu.
3. Click the *CAS* heading and near the bottom of the CAS Settings, use the drop-down menu to *Enable Show Multi-Session Menu*.
4. Click *Save*.

The Multi-Session Menu includes options that are dependent on the access rights of the user. If a user does not have rights to an option, that option is not displayed. For example, Options 0, 2 and 5 from the following table are displayed for a user who only has permission to open read-only sessions.

Table 3.14 Multi-Session Menu Options

Number	Option	Description
0	Quit	Closes the client session.
1	Initiate a regular session	Opens a read/write session.
2	Initiate a sniff session	Opens a read-only session.
3	Send messages to another user	Sends a message to all users who are sharing the serial port.
4	Kill session(s)	Displays all sessions and asks to close one or more shared sessions.
5	List shared session(s)	Lists all other shared sessions.
6	Show Databuffering	Shows the content of the target data buffering file.
7	Clean Databuffering	Resets the content of the target data buffering file.

Auxiliary ports

From the Auxiliary Ports screen, if the port name displays ttyM1, then the internal modem is present and can be enabled and configured. If there are no entries in the Auxiliary Port table, then the internal modem is not present and this port cannot be used.

For models with a cellular modem, the port name displays as ttyM1 and the device type displays as LTE. The cellular modem can only be configured for dial-out mode. By default, the cellular modem is disabled. For more information on configuring a cellular modem, see Cellular modem on page 51

To configure or edit an auxiliary port with an internal modem:

1. Select *Ports - Auxiliary Ports*.
2. Click the *Set Dial-In* or *Set Dial-Out* button and use the drop-down menus to configure the dial-in settings.

3. Configure the PPP parameters (address, authentication and so on).
4. Click *Save*.

CAS Profile

The CAS (Console Access Server) profile provides remote access to serial RS-232 console ports on your devices. Using a CAS profile, you can configure authentication, port configuration (such as speed and flow control), port aliasing, target auto discovery, data buffering type, port alerts, power integration and so on.

An administrator can configure the CAS profile by clicking *Ports-CAS Profile*.

Auto discovery

The auto discovery feature will discover the target name of the server connected to the serial port. This name will be used as the alias of the serial port.

When auto discovery is active for a certain serial device, upon target connection (DCD ON event), the appliance will send probe strings and start analyzing target device answers using regular expressions. There will be predefined probe and match strings as well as customer-defined ones.

For each probe string sent, all regular expressions defined by the match strings will be tested. After the last cycle, the sequence restarts. This procedure will run for a certain period (given by the auto discovery time-out parameter) or until the target is successfully detected. If auto discovery fails, the target name will be reset to the configured target name or to the corresponding unique default target name.

NOTE: The configured target name will be used only after the auto discovery process fails.

NOTE: The auto discovery process starts when there is variation in the DCD signal from OFF to ON (disconnect/connect the target's cable, turn off/on the target) and when the configuration of the serial port goes from disabled to enabled and there is a target connected in the port.

The probe strings will be used to stimulate the server (such as “\r”: a single carriage return).

The match strings are regular expressions where “%H” is a placeholder for the target name you want to detect, such as %H .*ogin:

or xxx%Hyyy

The first one will extract target name from things such as: MyServer Login: and will result in a target name of MyServer.

And the second one from things such as: Server xxxTARGETyyy and will result in a target name of TARGET.

To configure the strings for probe/match used by auto discovery:

Perform this procedure to change the default settings or the probe or match strings used in auto discovery.

1. Select *Ports - CAS Profile - Auto Discovery*. The Settings, Probe Strings and Match Strings options appear in the side navigation bar.
2. To change the default auto discovery time-out or probe time-out, perform the following steps.
   a. Select *Settings*.
   b. Enter a new value in the Auto Discovery Timeout and Probe Timeout fields.
   c. Select a speed from the Default Speed on Auto Discovery Failure drop-down menu and Probe Speed List.
   d. Click *Save*.
3. To add a new probe or match string or delete an existing string, perform the following steps.
   a. Select *Probe Strings* or *Match Strings*.

   b. To add a string, click *Add*, enter a new string in the New Probe String or New Match String field and click *Save*.
   c. To delete a string, select the checkbox for the string and click *Delete*.
4. Click *Save*.

To configure the input/output strings used by auto answer:

1. Select *Ports - CAS Profile - Auto Answer*.
2. To add an auto answer input and output string, click *Add*. Enter a new string in the Input String or Output String fields and click *Save*.

   -or-

   To delete an auto input and output string, select the checkbox next to the string you want to delete. Click *Delete*, then click *Save*.

Pool of ports

An administrator can create a pool of serial ports where each serial port in the pool shares a pool name, Telnet Port Alias, SSH Port Alias, Raw Mode Port Alias, IPv4 Alias and IPv6 Alias. The first available port in the pool is used as the serial port for connection.

NOTE: The multiple session access right does not have any effect when using a pool of CAS ports. When all ports in the pool are taken, the connection to the pool is denied.

NOTE: All ports in the pool must share the same CAS protocol. The protocol is validated during the connection to the serial port. If the protocol does not match, the connection will be denied.

To configure a pool of CAS ports:

1. Click *Ports - Pool of Ports*.
2. To create a pool, click the *Add* button.

   - or -

   To edit an existing pool, click the name of the pool you want to edit.

   - or -

   To delete a pool, check the box next to the pool you want to delete and click the *Delete* button.
3. Enter the parameters for the pool in the appropriate fields.
4. In the left side of the Pool Members field, select the ports to be added to the pool and click *Add*.

   - or -

   In the right side of the Pool Members field, select the ports to be removed from the pool and click *Remove*.
5. Click *Save*.

NOTE: A serial port can only belong to one pool at a time, but a user can create an empty pool and add ports to it later.

Table 3.15 Pool of CAS Ports Parameters

Parameter	Description
Pool Name	The name of the pool. The pool name is mandatory and should follow hostname guidelines, not exceed 64 characters and start with a letter.
Port Alias	The Port Alias where the pool responds for each protocol. • Telnet Port Alias for telnet protocol. It is optional. • SSH Port Alias for ssh protocol. It is optional. • Raw Mode Port Alias for raw mode protocol. • It is mandatory when Raw Mode is configured as protocol for the ports.
Pool IPv4 Alias	The IPv4 address used by the pool. This parameter is optional.
Pool IPv4 Alias Interface	The interface used by the IPv4 Alias. Default: Eth0.
Pool IPv6 Alias	The IPv6 address used by the pool. This parameter is optional.
Pool IPv6 Alias Interface	The interface used by the IPv6 Alias. Default: Eth0.

RESTful client

The console system supports a programmable RESTful client interface. After configuration of RESTful URLs, the console system performs, from within a serial session, menu-selected GET and POST operations to pre-programmed HTTP/HTTPS URLs for server resources on the network.

NOTE: URL options must be configured using either HTTP or HTTPS with the RESTful client menu.

To configure the RESTful client:

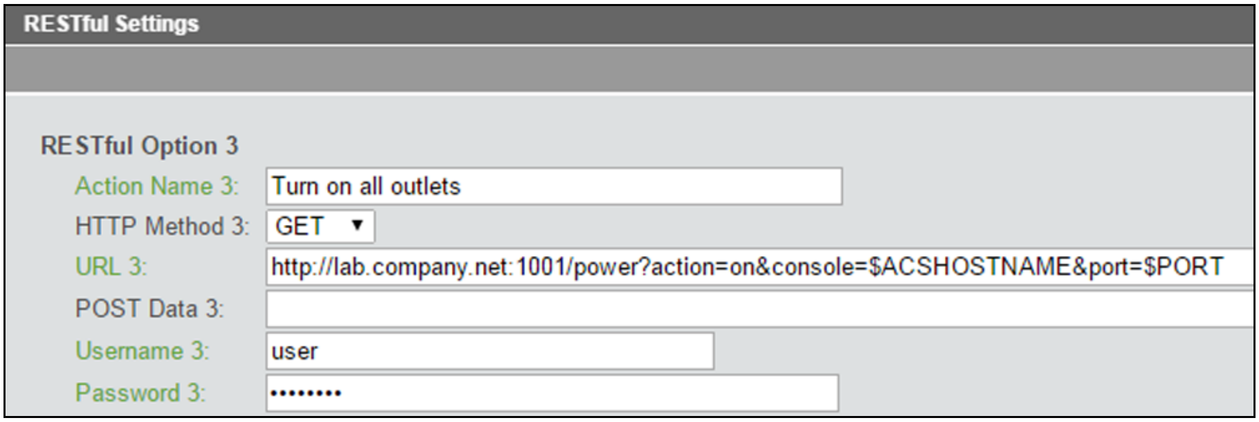
1. Click *Ports - CAS Profile - RESTful Settings*.
2. Enter the Action Name, URL, POST Data, Username and Password in the appropriate fields and use the drop-down menu to select GET or POST as the HTTP Method for each RESTful option. Click *Save* when finished.

When configuring actions, the following context variables can be used.

Table 3.16 Context Variables Descriptions

Context Variable	Description
$PORT	Identifies the serial port (1-48) when the menu is invoked.
$PORTNAME	The name of the port.
$IPPORTALIAS	The IPv4 alias of the port.
$TCPPORTALIAS	The TCP (Telnet port) alias of the port.
$ACSHOSTNAME	The host name of the console system.
$ACSIPADDR	The IP address of the console system.

Figure 3.3 RESTful Client Configuration Example


RESTful Settings

RESTful Option 3

Action Name 3: Turn on all outlets

HTTP Method 3: GET

URL 3: http://lab.company.net:1001/power?action=on&console=$ACSHOSTNAME&port=$PORT

POST Data 3:

Username 3: user

Password 3: ••••••••

NOTE: HTTP POSTs can sometimes use the HTTP request body to send appropriate information to servers, usually coded as XML or JSON.

To enable the RESTful client:

1. If port access applies to all users, from the side navigation bar of the *Expert* tab, click *System - Security - Security Profile*, then under Serial Devices, click the RESTful Menu checkbox and click *Save*.

   -or-

   If port access is controlled by authorization assigned to users groups, from the side navigation bar of the Expert tab, click *Users - Authorization - Groups*.

   a. Click the group for which you want to enable the RESTful client.
   b. From the side navigation bar, click *Access Rights - Serial*.
   c. Click the port for which you want to enable the RESTful menu. Under Target Access Rights, click the RESTful Menu box.
2. From the side navigation bar of the Expert tab, click *Ports - Serial Ports*.
3. Click the port for which you want to enable the RESTful menu and then click the CAS heading at the top of the window.
4. In the RESTful Hot Key field, enter the hotkey you want to use to initiate the RESTful client and click *Save*.

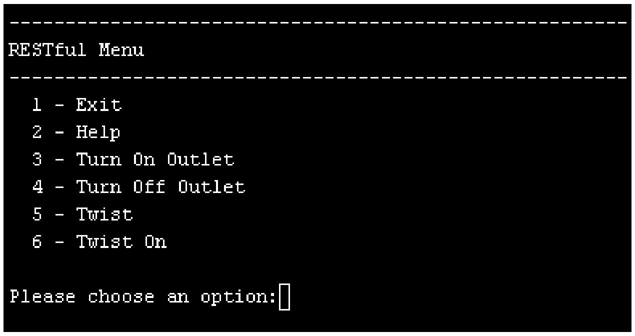
NOTE: The hotkey is not set by default.

Using the RESTful client interface

After opening a serial session, press the hot key to open the RESTful client interface for the current session. Enter the number of the RESTful client request you want to perform. By default, Exit and Help are the first two requests in the menu. You can configure up to eight additional requests from the web UI of the console system.

The following is an example of the RESTful menu from a serial session.

Figure 3.4 RESTful client Example



```
-----------------------------------------------------
RESTful Menu
-----------------------------------------------------
  1 - Exit
  2 - Help
  3 - Turn On Outlet
  4 - Turn Off Outlet
  5 - Twist
  6 - Twist On

Please choose an option:
```

Dial-in profile

An administrator can configure secure dial-in settings such as OTP login, PPP connections, PPP/PAP authentication, callback and OTP users for PPP connections.

NOTE: If pluggable devices are being used for dial-out, dial-in should be disabled.

To configure secure dial-in settings for ports with the Dial-in Profile:

1. Select *Ports - Dial-In Profile - Settings*.
2. To enable logging in to the console system through the modem and select a condition for which logging in is allowed, perform the following steps.
   a. To allow callback connections only, select *Callback*.
   b. To allow any connection, select *Enable*.
3. To enable OTP authentication, select *Enable* from the OTP Login Authentication menu.
4. To enable and select a condition for PPP connections, perform the following steps.
   a. To allow PPP callback connections only, select *Callback*.
   b. To allow any connection, select *Enable*.
5. When the PAP authentication protocol is configured for the port, select the authentication type from the PPP/PAP Authentication menu.
6. Use the drop-down menu to enable or disable the caller ID filter.
7. Click *Save*.

To configure callback users and phone numbers for ports with the Dial-in Profile:

1. Select *Ports - Dial-In Profile - Secure Dial-In - Callback Users*.
2. Click *Add*.
3. Enter the name and phone number used to perform the callback in the appropriate fields and click *Save*.

To configure PPP OTP users for ports with the Dial-in Profile:

1. Select *Ports - Dial-In Profile - Secure Dial-In - PPP OTP Users*.

2. Click *Add*.
3. Enter the username and passphrase in the appropriate fields and click *Save*.

NOTE: This PPP OTP user will establish PPP connection after being successfully authenticated.

To configure EAP-TLS as PPP authentication for ports with the Dial-in Profile:

1. Select *Ports - Auxiliary Ports*.
2. Check the box next to the port where the modem is connected and click *Set Dial-In*.
3. Configure the PPP Address settings. For example, set the PPP Address to Local Configuration using 10.0.0.1 as the Local IPv4 Address and 10.0.0.2 as the Remote IPv4 Address.
4. For PPP Authenticaion, select the button next to By Appliance, and then select the button next to EAP for the protocol. Click Save.
5. Select *Ports - Dial-In Profile - Settings*.
6. Use the drop-down menu to enable the PPP Connection and click *Save*.
7. Copy the certificates and keys to the /etc/ppp/cert file. They must be named server.crt (the ACS800/8000 certificate), ca.crt (the Certificate Authority's certificate) and server.key (the ACS800/8000 asymmetric key).

Caller ID

You can filter incoming calls based on caller ID by enabling the Caller ID Filter in the Secure Dial-In settings. When enabled, the incoming caller ID number must be listed for the call to be answered. By default, it is disabled.

You can add numbers directly, by range or by prefix.

To enter a number directly, enter the number without any symbols. For example: 8881234567.

You can enter a range by inserting a hyphen (-) between two caller ID numbers. Any number between and including those two numbers will be accepted. For example: 8881234560-8881234569.

NOTE: The range must be less than 100 phone numbers.

You can enter a prefix by putting an asterisk (*) after a partial phone number. The incoming call will be answered if the phone number begins with the partial number specified. For example: 8881234*.

If the Caller ID Filter is enabled and no numbers are specified, then all calls are blocked. Blocked calls are not answered and ring until timing out. If the Caller ID feature is disabled, then all calls are answered.

To enter a list of caller ID numbers:

1. Select *Ports - Dial-In Profile - Secure Dial-In - Caller ID*.
2. Click *Add* and enter the caller ID number, range or prefix.
3. Click *Save*.

To delete a caller ID number from the list:

1. Select *Ports - Dial-In Profile - Secure Dial-In - Caller ID*.
2. Check the box next to the number to be deleted.
3. Click *Delete*.

Dial-out profile

To configure the Dial-out profile for a serial port with a connected modem:

1. Select *Ports – Serial Ports*.
2. Click the checkbox for a serial port with a connected modem.
3. Click the *Set Dial-out* button.
4. Use the drop-down to enable/disable the port.
5. Configure the phone number to dial on-demand in the field Phone No.
6. Use the drop-down to configure the modem speed.
7. Configure the initial chat with modem in the Init Chat field.
8. Configure the PPP parameters (address, authentication and so on) and click *Save*.

NOTE: The Dial-out profile will work only to establish PPP link on-demand. The administrator must configure static route to have packages routed to the PPP interface.

Table 3.17 Dial-out Parameters

Parameter	Description
Status	Enables or disables the port. Default: Disabled.
Phone No.	The phone number to dial to.
Speed	The speed that will be used to configure the serial device and communicate with the connected modem.
Init Chat	Chat for modem initialization.
Local IPv4/IPv6 Address	Configures the local IPv4/IPv6 address for this PPP connection. If empty, PPP will accept the address from the remote peer.
Remote IPv4/IPv6 Address	Configures the remote IPv4/IPv6 address for this PPP connection. If empty, PPP will accept the address from the remote peer.
PPP Authentication Protocol	Configures which end of the connection controls this PPP authentication and selects the method to be used.
PPP Idle Timeout	Number of seconds being idle before PPP times out. Default: 0 (no time-out).
CHAP	Configures CHAP specific PPP authentication settings.

Socket client profile

To configure the socket client profile for a serial port with a connected device:

1. Select *Ports - Serial Ports*.
2. Click the checkbox for a serial port with a connected device.
3. Click *Set Socket Client* and use the drop-down menus to configure the physical settings.
4. Configure the Socket Client Settings (remote server address, TCP port and event trigger) and click *Save*.

Table 3.18 Socket Client Parameters

Parameter	Description
RJ-45 Pin-Out	Defines the serial port pinout.
Status	Defines the status of the serial port as either enabled or disabled. Default: Disabled.
Speed	Defines the speed as 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 or 230400. Default: 9600.
Parity	Defines the parity as Even, Odd or None. Default: None.
Data Bits	Defines the data bits as 5, 6, 7 or 8. Default: 8.
Stop Bits	Defines the stop bits as 1 or 2. Default: 1.
Flow Control	Defines the flow control as none, hardware, software, RxON software or TxON software. Default: None.
Remote Server	IPv4 or IPv6 address of the remote server.
Remote TCP Port	TCP port to be used to establish a connection with a remote server.
Establish Connection	Configure the event that will trigger the establishment of the connection: DCD Regards or Always.

3.3.8 Cellular modem

The Avocent® ACS800/8000 advanced console systemcellular modem configuration interface is similar to the internal 56k modem configuration interface. The cellular modem is configured through the auxiliary port of the console system.

To configure or edit an auxiliary port with a cellular modem:

1. Select *Ports - Auxiliary Ports*.
2. Click the *ttyM1* link to open the modem's dial-out configuration page.

NOTE: The cellular modem can only be configured for dial-out mode.

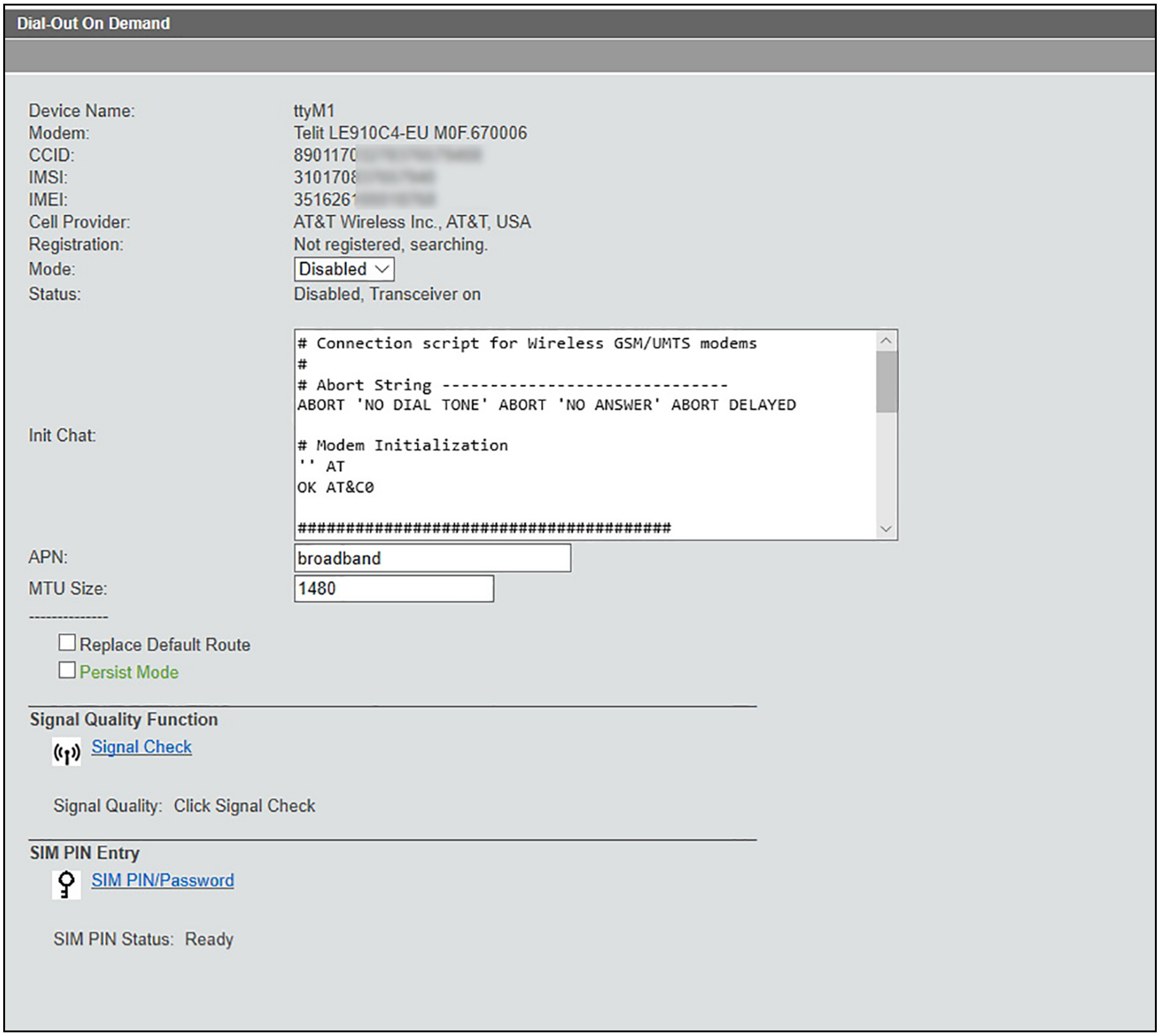
3. Use the drop-down menu to enable the modem. When enabled, the modem comes up after each reboot.
4. The chat script is a usable default for the provider. If desired, you can make changes to the chat script from the Init Chat window.
5. The APN field lists the default Access Point Name. You can change the APN here without having to edit the chat script.

NOTE: If you change the APN, any edits to the chat script will be lost.

6. Enable or disable the option to replace the default route.
7. Enable or disable Persist Mode.

For more information on configuring the cellular modem, see the following sections.

Figure 3.5 Dial-Out Configuration Page for the Cellular Modem



Dial-Out On Demand

Device Name: ttyM1
Modem: Telit LE910C4-EU M0F.670006
CCID: 8901170[redacted]
IMSI: 3101708[redacted]
IMEI: 3516261[redacted]
Cell Provider: AT&T Wireless Inc., AT&T, USA
Registration: Not registered, searching.
Mode: Disabled
Status: Disabled, Transceiver on

Init Chat:

```
# Connection script for Wireless GSM/UMTS modems
#
# Abort String -----------------------------
ABORT 'NO DIAL TONE' ABORT 'NO ANSWER' ABORT DELAYED

# Modem Initialization
'' AT
OK AT&C0

########################################
```

APN: broadband
MTU Size: 1480

□ Replace Default Route
□ Persist Mode

Signal Quality Function

Signal Check

Signal Quality: Click Signal Check

SIM PIN Entry

SIM PIN/Password

SIM PIN Status: Ready

The top of the screen shows the CCID and IMSI numbers read from the SIM card. If these numbers are not present, or show something invalid for the number, then there was a problem reading the SIM card. Verify the SIM card is installed properly. The IMEI number is from the chipset of the cell modem.

Mode

The mode selector is disabled by default. Setting it to enabled starts the point-to-point daemon (pppd) and brings up the cellular modem. When enabled, the cellular modem comes up after each reboot.

When in failover mode, the cellular modem comes up even if disabled. Failover conditions are still enabled.

Status

The status line indicates the current state:

- Disabled or Enabled - Indicates whether the cellular modem is enabled or disabled. The modem can be enabled manually or by failover.

- Transceiver off - The default setting. The transceiver is off when the modem is disabled.
- Transceiver on - The transceiver is on when the modem is enabled either manually or by failover.
- Failover: no - If configured as a failover device, indicates if the cell modem is in failover.
- Up or Down - indicates if the modem network interface is up.

Init Chat

The chat script, in an editor window. You can make custom changes to the chat script from this window. The default chat script is from the service provider.

NOTE: For most users, the default chat script should be used.

APN

The Access Point Name, which is listed in the chat script. From this field, you can change the APN without having to edit the chat script directly. If you change the APN here, the chat script will lose any other changes you have made.

Replace Default Route

Sends a configuration option to the ppp daemon to make the cellular modem the default gateway. The gateway is restored when the cellular modem is shut down. This is similar to entering a static route, but useful to make the cellular modem the default gateway for internet access.

Persist Mode

When Persist Mode is enabled, the console system tries to bring the cellular modem back up if the ppp daemon shuts down for any reason. When disabled, the cellular modem stays down if the ppp daemon shuts down (for example, if cellular service is lost).

Signal Quality Function

Allows obtaining raw signal level and bit error rate readings, to allow diagnosing a problem connecting to the cell network or slow connection. Click *Signal Check* to obtain a response.

The signal level can range from -113db or less, to -51db or greater. The bit error rate ranges from less than 1%, to 12.8% or greater.

You can't obtain a signal quality check while the modem is in session. The modem transceiver is turned on, but the chat script isn't running. In session, the cellular modem serial interface is locked to the ppp daemon.

SIM PIN Entry

Click *SIM PIN/Password* to enter your PIN to activate cellular service with a SIM card.

Verifying the cellular connection

The status line on the dial-out screen indicates if the cellular modem is up. You can get the IP address of the cellular modem from the Monitoring page. Go to *Monitoring - Network - Devices*.

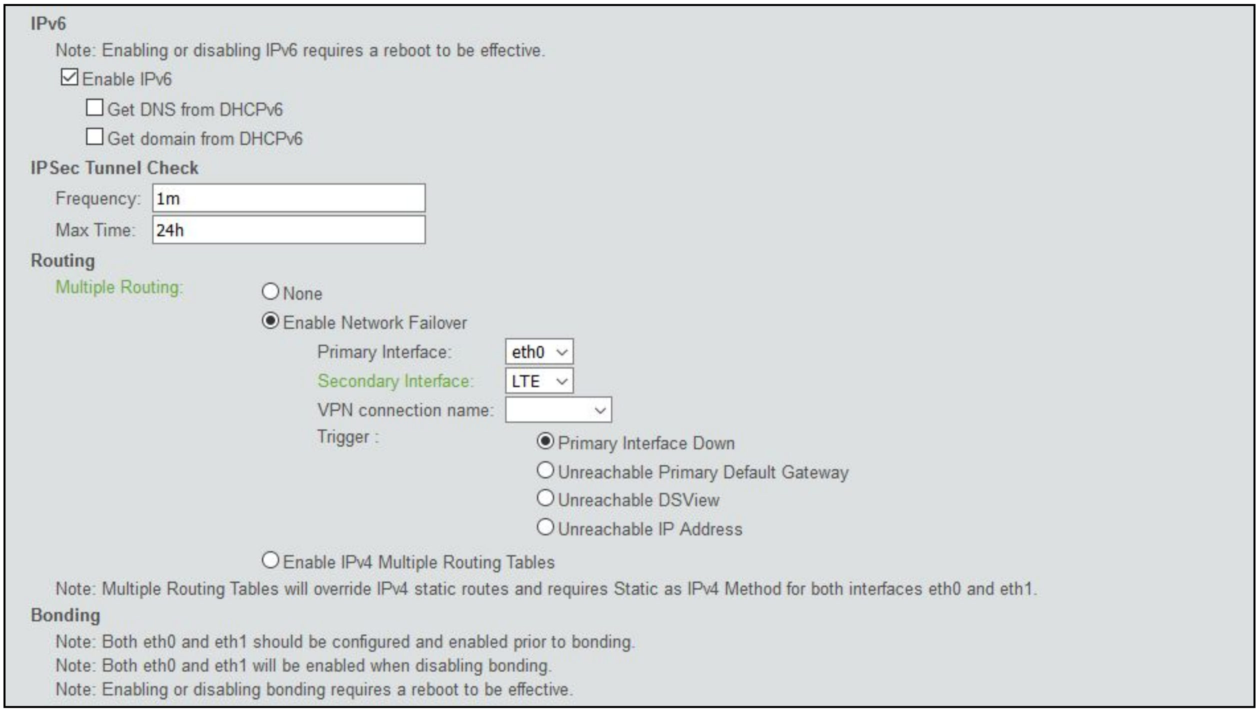
From the Devices page, the ppp0-LTE device is the modem. The IPv4 address displays and the link status is up when the modem is enabled. The IP address is for the private network service. The IPv4 address is not fixed and changes each time you reboot or re-establish the cell network connection.

NOTE: Advanced users can run a script for more debug information.

Using the cellular modem in failover

Navigate to *Network - Settings* and select *Routing - Enable Network Failover*. From the Secondary Interface list, select the ppp0 (or lte0) device. You can do this whether the modem is enabled or not.

Figure 3.6 Configuring the Cellular Modem as a Failover Device



IPv6

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

☑ Enable IPv6

☐ Get DNS from DHCPv6

☐ Get domain from DHCPv6

IPSec Tunnel Check

Frequency: 1m

Max Time: 24h

Routing

Multiple Routing:

○ None

● Enable Network Failover

Primary Interface: eth0

Secondary Interface: LTE

VPN connection name:

Trigger :

● Primary Interface Down

○ Unreachable Primary Default Gateway

○ Unreachable DSView

○ Unreachable IP Address

○ Enable IPv4 Multiple Routing Tables

Note: Multiple Routing Tables will override IPv4 static routes and requires Static as IPv4 Method for both interfaces eth0 and eth1.

Bonding

Note: Both eth0 and eth1 should be configured and enabled prior to bonding.

Note: Both eth0 and eth1 will be enabled when disabling bonding.

Note: Enabling or disabling bonding requires a reboot to be effective.

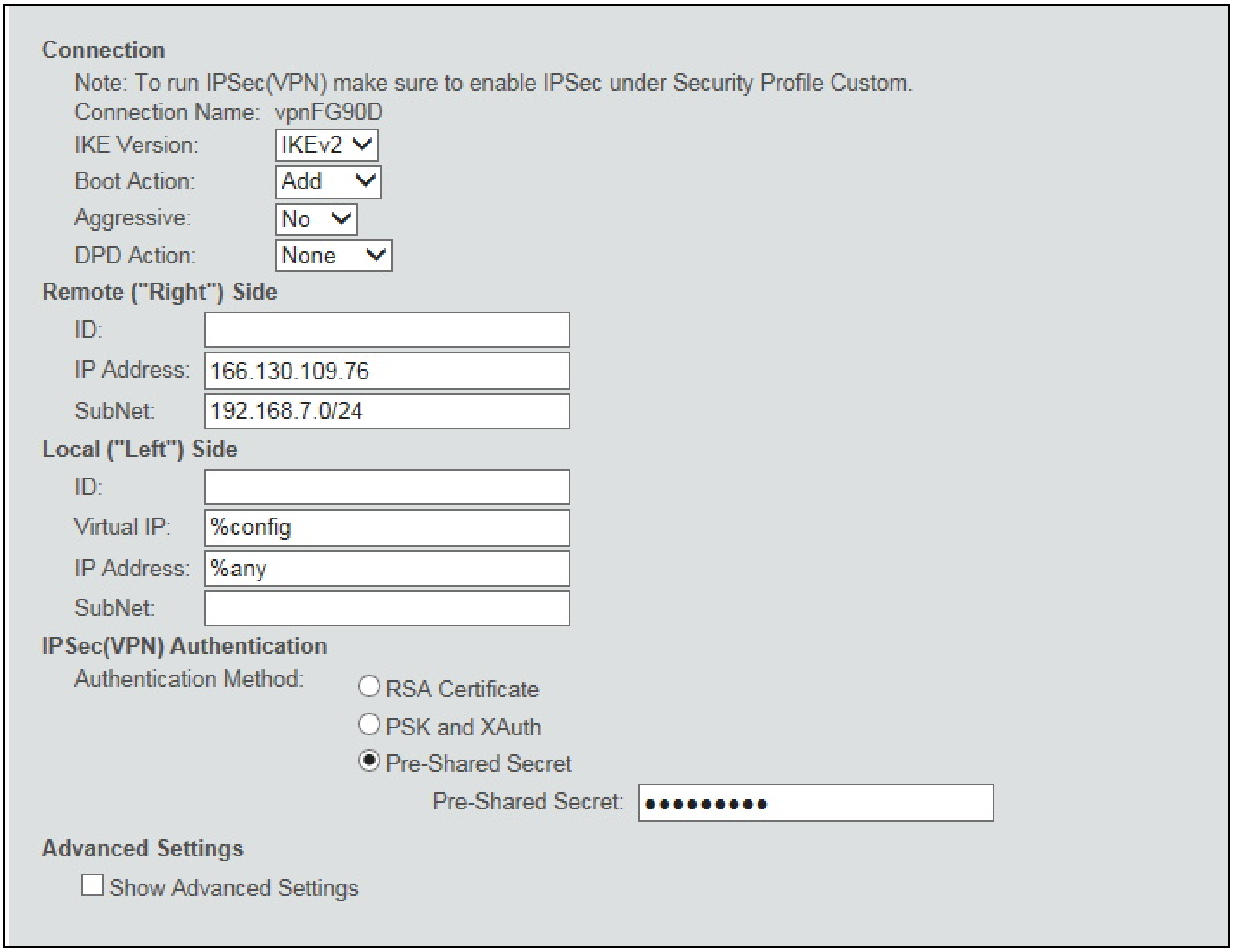
The failover condition, in this case, is the primary interface is down. With failover enabled, if eth0 goes down, then the cell modem is triggered to come up. With the service provider, this only provides internet access. A server on the internet can't log in directly. A different type of service, or provider, may be able to provide access.

The other alternative is to use a VPN service. Configure the VPN to connect via IPsec to a secure gateway with a public IP address, and then you can access the console system through the IPsec tunnel.

To configure IPsec:

1. Turn on the IPsec service. Go to *System - Security - Security Profile* page, scroll down, and select the box to Enable IPsec.
2. Go to the *Network - IPSec(VPN)* page, and add a new VPN profile.
3. Enter the VPN parameters. The following image is an example. When finished, click *Save*.
4. Navigate back to the failover screen at *Network - Settings* and select the VPN for failover.

Figure 3.7 IPsec VPN Example



Connection

Note: To run IPSec(VPN) make sure to enable IPSec under Security Profile Custom.

Connection Name: vpnFG90D

IKE Version: IKEv2

Boot Action: Add

Aggressive: No

DPD Action: None

Remote ("Right") Side

ID:

IP Address: 166.130.109.76

SubNet: 192.168.7.0/24

Local ("Left") Side

ID:

Virtual IP: %config

IP Address: %any

SubNet:

IPSec(VPN) Authentication

Authentication Method:

○ RSA Certificate
○ PSK and XAuth
● Pre-Shared Secret

Pre-Shared Secret: ●●●●●●●●●●

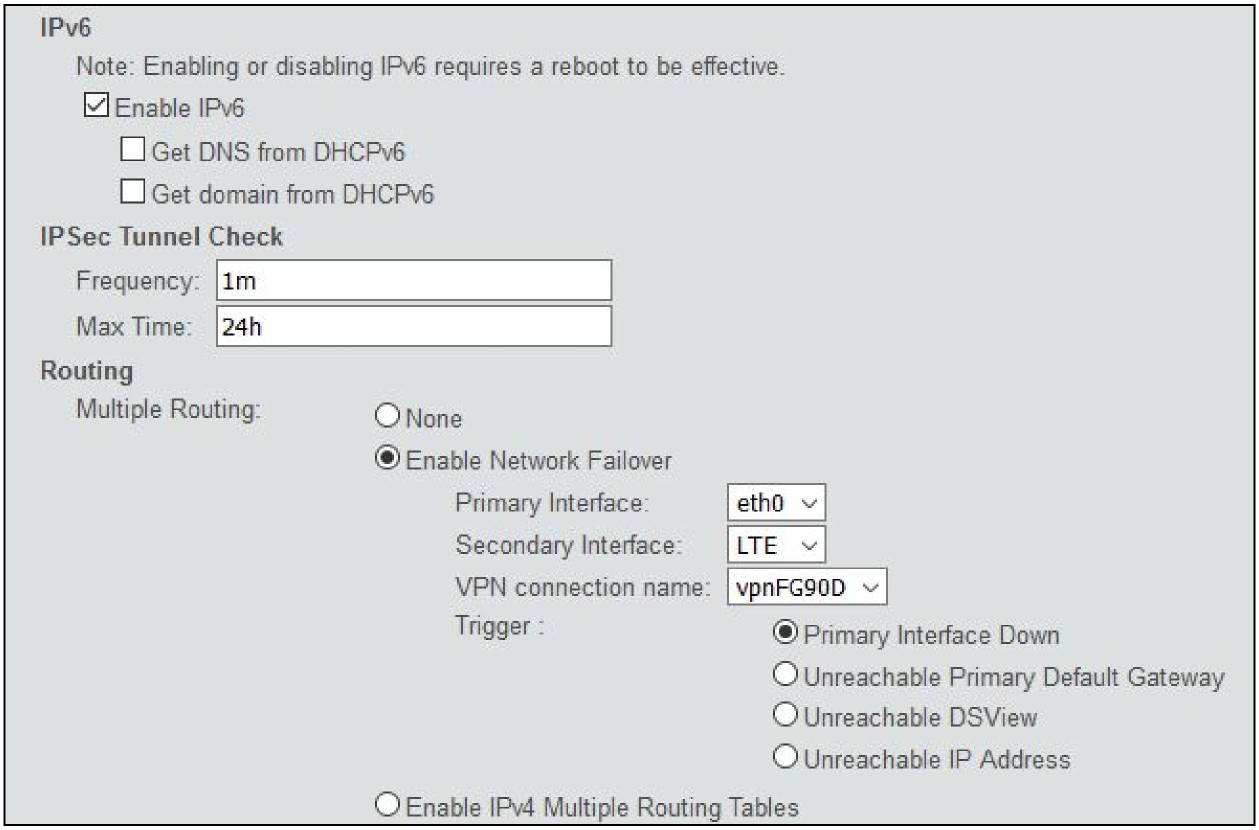
Advanced Settings

□ Show Advanced Settings

Table 3.19 IPsec Descriptions

Item	Description
IKE Version	Normally IKEv2 unless the gateway it's connecting to is old.
Boot Action	Set it to Add for failover. If you set it to start, the VPN tries to come up as soon as the console system boots up.
Aggressive	Should be set to No.
DPD Action	None. Could set it to "Restart." Means "Dead Peer Detect."
ID	Left blank because you want to identify the remote gateway by IP address.
Subnet	The subnet we are accessing behind the remote secure gateway. In this case, a Fortigate is being used, and its LAN subnet is used.
Local Left Side	
ID	IDs are used to identify each side, but leaving it blank just uses the IP address.
Virtual IP	Assigns the IP address for the tunnel. Setting it to **%config** means we are acquiring an address from the remote secure gateway.
IP Address	The console system IP address participating on the tunnel. For a regular Ethernet, this can be set to a fixed IP address. For the cell modem, the provider is assigning the IP address, and in the case of the AT&T service, it changes. Setting this to **%any** means use any interface or IP address that is up.
IPsec(VPN) Authentication	Set it "pre-shared secret" to use a passkey/password unique to the tunnel. Each side of this IPsec tunnel must use the same password/secret word. Of course, alternatively, you could use X509/RSA certificates.
Advanced Settings	Left these at defaults so IPsec will negotiate the cipher suite.

Figure 3.8 VPN Selected for Failover Example



IPv6

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

☑ Enable IPv6

□ Get DNS from DHCPv6

□ Get domain from DHCPv6

IPSec Tunnel Check

Frequency: 1m

Max Time: 24h

Routing

Multiple Routing:

○ None

● Enable Network Failover

Primary Interface: eth0

Secondary Interface: LTE

VPN connection name: vpnFG90D

Trigger :

● Primary Interface Down

○ Unreachable Primary Default Gateway

○ Unreachable DSView

○ Unreachable IP Address

○ Enable IPv4 Multiple Routing Tables

With Replace Default Route enabled, a failover event (eth0 goes down) brings up the cellular modem and then starts the VPN. The LAN clients on the remote gateway can access the console system via the tunnel virtual IP address.

3.3.9 Pluggable devices

The console system supports a variety of pluggable devices connected to its USB ports. Some models also support a single SD card in the SD card slot.

NOTE: When a pluggable device is not in the current list of supported pluggable devices, the console system may attempt to configure the device with standard settings, allowing it to work normally. Also, when a pluggable device is not listed in the internal database, the Device Info column may show no text at all or show different text based on the type of card. One example is Unknown device f024 (rev 01).

To install and detect a pluggable device:

1. From the side navigation bar, select *Pluggable Devices*.
2. Click *Enable Pluggable Device Detection* to detect connected pluggable devices, unless it has already been enabled from the System - Security page.
3. Connect a device to a USB port or insert an SD card into the SD card slot on the console system.
4. The Pluggable Devices table displays all detected pluggable devices.

NOTE: To disable pluggable device detection, click *Disable Pluggable Device Detection*.

To eject or delete a pluggable device:

1. From the side navigation bar, select *Pluggable Devices*.
2. Select the checkbox next to the pluggable device you want to eject or delete.
3. Click *Eject* or *Delete* as desired.Click *Save*.

NOTE: Always eject a pluggable device from the web UI before physically removing the device.

Device configuration

Storage devices are automatically mounted and configured once detected by the console system unless storage device support is disabled. Ethernet cards, modems and USB console devices must be configured.

NOTE: Configuration of wireless devices takes effect only after the device is ejected and re-inserted.

To configure a pluggable device:

1. From the side navigation bar, click *Pluggable Devices*.
2. For a network device, click its name to configure its network parameters.

   -or-

   For a modem (V.92), click the box next to its name and then click either *Set Dial-In* or *Set Dial-Out* to configure its dial-in or dial-out parameters.

   -or-

   For a USB console device, click the box next to its name and then click *Set Console* to add it to the system as another port. You can either accept the default port assignment or enter an unused port in the Port field and click *Assign*. Then go to the *Ports - Serial Ports* page to configure and enable the added port.

USB console mapping

USB console devices will default to a port based on the number of console system serial ports. The following table shows the default port assignments.

Table 3.20 ACS80X USB Console Mapping

	USB POrts			
MODEL	Top left	bottom left	top right	bottom right
ACS802	3	4	5	6
ACS804	5	6	7	8
ACS808	9	10	11	12

Table 3.21 ACS80XX USB Console Mapping

	Back USB Ports						Front USB Ports	
Model	Top Left	Bottom Left	Top Middle	Bottom Middle	Top Right	Bottom Right	Top	Bottom
ACS8008	9	10	11	12	13	14	15	16
ACS8016	17	18	19	20	21	22	23	24
ACS8032	33	34	35	36	37	38	39	40
ACS8048	49	50	51	52	53	54	55	56

If the default assigned port is already in use or if the USB device is not plugged directly into the console system, the next available port after the reserved ports will be used. For example, on an ACS808 console system, port 13 is the next available port.

Hot plugging

Serial console devices can be unplugged and plugged back into the same USB port without interrupting any open serial sessions. In most cases, the USB device receives the same Linux-assigned device name. In some cases, a different device name is assigned if the original name appears in use.

NOTE: The device must be plugged back into the same port to enable hot plugging.

3.3.10 Authentication

Authentication can be performed locally, with OTP, or remotely on a LDAP, Radius, Kerberos or TACACS+ authentication server. If the console system is managed by a DSView server, DSView authentication is also supported. The console system also supports remote group authorizations for the LDAP, Radius, Kerberos and TACACS+ authentication methods.

Fallback mechanisms of the following types are available:

Local authentication can be tried first, followed by remote, if the local authentication fails (Local/Remote_Method).

-or-

Remote authentication may be tried first, followed by local (Remote_Method/Local).

-or-

Local authentication may be tried only if a remote authentication server is down (Remote_Method_Down_Local).

An administrator can configure authentication using the CLI utility and the web UI. The default authentication method for the console system and the serial ports is Local. Any authentication method that is configured for the console system or the ports is used for authentication of any user who attempts to log in through Telnet, SSH or the web UI.

Appliance authentication

The console system authenticates for the console system and the ports, either in groups or individually.

NOTE: It is advised when using group authorization that you use the same authentication for both the console system and all serial ports, or use Single Sign-on Authentication to facilitate group authorization.

When Single Sign-on Authentication is disabled, the console system uses the individual configuration based in the destination of the access: the console system itself or each serial port. Users must use their password each time they access an individual port. If enabled, Single Sign-on Authentication will use the authentication server you choose from the pull-down menu for all access and no further authentication will be needed.

NOTE: Selecting *unconfigured* from the pull-down menu will allow the ports to continue to use individual authentication servers, and will require your password the first time you access any port. After that, the port will not require password authentication if Single Sign-on Authentication is enabled.

To set authentication for the console system:

1. Click *Authentication - Appliance Authentication*.
2. Select the desired authentication server from the Authentication Type drop-down menu.
3. Select *Enable fallback to Local type for root user in appliance console port* when the remote authentication fails and an administrator wants to access the appliance via console port as the root user.
4. Select *Enable single sign-on* to enable single sign-on authentication, and select the desired authentication server from the Authentication Type drop-down menu.
5. Click *Save*.

Authentication servers

When using an authentication server, you must configure its IP address and in most cases other parameters before it can be used. The following authentication servers require configuration: RADIUS, TACACS+, LDAP(S)|AD, Kerberos, and DSView servers.

To configure a RADIUS authentication server:

1. Select *Authentication - Authentication Servers - RADIUS*.
2. Enter the IP addresses of the First Authentication Server and First Accounting Server.
3. If used, enter the IP addresses for the Second Authentication Server and Second Accounting Server.
4. Enter your secret word or passphrase in the Secret field (applies to both first and second authentication and accounting servers), then re-enter the secret word or passphrase in the Confirm Secret field.
5. Enter the desired number of seconds for server time-out in the Timeout field.
6. Enter the desired number of retries in the Retries field.
7. If you select the *Enable Service-Type attribute to specify the authorization group* checkbox, enter the authorization group name for each of the following Service Types: Login, Framed, Callback Login, Callback Framed, Outbound and Administrative.
8. Click *Save*.

To configure a TACACS+ authentication server:

1. Select *Authentication - Authentication Servers - TACACS+*.

2. Enter the IP addresses for the First Authentication Server and First Accounting Server.
3. If used, enter the IP addresses of the Second Authentication Server and Second Accounting Server.
4. Select the desired service (PPP or raccess) from the Service drop-down menu.
5. Enter your secret word or passphrase in the Secret field (applies to both first and second authentication and accounting servers), then re-enter the secret word or passphrase in the Confirm Secret field.
6. Enter the desired number of seconds for server time-out in the Timeout field.
7. Enter the desired number of retries in the Retries field.
8. If you select the *Enable User-Level attribute to specify the authorization group* checkbox, enter the authorization group name for up to 15 User-Levels.
9. Click *Save*.

To configure an LDAP(S)|AD authentication server:

1. Select *Authentication - Authentication Servers - LDAP(S)|AD*.
2. Enter the IP address of the server.
3. Enter the Base.
4. At the Secure drop-down menu, select *Off, On* or *Start_TLS*.
5. Enter the Database User Name.
6. Enter your Database Password, then re-type the database password in the Confirm Password field.
7. Enter your desired Login Attributes.
8. Click *Save*.

To configure a Kerberos authentication server:

1. Select *Authentication - Authentication Servers - Kerberos*.
2. Enter the IP address (Realm) of the server.
3. Enter the Realm Domain Name (example: AVOCENT.com).
4. Enter the Domain Name (example: .avocent.com).
5. Click *Save*.

To configure a DSView authentication server:

1. Select *Authentication - Authentication Servers - DSView*.
2. Enter IP Address 1 - 4 for the DSView servers in the relevant fields.
3. Click *Save*.

3.3.11 Users accounts and user groups

Access to ports and other privileges can be managed based on authorizations that an administrator can assign to custom user groups and individual user accounts.

Groups and users can also be authorized to manage power while connected to devices. The console system has two default users (admin and root) and four pre-defined user groups: admin, appliance-admin, shell-login-profile and user.

A user account must be defined for each user on the console system or on an authentication server. The admin and root users have accounts by default, and either administrator can add and configure other user accounts. Each local user account is assigned to one or more of the user groups.

NOTE: When a user is removed from all groups, that user's privileges revert to those of the default user group. For this reason, it is recommended custom groups be used and the default user group is not granted additional privileges.

By default, all users have access to all ports on the console system. In order to authorize access via user groups, an administrator must enable port access to be controlled by authorizations assigned to user groups.

To enable port access to be controlled by authorizations assigned to user groups:

1. From the Expert tab of the side navigation bar, click *System - Security - Security Profile*.
2. Under the Serial Devices heading, click Controlled by Access Rights assigned to User Groups and specific users button, then click *Save*.

Local accounts

The console system has two local user accounts by factory default:

- admin: Performs the initial network configuration. The admin user is a member of the admin group and can configure the console system and ports as well as user and group authorizations.
- root: Has the same administrative permissions as the admin user but also has unlimited privileges from the shell. The root user is a member of the admin and shell-login-profile groups. When a root user logs in via the CONSOLE port, SSH or Telnet, the session is pre-defined by the login profile to go directly to shell. The login profile can be customized so that it does not go directly to shell.

To view user appliance access rights:

1. Click *Users - Local Accounts - User Names*. The list of usernames displays in the content area.
2. Click a username under the User Name heading. The content area displays the user information for the selected user.

NOTE: When any username is selected, both the content area and side navigation bar change. The side navigation bar displays specific menu options for Members and Access Rights (which include Serial, Power and Appliance rights).

3. From the side navigation bar, click *Access Rights - Serial* or *Access Rights - Power* to access the screens displaying the fixed access rights and permissions for the selected user.

NOTE: The Serial and Power screens are read-only and cannot be changed.

4. From the side navigation bar, click *Access Rights - Appliance*. The Appliance Access Rights screen appears and lists all access rights available to the user. Available appliance access rights are:
   - View Appliance Information
   - Disconnect Sessions
   - Reboot Appliance
   - Appliance Flash Upgrade and Reboot Appliance
   - Configure Appliance Settings
   - Configure User Accounts
   - Backup/Restore Configuration
   - Shell Access
   - Transfer Files
   - Dial-In Access

To add new users:

1. Click *Users - Local Accounts - User Names*. The User Names screen is displayed with a list of all users.

2. Click *Add*. The Local User Information screen is displayed.
3. Enter the new username and enter a password, then confirm the password.
4. Select or deselect *User must change password at the next login* checkbox.
5. To add the user to an available user group, select the user group name in the box on the left and click *Add* (user is the default group). You can remove a user group from the box at right by selecting it and clicking *Remove*.
6. Enter the desired parameters for Password Expiration.
   - Min Days: Enter the minimum number of days allowed between password changes. Password changes attempted sooner will be rejected. To disable the restriction on the number of days allowed between password changes, leave this field empty.
   - Max Days: Enter the maximum number of days a password is valid. After this period, a password change will be forced. To disable the restriction for the maximum number of days a password is valid, leave this field empty.
   - Warning Days: Enter the number of days that a warning is issued to the user prior to expiration. Entering 0 will cause the warning to be issued on the expiration day. To disable the warning, leave this field empty.
7. Enter the desired Account Expiration date (YYYY-MM-DD).
8. Click *Save*.

To configure password rules:

1. Click *Users - Local Accounts - Password Rules*.
2. If password complexity is desired (recommended), make sure *Check Password Complexity* is selected.
3. If password complexity is enabled, enter the desired values for password complexity.
4. Enter the desired values for Default Expiration.
5. Click *Save*.

User groups

User groups are given access and authorizations either by default or as assigned by an administrator. Administrators can alter the permissions and access rights of users belonging to the appliance-admin or user groups or create additional groups with custom permissions and access rights. Administrators can add, delete or modify permissions and access rights for users from any group at any time.

If an administrator configures the console system to restrict user access to ports, the administrator can assign users to groups that are authorized for port access. The administrator can also authorize groups for power management and data buffer management.

This document and the software refer to users whose accounts are configured on remote authentication servers as remote users. Remote users do not need local accounts.

NOTE: When a user is removed from all groups, that user's privileges revert to those of the default user group. For this reason, it is recommended custom groups be used and the default user group is not granted additional privileges.

Radius, TACACS+ and LDAP authentication services allow group configuration. If a remote user is configured as a member of a remote group, the authentication server provides the group name to the console system when it authenticates the user. A local group by the same name must also be configured on the console system. If an authentication server authenticates a remote user but does not return a group, then the remote user is, by default, assigned to the user group.

admin group

Members of the admin group have full administrative privileges that cannot be changed. They have the same access and configuration authorizations as the default admin user. Administrators can configure ports, add users and manage power devices connected to the console system.

To view admin appliance access rights:

1. Click *Users - Authorization - Groups*. The Group Names screen is displayed, showing the three default user groups along with any groups that have been created.
2. Click on *admin* under the Group Name heading. The content area will display the Members screen listing all members belonging to the admin group (default members are admin and root users).

NOTE: When any Group Name is selected, both the content area and side navigation bar change. The side navigation bar will display specific menu options for Members and Access Rights (which include Serial, Power and Appliance rights).

3. In the side navigation bar, click *Access Rights - Serial* or *Access Rights - Power* to access the screens displaying the fixed access rights and permissions for members of the admin group pertaining to serial ports and power management.

NOTE: The Serial and Power screens are read-only and cannot be changed.

4. In the side navigation bar, click on *Access Rights - Appliance*. The Appliance Access Rights screen appears and lists all access rights available to a member belonging to the admin group. All appliance access rights are shown enabled (checked). Available appliance access rights are:
   - View Appliance Information
   - Disconnect Sessions
   - Reboot Appliance
   - Appliance Flash Upgrade and Reboot Appliance
   - Configure Appliance Settings
   - Configure User Accounts
   - Backup/Restore Configuration
   - Shell Access
   - Transfer Files
   - Dial-In Access

NOTE: The Appliance Access Rights screen for the admin and appliance-admin user groups is read-only and cannot be changed. Unchecking any box and clicking *Save* will result in an error message. The console system will maintain all rights selected.

appliance-admin group

Appliance-admin user group members have access to the serial ports and power management options, unless that access is restricted by the security profile. Members of the group also share all of the appliance access rights as admin except for Configure User Accounts and Shell Access, which are permanently disabled for this group.

user group

User group members have access to target devices, unless that access is restricted by an administrator. When a security profile restricts port access globally, an administrator may grant port access to members of the user group. User group members have no access rights for the console system.

Administrators can add appliance access rights and permissions. Administrators can also add users to custom user groups to add permissions and access rights as needed. By default, all selections on the Appliance Access Rights screen will be disabled.

NOTE: The Appliance Access Rights screen for the user group can be changed at any time by an administrator. This will change the access rights for all members of the console system's user group.

shell-login-profile

Members of the shell-login-profile group have access to the shell after logging in. By default, the root user belongs to this group. This is not a protected group and can be deleted.

Managing user groups

Administrators and members of the admin group can create custom user groups that contain any users.

To create a custom user group:

1. Click *Users - Authorization - Groups*. The Groups screen is displayed and contains a list of the three default user groups and any additional custom user groups that have been created.
2. Click *Add* in the content area.
3. Enter the name of the new user group you are creating.
4. Click *Save*.

To add members to a user group:

1. Click *Users - Authorization - Groups*.
2. Click the user group name.
3. Click *Add*. The Members Assignment screen is displayed showing a list of available users in the left box and an empty box on the right.
4. Move users from the Available Users box on the left to the box on the right by double-clicking on the username, or by selecting the name and clicking the *Add* button. You can remove any names from the box on the right by double-clicking on the name or by selecting the name and clicking the *Remove* button.
5. If you want to add remote users to the new user group (these must be valid names in your remote authentication server), add them in the New Remote Users field.
6. Click *Save*.

To remove members from a user group:

1. Click *Users - Authorization - Groups*.
2. Click the user group name.
3. Check the box(es) of the member(s) you want to remove. Click *Delete* to delete the selected members.

To configure a session idle time-out and/or login profile for a group:

1. Click *Users - Authorization - Groups*.
2. Click on the name of the group whose session idle time-out and/or login profile you want to set. In the side navigation bar, click *Login Profile*.
3. Select the radio button to use either the global settings for the Session Timeout or to use custom settings for the user group. If using custom settings, enter the custom session timeout (in seconds) in the field.
4. Check the *Enable Log-In Profile* box.
5. Click *ts_menu* to use the ts_menu application when a member of the selected user group opens a session in the console system. Enter the ts_menu options in the Options field.

-or-

Click *CLI* to use CLI when opening a session. Enter the CLI command in the CLI cmd field and check the box if you want to exit after executing the command.

6. Click *Save*.

NOTE: If the user belongs to multiple groups, the login profile used will be the first enabled login profile based on alphabetical order of the group.

Table 3.22 ts_menu Options

Command	Description
-p	Displays TCP port
-i	Displays local IPv4 assigned to the serial port
-i6	Displays local IPv6 assigned to the serial port
-u <name>	Username to be used in the target session
-e <[^]char>	Escape character used to close the target session. Default value: Ctrl-X
-l	Sorted lists ports and exit
-ro	Read-Only mode
<portname>	Connect directly to a serial port
-t	Idle time-out in seconds to choose the target

To add access to serial ports for a user group:

1. Click *Users - Authorization - Groups*.
2. Click the new user group name.
3. In the side navigation bar, click *Access Rights*.
4. In the content area, click *Add*.
5. Move serial target devices from the Available Target box on the left to the box on the right by double-clicking on the serial target name

   -or-

   by selecting the target and clicking the *Add* button. You can remove any targets from the box on the right by double-clicking on the target or by selecting the target and clicking the *Remove* button.
6. Select the desired access rights.
7. Click *Save*. The Serial screen will appear and show the serial target devices you have authorized for use by the user group with configured permission(s).
8. Edit the access rights by selecting the checkbox next to one or more of the target names in the list as needed and click *Edit*. The Target Access Rights screen is displayed with the access rights. Select the desired access rights and click *Save*.

To assign PDU access for a user group:

NOTE: Assigning PDU access to a user group gives them full access to all power management functions for that PDU. If you want the user group to have access to outlets only, use the procedure *To assign outlet access for a new custom user group* below.

1. Click on *Users - Authorization - Groups*.
2. Click on the user group name.
3. In the side navigation bar, click *Access Rights - Power*.

4. In the content area, click *Add*. The PDU Assignment screen appears with the list of available PDUs in the left box.
5. Move PDU devices from the Available PDU box on the left to the box on the right by double-clicking on the PDU name, or by selecting the PDU and clicking the *Add* button. You can remove any PDUs from the box on the right by double-clicking on the PDU name or by selecting the PDU and clicking the *Remove* button.
6. You can specify a custom PDU ID in the field at bottom and assign it a custom PDU ID.

NOTE: The custom PDU ID is for assigning user group authorization to manage PDUs that have not yet been connected to the console system.

7. Click *Save*.

To assign outlet access for a new custom user group:

NOTE: Assigning outlet access to user groups allows group members to turn outlets on or off, and enable locking and power cycle capabilities on compatible PDUs.

1. Click *Users - Authorization - Groups*.
2. Click on the new user group name.
3. In the side navigation bar, click *Access Rights - Power - Outlets*.
4. Click *Add*. The Add Outlet screen is displayed.
5. For connected PDUs, click the *Select PDU* button to activate the Connected PDUs and Outlets fields.
6. Select *Connected PDU* from the pull-down menu.
7. Enter the outlets assigned to the user group.

NOTE: Outlets can be specified individually, (for example 1,3,6,8) or as a range (for example 1-4) or a combination of both, (for example 1-4,6,8 which assigns access to outlets 1, 2, 3, 4, 6 and 8).

8. If a custom PDU ID has been created for future use, and you want to pre-assign outlets, click the *Custom* button to enter the custom PDU ID name and specify the outlets.
9. Click *Save*.

To assign UPS access for a user group:

1. Click *Users - Authorization - Groups*.
2. Click the user group name.
3. From the side navigation bar, click *Access Rights - Power - UPS*.
4. From the content area, click *Add*. The UPS assignment screen appears with the list of available UPS devices in the left box.
5. Move UPS devices from the Available UPS box on the left to the box on the right by double-clicking the UPS name, or by selecting the UPS and clicking *Add*. You can remove any UPS devices from the box on the right by double-clicking the UPS name, or by selecting the UPS and clicking *Remove*.
6. You can specify a custom UPS ID in the field at the bottom of the page and assign it a custom UPS ID.

NOTE: The custom UPS ID is for assigning user group authorization to manage UPS devices that have not yet been connected to the console system.

To assign appliance access rights for custom user groups:

1. Click *Users - Authorization - Groups*.
2. Click the new user group name.
3. In the side navigation bar, click *Access Rights - Appliance*.
4. Select the desired appliance access rights and click *Save*.

To configure a group in a TACACS+ authentication server:

1. On the server, add raccess service to the user configuration.
2. Define which group(s) the user belongs to in the raccess service following this syntax:

group_name = <Group1>[,<Group2,...,GroupN>];

For example:

In the console system, configure a new authorization group TACACS_1, and configure the access rights for this group. In the TACACS+ server, configure the user "regina" with the following attribute: `raccess = group_name=TACACS_1;`

Then, configure the user "special" with the following attribute: `raccess = group_name=admin;`

During the authentication phase, the console system will receive the attribute raccess from the TACACS+ server. The user regina belongs to the authorization group TACACS_1 and the user special belongs to the authorization group admin.

To configure a group in a RADIUS authentication server:

Define which group(s) the user belongs to in the attribute FRAMED_FILTER_ID with the following syntax:

```
[:group_name=]<acs800/8000_group1>[,<acs800/8000_group2>];
```

NOTE: The group names should be separated by a comma and end with a semi-colon.

NOTE: The ACS 800/8000 accepts multiple FRAMED_FILTER_ID attributes.

For example:

In the console system, configure new authorization groups RADIUS_1 and RADIUS_2, and configure the access rights for these groups. In the Radius server, configure the user regina with the following attribute:

```
FramedFilterID = group_name=RADIUS_1,RADIUS_2;
```

-or-

```
FramedFilterID = RADIUS_1,RADIUS_2;
```

-or-

```
FramedFilterID = RADIUS_1;
FramedFilterID += RADIUS_2;
```

Then, configure the user special with the following attribute:

```
FramedFilterID = group_name=admin;
```

During the authentication phase, the console system will receive the attribute FramedFilterID from the RADIUS server. The user regina belongs to authorization group RADIUS_1 and RADIUS_2 and the user special belongs to authorization group admin.

To configure a group in an LDAP authentication server:

On the LDAP server, edit the info attribute for the user and add the following syntax.

```
info: group_name=<Group1>[,<Group2>,...,<GroupN>];
```

DSView software access rights

An administrator can configure how the DSView software's viewer session rights will be mapped to the console system's access rights when a user accesses a target via the DSView software's serial viewer.

To configure the map of DSView software access rights to console system access rights:

1. Click *Users – Authorization – DSView Access Rights*.
2. Select the desired access rights and click *Save*.

3.3.12 Event notifications

The console system will generate notifications for a variety of events. You can configure the console system to direct or store those event notifications to various destinations for immediate use or for analysis later.

Event list

The Event List screen lists console system events, each of which can be configured for SNMP Traps, Syslog, DSView software, Email and SMS.

To configure Events:

1. Click *Events and Logs - Events*.
2. Locate the events for which you want notification sent and select the checkbox(es) next to the event number(s).
3. Click *Edit*.
4. If you want an event notification sent for any configured event destination type, click its associated *Send* checkbox.
5. Click *Save*. The Events page appears with an X in the column below the destination type if the Send box was checked on the Events Settings screen.

Event destinations

To configure event destinations:

1. Click on *Event and Logs - Event Destinations*.
2. Under the Syslog heading, use the drop-down menu to select the Facility.

   Select *Remote Server - IPv4* to enable syslog messages to be sent to one or more remote IPv4 syslog servers, and enter the IPv4 Address or Hostname and the UDP port for each remote syslog server.

   -or-

   Select *Remote Server - IPv6* to enable syslog messages to be sent to one or more remote IPv6 syslog servers, and enter the IPv6 Address or Hostname and the UDP port for each remote syslog server.
3. Select *Appliance Console* to send messages to the console system’s console.
4. Select *Root Session* to send syslog messages to all sessions where you are logged in as root user.

5. Under the SNMP Trap heading, enter the name of the community defined in one or more of the SNMP trap servers in the Community field then enter the IP addresses of up to five servers in the server fields.
6. Under the SMS heading, enter the SMS Server, Port and Pager Number information in the appropriate fields.
7. Under the Email heading, enter the Server, Port and Destination Email information in the appropriate fields.
8. Under the DSView heading, enter the IP address of the DSView server where event notifications will be sent in the DSView server field. Enter the syslog server port number for the DSView server, the SSH information and the buffer warning information in the appropiate fields.
9. Click *Save*.

Trap forward

The console system will receive SNMP traps and forward them to a remote SNMP trap server.

To add a SNMP trap server to forward traps:

1. Click *Events and Logs – Trap Forward*.
2. Click *Add*.
3. Enter the IP address of the remote server and the UDP port.
4. Enter the OID to filter traps to send to this server (optional).

To edit SNMP trap server configuration:

1. Click *Events and Logs – Trap Forward*.
2. Click the index of the server to be edited.
3. Update the UDP port and/or the OID and click *Save*.

Data buffering

When data buffering is enabled on one or more serial ports, the settings on the Events and Logs - Data Buffering page apply to the type (destination) of the buffering. Segment size, which is specified in kilobytes, determines the size of each data buffering file saved. Spare segments determines how many additional historical buffering files of segment size are retained and named with suffix .1, .2 etc.

To configure data buffering:

1. Select *Events and Logs - Data Buffering*.
2. Enter the segment size in kilobytes and spare segments in the Local Data Buffering Settings section.
3. In the NFS Data Buffering Settings section, enter the following information: NFS Server, NFS Path, Segment Size (Kbytes) and Spare Segments.

NOTE: RPC service must be enabled in the Security Profile screen before configuring NFS Data Buffering Settings.

4. To segment data buffering files every day based in hour, enter the time in the Close Log Files and Open New Ones at Time (HH:MM) field. This will be valid for local and NFS data buffering.
5. To configure data buffer storage on a syslog server in the Syslog Data Buffering Settings section, select a facility number from the drop-down menu: Log Local 0, Log Local 1, Log Local 2, Log Local 3, Log Local 4 or Log Local 5.
6. Click *Save*.

To enable data buffering:

1. Select *Ports - Serial Ports*.
2. Click on the port where you want to enable data buffering.

3. Under the Data Buffering tab, use the drop-down menu next to Status to *Enable* data buffering.

Appliance logging

When Appliance Logging is enabled, the commands (input) and output from SSH and Telnet sessions to the appliance are recorded for auditing purposes

To configure appliance logging:

1. Click *Enable appliance session data logging*.
2. Select the destination for appliance session data logs from the pull-down menu. Choices are *Local*, *NFS*, *Syslog* and *DSView*.
    a. If using local as the destination, use the drop-down menu to select the local destination.Destination *mmcblk0* is the built-in flash storage. SD card (if present and enabled) is *mmcblk1*. USB devices (if present and enabled) are *sda1*, *sda2* and so on.

NOTE: When the local destination is mmcblk0, the logging directory on the appliance is /mnt/hdUser/db. When the local destination is mmcblk1 or a USB device the logging directory is the top (root) directory of that device.

3. Enable or disable timestamping the appliance session data logs.
4. Click *Enable appliance session data logging alerts*.
5. Enter the desired alert strings (up to ten) in the fields provided.
6. Click *Save*.

3.3.13 Power management

Connected power devices can be used for remote power management. The console system enables users who are authorized for power management to turn power on, turn power off and reset devices that are plugged into a connected PDU. Authorized users can also monitor and control a connected Liebert GXT4 or GXT5 uninterruptible power supply (UPS) device.

The following types of PDUs can be connected to any serial port.

- Avocent Power Management Power Distribution Unit (PM PDU).
- Vertiv MPH2 Rack Power Distribution Units (PDUs) as well as MPX and MPH rack PDUs with RPC2 cards installed.
- Cyclades PM Intelligent Power Distribution Units (IPDUs) - With Cyclades PM IPDUs, up to 128 outlets can be daisy-chained and managed from a single serial port.
- Avocent SPC power control devices.
- Server Technology Sentry family of Switched Cabinet Power Distribution Units (CDUs), Smart Cabinet Power Distribution Units (Smart CDUs) and switched CDU Expansion Module (CW/CX) power devices. One additional level of power devices can be daisy-chained with ServerTech Expansion modules.
- Server Technology Sentry Power Tower XL (PTXL) and Power Tower Expansion Module (PTXM) power devices.
- Eaton ePDU G3 PDUs. Up to eight ePDUs can be chained together and managed from a single serial port.
- Raritan PX G2 PDUs.
- APC rPDU2 PDUs.
- Geist GU2 and R-Series Rack PDUs running firmware 5.3 or later are supported.

NOTE: The term PDU refers to any of these types of power devices.

The console system automatically recognizes and supports Liebert RPC2 cards, Avocent PM PDUs, Cyclades PM PDUs, Raritan PDUs, Eaton ePDUs, APC PDUs, Vertiv PDUs, Geist PDUs and Avocent SPC devices when the corresponding serial port is configured for power management.

PDUs

To manage a PDU:

1. Select *Power Management - PDUs*.
2. Select the checkbox next to the PDU you want to manage.
3. Click *On, Off, Cycle, Reboot PDU, Reset HW Overcurrent Protection* or *Factory Defaults* if desired. A confirmation appears. Click *OK*.

NOTE: The power controls (On, Off and Cycle) will be applied to all outlets of the PDU.

4. To change the PDU ID, click *Rename* and enter the name in the New PDU ID field.
5. Click *Save*.

To upgrade firmware:

1. Select the checkbox next to the PDU you want to upgrade and click the *Upgrade Firmware* button.

NOTE: You can upgrade the firmware for multiple PDUs at the same time for Avocent PM PDUs and Vertiv (MPH2, MPH and MPX with RPC2 cards installed) PDUs only. If upgrading PDUs in a daisy chain, select only the first PDU in the chain as the rest of the PDUs in the chain will be upgraded automatically.

2. Select *Remote Site* and enter the remote server information.

   -or-

   Select *My Computer* and browse to the location where you saved the firmware file.
3. Click *Download* to download the firmware to the console system.
4. When the download finishes, the console system displays the current and downloaded firmware versions. If the downloaded version information is correct, click *Upgrade Now* to start the upgrade of the firmware in the PDU.
5. Once the upgrade has started, click *Finish*. A message stating the upgrade has successfully started will display. The PDU Overview page displays the upgrade status. The PDU reboots when the upgrade is complete.

To view a PDU's information and manage outlets:

1. Select *Power Management - PDUs*.
2. Click the name of the PDU you want to view or manage.
3. The Outlet Table with power controls window appears and the side navigation bar displays a list of options.
4. To manage outlets of PDU:
   a. Check the box(es) of the outlet number(s) you want to manage.
   b. Click *On, Off, Cycle, Lock* or *Unlock* to perform that function for the selected outlet(s).
5. Click *Information* in the side navigation bar to view a PDU's information.
6. Click *Overview* in the side navigation bar to view data monitoring information.
7. Click *Current, Voltage, Power Consumption, Energy Consumption* or *Environment* in the side navigation bar to view a table with appropriate information. Click *Reset Values* to clear Max, Min and Average values.

To configure a PDU:

1. Click *Settings* to expand the side navigation bar.
2. Click *Outlets*.

3. Click on an outlet number to change its settings. Click *Save,* then click *Close*.

   -or-

   Check two or more boxes next to the outlets for which you want to change settings. Click *Edit* to change the settings for the outlets you selected. Click *Save*.

4. Click *PDU* to view and configure PDU settings. Click *Save* when finished.
5. Click *Phases* or *Banks*.
   a. Click on the name of a phase or bank to change its settings, or click one or more boxes next to the phase (s) or bank(s) you want to change.
   b. Click *Save* to save the settings and click *Close* to return to the Phase screen.

NOTE: The PDU model defines available parameters in the Settings window.

UPS

To manage a UPS:

1. Select *Power Management - UPS*.
2. Select the checkbox next to the UPS you want to manage.
3. Click *Turn Output Off, Turn Output On*, or *Cycle Output* if desired. An option appears to insert the desired delay time before the operation is performed. Click the button to perform the operation.
4. To change the UPS ID, click *Rename* and enter the name in the New UPS ID field.
5. Click *Save*.

To view a UPS device's information:

1. Select *Power Management - UPS*.
2. Click the name of the UPS you want to view or manage.
3. Click the options in the side navigation bar to view UPS information.

To configure a UPS:

1. Click *Settings* to expand the side navigation bar.
2. Click on the options in the side navigation bar to configure the UPS.

Login

An administrator can change the login password for a supported PDU type. This password is used by the console system to communicate with the PDU. (Only one password is supported for all PDUs of the same type.)

To change a PDU password:

1. Select *Power Management - Login*.
2. Enter the new password for each type of PDU you want to change.
3. Click *Save*.

Outlet groups

By selecting the *Outlet Groups* tab, you can view status, outlet and power consumption for outlet groups, as well as configure them. You can also turn on, turn off or cycle selected outlet groups.

To manage outlet groups:

1. Select *Power Management - Outlet Groups*.
2. Check the box next to the name of the Outlet Group you want to manage.
3. Click the *On*, *Off* or *Cycle* radio button, if desired.

   -or-

4. Click *Add* to add an outlet group. The Add Group screen appears. Enter the name in the Group Name field.
5. Click *Save*.

To view and change outlet group information:

1. Select *Power Management - Outlet Groups*.
2. Click the name of the outlet group you want to view or manage.
3. To add outlets, click *Add* to add a new outlet to the group. Fill the fields and click *Save* to return to the Outlet Group Details table.
4. To delete outlets, check one or more boxes next to the outlet(s) you want to remove from the group. Click *Delete*, then click *Close* when finished.

Network PDUs

Power devices connected to the network with SNMP (read/write) enabled can be used for remote power management. The console system enables authorized users to turn power on and turn power off in devices that are plugged into the network PDU.

NOTE: SNMP needs to be enabled and have one community with write permission enabled in the PDU.

By selecting the *Network PDUs* node, an administrator can add new Network PDUs or edit configuration of current ones.

The following functionalities are supported for Network PDUs:Power Control (turn on, turn off and cycle/reboot) outlets, rename the PDU and rename the outlets

To add a network PDU:

1. Select *Power Management – Network PDUs*.
2. Click *Add*.
3. Enter the IP address of the network PDU.
4. Select the PDU type.
5. Enter the interval to poll the PDU for the status of the outlets.
6. Enter the community name that has write permission in the PDU.

Network UPS

Liebert GXT4 and GXT5 UPS devices with installed Liebert Intellislot Unity Cards, connected to the network with SNMP (read/write) enabled, may be monitored and controlled. The console system enables authorized users to monitor battery information, system input and output information, and to control output receptacles.

NOTE: SNMP needs to be enabled and have one community with write permission enabled in the UPS.

By selecting the Network UPS node, an administrator can add new network UPS devices or edit the configuration of current ones.

3.3.14 Sensors

Internal

The console system has sensors that monitor the internal temperature. You can specify an operating range for the console system that fits its environment. There are two internal temperature sensors that can generate event notifications: the CPU temperature sensor and the Board temperature sensor.

CAUTION: Do not use values that exceed the maximum and minimum temperatures. Appendices on page 79.

To configure the temperature sensors:

1. Click *Sensors - Appliance - Internal* to open the Internal page displaying both the CPU and Board temperature sensors.
2. In the Maximum Temperature field for either the CPU or Board temperature sensor, enter the temperature in degrees Celsius that, if exceeded, will generate an event notification.
3. In the Maximum Temperature Threshold field for either the CPU or Board temperature sensor, enter the temperature threshold in degrees Celsius below the maximum temperature.

NOTE: The Maximum Temperature Threshold field will define a region around the maximum temperature. When the temperature exceeds the Maximum Temperature plus Threshold, an event notification will be generated. When the temperature falls below the Maximum Temperature minus Threshold, an even notification that the console system has returned to normal operating temperature will be generated. This is also true for setting the minimum temperature threshold.

4. In the Minimum Temperature field, enter the temperature in degrees Celsius that, if the console system's temperature falls below, will generate an event notification.
5. In the Minimum Temperature Threshold field, enter the temperature threshold in degrees Celsius above the minimum temperature.
6. Click *Save*.

1-Wire external sensors

An external 1-Wire sensor can be connected to the SENSOR port on the front of the console system with a CAT 5 cable. By default, 1-Wire sensor support is enabled. It can be disabled via the Security Profile page.

To configure a 1-wire sensor:

From the side navigation bar, click *Sensors - Appliance - 1-Wire*. Detected sensors display in a table with the sensor type and present value information.

NOTE: This option appears for all console system models, even though some models do not have a SENSOR port. If your model does not have a SENSOR port, leave this option disabled.

NOTE: If a connected sensor does not display, click *Update List* to refresh the page.

NOTE: Sensor configuration options are dependent on the sensor type. Sensors have common configuration settings for Name and Location.

Contact sensors (SN-2D/SN-3C)

This sensor type can generate an event notification when one of their inputs change state. An input can be *Disabled*, *Alarm when open* or *Alarm when closed*.

External temperature

This sensor type can generate an event notification when the temperature crosses a user-defined threshold. The measurement unit can be configured as *Celsius* or *Fahrenheit*. The thresholds for Low Warning, Low Critical, High Warning or High Critical must be set to allow event generation. Additionally, the alarm state must be set to *Enabled* to generate an alert.

External humidity

This sensor type can generate an event notification when the humidity crosses a user-defined threshold. The thresholds for Low Warning, Low Critical, High Warning, or High Critical must be set to allow event generation. Additionally, the alarm state must be set to *Enabled* to generate an alert.

Differential pressure (SN-DP)

This sensor type can generate an event notification when the differential pressure crosses a user-defined threshold. The thresholds for Low Warning, Low Critical, High Warning, or High Critical must be set to allow event generation. Additionally, the alarm state must be set to *Enabled* to generate an alert.

Leak sensor (SN-L)

This sensor type can generate two types of alarms: a leak alarm, which occurs when a leak is detected; and a cable fail alarm, which occurs when a cabling connection problem is detected. One configuration parameter is the Filter Time (seconds). This is the time, in seconds, the leak must persist before an event is generated.

Digital In sensors

An external Digital In sensor can be connected to the DIGITAL IN port on the front of the console system with a CAT 5 cable.

To configure a Digital In sensor:

1. From the side navigation bar, click *Sensors - Appliance - Digital In*. Detected digital inputs display in a table.
2. Click the number associated with the position of the sensor to open the settings page.
3. Enter the name and location of the sensor and use the drop-down menu to select the sensor type.
4. A Digital In sensor can be configured to generate an event by configuring the Alarm parameter. Use the drop-down menu to select *Alarm when open, Alarm when closed* or to *disable* the alarm.

NOTE: This option appears for all console system models, even though some models do not have a DIGITAL IN port. If your model does not have a DIGITAL IN port, leave this option disabled.

Digital Out sensors

The ACS800 Advanced Console System supports two digital outputs. The digital outputs are remote-controlled relay ports that can be used to open or close an electric circuit.

NOTE: Digital outputs are not supported on the ACS8000 Advanced Console System.

To configure a Digital Out sensor:

1. From the side navigation bar, click Digital Out.
2. Click the number associated with the position of the sensor to open the settings page.
3. If desired, enter a name for the sensor.
4. Use the drop-down menu turn *ON* or *OFF* an electric circuit, then click *Save*.

3.3.15 Active sessions

The console system allows multiple users to log in and run sessions simultaneously. The active sessions feature allows you to view all active sessions and kill any unwanted sessions. Click *Active Sessions* to view all open sessions on the console system.

NOTE: If you start another session with the console system while viewing this screen, it will not be visible until you click *Refresh* at the top of the web UI window.

To kill an active session:

1. Click *Active Sessions*. The Active Sessions screen appears and lists all open sessions to the console system by the user's workstation IP.
2. Select the checkbox next to the session you want to kill, then click the *Kill* button. After a few seconds, the Active Session screen will redisplay the open sessions, minus the one you killed.

3.3.16 Monitoring

When you click *Monitoring,* a variety of network and console port information is available for viewing. The screens are only for viewing and have no interactivity with the user. The following table shows the types of information available.

Table 3.23 Monitoring Screens

Screen Name	Definition
Network - Devices	Shows Ethernet ports and USB network adaptor, Status (enabled/disabled), IPv4 Address, IPv4 Mask and IPv6 Address.
Network - IPv4 Routing Table	Shows Destination, Gateway, Genmask, Flags, Metric, Ref, Use and Iface (interface).
Network - IPv6 Routing Table	Shows Destination, NextHop, Flags, Metric, Ref, Use and Iface (interface).
Serial Ports	Shows Device Name, Profile, Settings, Signals, TX Bytes, RX Bytes, Frame Error, Parity Error, Break and Overrun. The Reset Counters button allows administrators to reset the statistic counters for selected ports.
FIPS Mode	Shows Service Name and Mode Indication.
Zero-touch Log	Shows the Zero-touch Provisioning log file and allows an administrator to clear it.
Caller ID Log	Shows the last 20 calls.
IPSec Tunnel Status	Shows the IPSec connection details, including tunnel status, remote IP address, IKE lifetime, established time, phase algorithms and certificate name.

3.3.17 Change password

An administrator or user can change their own password from this screen.

To change your own password:

1. Select *Change Password*.
2. Enter the old password and new password in the appropriate fields.
3. Confirm the new password, then click *Save*.

3.4 Web UI Overview for Regular Users

Table 3.24 Web UI Options for Regular Users

Menu Option	Description
Access	Displays all the devices the user can access. Click on *Serial Viewer* in a device's Action column to launch a terminal session with that device.
Power Management PDUs Outlet Groups	Click *PDUs* to turn on, turn off, cycle, reboot, reset the HW overcurrent protection, return to factory defaults or rename PDUs connected to the console system. Click *Outlet Groups* to manage groups of outlets on connected PDUs. Click UPS to monitor and control connected UPS devices.
Change Password	Change your own password.

This page intentionally left blank

Appendices

Appendix A: Technical Specifications

Table A.1 Technical Specifications for the ACS8000 Advanced Console System Hardware

Category	Value
General Information	
CPU	Dual Core ARM Cortex-A9 @ 766MHz
Memory	1GB DDR3L / 16GB eMMC FLASH
Interfaces	• Two dual media 1000Base-TX Copper/1Gbps SFP Fiber ports • 48 serial ports with autosensing and switching support of Cyclades and Cisco pinouts • Two of the serial ports support RS232/422/485 multi-protocol with autosensing and switching support of Cyclades and Cisco pinouts in RS232 mode • One serial console port • Eight USB 2.0 host ports (front ports not available on some models) • One SD card slot (not available on some models) • Optional V.92/56K analog MODEM port • 1-Wire interface for external sensors (not available on some models) • Single RJ45 connector with four digital-in ports for external contact closure sensors (not available on some models)
Power Information	
Power Supply	Internal 100-240 VAC, 50/60 Hz Optional Dual entry, redundant power supplies-48 VDC option available
Power Consumption	Nominal voltage 120 VAC: Typical 0.17A, 20W, Maximum 0.25A, 30W Nominal voltage 230 VAC: Typical 0.1 A, 23 W, Maximum 0.15A, 35W Nominal voltage -48 VDC (20% tolerance) Typical 0.5 A
Ambient Atmospheric Condition Ratings	
Operating Temperature	32 ˚F to 122°F (0˚ C to 50˚C) (DC powered units) 14°F to 158°F (-10° C to 70°C) (AC powered units)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)
Humidity	20% to 80% relative humidity (non-condensing) across the operating temperature range
Dimensions	
Height x Width x Depth	1.7 x 17.1 x 9.5 in (4.318 x 43.434 x 24.13 cm)
Weight	6-7 pounds (2.722- 3.175 kg) depending on the model

Table A.2 Technical Specifications for the ACS800 Advanced Console System Hardware

Category	Value
General Information	
CPU	Dual Core ARM Cortex-A9 @ 766 MHz
Memory	1GB DDR3L / 16GB eMMC FLASH
Interfaces	• Two dual media 1000Base-TX Copper ports • Eight serial ports with autosensing and switching support of Cyclades and Cisco pinouts • All eight ports support RS232/422/485 multi-protocol with autosensing and switching support of Cyclades and Cisco pinouts in RS232 mode • One serial console port • Four USB 2.0 host ports • V.92/56K analog MODEM port • 1-Wire interface for external sensors • Single RJ45 connector with four digital inputs for contact closure sensors • Digital output connectors providing four output signals.
Power Information	
Power Supply	Internal 100-240 VAC, 50/60 Hz
Power Consumption	Nominal voltage 120 VAC: Typical 80.5mA/3.5W, Maximum 306mA/17W Nominal voltage 240VAC: Typical 60mA/3.75W, Maximum 191mA/17W
Ambient Atmospheric Condition Ratings	
Operating Temperature	-4°F to 158°F (-20°C to 70°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)
Humidity	20% to 80% relative humidity (non-condensing) across the operating temperature range
Dimensions	
Height x Width x Depth	1.3 x 8.38 x 7.16 in (3.302 x 21.2852 x 18.1864 cm)
Weight	3.8 pounds (1.72365 kg)

Appendix B: Zero-touch provisioning

The zero-touch provisioning feature is an extension of the console system's BootP configuration retrieval and is a method for deploying many console systems into an environment. You will need a valid DHCP server and TFTP server to use zero-touch provisioning. You can configure your DHCP servers to instruct newly introduced console systems to download a template configuration and upgrade/downgrade firmware.

Setting up the DHCP/TFTP/configuration files should take only a few minutes and will potentially save hours of configuration time for console systems subsequently added to your network. After the provisioning step is completed, console systems can be accessed individually for any post-provision configuration desired (for example, assigning a static IP and a hostname).

With zero-touch provisioning, console systems can be automatically configured and upgraded after they are booted and initialized. This helps facilitate the introduction and installation of the console system into the existing network.

An administrator can view a log of zero-touch configurations by clicking *Monitoring-Zero-touch Log* from the sidebar of the Expert tab.

B.1 Zero-touch provisioning configuration file

In order to utilize the zero-touch provisioning feature, an administrator must first save a console system's configuration file on a remote server. The configuration file will be referenced by the setup file that will be created for zero-touch provisioning. For information on creating and saving a configuration file, see Configuration files on page 17.

NOTE: Parameters in the configuration file will apply to all console systems receiving the file. If you do not want a parameter to apply to all console systems, for example a host name, make sure you comment it out by entering a pound sign (#) in front of the parameter.

B.2 Setup file

Once the configuration file has been saved on a remote server and the DHCP server has been configured, an administrator needs to create a setup file. The setup file is used by the console system to identify configuration parameters and important provisioning information, such as the firmware image filename, configuration filename and the IP address for the remote server where the configuration file has been saved. The setup file needs to be stored on a server accessible via tftp or wget. The address of the server is sent in the DHCP offer message.

NOTE: It is recommended you store the setup file in the root folder if you're storing it on a TFTP server.

The following is an example of the setup file.

```
ONE_TIME_CONFIG=yes
FIRMWARE_VERSION=2.12.4
FIRMWARE_FILENAME=/tftpboot/firmware_acs8_2.12.4.fl

FIRMWARE_SERVER_IP=192.168.8.100
FIRMWARE_SERVER_PROTOCOL=tftp
CONFIG_FILENAME=/tftpboot/acs8000.cfg
CONFIG_SERVER_IP=192.168.8.100
CONFIG_SERVER_PROTOCOL=tftp
```

Table A.3 Setup File Descriptions

Parameter	Description
ONE_TIME_CONFIG	When the parameter is set to Yes, the configuration file is retrieved by the console system on the initial boot; it is not sent on subsequent boots. When set to No, the configuration file is retrieved by the console system each time it is booted.
FIRMWARE_VERSION	The version of the firmware to be sent to the appliance.
FIRMWARE_FILENAME	The path and file name of the firmware.
FIRMWARE_SERVER_IP	The IP address or hostname of the server hosting the firmware.
FIRMWARE_SERVER_USERNAME	If the firmware is hosted on a secure server, the credentials to access the server.
FIRMWARE_SERVER_PASSWORD	
FIRMWARE_SERVER_PROTOCOL	The protocol of the server used to host the firmware. Supported protocols include tftp, ftp, stfp, scp and wget.
CONFIG_FILENAME	The path and file name of the of the configuration file.
CONFIG_SERVER_IP	The IP address or hostname of the server hosting the configuration file.
CONFIG_SERVER_USERNAME	If the configuration file is hosted on a secure server, the credentials to access the server. In most cases, the credentials will be required. The username is plain text, however the password must be encrypted.
CONFIG_SERVER_PASSWORD	
CONFIG_SERVER_PROTOCOL	The protocol of the server used to host the configuration file. Supported protocols include tftp, ftp, stfp, scp and wget.

Password encryption

An encrypted hash of a password should be created for the FIRMWARE_SERVER_PASSWORD or CONFIG_SERVER_PASSWORD parameters. The hash needs to be generated from a Linux environment running openSSL. Enter the following commands at a Linux command prompt or on a console system's shell, as shown. Then enter the resulting hash password into the setup file for the defined server type.

```
echo ACS6000KEYAVOCENTEMERSON > mykey
echo <MyPassword> | openssl enc -base64 -salt -aes-256-cbc -pass file:./mykey
```

NOTE: In the preceding example, replace <MyPassword> with a valid password.

B.3 Copying the setup file to a server

After creating the setup file, it must be copied to a TFTP server. The following example shows what to enter in your system to copy the files to your server and then verify that the console system can download the file.

Copying the Setup File to a TFTP server:

```
Example: tftpd-hpa
Default TFTP root directory /var/lib/tftpboot
~$ sudo cp zerotouch.setup /var/lib/tftpboot
```

B.4 Obtaining the setup file

After obtaining the IP addresses for both the console system and the TFTP server where you uploaded the setup file, the zero-touch provisioning process will attempt to download the setup file. Once the console system downloads the setup file, it will use the information contained in the file to obtain the image and/or process the configuration of the console system.

B.5 DHCP server configuration

During the boot process, the console system may issue a request, if needed, for an IP address assignment. During this process, the DHCP server will query the DNS server to get the location of the TFTP or HTTP server where the setup file resides. An administrator can, if desired, create an entry on the DHCP server that uniquely identifies a specific console system or range of console systems. This entry filters which console systems are provisioned.

An administrator needs to configure two options. Option 66 defines the hostname or IP address of the TFTP server where the setup file resides. Option 67 defines the name of the setup file (for example acszero.cfg).

To configure Options 66 and 67:

1. Using the Windows Server Manager or DHCP tools snap-in Microsoft Management Console (MMC), open your DHCP server console.
2. In the left panel of the DHCP server window, click *IPv4*.
3. Right-click on *Server Options* and click *Configure Options* to configure a global scope.

   -or-

   Right-click on *Scope Options* and click *Configure Options* to configure a single scope.
4. Click on Option *066* to enter the location of the server that will host the setup file.
5. Enter the host name for the TFTP server.
6. Click on Option *067* to enter the name of the setup file.

An administrator can use two additional DHCP options to filter zero-touch provisioning for select console systems. Option 60 defines the vendor class, Avocent_ACS800/8000<serial number of the console system>. Option 61 defines the MAC address of the console system.

To create Options 60 and 61 (optional):

1. Using the Windows Server Manager or DHCP tools snap-in MMC, open your DHCP server console.
2. In the left panel of the DHCP window, click *IPv4*.
3. From the tab bar, click *Action*, then click *Set Predefined Options* from the pull-down menu.
4. Under the Options Class, select *DHCP Standard Options*, then click *Add*.

5. Enter a name for the option in the Name field, select *String* from the Data type drop-down menu, enter **060** in the Code field and enter a description for the option. Click *OK*.
6. Repeat step 5, entering **061** in the Code field.

DNS server

If the DNS scope option is not already defined on your DHCP server, and if the Option 66 entry is a hostname instead of an IP address, you can configure the DNS server.

To configure the DNS server:

1. Using the Windows Server Manager or DHCP tools snap-in MMC, open your DHCP server console.
2. In the left panel of the DHCP window, click *IPv4*.
3. Right-click on *Server Options* and click *Configure Options*.
4. Click Option *006* to define the DNS servers.
5. Enter the IP address in the appropriate field and click *Add*.

NOTE: If you enter the server name, the DNS server will resolve it.

Reservations

You can reserve IP addresses for each console system to be updated. A reservation is an IP address that will be always be issued to a specified console system when it renews its DHCP lease.

To reserve an IP address:

1. Using the Windows Server Manager or DHCP tools snap-in Microsoft Management Console (MMC), open your DHCP server console.
2. In the left panel of the DHCP window, click *IPv4*.
3. Right-click *Reservations*, then click *New Reservation*.
4. Enter a name for the reservation, the IP address to be assigned to the console system, the MAC address for the console system and a description in the appropriate fields.

NOTE: The console system's MAC address can be found on the bottom of console system.

5. Under Supported types, use the radio button to select either Both or DHCP only.
6. Click *Add*. The reserved IP address will be displayed in the Reserve table.

The following is an example of a Linux DHCP server configuration.

```
Example: ISC DHCP Server for Linux
Edit /etc/dhcp/dhcpd.conf ...
host acs8048 {
hardware ethernet 00:e0:86:12:34:56;
fixed-address 10.207.24.134;
filename "zerotouch.setup";
next-server 10.207.24.18;
```

B.6 Enabling zero-touch provisioning

An administrator can enable zero-touch provisioning from either the web UI or the CLI. Once zero-touch provisioning is enabled, you must clear the zero-touch provisioning log.

To enable zero-touch provisioning from the web UI:

1. From the sidebar of the web UI, click *System - Security - Security Profile*.
2. Under the Bootp Configuration Retrieval heading, check the boxes to enable Bootp and enable Live Configuration Retrieval.
3. Use the drop-down to select *eth0* as the Bootp Interface.
4. Click *Save*.
5. From the sidebar of the web UI, click *Monitoring - Zero-touch Log* then click *Clear Log*.

To enable zero-touch provisioning from the CLI:

1. Log in to the console system as the **root** user.
2. Type **cd system/security/security_profile/** to navigate to the security profile level.
3. Type set **bootp_enabled=yes**. and press **enter**.
4. Type set **bootp_interface=eth0**. and press **enter**.
5. Type set **enable_live_configuration_retrieval_(any_time_dhcp_renews)=yes** and press **enter**.
6. Type **commit** to save the configuration.
7. Type **cd /monitoring/zero-touch_log/** to navigate to the zero-touch log level.
8. Type **clear_log**. Type **Yes** when prompted if you want to clear the zero-touch provisioning log.

Appendix C: Bootp Configuration Retrieval

You can set your console system to be reconfigured during boot or at IP renewal.

To generate configuration to be retrieved:

1. Click *System Tools - Save Configuration* and save the configuration to either an FTP site or locally.

   -or-

   Use the list_configuration command to get the CLI template scripts, edit the configuration of the console system and save it as a text file.

   -or-

   Edit a file with CLI commands and save it.
2. Transfer the saved file to a DHCP server.
3. Configure the DHCP server to transfer the configuration file to the console system.

To reconfigure a console system with bootp:

1. Click *System - Security - Security Profile*. Under the Bootp Configuration Retrieval heading, ensure *Enabled* box is checked.
2. Uncheck the *Enable Live Configuration* box. The saved configuration is retrieved and applied on the next reboot.

   -or-

   Ensure the *Enable Live Configuration* box is checked. The saved configuration is retrieved and applied on the next IP renewal.

NOTE: You must configure your DHCP server in order to transfer the configuration file to your console system.

Appendix D: Recovering a Console System Password

To recover the console system's root password:

1. Connect directly to the console system’s CONSOLE port.
2. Turn the console system off, then on again.
3. Press the **Spacebar** to access the uboot prompt.
4. Type **hw_boot single** and press **Enter**.
5. The console system will boot into single-user mode. Type **passwd** and press **Enter**.
6. Enter the new password and confirm.
7. Type **reboot** and let the console system boot normally.

Appendix E: SSH Setup Allowing RSA Keypair Authentication Instead of a Username/Password

To set up a client Linux system to access the ACS800/8000 Advanced Console System:

1. On the console system, create a new admin user. For example: acsadmin.
2. Add the new user to the admin and shell-login-profile groups.
3. On your Linux-client-system, generate a key pair to use for ssh access to your console system.

```
ssh-keygen -t rsa -b 4096 -C "acsadmin" -f ~/.ssh/acsadmin-id_rsa
```

4. Press **Enter** twice to not install a pass phrase for this keypair on your server,

   -or-

   Enter a pass phrase

NOTE: Note: these two files are created by the ssh-keygen above:

```
$HOME/.ssh/acsadmin-id_rsa
$HOME/.ssh/acsadmin-id_rsa.pub
```

5. On your Linux-client-system, add lines similar to the ones below to your $HOME/.ssh/config file:

```
Host acsadmin132
HostName <IP address of the console system> for example, 10.207.24.132
User acsadmin
IdentityFile ~/.ssh/acsadmin-id_rsa
```

6. Log in to the console system via SSH as the user **acsadmin** (the new user).
7. Use the four following commands to install the public key for the acsadmin account on the console system.

```
mkdir -p ~/.ssh
touch .ssh/authorized_keys
chmod 600 .ssh/authorized_keys
ssh username@linuxclientsystem "cat .ssh/acsadmin-id_rsa.pub" >> .ssh/authorized_keys
```

For example for the ssh command

```
ssh adminuser@10.207.24.28 "cat .ssh/acsadmin-id_rsa.pub" >> .ssh/authorized_keys
```

8. From the *System - Security - Security Profile* tab of the web UI, uncheck the box to disable *SSH allows authentication via username/password*. The next SSH login from your Linux-client-system to the console system will succeed using the keypair and you will not be prompted for a password.

NOTE: Disabling this feature will prevent any user who does not have a keypair established on both the client and the console system from logging in to the console system via SSH. You also will not be able to launch serial sessions from the web UI, since those require username/password authentication.

An example ssh login command using the given.ssh/config host entry is: ssh acsadmin@acsadmin132.

Appendix F: Port Information for Communication with the DSView Software

The following ports on an Avocent® ACS800/8000 advanced console system can accept connections from the DSView management software:

- TCP port 3502 (https)
- TCP port 3871 (adsap2)
- UDP port 3211 (aidp)
- TCP port 22 (sshd)

The following ports in the DSView software can accept connections from the console system:

- TCP port 4122 (default: SSH server)
- TCP port 4514 (default: data logging or Syslog server)

Appendix G: Accessing a Console System with a DSView Software Installation via Dial-up

When a DSView software user establishes a serial session, the following events occur:

- The user selects a serial port to access.
- A viewer is downloaded from the DSView server to the user's workstation.
- The DSView software passes information to the viewer, such as an authorization key, the IP address and serial port of the console system.
- The viewer then accesses the serial port of the console system through an SSH session by passing the authorization key obtained from the DSView server.
- The serial session begins.

To ensure constant connectivity, a DSView server can be configured out of band (OOB) that will allow it to call a console system via modem in the event of a network or Internet failure.

G.1 Installing DSView software out of band

The DSView server must be running on hardware that has a connected modem, and the console system must have a built-in modem or access to a modem via USB or serial port.

For this installation, the DSView server must be the central point of reception of both the packets leaving the downloaded viewer and the console system. To ensure this, Proxy mode must be configured within the DSView software. The viewer will then point to the DSView server (not the console system) to establish the SSH connection. The DSView server would then route the packets by changing both the source and destination IP addresses and act as a middle point of communication.

Under normal operating conditions, packets received from the serial viewer would route through the DSView server via Ethernet. In an error state, the DSView server would detect that the normal path to the console system was interrupted and would dial out to the console system, pass authentication and establish a PPP connection. Packets that would normally pass via Ethernet would instead be routed via PPP.

Because of the speed differences between Ethernet and dial-up, performance would be notably slower. Multiuser connections would further degrade performance and are not recommended. For this reason, dial-up backup is recommended as an emergency backup feature only.

G.2 Configuring dial-up for a console system

To configure dial-up to a console system within the DSView software:

1. In a Units view window containing appliances, select the ACS 800/8000 you want to configure. For dial-in with callback, you must first select *DSView Server - Properties - DSView Modem Sessions* under the System tab and enter the the phone number assigned to the DSView server in the Analog Phone Number field.
2. Select *DSView Settings - Dial-up,* and click *Enable Dial-up*.
3. Select *Modem Type - Analog*.
4. Enter the phone number for the console system you want to use.
5. Enter the PPP User and select the PPP Auth Protocol in the appropriate fields.
6. For dial-in with callback, enable the dial-back checkbox.
7. Select *DSView Settings - Dial-up - PPP Password*, then enter and confirm the password needed to access the ACS 800/8000 console system.
8. Select *DSView Settings - Dial-up - IP Addresses*.

9. Click *Generate Automatically* to set the IP address automatically, or enter the PPP Local IP address and Appliance IP address manually.
10. Select DSView Settings - Dial-up and click Save.
11. To configure a console system to receive the dial-up connection within the DSView software:
12. In a Units view window containing appliances, select the ACS 800/8000 you want to configure.
13. For the internal modem, select *Ports - Auxiliary Ports* and select the modem.
14. Select DSView Settings - Dial-up and click *Push Configuration*.

NOTE: The following step is only required if *CHAP* was selected in the PPP Auth Protocol field in the DSView software Settings Dial-up window.

15. Log in to the CLI of the console system and access the Linux shell. Edit the /etc/ppp/chap-secrets and add a line in the format, where the first column should have the PPP user and the third column should have the PPP password as is shown in the following example:

    ```
    pppuser * "ppppassword" *
    ```

Appendix H: Internal Modem

Some models of the console system come equipped with an internal modem. This modem is used to originate and answer phone calls and establish communication with other modems to transmit data.

Controlling the modem's functions is done by using the "AT" commands. These commands are used to instruct the modem to perform functions such as dialing or answering calls and are normally automatically issued by communication software. However, for some applications, custom software may have to be written due to the absence of a normal operating system.

The modem will automatically accept and process AT commands at most standard DTE (Data Terminal Equipment) speeds and parity settings. For each command issued, the modem will respond with a result code to inform you of the modem's status. The format of a basic AT command and result code is as follows:

AT<Command><CR>

OK

AT = Attention.

<Command> = any valid command

<CR> = Carriage Return or Enter key

OK = Result Code

Table A.4 Sample Command String

Command	Description
ATDT7678900<CR>	Instructs the modem to dial the number 7678900 and attempt to connect to the remote device.
ATS0=2<CR>	Enables auto answer option. When the modem detects a ring, it will attempt to answer after two rings.

Table A.5 Basic AT Commands

Command	Description
ATA/	Repeat the previous command.
ATA	Answer.
ATB0	CCITT operation at 300 or 1200 bps.
ATB1	Bell operation at 300 or 1200 bps (default).
ATD	Dial.
ATD0-9	Dial the DTMF digits 0 to 9.
ATDA-D	Dial the DTMF digits A, B, C and D.
ATDP	Select pulse dialing; effects current and subsequent dialing.
ATDT	Select tone dialing; effects current and subsequent dialing.
ATD!	Flash: go on-hook by time defined by S29.
ATDW	Wait for dial tone detection before dialing a number. If no dial tone is detected within the time specified by S7, the modem aborts the rest of the sequence, goes on-hook and generates an error message.
ATD@	Wait for five seconds of silence before proceeding with next dialing string and then complete handshake sequence.
ATD,	Pause. The modem pauses for a time specified by S8 before dialing the number. Most often used when dialing an outside line through a PBX.
ATD;	Return to the command mode after processing the command.
ATE0	Disables the command echo.
ATE1	Enables the command echo (default).
ATH0	Hang up.
ATH1	Forces the modem off-hook.
ATI0	Reports product code.
ATI2	Reports OK (for software compatibility).
ATI3	Reports the firmware version of the modem. Example: CX810801-V90.
ATL0	Sets the speaker volume off.
ATL1	Sets the speaker volume low (default).
ATL2	Sets the speaker volume medium.
ATL3	Sets the speaker volume high.
ATM0	Speaker is always off.
ATM1	Speaker is on during call establishment but goes off when carrier is detected (default).
ATM2	Speaker is always on.
ATM3	Speaker if off during dialing and when receiving carrier but on during answering.
ATQ0	Enables result codes to the DTE (default).
ATQ1	Disables result codes to the DTE.
ATSr	Establishes S-register “r” as the default register.
ATSr=n	Sets S-register “r” to the value “n.”
ATSr?	Reports the value of S-register “r.”
ATV0	Enables short-form result codes.
ATV1	Enables long-form result codes.

Table A.5 Basic AT Commands (continued)

Command	Description
ATW0	Upon connection, the modem reports only the DTE speed (for example, CONNECT 9600). Subsequent responses are disabled (default).
ATW1	Upon connection, the modem reports the modulation type, line speed, the error correction protocol and the DTE speed. Subsequent responses are disabled.
ATW2	Upon connection, the modem reports DCE speed (for example, CONNECT 2400). Subsequent responses are disabled.
ATX0	Ignores dial and busy tone. Sends CONNECT message when a connection is established by blind dialing.
ATX1	Disables monitoring of busy tones. Sends only OK, CONNECT, RING, NO CARRIER and ERROR messages. If busy tone detection is enforced and busy tone is detected, NO CARRIER will be reported instead of BUSY. If dial tone detection is enforced or selected and dial tone is not detected, NO CARRIER will be reported instead of NO DIALTONE.
ATX2	Disables monitoring of busy tones. Sends only OK, CONNECT, RING, NO CARRIER, ERROR, NO DIALTONE and CONNECT XXXX. If busy tone detection is enforced and busy tone is detected, NO CARRIER, will be reported instead of BUSY. If dial tone detection is enforced or selected and dial tone is not detected, NO CARRIER will be reported instead of NO DIALTONE.
ATX3	Enables monitoring of busy tones. Sends only OK, CONNECT, RING, NO CARRIER, ERROR, NO DIALTONE and CONNECT or CARRIER XXXX. If dial tone detection is enforced and dial tone is not detected, NO CARRIER will be reported.
ATX4	Enables monitoring of busy tones. Sends all messages (default).
ATZ0	Soft reset.
AT&C0	DCD remains on at all times.
AT&C1	DCD follows the state of the carrier (default).
AT&D0	Ignores DTR.
AT&D1	Enters the escape mode when ON-to-OFF transition is detected on DTR.
AT&D2	Hangs up, assumes command state and disables auto answer upon detecting ON-to-OFF transition of DTR (default).
AT&D3	ON-to-OFF transition causes the modem to perform a soft reset. It is the same as if an ATZ command is issued.
AT&F	Restores factory configuration.
AT&G0	Disables guard tone (default).
AT&G1	Enables 550-Hz guard tone.
AT&G2	Enables 1800-Hz guard tone.
AT&K0	Disables flow control.
AT&K3	Enables RTS/CTS flow control (default for data modes).
AT&K4	Enables XON/XOFF flow control.
AT&K5	Supports transparent XON/XOFF flow control.
AT&P0	39/61 make/break ratio at 10 pulses per second (default).
AT&P1	33/67 make/break ratio at 10 pulses per second.
AT&P2	39/61 make/break ratio at 20 pulses per second.
AT&P3	33/67 make/break ratio at 20 pulses per second.
AT&Q0	Selects direct asynchronous operation.
AT&Q5	Modem will try an error-corrected link.
AT&Q6	Selects asynchronous operation in normal mode (allows speed buffering and flow control but no error correction).
AT&V	Displays modem's current configuration. When this command is entered, the modem will display its current command and register settings.
AT%C0	Disables data compression.
AT%C1	Enables MNP 5 data compression.

Table A.5 Basic AT Commands (continued)

Command	Description
AT%C2	Enables V.42 bis data compression (sets S46 bit 1).
AT%C3	Enables V.42 bis and MNP 5 data compression (default).
AT%E0	Disables line quality monitor and auto-retrain.
AT%E1	Enables line quality monitor and auto-retrain.
AT%E2	Enables line quality monitor and fallback/fall-forward (default).
AT%L	Line signal level. Returns a value that indicates the received signal level. Example, 009 = -9dBM.
AT%Q	Line signal quality. Reports line signal quality (DAA-dependent). Returns higher order byte of the EQM value. Based on EQM value, retrain or fallback/fall-forward may be iniated if enabled with AT%E1 or AT%E2 commands.
AT+MS	Select/force modulation.

H.1 AT+MS modulation selection

This extended-format compound parameter controls the manner of operation of the modulation capabilities in the modem. It accepts six sub-parameters:

+MS=<carrier>, <automode>, <min_tx_rate>, <max_tx_rate>, <min_rx_rate), <max_rx_rate><CR>.

To read the current settings, enter AT+MS?<CR>

Table A.6 +MS Command Supported Rates

Modulation	Carrier	Description
Bell 103	B103	300
Bell 212	B212	1200
V.21	V21	300
V.22	V22	1200
V.22 bis	V22	2400 or 1200
V.23	V23C	1200rx/75tx or 75rx/1200tx
V.32	V32	9600 or 4800
V.32 bis	V32B	14400, 12000, 9600, 7200 or 4800
V.34	V34	33600, 31200, 28800, 26400, 19200, 16800, 14400, 12000, 9600, 7200, 4800 or 2400
V.90	V90	56000, 54667, 53333, 52000, 50667, 49333, 48000, 46667, 45333, 42667, 41333,, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000
K56flex	K56	56000, 54000, 52000, 50000, 48000, 46000, 44000, 42000, 40000, 38000, 36000, 34000, 32000
V92 downstream	V92	56000, 54667, 53333, 52000, 50667, 49333, 48000, 46667, 45333, 42667, 41333,, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000
V92 upstream	V92	48000, 46667, 45333, 42667, 41333,, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000, 26667, 25333, 24000

H.2 Set telephone extension option

This command enables/disables “line-in-use” and “extension pickup” options.

Table A.7 Set Telephone Extension Options

-STE=n Value	Extension Pickup	Line-In-Use
0 (default)	Disabled	Disabled
1	Disabled	Enabled
2	Enabled	Disabled
3	Enabled	Enabled

If the line is in use and the modem receives an ATDT command to dial out, the modem will not go off hook and will display the "LINE-IN-USE" result code. If the modem is off hook and the extension is picked up, the modem will drop the connection and display the "OFF-HOOK INTRUSION" result code.

H.3 AT S registers

The S registers use the following format: ATSr=n<CR> where the "r" is the S register number and "n" is the parameter to set it to. To read the current contents of an S register, issue an ATSr?<CR> command where "r" is the register in question. The modem will then display the value of the S register.

Table A.8 AT S Registers

Register	Range	Units	Default	Description
S0	0-255	Rings	0	Ring to answer on. ATS0=1<CR> means answer call on first ring detected.
S1	0-255	Rings	0	Number of rings counted.
S2	0-127	ASCII	43	Escape code character.
S3	0-127	ASCII	13	Command terminator<CR>.
S4	0-127	ASCII	10	Line feed character.
S5	0-127	ASCII	8	Backspace character.
S6	2-255	Seconds	2	Wait time for dial-tone detection.
S7	1-255	Seconds	50	Wait time for carrier.
S8	0-255	Seconds	2	Pause time for coma in dial string.
S10	1-255	.1sec	14	Loss of carrier to hang up delay.
S11	50-255	.01sec	85	DTMF tone duration.
S12	0-127	1/50 sec	50	Escape code guard time.
S24	0-255	1sec	0	Sleep mode inactivity timer.
S29	0-255	10mS	70	Hook flash dial modifier time.
S30	0-255	10Sec	0	Inactivity disconnect timer.
S95			0	Result code control.

H.4 Basic modem result codes

There are basic codes the modem will issue in response to processing an AT command. Result codes may be displayed either in word (V1) or numeric (V0) format by using the Vn command. The Qn command controls if result codes are issued (Q0) or not issued (Q1). The Xn, Wn commands and register S95 determines which result code format the modem will display to indicate the type of connection established. There are more than 300 codes. The most commonly used are listed in the table below.

Table A.9 Basic Result Code Listing

Numeric	Verbose	Description
0	OK	The modem has received and acknowledged the command.
1	CONNECT	Connection made at 300bps or extended result codes are off (X0).
2	RING	An incoming ring signal has been detected.
3	NO CARRIER	This result code reflects either an intended disconnect or a failure to complete a connection.
4	ERROR	An invalid command was issued to the modem.
5	CONNECT 1200	Indicates a 1200bps line or DTE connection.
6	NO DIALTONE	
7	BUSY	The modem has detected a busy tone.
8	NO ANSWER	After S7 time has elapsed, the remote server never answered.
10	CONNECT 2400	Line speed or DTE connection at 2400bps.
12	CONNECT 9600	Line speed or DTE connection at 9600bps.
15	CONNECT 14400	Line speed or DTE connection at 14400bps.
16	CONNECT 19200	Line speed or DTE connection at 19200bps.
17	CONNECT 38400	Line speed or DTE connection at 38400bps.
18	CONNECT 57600	Line speed or DTE connection at 57600bps.

H.5 Digital line guard

The modem has an optional Digital Line Guard Circuit that automatically detects an over current situation on the Tip and Ring pins. When the modem goes off hook, it will immediately check the current on the Tip and Ring pins. If the current exceeds 150 mA, the modem will display the “DIGITAL LINE DETECTED” result code and then go back on hook. The modem will continue to display this result code until normal current is detected on the Tip and Ring pins during an off hook condition. The DLG feature will protect the modem in case it is accidentally connected to a Digital Telephone Line.

H.6 Sleep mode operation

The modem can be set to enter the low power sleep mode by setting ATS24=n. In this case, “n” is time, in seconds, that the modem will operate in normal mode with no detected telephone line or DTE line activity before entering low power sleep mode. The timer is reset upon any DTE or telephone line activity. If S24 is set to zero, the modem will never enter the low power sleep mode.

H.7 Disconnecting a call

There are several ways to disconnect a call. Below are the choices.

Resetting the modem’s power or toggling the Reset Line (Pin #12) will disconnect and put the modem back into the OFF line state.

An ON to OFF transition of the DTR signal (Pin #4) will also disconnect the modem. If you use this method, check to make sure that the DTR command is set to &D2 or &D3 and not forced (&D0).

The remote device can also cause the modem to disconnect. If the remote modem disconnects your modem will automatically sense the loss of the carrier signal and return to the OFF line state.

The ATH or ATZ commands can also be used to disconnect a call. In order to issue a command to the modem when it is On Line, the modem must be placed into the On Line Command State. This is accomplished by issuing a special escape sequence. The default value of this three digit escape sequence is the "+" character (see S2 to change). The "+++" is protected by a one-second delay before and after it is sent (see S12 to change the time) When the modem detects the escape sequence, the OK result Result code will be displayed and the modem is in the On Line Command State. The ATH or ATZ command can now be issued to disconnect the call.

H.8 Selecting country codes

Setting the modem's country code is done by with the +GCI command. To change to one of the 30 available countries, issue the AT+GCI=n command where "n" is one of the two digit country codes. This command must be issued each the modem is turned on. It will not automatically store or save this setting. It should be part of the Initialization string.

Example: AT+GCI=00<CR> Meaning: Change country code to Japan.

OK Meaning: The modem has accepted the command and is

now configured to operate in Japan

AT+GCI?<CR> Meaning: Display current country code

+GCI:00 Meaning: (Japan is the current country selected).

OK

To view which countries are available in the modems firmware, enter AT+GCI=?<CR>.

The modem will display all of the possible two digit country codes available.

Table A.10 Country Codes List

Country	Code	Country	Code	Country	Code
Australia	09	Hong Kong	50	Poland	8A
Austria	0A	India	53	Portugal	8B
Belgium	0F	Ireland	57	South Africa	9F
Brazil	16	Italy	59	Singapore	9C
China	26	Japan	00	Spain	A0
Denmark	31	Korea	61	Sweden	A5
Finland	3C	Mexico	73	Switzerland	A6
France	3D	Netherlands	7B	Taiwan	Fe
Germany	42	Norway	82	TBR21	FD
United States	B5	United Kingdom	B4		

H.9 Using caller ID

The modem can be used to display certain information about incoming telephone calls. The modem can inform you of the date, time, telephone number and name associated with incoming calls. When the CID option is enabled, information will be displayed between the first and second incoming "RING." In order for this feature to work properly, the telephone line connected to the modem must subscribe to caller ID service offered by the local telephone company. A sample of the displayed information is shown below:

RING

DATE = 0513

TIME = 1346

NMBR = 408 767 8900

NAME = RADICOM RESEARCH

RING

The CID information can either be presented formatted as shown previously or unformatted. The +VCID and +VRID commands control the modem CID option.

Table A.11 Caller ID Information

Command	Parameter	Description
+VCID?	NA	Display current +VCID setting (0-2)
+VCID=	0	Disable caller ID reporting (default).
+VCID=	1	Enable caller ID with formatted presentation to the DTE.
+VCID+	2	Enable caller ID with unformatted presentation to the DTE.
+VRID=	0	Displays the formatted caller ID of the last received call.
+VRID+	1	Displays the unformatted caller ID of the last received call.

Appendix I: Regulatory Information Concerning the Analog Modem Installed in This Product

I.1 Analog Telecom Safety Warnings

Before servicing, disconnect this product from its power source and telephone network. Also:

- Never install telephone wiring during a lightning storm.
- Never install a telephone jack in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

I.2 Avertissements de sécurité télécom analogique

Avant de l'entretien, débrancher ce produit de son réseau d'alimentation et de téléphone. également:

- Ne jamais installer du câblage téléphonique pendant un orage électrique.
- Ne jamais installer de prises téléphoniques à des endroits mouillés à moins que la prise ne soit conçue pour de tels emplacements.
- Ne jamais toucher fils ou des bornes téléphoniques non isolés à moins que la ligne téléphonique n'ait été déconnectée au niveau de l'interface réseau.
- Faire preuve de prudence au moment d'installer ou de modifier des lignes téléphoniques.

I.3 International Modem Restrictions

Some dialing and answering defaults and restrictions may vary for international modems. Changing settings may cause a modem to become non-compliant with national regulatory requirements in specific countries. Also note some software packages may have features or lack restrictions that may cause the modem to become noncompliant.

U.S.A., 47 CFR Part 68 Telecom

1. This equipment complies with Part 68 of the 47 CFR rules and the requirements adopted by the ACTA (Administrative Council for Terminal Attachments). Located on this equipment is a label that contains, among other information, the registration number and Ringer Equivalence Number (REN) for this equipment or a product identifier in the format:

   For current products: US:AAAEQ##Txxxx.

   For legacy products: AU7USA-xxxxx-xx-x.

   If requested, this number must be provided to the telephone company.

2. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable 47 CFR Part 68 rules and requirements adopted by the ACTA. It's designed to be connected to a compatible modular jack that is also compliant.
3. The Ringer Equivalence Number (REN) is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##Txxxx. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.
4. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
5. The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.
6. If trouble is experienced with this equipment, please contact Vertiv at the address shown below for details of how to have the repairs made. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.
7. Manufacturing Information on telecommunications device (modem):

   Manufacturer: Multi-Tech Systems, Inc.

   Trade Name: Socket Modem SocketModem SocketModem

   Model Number: MT5692SMI

   Registration No: US:AU7MM01BMT5692SMI

   Ringer Equivalence: 0.1B

   Modular Jack (USOC): RJ11C or RJ11W or RJ45 (single line)

   Vertiv

   4991 Corporate Drive

   Huntsville, AL 35805 USA

   1-888-793-8763

I.4 Thailand Approval for MT5692SMI

This telecom device conforms to NTC1 requirements.

1NTC is the National Telecommunications Commission, Thailand’s telecommunications regulator.

“เครื ่ องโทรคมนาคมและอุ ปกรณ์ นี ้ มี ความสอดคล้ องตามข้ อก าหนดของ กทช.”

I.5 New Zealand Telecom Warning Notice

1. The grant of a Telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom’s network services.

   This equipment is not capable under all operating conditions of correct operating conditions of correct operation at the higher speed which it is designated. 33.6 kbps and 56 kbps connections are likely to be restricted to lower bit rates when connected to some PSTN implementations. Telecom will accept no responsibility should difficulties arise in such circumstances.

2. Immediately disconnect this equipment should it become physically damaged, and arrange for its disposal or repair.
3. This modem shall not be used in any manner which could constitute a nuisance to other Telecom customers.
4. This device is equipped with pulse dialing, while the Telecom standard is DTMF tone dialing. There is no guarantee that Telecom lines will always continue to support pulse dialing.

   Use of pulse dialing, when this equipment is connected to the same line as other equipment, may give rise to 'bell tinkle' or noise and may also cause a false answer condition. Should such problems occur, the user should NOT contact the Telecom Faults Service.

   The preferred method of dialing is to use DTMF tones, as this is faster than pulse (decadic) dialing and is readily available on almost all New Zealand telephone exchanges.

5. Warning Notice: No '111' or other calls can be made from this device during a mains power failure.
6. This equipment may not provide for the effective hand-over of a call to another device connected to the same line.
7. Some parameters required for compliance with Telecom’s Telepermit requirements are dependent on the equipment (PC) associated with this device. The associated equipment shall be set to operate within the following limits for compliance with Telecom’s Specifications:

For repeat calls to the same number:

- There shall be no more than 10 call attempts to the same number within any 30 minute period for any single manual call initiation, and
- The equipment shall go on-hook for a period of not less than 30 seconds between the end of one attempt and the beginning of the next attempt.
- For automatic calls to different numbers:
- The equipment shall be set to ensure that automatic calls to different numbers are spaced such that there is no less than 5 seconds between the end of one call attempt and the beginning of another.

8. For correct operation, total of the RN’s of all devices connected to a single line at any time should not exceed 5.

I.6 Japan Requirements

The modem conforms to (JATE) Japan Approval Institute for Telecommunications Equipment:

MT5692SMI – JATE Approval A09-0123001

Connect with Vertiv on Social Media

https://www.facebook.com/vertiv/

https://www.instagram.com/vertiv/

https://www.linkedin.com/company/vertiv/

https://www.twitter.com/Vertiv/

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