Avocent® ACS800/8000 Advanced Console System

Installations- und Bedienungsanleitung

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und sind möglicherweise nicht für alle Anwendungen geeignet. Es wurde jede Anstrengung unternommen, um die Richtigkeit und Vollständigkeit dieses Dokuments zu gewährleisten, Vertiv übernimmt jedoch keine Verantwortung für Schäden, die aus der Nutzung dieser Informationen entstehen, sowie für Fehler oder Auslassungen und lehnt jegliche Haftung hierfür ab. Verwenden Sie für die richtigen Methoden, Werkzeuge und Materialien zur Durchführung von Verfahren, die nicht ausdrücklich in diesem Dokument beschrieben sind, auf andere örtliche Praktiken oder Verfahren, sofern anwendbar.

Die in dieser Bedienungsanleitung behandelten Produkte werden von Vertiv hergestellt und/oder verkauft. Dieses Dokument ist Eigentum von Vertiv und enthält vertrauliche und geschützte Informationen im Besitz von Vertiv. Jegliches Kopieren, Verwenden oder Offenlegen ohne schriftliche Genehmigung von Vertiv ist strengstens untersagt.

Die Namen von Unternehmen und Produkten sind Marken oder eingetragene Marken der jeweiligen Unternehmen. Alle Fragen bezüglich der Verwendung von Markennamen sollten an den Originalhersteller gerichtet werden.

Website des technischen Supports

Wenn bei der Installation oder Verwendung dieses Produkts Probleme auftreten, schlagen Sie im jeweiligen Abschnitt dieses Handbuchs nach und versuchen Sie, das Problem anhand der beschriebenen Verfahren zu beheben.

Besuchen Sie https://www.vertiv.com/en-us/support/ für weitere Unterstützung.

INHALTSVERZEICHNIS

1 Einführung

Das Avocent® ACS800/8000 Advanced Console System dient als zentraler Punkt für den Zugriff und die Verwaltung der angeschlossenen Geräte, wie serielle Konsolen, Modems und Stromversorgungsgeräte. Das Konsolensystem unterstützt völlig standortunabhängig die sichere Remote-Verwaltung von Rechenzentren sowie die Out-of-Band-Verwaltung von IT-Ressourcen.

HINWEIS: Sofern nicht anders angegeben, beziehen sich Verweise auf ein Konsolensystem auf alle Modelle der 800/8000-Serie.

Das Konsolensystem bietet auf sichere Weise lokalen Zugriff (Konsolenport) und Remote-Zugriff (IP und DFÜ). Auf dem Konsolensystem wird das Betriebssystem Linux® mit einem persistenten Dateisystem im Flash-Speicher ausgeführt. Ein System-Upgrade kann mit einer lokalen Datei auf einem Computer, der an das Konsolensystem angeschlossen ist, erfolgen.

Mehrere Administratoren können gleichzeitig beim Konsolensystem angemeldet sein und die Web-Benutzeroberfläche (Weboberfläche), die Befehlszeile (CLI-Dienstprogramm) oder die DSView™ 4-Managementsoftware verwenden, um auf das Konsolensystem zuzugreifen und es zu konfigurieren.

HINWEIS: Sofern nicht anders angegeben, beziehen sich alle in diesem Dokument genannten Verweise auf die DSView-Software auf Version 4 oder neuer.

Je nach Modell verfügt das Konsolensystem über vier bzw. acht USB-Ports, die Modems, Speichergeräte, Netzwerkadapter, USB-Hubs und USB-Konsolengeräte unterstützen. Einige Modelle verfügen über einen SD-Kartensteckplatz zur Unterstützung eines zusätzlichen Speichergeräts.

Zwei Netzwerkports unterstützen Verbindungen mit mehreren Netzwerken oder können für Ethernet-Bündelung konfiguriert werden. Dies sorgt für Redundanz und eine höhere Zuverlässigkeit oder Netzwerk-Failover-Unterstützung.

Für die Einwahl und die sichere Rückwahl mit dem Point-to-Point-Protokoll (PPP) kann werkseitig ein optionales internes Modem installiert werden. Sie können zu diesem Zweck aber auch ein externes Modem an einen seriellen Port oder einen USB-Port anschließen.

Einige Modelle sind auch mit einer Antenne für Funkverbindungen ausgestattet.

1.1 Funktionsmerkmale und Vorteile

1.1.1 Zugriffsoptionen

Der sichere Zugriff ist über die folgenden Optionen für den lokalen Zugriff (analoger Konsolenport) und den Remote-Zugriff (digitales IP und DFÜ) möglich:

- LAN/WAN-IP-Netzwerkverbindung.
- DFÜ-Verbindung über ein werkseitig konfiguriertes internes Modem (optional) oder über ein Modem, das an einen der seriellen oder USB-Ports angeschlossen ist.
- Einige Modelle verfügen auch über eine Antenne für Funkverbindungen.
- Verbindung mit Zielgerät. Autorisierte Benutzer können eine Telnet-, SSH V2- oder Raw-Verbindung mit einem Zielgerät herstellen. Damit Verbindungen mit dem Zielgerät über Telnet oder SSH hergestellt werden können, muss der Telnet- oder SSH-Dienst im aktiven Sicherheitsprofil konfiguriert sein.

- Konsolenverbindung mit Konsolensystem. Administratoren können sich von einem lokalen Terminal anmelden oder von einem Computer, auf dem ein Terminalemulationsprogramm installiert ist und der mit dem Konsolenport verbunden ist und das CLI-Dienstprogramm verwenden kann. Bei der Anmeldung wird die Aufforderung (--:- cli->) des CLI-Dienstprogramms angezeigt.

Mehr als ein Administrator kann sich beim Konsolensystem anmelden und eine aktive CLI- oder Weboberflächen-Sitzung verwenden. In allen Sitzungen wird die folgende Warnmeldung eingeblendet, wenn die Konfiguration von einem anderen Administrator oder vom System geändert wird: *Die Konfiguration der Einheit wurde außerhalb Ihrer Sitzung geändert*. Nach Erhalt dieser Meldung muss jeder Administrator überprüfen, ob die während der Sitzung vorgenommenen Änderungen gespeichert wurden.

1.1.2 Web-Benutzeroberfläche (Weboberfläche)

Benutzer und Administratoren können die meisten Aufgaben über die Web-Benutzeroberfläche (Weboberfläche) ausführen, die über HTTP oder HTTPS aufgerufen werden kann. Die Weboberfläche kann unter Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome und Apple Safari auf jedem unterstützten Computer mit Netzwerkzugriff auf das Konsolensystem ausgeführt werden. Eine Liste der unterstützten Client-Browser und ihrer Versionen finden Sie in den Versionshinweisen.

HINWEIS: Wenn Sie über die Weboberfläche auf das Konsolensystem zugreifen, deaktivieren Sie keine zusätzlichen Dialoge, wenn Sie von Ihrem Browser dazu aufgefordert werden. Die Deaktivierung von Dialogen deaktiviert einige Funktionen der Weboberfläche.

1.1.3 Unterstützung für IPv4 und IPv6

Das Konsolensystem unterstützt die IPv4- und IPv6-Protokolle im Dual-Stack-Modus. Der Administrator kann über die Weboberfläche oder die CLI festlegen, dass entweder nur IPv4-Adressen oder IPv4- und IPv6-Adressen unterstützt werden. Die folgende Liste enthält Einzelheiten zur IPv6-Unterstützung im Konsolensystem:

- DHCP
- Sitzungen zum Einwählen und Hinauswählen (PPP-Verbindungen)
- DSView-Softwareintegration
- Ethernet-Schnittstellen eth0 und eth1
- Firewall (IP-Tabellen)
- HTTP/HTTPs
- Linux-Kernel
- Remote-Authentifizierung: Radius-, TACACS+-, LDAP- und Kerberos-Server
- SNMP
- SSH- und Telnet-Zugriff
- Syslog-Server

HINWEIS: IPSec wird mit IPv6 nicht unterstützt.

1.1.4 Flexible Benutzer und Gruppen

Für jeden Benutzer kann ein Konto auf dem Konsolensystem oder auf einem Authentifizierungsserver eingerichtet werden. Die Admin- und Stammbenutzer (admin und root) verfügen standardmäßig über Konten. Diese Benutzer können auch Konten für andere Benutzer hinzufügen und konfigurieren. Administratoren können den Zugriff auf Ports wahlweise beschränken, indem sie benutzerdefinierten Benutzergruppen oder einzelnen Benutzern entsprechende Berechtigungen zuweisen. Weitere Informationen finden Sie unter Benutzerkonten und Benutzergruppen auf Seite 72.

1.1.5 Sicherheit

Sicherheitsprofile bestimmen, welche Netzwerkdienste auf dem Konsolensystem aktiviert sind. Administratoren können entweder allen Benutzern den Zugriff auf aktivierte Ports gewähren oder den Zugriff beschränken, indem sie die Konfiguration von Gruppen- und Benutzerberechtigungen zulassen. Sie können auch ein Sicherheitsprofil auswählen. Ein Sicherheitsprofil regelt den SSH- und HTTP/HTTPS-Zugriff und bestimmt, welche Dienste (FTP, TFTP, ICMP, IPSec und Telnet) aktiviert sind. Administratoren können entweder ein vorkonfiguriertes Sicherheitsprofil auswählen oder ein benutzerdefiniertes Sicherheitsprofil erstellen. Weitere Informationen finden Sie unter Sicherheit auf Seite 23.

1.1.6 Authentifizierung

Die Authentifizierung kann auf verschiedene Weise erfolgen: lokal, über Einmalkennwörter (One Time Passwords, OTP), über einen Remote-Authentifizierungsserver auf Grundlage von Kerberos, , LDAP, RADIUS oder TACACS+ oder über einen DSView-Server. Das Konsolensystem unterstützt auch Remote-Gruppenautorisierungen für die Authentifizierungsmethoden LDAP, RADIUS und TACACS+. Auch Ausweichmechanismen (Fallback) sind verfügbar.

Die für das Konsolensystem oder für die Ports konfigurierten Authentifizierungsmethoden werden für die Authentifizierung aller Benutzer verwendet, die versuchen, sich über Telnet, SSH oder die Weboberfläche anzumelden. Weitere Informationen finden Sie unter Authentifizierung auf Seite 69.

1.1.7 VPN auf Basis von IPSec mit NAT-Traversal

Wenn IPSec im ausgewählten Sicherheitsprofil aktiviert ist, können Administratoren die VPN-Funktion verwenden, um sichere Verbindungen zu ermöglichen. Weitere Informationen finden Sie unter IPSec (VPN) auf Seite 34.

1.1.8 Paketfilterung

Administratoren können das Konsolensystem so konfigurieren, dass es Pakete ähnlich wie eine Firewall filtert. Die Paketfilterung wird von Ketten gesteuert, das heißt von benannten Profilen mit benutzerdefinierten Regeln. Die Filtertabelle des Konsolensystem enthält mehrere integrierte Ketten, die geändert, aber nicht gelöscht werden können. Administratoren können auch neue Ketten erstellen und konfigurieren.

1.1.9 SNMP

Wenn SNMP im ausgewählten Sicherheitsprofil aktiviert ist, können Administratoren den SNMP-Agenten (SNMP = Simple Network Management Protocol) auf dem Konsolensystem konfigurieren, der Anforderungen beantwortet, die von einer SNMP-Verwaltungsanwendung gesendet werden.

Der SNMP-Agent des Konsolensystems unterstützt SNMP V1/V2 und V3, MIB-II und Enterprise MIB. Weitere Informationen finden Sie unter SNMP-Konfiguration auf Seite 41.

HINWEIS: Die Textdateien mit der Enterprise MIB (ACS8000-MIB.asn) und der TRAP MIB (ACS8000-TRAP-MIB.asn) stehen auf der Einheit im Verzeichnis /usr/local/mibs zur Verfügung.

1.1.10 Datenprotokollierung, Benachrichtigungen, Alarme und Datenpufferung

Administratoren können die Datenprotokollierung, Benachrichtigungen und Alarme einrichten, damit sie bei Problemen per E-Mail, SMS, SNMP-Trap oder über die DSView-Software benachrichtigt werden. Weiterhin können Administratoren festlegen, dass gepufferte Daten lokal, an einem Remote-Speicherort oder mit der DSView-Managementsoftware gespeichert werden. Nachrichten über das Konsolensystem sowie verbundene Server oder Geräte können auch an Syslog-Server gesendet werden.

1.1.11 Stromverwaltung

Mithilfe des Konsolensystems können Benutzer, die zur Stromverwaltung berechtigt sind, den Strom ein- oder ausschalten sowie Geräte zurücksetzen, die an eine verbundene PDU (Power Distribution Unit, Stromverteilungseinheit) angeschlossen sind. Die Stromversorgungsgeräte können an jeden seriellen Port angeschlossen werden. Berechtigte Benutzer können weiterhin ein angeschlossenes USV-Gerät (USV = unterbrechungsfreie Stromversorgung) überwachen und steuern. Weitere Informationen finden Sie unter Stromverwaltung auf Seite 84.

1.1.12 Automatische Erkennung

Administratoren können die automatische Erkennung aktivieren, um den Hostnamen eines Zielgeräts, das an einen seriellen Port angeschlossen ist, zu ermitteln. Für die automatische Erkennung steht ein umfassender Bereich an standardmäßigen Test- und Antwortzeichenfolgen zur Verfügung. Administratoren können standortspezifische Test- und Antwortzeichenfolgen konfigurieren. Die automatische Erkennung kann auch über die DSView-Software konfiguriert werden.

1.1.13 FIPS-Modul

Die FIPS 140-Standards (FIPS = Federal Information Processing Standards, Bundesstandards für Informationsverarbeitung) sind von der US-Regierung entwickelte Standards für die Computersicherheit. Sie definieren die Anforderungen für kryptografische Module.

Das Konsolensystem verwendet ein eingebettetes kryptografisches Modul auf Grundlage des validierten kryptografischen FIPS 140-2-Moduls (Zertifikatsnummer 1747), das auf einer Linux ARM-Plattform ausgeführt wird. Weitere Informationen finden Sie unter FIPS-Modul auf Seite 25.

1.2 Beispielkonfigurationen

Die folgende Grafik und Tabelle veranschaulichen eine Avocent® ACS800/8000 Advanced Console System-Konfiguration mit allen möglichen Optionen. Die Optionen variieren je nach Modell und kein Modell verfügt über alle gezeigten Optionen.

Abbildung 1.1 Konfiguration für das ACS8000 Advanced Console System mit allen angezeigten Optionen

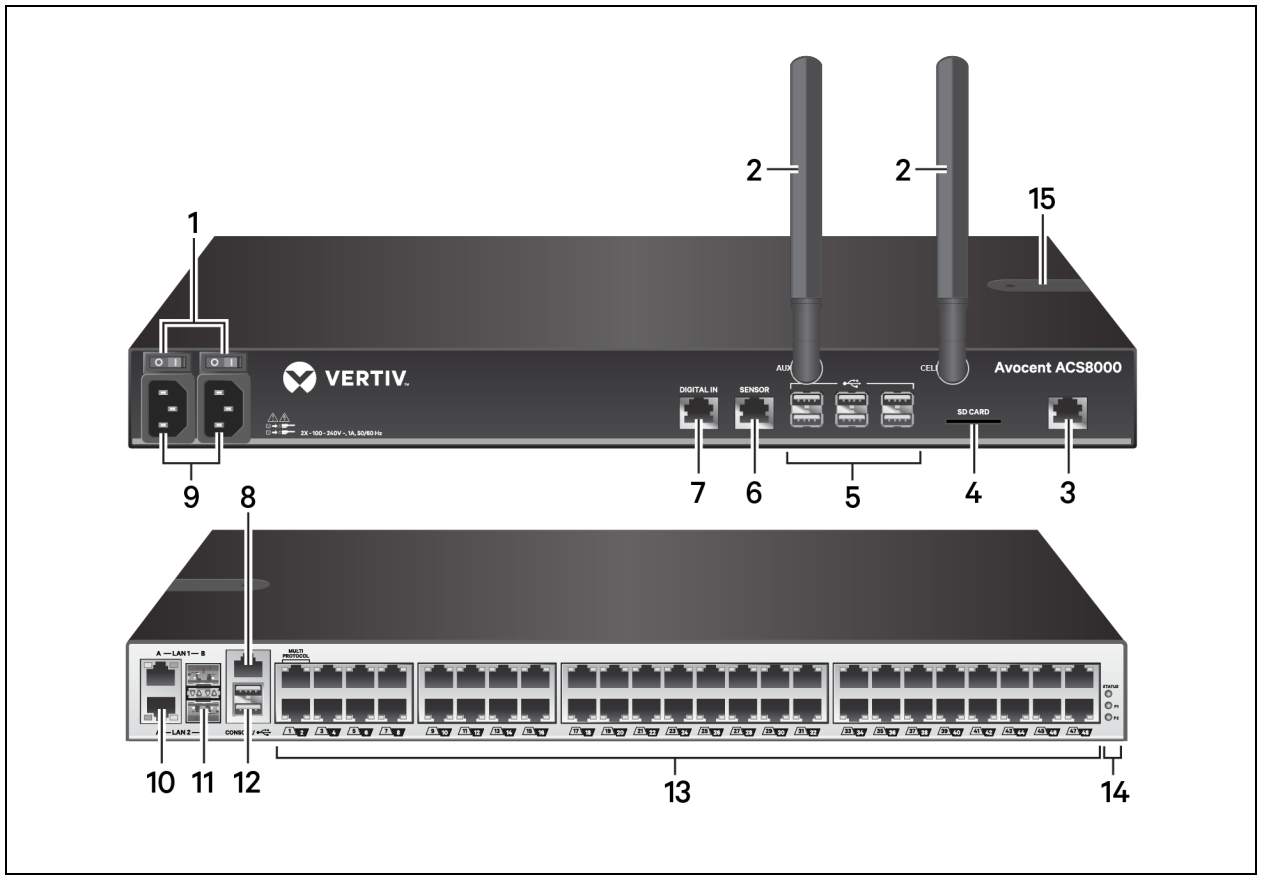


Tabelle 1.1 Konfiguration für das ACS8000 Advanced Console System – Beschreibungen

Nummer	Beschreibung
1	Netztasten (Doppelstromversorgung abgebildet).
2	Funkantennen für das Funkmodem (nicht bei allen Modellen verfügbar).
3	Anschluss einer Telefonleitung an den Modemport für das interne Modem.
4	SD-Kartensteckplatz (nicht bei allen Modellen verfügbar).
5	USB-Ports für unterstützte USB-Geräte (nicht bei allen Modellen verfügbar).
6	Sensorport für 1-Wire-Sensor für Umgebungsbedingungen (nicht bei allen Modellen verfügbar).
7	Digitaler Eingang für Sensoren für Rauch, Leck, Druck oder potenzialfreien Kontakt (nicht bei allen Modellen verfügbar).
8	Konsolenanschluss für den Anschluss eines Terminals oder einer Workstation. Das Konsolensystem wird mit einem Terminal oder Terminalemulator mit folgenden Sitzungseinstellungen konfiguriert: 9600, 8, N und 1 ohne Flusssteuerung.
9	Stromversorgung (Doppelstromversorgung abgebildet).
10/11	LAN-Ports. Die Ports auf der linken Seite sind für Verbindungen mit Kupferkabeln vorgesehen. Die Ports auf der rechten Seite eignen sich für Glasfaserkabel. Sie können einen oder zu Redundanzzwecken auch beide Netzwerkports verwenden, aber es kann jeweils nur ein LAN1- bzw. nur ein LAN2-Anschluss genutzt werden. Wenn beide LAN1- bzw. LAN2-Ports genutzt werden, hat die Glasfaserverbindung Priorität.
12	Zwei USB-Ports auf der Rückseite des Konsolensystems zum Anschluss weiterer USB-Geräte.
13	Serielle Ports. Schließen Sie die entsprechenden seriellen Geräte und Stromversorgungsgeräte mithilfe von CAT 5e- oder CAT 6-Kabeln und DB9- oder DB25-Konsolenadaptern an die seriellen Ports des Konsolensystems an.
14	Status-LEDs.
15	SIM-Kartensteckplatz

In der folgenden Abbildung und Tabelle werden die Multiprotokoll-Ports sowie die LEDs veranschaulicht.

Abbildung 1.2 Avocent® ACS8000 Advanced Console System Multiprotokoll-Ports und LEDs

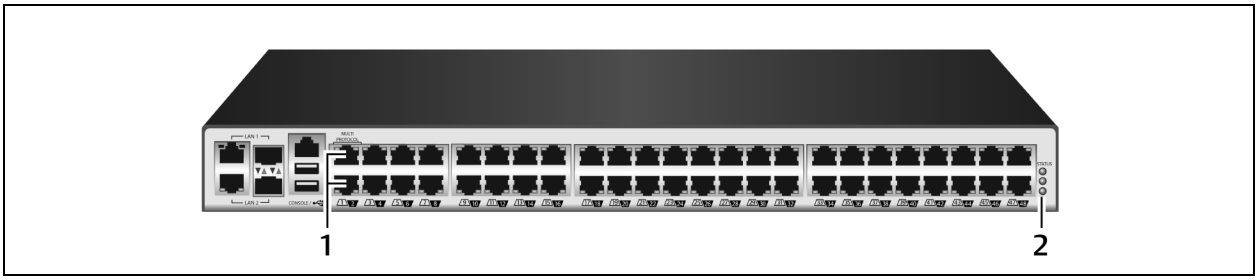


Tabelle 1.2 Multiprotokoll-Ports und LEDs – Beschreibungen

Nummer	Beschreibung
1	Multiprotokoll-Ports. Diese beiden Ports unterstützen zusätzlich zu Cyclades- und Cisco-Pinbelegungen auch RS422- und RS485-Pinbelegungen.
2	LEDs. Die STATUS-LED leuchtet grün, wenn das Starten und Initialisieren des Konsolensystems abgeschlossen ist. Die P1- und P2-LEDs zeigen eine aktive Stromversorgung an. P1 leuchtet grün, wenn die Stromversorgung 1 eingeschaltet ist. P2 leuchtet grün, wenn die Stromversorgung 2 eingeschaltet ist.

Abbildung 1.3 Einlegen der SIM-Karte

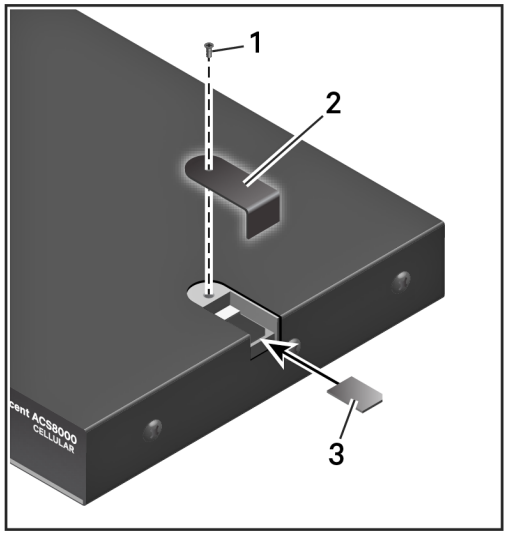


Tabelle 1.3 Einlegen der SIM-Karte – Beschreibungen

Element	Beschreibung
1	Entfernen Sie die Schraube, um die Abdeckung zu lösen. Sobald die Karte eingelegt ist, setzen Sie die Abdeckung wieder auf und setzen Sie die Schraube wieder ein.
2	Entfernen Sie die Abdeckung, um den SIM-Kartensteckplatz freizulegen. Setzen Sie die Abdeckung wieder auf, sobald die Karte eingelegt ist.
3	Legen Sie die Karte ein.

Abbildung 1.4 Typische Konfiguration für das ACS800 Advanced Console System

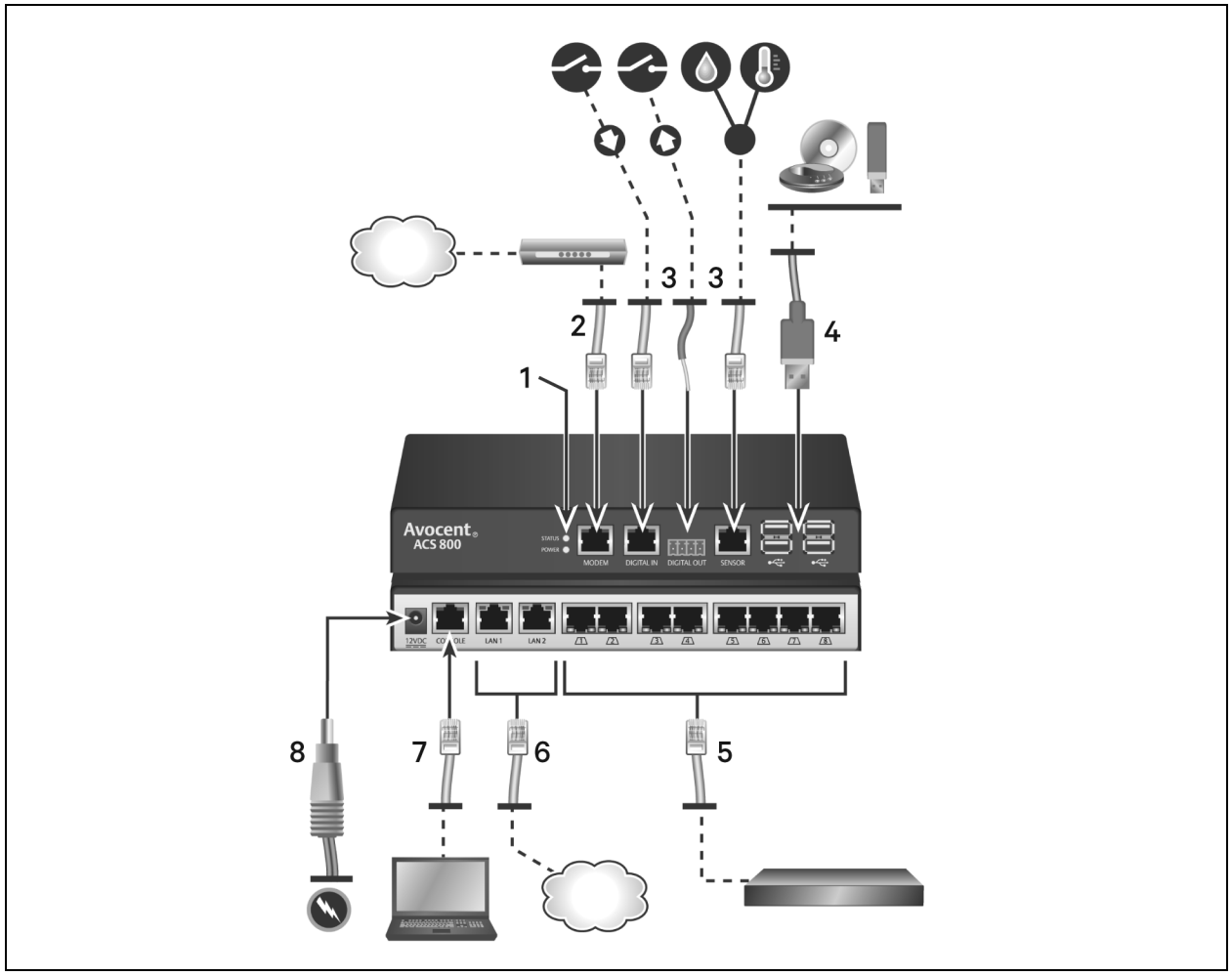


Tabelle 1.4 Typisches ACS800 Advanced Console System – Beschreibungen

Nummer	Beschreibung
1	LEDs. Die STATUS-LED leuchtet grün, wenn das Starten und Initialisieren des Konsolensystems abgeschlossen ist. Die Strom-LED leuchtet grün, wenn das Konsolensystem mit Strom versorgt wird.
2	Anschluss einer Telefonleitung an den Modemport für das interne Modem.
3	Sensorports für 1-Wire-Sensoren für Umgebungsbedingungen, Rauch, Leck, Druck oder potenzialfreien Kontakt.
4	USB-Ports für unterstützte USB-Geräte.
5	Serielle Ports. Schließen Sie die entsprechenden seriellen Geräte und Stromversorgungsgeräte mithilfe von CAT 5e- oder CAT 6-Kabeln und DB9- oder DB25-Konsolenadaptern an die seriellen Ports des Konsolensystems an. Alle seriellen Ports sind Multiprotokoll-Ports und können vom Benutzer mit RS485-, RS422- und RS232-Pinbelegung ausgewählt werden.
6	Kupfer-LAN-Ports. Sie können einen oder zu Redundanzzwecken auch beide Netzwerkports verwenden.
7	Konsolenport.
8	Stromversorgung.

1.2.1 LED-Status der seriellen Ports

Jeder serielle Port hat zwei LEDs, die entweder grün oder gelb leuchten. Grüne LEDs zeigen den Status der physischen Verbindung mit einem seriellen Port sowie den Status der Remote-Konnektivität (falls zutreffend) und der Datenübertragung. Gelbe LEDs zeigen, ob ein serieller Port überwacht wird, und geben außerdem die Alarmstufe des überwachten Ziels an (Notfall, Alarm, keine Angabe). In der folgenden Tabelle wird die Bedeutung für jeden LED-Status erläutert.

Tabelle 1.5 LED-Status-Beschreibungen

Status	Beschreibung der grünen LEDs	Beschreibung der gelben LEDs
Aus (leuchtet nicht)	Keine physische Verbindung	Keine Datenpufferung
Ein (leuchtet grün oder gelb)	Gerät ist physisch mit dem seriellen Port verbunden	Datenpufferung ist für den seriellen Port aktiviert
Langsames Blinken	Telnet-, SSH- oder Raw-Sitzung ist aktiv	Alarm ist aktiv
Schnelles Blinken	TX- oder RX-Datenaktivität	Notfall

Diese Seite wurde frei gelassen.

2 Erste Schritte

2.1 Installation

Anleitungen zur Installation Ihres Konsolensystems finden Sie in der Schnellinstallationsanleitung für das ACS800 oder ACS8000, die mit dem Produkt geliefert wurde.

2.2 Einschalten des Konsolensystems

Je nach Modell wird das Konsolensystem mit einer Einzel- oder Doppelstromversorgung (AC oder DC) geliefert.

WARNUNG! Führen Sie immer den Befehl zum Herunterfahren (shutdown) über die Weboberfläche, CLI oder die DSView-Software unter dem Knoten „Übersicht/Tools“ aus, bevor Sie das Konsolensystem aus- und dann wieder einschalten. Dies verhindert, dass das System zurückgesetzt wird, während auf das Dateisystem im Flash-Speicher zugegriffen wird. Außerdem verringert sich so das Risiko von Beschädigungen des Flash-Speichers.

2.2.1 AC-Stromversorgung

So schalten Sie ein Konsolensystem mit AC-Stromversorgung ein:

1. Stellen Sie sicher, dass das Konsolensystem ausgeschaltet ist.
2. Schließen Sie das Stromkabel an das Konsolensystem und an eine Stromquelle an.
3. Schalten Sie das Konsolensystem ein.
4. Schalten Sie die Stromversorgung der angeschlossenen Geräte über die entsprechenden Schalter ein.

2.2.2 DC-Stromversorgung

Das Konsolensystem wird mithilfe von drei Leitungen mit DC-Strom versorgt: Rückleitung (RTN), Masse (GND) und -48 VDC. Zur Redundanz sind zwei Leitungssätze verfügbar, die an zwei separate Stromquellen angeschlossen werden können.

WARNUNG! Es ist zwingend erforderlich, dass die Stromquelle die DC-Stromanforderungen des Konsolensystem unterstützt. Bevor Sie fortfahren, stellen Sie sicher, dass die Stromquelle den richtigen Typ aufweist und dass sich die DC-Stromkabel in einwandfreiem Zustand befinden. Wenn Sie dies versäumen, können Verletzungen oder Geräteschäden die Folge sein.

In der folgenden Abbildung wird die Anschlusskonfiguration für die DC-Stromversorgung gezeigt.

HINWEIS: DC-Stromversorgung ist nur beim ACS8000 Konsolensystem erhältlich.

Abbildung 2.1 Anschlussblock für DC-Stromversorgung

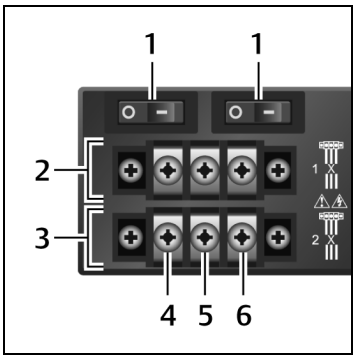


Tabelle 2.1 Details zum DC-Stromanschluss

Nummer	Beschreibung	Nummer	Beschreibung
1	Je ein Netzschalter für jede Stromquelle	4	RTN (Rückleitung)
2	Anschlüsse für die erste Stromquelle	5	GND (Masse)
3	Anschlüsse für die zweite Stromquelle	6	-48 VDC

So schalten Sie ein Konsolensystem mit DC-Stromversorgung ein:

1. Stellen Sie sicher, dass das Konsolensystem ausgeschaltet ist.
2. Stellen Sie sicher, dass die DC-Stromkabel nicht mit einer Stromquelle verbunden sind.
3. Entfernen Sie die Schutzabdeckung vom DC-Stromversorgungsblock, indem Sie sie nach links oder rechts schieben.
4. Lösen Sie alle drei Schrauben des DC-Stromanschlusses.
5. Schließen Sie den Rückleiter an den RTN-Anschluss, den Masseleiter an den GND-Anschluss und den -48 VDC-Leiter an den -48 VDC-Anschluss an. Ziehen Sie dann die Schrauben fest.
6. Schieben Sie die Schutzabdeckung wieder über den DC-Anschlussblock.
7. Wenn Ihr Konsolensystem über doppelte DC-Eingangsanschlüsse verfügt, wiederholen Sie die Schritte 3–6 für den zweiten Anschluss.
8. Schließen Sie die DC-Stromkabel an die DC-Stromquelle an und schalten Sie die DC-Stromquelle ein.
9. Schalten Sie das Konsolensystem ein.
10. Schalten Sie die Stromversorgung der angeschlossenen Geräte über die entsprechenden Schalter ein.

2.3 Konfiguration eines Konsolensystems

Ein Konsolensystem kann auf Ebene der Einheit über die Befehlszeile konfiguriert werden, die über den KONSOLEN- oder Ethernet-Port aufgerufen werden kann. Der Zugriff auf alle Terminalbefehle erfolgt über ein Terminal oder über einen PC, auf dem Terminalemulationssoftware ausgeführt wird.

HINWEIS: Anleitungen zur Konfiguration des Konsolensystems mithilfe der DSView-Software finden Sie im Installations- und Benutzerhandbuch für die Avocent® DSView 4.5-Managementsoftware. Anleitungen zur Konfiguration des Konsolensystems mithilfe der Weboberfläche finden Sie unter Weboberfläche für Administratoren – Übersicht **auf Seite 18****. Anleitungen zur Konfiguration des Konsolensystems mithilfe von Telnet oder SSH finden Sie in der Befehlsreferenz für das Avocent® ACS 800/8000 Advanced Console System.**

So schließen Sie ein Terminal an das Konsolensystem an:

1. Schließen Sie ein Terminal oder einen PC, auf dem Terminalemulationssoftware (wie beispielsweise HyperTerminal) ausgeführt wird, mit einem Nullmodemkabel an den KONSOLEN-Port an der Rückseite des Konsolensystems an. Ein RJ-45-auf-DB9-Crossover-Adapter (Buchse) ist im Lieferumfang enthalten.

   Die Terminaleinstellungen lauten: 9600 Bit pro Sekunde (bit/s), 8 Bit, 1 Stoppbit, keine Parität, keine Flusskontrolle.

2. Schalten Sie das Konsolensystem ein. Nach der Initialisierung des Konsolensystems werden auf dem Terminal das Anmeldebanner und die Anmeldeaufforderung angezeigt.

2.3.1 Verwenden von Telnet oder SSH

Autorisierte Benutzer können über einen Telnet- oder SSH-Client eine direkte Verbindung mit der Konsole eines Geräts herstellen, sofern alle der folgenden Voraussetzungen erfüllt sind:

Telnet- oder SSH-Voraussetzungen:

- Das Protokoll muss im ausgewählten Sicherheitsprofil aktiviert sein.
- Der Client muss verfügbar und auf dem Computer aktiviert sein, von dem aus die Verbindung hergestellt wird.

So stellen Sie mit Telnet über einen seriellen Port eine Verbindung mit einem Gerät her:

Dieses Verfahren erfordert den Benutzernamen, der für den Zugriff auf den seriellen Port konfiguriert ist, den Portnamen (zum Beispiel 14-35-60-p-1), den Gerätenamen (zum Beispiel ttyS1), den TCP-Port-Aliasnamen (zum Beispiel 7001) oder den IP-Port-Aliasnamen (zum Beispiel 100.0.0.100) und den Hostnamen oder die IP-Adresse des Konsolensystem.

Zur Verwendung eines Telnet-Clients geben Sie die Informationen in die Dialogfelder für den Client ein.

– oder –

Zur Verwendung von Telnet in einer Shell geben Sie den folgenden Befehl ein:

```
#telnet [Hostname | IP-Adresse]
login: Benutzername:[Portname | Gerätename | TCP-Port-Aliasname]
– oder –
#telnet [Hostname | IP-Adresse] TCP-Port-Aliasname
login:Benutzername
– oder –
#telnet IP-Port-Aliasname
login:Benutzername
```

So schließen Sie eine Telnet-Sitzung:

Geben Sie den Telnet-Hotkey ein, der für den Client definiert wurde. Der Standard-Hotkey zum Beenden lautet Strg] + q.

– oder –

Geben Sie den Hotkey für die Textsitzung für die CLI-Aufforderung und dann exit ein.

So stellen Sie mit SSH über einen seriellen Port eine Verbindung mit einem Gerät her:

Dieses Verfahren erfordert den Benutzernamen, der für den Zugriff auf den seriellen Port konfiguriert ist, den Portnamen (zum Beispiel 14-35-60-p-1), den TCP-Port-Aliasnamen (zum Beispiel 7001), den Gerätenamen (zum Beispiel ttyS1) und den Hostnamen des Konsolensystem, die IP-Adresse oder den IP-Port-Aliasnamen (zum Beispiel 100.0.0.100).

So verwenden Sie einen SSH-Client:

Geben Sie die Informationen in die Dialogfelder für den Client ein.

– oder –

Zur Verwendung von SSH in einer Shell geben Sie den folgenden Befehl ein:

```
ssh -l  Benutzername : Portname  [Hostname | IP-Adresse]
– oder –
ssh -l Benutzername:Gerätename [Hostname | IP-Adresse]
– oder –
ssh -l Benutzername:TCP-Port-Aliasname [Hostname | IP-Adresse]
– oder –
ssh -l Benutzername IP-Port-Aliasname
```

So schließen Sie eine SSH-Sitzung:

Geben Sie am Anfang einer Zeile den für den SSH-Client definierten Hotkey gefolgt von einem Punkt ein. Der Standard lautet **~**.

– oder –

Geben Sie den Hotkey für die Textsitzung für die CLI-Aufforderung und dann **exit** ein.

3 Zugriff auf das Konsolensystem über die Weboberfläche

Nachdem Sie das Avocent® ACS800/8000 Advanced Console System mit einem Netzwerk verbunden haben, können Sie über die Web-Benutzeroberfläche (Weboberfläche) auf das Konsolensystem zugreifen. Die Weboberfläche ermöglicht den Direktzugriff auf das Konsolensystem über eine grafische Benutzeroberfläche anstatt über eine Befehlszeile.

HINWEIS: Bei einem neuen Konsolensystem, das die standardmäßigen Werkseinstellungen verwendet, versucht LAN1, eine IP-Adresse über DHCP abzurufen, während LAN2 die statische IP-Adresse 192.168.161.10 hat. Verwenden Sie LAN2 für die Erstkonfiguration, oder nutzen Sie den Konsolenport, um die von DHCP zugewiesene IPv4-Adresse für LAN1 zu ermitteln.

HINWEIS: Anleitungen zum Zugriff auf das Konsolensystem über die CLI oder die DSView-Software finden Sie in der Befehlsreferenz für das Avocent® ACS800/8000 Advanced Console System oder im Installations- und Benutzerhandbuch für die Avocent® DSView 4.5-Managementsoftware.

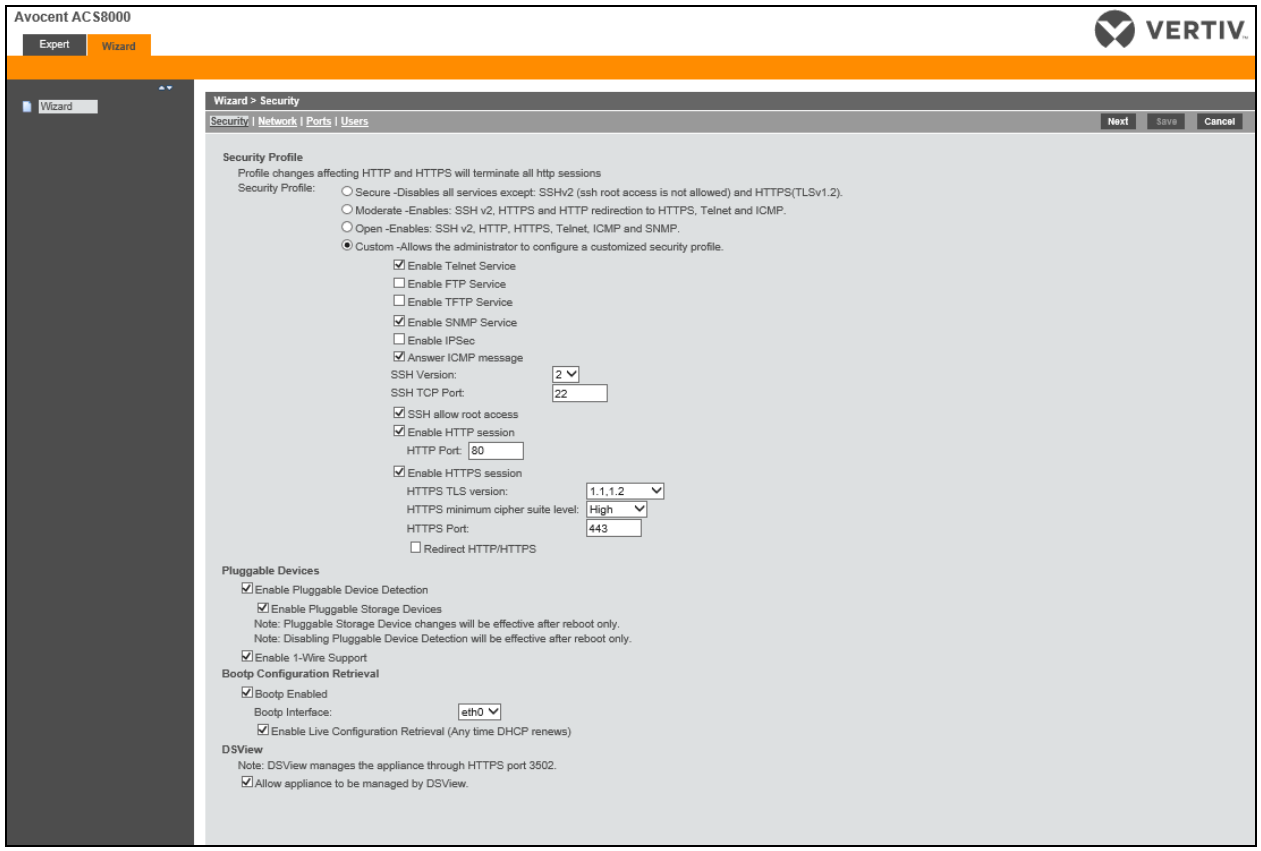
3.1 Assistentenmodus

Der Assistentenmodus vereinfacht Setup und Konfiguration, indem er den Administrator durch die einzelnen Konfigurationsschritte führt. Mithilfe des Assistenten kann der Administrator alle Ports im CAS-Profil konfigurieren und Einstellungen für das Sicherheitsprofil, das Netzwerk und die Benutzer festlegen.

Der Assistent wird standardmäßig angezeigt, wenn der Administrator das erste Mal über die Weboberfläche auf das Konsolensystem zugreift. Bei weiteren Anmeldungen wird der Expertenmodus verwendet, der zum Standardmodus wird, sobald das Konsolensystem konfiguriert wurde. Administratoren können zwischen dem Experten- und dem Assistentenmodus wechseln, indem sie auf die Registerkartenleiste auf dem Administrator-Bildschirm der Weboberfläche klicken.

Die folgende Abbildung zeigt einen typischen Bildschirm für Administratoren im Assistentenmodus.

Abbildung 3.1 Bildschirm im Assistentenmodus



Im Folgenden wird beschrieben, wie Sie das Konsolensystem mithilfe des Assistenten konfigurieren.

So können Sie Sicherheitsparameter konfigurieren und ein Sicherheitsprofil auswählen:

1. Wählen Sie im Inhaltsbereich den Link *Sicherheit* aus.
2. Wählen Sie das gewünschte Sicherheitsprofil aus. Wenn Sie ein benutzerdefiniertes Sicherheitsprofil verwenden, aktivieren Sie die gewünschten Kontrollkästchen und geben Sie die erforderlichen Werte ein, um die Dienste sowie die Optionen für SSH, HTTP und HTTPS gemäß den Sicherheitsrichtlinien Ihres Unternehmens zu konfigurieren.
3. Austauschbare Geräte sind standardmäßig deaktiviert. Dazu zählen Geräte, die an den SD-Kartensteckplatz oder an USB-Anschlüsse angeschlossen sind. Wenn Sie diese Geräte aktivieren möchten, klicken Sie auf das Kontrollkästchen „Erkennung austauschbarer Geräte aktivieren“. Wenn die Erkennung austauschbarer Geräte aktiviert ist, sind Speichergeräte (SD-Karten und USB-Speichergeräte) standardmäßig aktiviert. Um diese Art von austauschbaren Geräten zu deaktivieren, entfernen Sie das Häkchen aus dem Kontrollkästchen „Erkennung austauschbarer Geräte aktivieren“. Zu den austauschbaren Geräten gehört auch der 1-Wire-Sensor-Port, der standardmäßig aktiviert ist. Um den 1-Wire-Sensor-Port zu deaktivieren, entfernen Sie das Häkchen aus dem Kontrollkästchen „1-Wire-Unterstützung aktivieren“.

HINWEIS: Diese Optionen werden für alle Konsolensystem-Modelle angezeigt, auch wenn einige Modelle nicht über Ports für SD-Karten oder 1-Wire-Sensoren verfügen. Wenn Ihr Modell nicht über diese Ports verfügt, lassen Sie diese Optionen deaktiviert.

4. Deaktivieren Sie unter „Abruf der BOOTP-Konfiguration“ das Kontrollkästchen für den Abruf der BOOTP-Konfiguration und/oder den Live-Konfigurationsabruf.

5. Wenn Sie die Einheit nicht mithilfe der DSView-Software verwalten, deaktivieren Sie das Kontrollkästchen *Verwaltung der Einheit durch DSView zulassen*.
6. Klicken Sie auf *Weiter*, um das Netzwerk zu konfigurieren, oder klicken Sie auf die Links *Netzwerk*, *Ports* oder *Benutzer*, um den entsprechenden Bildschirm zu öffnen.

So konfigurieren Sie Netzwerkparameter:

1. Wählen Sie im Inhaltsbereich den Link *Netzwerk* aus.
2. Geben Sie den Hostnamen, das Primär-DNS und die Domäne in die vorgesehenen Felder ein.
3. Wählen Sie die IPv4- oder IPv6-Methode für die ETH0-Schnittstelle aus. Bei Verwendung von „Statisch“ geben Sie die Adresse, die Maske und das Gateway in die vorgesehenen Felder ein.
4. Aktivieren oder deaktivieren Sie LLDP (Link Layer Discovery Protocol).
5. Aktivieren oder deaktivieren Sie die IPv6-Unterstützung.
6. Klicken Sie auf *Weiter*, um Ports zu konfigurieren, oder klicken Sie auf die Links *Sicherheit*, *Ports* oder *Benutzer*, um den entsprechenden Bildschirm zu öffnen.

So konfigurieren Sie Ports:

1. Wählen Sie im Inhaltsbereich den Link *Ports* aus.
2. Aktivieren Sie das Kontrollkästchen, um alle Ports zu aktivieren.
3. Wählen Sie in den Dropdown-Menüs die gewünschten Werte für RJ45-Pinbelegung, Geschwindigkeit, Parität, Datenbits, Stoppbits, Flusssteuerung, Protokoll, Authentifizierungstyp, Status der Datenpufferung und Zeitstempel der Datenpufferung aus.
4. Wählen Sie den Typ der Datenpufferung aus. Bei Verwendung von NFS geben Sie den NFS-Server und den NFS-Pfad in die vorgesehenen Felder ein.
5. Klicken Sie auf *Weiter*, um Benutzer zu konfigurieren, oder klicken Sie auf die Links *Netzwerk*, *Sicherheit* oder *Benutzer*, um den entsprechenden Bildschirm zu öffnen.

So können Sie Benutzer konfigurieren und ändern:

1. Wählen Sie im Inhaltsbereich den Link *Benutzer* aus.
2. Klicken Sie auf einen Benutzernamen (*admin* oder *root*) und geben Sie das neue Kennwort in die Felder „Kennwort“ und „Kennwort bestätigen“ ein.

   – oder –

3. Klicken Sie auf *Hinzufügen*, um einen Benutzer hinzuzufügen. Geben Sie den neuen Benutzernamen und das Kennwort in die vorgesehenen Felder ein.
4. (Optional) Wenn Sie festlegen möchten, dass der Benutzer sein Kennwort bei der nächsten Anmeldung ändern muss, aktivieren Sie das Kontrollkästchen *Benutzer muss das Kennwort bei der nächsten Anmeldung ändern*.
5. Weisen Sie den Benutzer mindestens einer Gruppe zu.
6. (Optional) Konfigurieren Sie den Kontoablauf und den Kennwortablauf.
7. Klicken Sie auf *Weiter*.
8. Wiederholen Sie die Schritte 3 bis 7 nach Bedarf, um neue Benutzerkonten zu konfigurieren und sie Standardgruppen zuzuweisen.

HINWEIS: Standardmäßig können alle konfigurierten Benutzer auf alle aktivierten Ports zugreifen. Wenn der Benutzerzugriff auf Ports eingeschränkt werden muss, um die Sicherheitsrichtlinien Ihres Unternehmens zu erfüllen, sind weitere Konfigurationsschritte erforderlich.

9. Klicken Sie auf *Speichern* und dann auf *Fertigstellen*.

3.2 Weboberfläche für Administratoren – Übersicht

HINWEIS: Eine Übersicht über die Weboberfläche für reguläre Benutzer finden Sie unter Weboberfläche für reguläre Benutzer – Übersicht auf Seite 92.

So melden Sie sich bei der Weboberfläche an:

1. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse des Konsolensystems in das Adressfeld ein.
2. Melden Sie sich mit Ihrem Benutzernamen und Kennwort an. Der Standard-Benutzername lautet **admin**. Wenn Sie sich zum ersten Mal als Administrator anmelden, lassen Sie das Kennwortfeld leer. Sie werden aufgefordert, ein neues Kennwort zu erstellen.

HINWEIS: Der Stammbenutzer ist standardmäßig deaktiviert. Ein Administrator kann den Stammbenutzer über die Seite „Benutzer – Lokale Konten – Benutzernamen“ aktivieren.

Die folgende Abbildung zeigt einen typischen Bildschirm der Weboberfläche für Administratoren.

Abbildung 3.2 Bildschirm der Weboberfläche für Administratoren

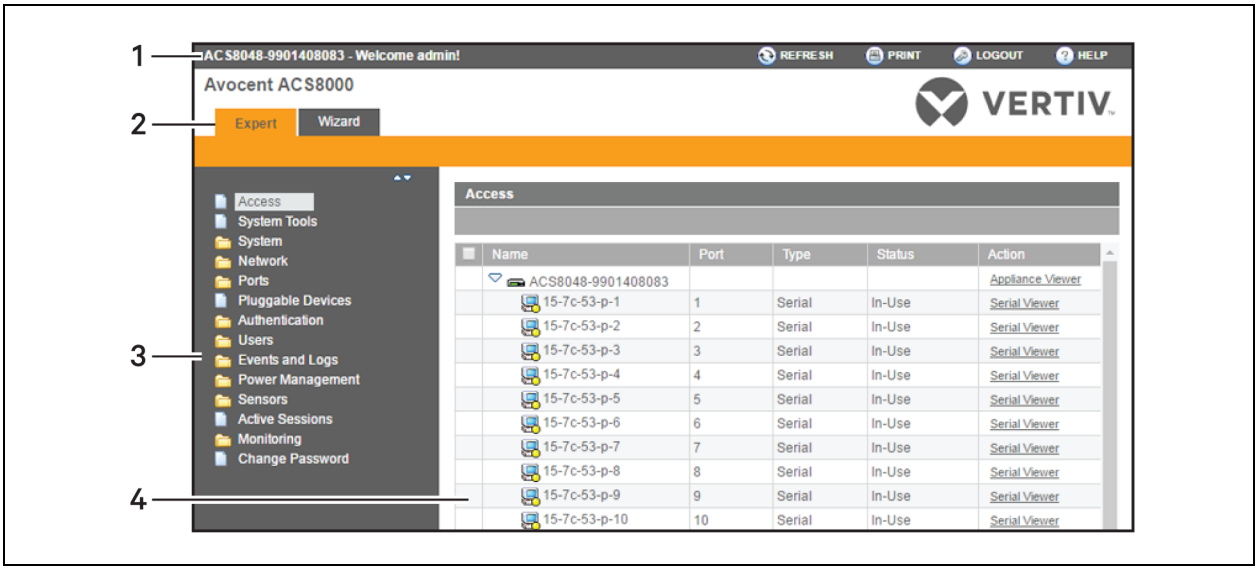


Tabelle 3.1 Bildschirmbereiche der Weboberfläche

Nummer	Beschreibung
1	Obere Optionsleiste. Der Name der Einheit und der Name des angemeldeten Benutzers werden auf der linken Seite angezeigt. Die Schaltflächen „Aktualisieren“, „Drucken“, „Abmelden“ und „Hilfe“ befinden sich auf der rechten Seite.
2	Registerkartenleiste. Zeigt an, ob sich der Administrator im Expertenmodus oder im Assistentenmodus befindet.
3	Seitliche Navigationsleiste. Menüoptionen für die Konfiguration, die Anzeige von Systeminformationen und den Zugriff auf Geräte. Diese Optionen variieren je nach den Benutzerberechtigungen.
4	Inhaltsbereich. Der Inhalt richtet sich nach den Optionen, die in der seitlichen Navigationsleiste ausgewählt sind.

3.3 Expertenmodus

Wenn sich der Administrator im Expertenmodus befindet, stehen in der seitlichen Navigationsleiste der Weboberfläche die folgenden Registerkarten zur Verfügung.

3.3.1 Zugriff

Klicken Sie auf Zugriff, um alle Geräte anzuzeigen, die mit dem Konsolensystem verbunden sind.

So können Sie über die Weboberfläche Geräte anzeigen und eine Verbindung mit Geräten herstellen:

1. Wählen Sie in der seitlichen Navigationsleiste die Option *Zugriff*. Der Inhaltsbereich zeigt den Namen des Konsolensystem sowie eine Liste der Namen bzw. Aliasnamen aller installierten und konfigurierten Geräte, für die der Benutzer eine Zugriffsberechtigung besitzt.
2. Wählen Sie *Serieller Viewer* in der Spalte „Aktion“, um eine Verbindung mit dem ausgewählten seriellen Port zu öffnen.

   – oder –

   Wählen Sie *Einheiten-Viewer* in der Spalte „Aktion“, um eine Verbindung mit dem Konsolensystem zu öffnen.

HINWEIS: Der HTML5-Viewer wird standardmäßig geöffnet; wenn jedoch ein Administrator den JNLP-Viewer ausgewählt hat, erscheint der Java-Applet-Viewer.

3. Wenn Sie nicht automatisch angemeldet werden, melden Sie sich an, wenn Sie dazu aufgefordert werden.

3.3.2 Systemtools

Durch Klicken auf *Systemtools* werden Symbole für verschiedene Aktionen angezeigt. Sie können über diese Symbole das Konsolensystem neu starten oder herunterfahren, die Firmware des Konsolensystem aktualisieren, seine Konfiguration speichern oder wiederherstellen und eine Terminalsitzung mit dem Konsolensystem öffnen.

Firmware-Upgrade

Das Konsolensystem ermöglicht es Ihnen, zwei Firmware-Images zu speichern. Bei einem Firmware-Upgrade wird das derzeit nicht aktive Image durch die neue Firmware überschrieben. Die neueste Firmware kann von der Vertiv-Website heruntergeladen werden. Das Konsolensystem kann über einen FTP-Server (File Transfer Protocol), einen SFTP-Server (Secure File Transfer Protocol) oder einen SCP-Server (Secure Copy Protocol) auf die Firmware zugreifen. Die Firmware kann auch über einen Webbrowser vom lokalen Computer des Benutzers heruntergeladen werden.

Wenn Sie die aktuelle Firmware-Version des Konsolensystem anzeigen möchten, klicken Sie in der Seitenleiste der Registerkarte „Experte“ auf *System – Informationen*.

So führen Sie ein Firmware-Upgrade des Konsolensystem durch:

1. Navigieren Sie auf der Website http://www.VertivCo.com zum Bereich mit Produktaktualisierungen und suchen Sie nach der Firmware für Ihr Konsolensystem.
2. Speichern Sie die neue Firmware auf einem Server, der den Zugriff über FTP, SFTP oder SCP ermöglicht, oder auf Ihrem Desktop.
3. Klicken Sie in der Seitenleiste der Weboberfläche des Konsolensystem auf *Systemtools* und dann auf *Firmware-Upgrade durchführen*.
4. Laden Sie die Datei von dem Server herunter, den Sie in Schritt 2 ausgewählt haben.
    a. Klicken Sie auf das Optionsfeld neben „Remote-Server“ und wählen Sie dann im Dropdown-Menü das Protokoll des Servers aus, auf dem Sie die Datei gespeichert haben.
    b. Geben Sie die IP-Adresse des Servers, auf dem die Firmware gespeichert ist, in das vorgesehene Feld ein.
    c. Geben Sie den Benutzernamen und das Kennwort für den Server in die vorgesehenen Felder ein.
    d. Geben Sie das Dateiverzeichnis, in dem die Firmware gespeichert ist, und den Dateinamen der Firmware in die vorgesehenen Felder ein.

    – oder –

    Wählen Sie *Eigener Computer* aus, um die Datei von Ihrem Desktop herunterzuladen.

    a. Geben Sie den Dateinamen der neuen Firmware ein oder klicken Sie auf *Durchsuchen* und navigieren Sie im angezeigten Fenster zur Datei.
5. Klicken Sie auf *Download*. Das Konsolensystem lädt die Firmware vom angegebenen Speicherort herunter und zeigt eine Meldung an, wenn der Download abgeschlossen ist.
6. Klicken Sie auf *Installieren*.
7. Nach der Installation der neuen Firmware muss das Konsolensystem neu gestartet werden.

Konfigurationsdateien

Administratoren können ein Sicherungs-Image der Konfiguration des Konsolensystem erstellen. Während der Erstellung sollten keine Änderungen an der Konfiguration vorgenommen werden. Die Konfigurationssicherungsdatei kann auf einen Remote-Server hochgeladen oder lokal auf dem Konsolensystem oder auf dem Computer des Webbenutzers gespeichert werden. Konfigurationsdateien können als komprimierte Datei, CLI-Skript oder XML-Datei gespeichert werden.

So speichern Sie die aktuelle Konfiguration in einer Datei:

1. Klicken Sie in der Seitenleiste der Registerkarte „Experte“ auf *Systemtools*.

2. Klicken Sie auf *Konfiguration speichern*.
3. Wählen Sie das Dateiformat im Dropdown-Menü aus.
4. Laden Sie die Datei auf einen Remote-Server hoch.
    a. Klicken Sie auf das Optionsfeld „Remote-Server“ und wählen Sie dann im Dropdown-Menü das Protokoll des Servers aus, auf dem Sie die Datei speichern möchten.
    b. Geben Sie die IP-Adresse des Servers, auf dem Sie die Datei speichern möchten, in das vorgesehene Feld ein.
    c. Geben Sie den Benutzernamen und das Kennwort für den Server in die vorgesehenen Felder ein.
    d. Geben Sie das Dateiverzeichnis, in dem die Konfigurationsdatei gespeichert werden soll, und den Dateinamen in die vorgesehenen Felder ein.

    – oder –

    Wenn Sie die Datei lokal speichern möchten, klicken Sie auf das Optionsfeld „Lokale Datei“ und geben Sie dann den Dateinamen ein.

HINWEIS: Der Dateiname kann den vollständigen Pfad des Verzeichnisses enthalten, in dem die Datei gespeichert werden soll. Durch Angabe des vollständigen Pfades kann die Datei auf einem bereitgestellten USB-Speichergerät gespeichert werden, zum Beispiel /media/sda1/Dateiname. Wenn nicht der vollständige Pfad angegeben wird, wird die Datei unter /mnt/hdUser/backup/<Dateiname> gespeichert.

    – oder –

    Wenn Sie die Datei auf Ihrem Computer speichern möchten, klicken Sie auf das Optionsfeld „Eigener Computer“. Die Datei wird in Ihrem Downloads-Ordner gespeichert.

5. Klicken Sie auf *Speichern*.

So stellen Sie eine vorige Konfiguration wieder her:

1. Klicken Sie in der Seitenleiste der Registerkarte „Experte“ auf *Systemtools*.
2. Klicken Sie auf *Konfiguration wiederherstellen*.
3. Stellen Sie die Datei von einem Remote-Server wieder her.
    a. Klicken Sie auf das Optionsfeld „Remote-Server“ und wählen Sie dann im Dropdown-Menü das Protokoll des Servers aus, auf dem die Konfigurationsdatei gespeichert ist.
    b. Geben Sie die IP-Adresse des Servers, auf dem die Datei gespeichert ist, in das vorgesehene Feld ein.
    c. Geben Sie den Benutzernamen und das Kennwort für den Server in die vorgesehenen Felder ein.
    d. Geben Sie den Pfad und den Dateinamen der Konfigurationsdatei ein.

    – oder –

    Wenn Sie die Konfiguration von einer lokalen Datei wiederherstellen möchten, klicken Sie auf das Optionsfeld „Lokal“ und geben Sie dann den Dateinamen ein.

    – oder –

    Wenn Sie die Konfiguration von einer Datei auf Ihrem Computer wiederherstellen möchten, klicken Sie auf das Optionsfeld „Eigener Computer“, wechseln Sie zum Speicherort der Datei und klicken Sie dann auf *Öffnen*.

4. Klicken Sie auf *Wiederherstellen*.

Konfigurationsintegrität

Zur Gewährleistung der Konfigurationsintegrität bietet das Konsolensystem dem Administrator die Möglichkeit, eine digitale Signatur (MD5) für die Konfiguration des Konsolensystem zu generieren und zu überprüfen. Das Konsolensystem vergleicht seinen MD5-Prüfsummenwert mit einem bekannten MD5-Prüfsummenwert, um seine Konfiguration zu überprüfen und ihn vor Beschädigungen zu schützen.

Administratoren können eine aktive Konfiguration als vertrauenswürdig definieren und das Konsolensystem anweisen, ein MD5-Tag für die vertrauenswürdige Konfiguration zu generieren. Administratoren können die Konfiguration auch überprüfen, indem sie sie mit einer anderen bekannten oder vertrauenswürdigen Konfiguration vergleichen. Nach Abschluss der Prüfung deklariert das Konsolensystem die Konfiguration als „Unverändert“ oder „Geändert“.

Die Konfigurationsintegrität stützt sich auf die gespeicherten und wiederhergestellten Konfigurationsdateien des Konsolensystem. Weiterhin ist sie von der interaktionslosen Bereitstellung abhängig.

HINWEIS: Zur Verwendung der Konfigurationsintegrität müssen Sie die Konfiguration mit der Option „Komprimierte Datei“ speichern. Die Datei im komprimierten Format erfasst mehr Konfigurationsdaten und gewährleistet so die Genauigkeit der Ergebnisse für die Konfigurationsintegrität. Wenn die Konfiguration als CLI-Skript oder im XML-Dateiformat gespeichert wird, sind die Ergebnisse der Konfigurationsintegrität ungültig.

Das Konsolensystem erstellt bei jeder Generierung eines MD5-Tags eine Ereignisbenachrichtigung. Weitere Informationen über Ereignisse finden Sie unter Ereignisliste auf Seite 82.

So generieren Sie ein MD5-Tag:

1. Klicken Sie in der Seitenleiste der Weboberfläche des Konsolensystem auf *Systemtools* und dann auf *Konfigurationsintegrität*.
2. Klicken Sie auf das Optionsfeld „MD5-Tag für die aktive Konfiguration generieren“ und dann auf *Ausführen*.
3. Das generierte MD5-Tag wird als Hexadezimalwert mit 32 Zeichen auf dem Bildschirm angezeigt. Außerdem wird es im Konsolensystem als der Wert gespeichert, der später für den Vergleich herangezogen wird. Administratoren können diese Zeichenfolge kopieren und zur Verwendung in anderen Systemen wieder einfügen.

So überprüfen Sie ein MD5-Tag:

1. Klicken Sie in der Seitenleiste der Weboberfläche des Konsolensystem auf *Systemtools* und dann auf *Konfigurationsintegrität*.
2. Klicken Sie auf das Optionsfeld „Aktive Konfiguration überprüfen“.
3. Lassen Sie das Feld „MD5“ leer, um die aktive Konfiguration zu überprüfen.

   – oder –

   Geben Sie eine Zeichenfolge für die MD5-Prüfsumme ein, um eine bekannte Konfiguration zu überprüfen.
4. Klicken Sie auf *Ausführen*.

HTTPS-Zertifikat

Sie können ein neues selbstsigniertes Zertifikat generieren oder ein signiertes Zertifikat von einem FTP-Server oder von Ihrem Desktop auf die Einheit herunterladen.

So generieren Sie ein neues selbstsigniertes Zertifikat:

1. Klicken Sie in der Seitenleiste der Registerkarte „Experte“ auf *Systemtools*.
2. Klicken Sie auf *Zertifikat erstellen/herunterladen*.
3. Wenn Sie ein neues Zertifikat generieren möchten, klicken Sie auf das Optionsfeld neben „Selbstsigniertes Zertifikat erstellen“ und geben Sie dann die gewünschten Informationen in die Felder für das selbstsignierte Zertifikat ein: Land, Bundesland, Stadt oder Ort, Organisation, Organisationseinheit, allgemeiner Name, E-Mail-Adresse und Netscape-Kommentar.

   – oder –

   Wenn Sie ein signiertes Zertifikat von einem FTP-, SFTP- oder SCP-Server herunterladen möchten, klicken Sie auf das Optionsfeld neben „Remote-Server“ und geben Sie dann die erforderlichen Informationen über den Server ein: IP-Adresse, Benutzername, Kennwort, Dateiverzeichnis und Dateiname.

   – oder –

   Wenn Sie ein Zertifikat von Ihrem Desktop herunterladen möchten, klicken Sie auf das Optionsfeld neben „Zertifikat vom eigenen Computer herunterladen“, klicken Sie auf *Datei auswählen* oder *Durchsuchen*, navigieren Sie zum Speicherort der Datei und klicken Sie auf *Öffnen*.
4. Klicken Sie auf *Erstellen/Herunterladen*. Die Informationen des Zertifikats werden angezeigt.
5. Klicken Sie auf *Anwenden*. Folgende Meldung wird eingeblendet: *Durch Anwenden des neuen Zertifikats werden alle HTTP/HTTPS-Sitzungen beendet. Sie müssen Ihren Browser neu starten. Möchten Sie wirklich fortfahren?*
6. Klicken Sie auf *OK*, um fortzufahren. Das Zertifikat wird gespeichert und der Browser wird neu gestartet, damit das neue Zertifikat verwendet wird.

HINWEIS: Alle HTTP/HTTPS-Sitzungen werden geschlossen. Der Benutzer muss die Verbindung neu herstellen.

3.3.3 System

Durch Klicken auf *System* können Administratoren Informationen über das Konsolensystem anzeigen und die Parameter des Konsolensystem konfigurieren. Unter „System“ in der seitlichen Navigationsleiste befinden sich die folgenden Registerkarten.

Sicherheit

Sicherheitsprofil

Ein Sicherheitsprofil bestimmt, welche Dienste auf dem Konsolensystem aktiviert sind.

Bei der Erstkonfiguration muss der Administrator des Konsolensystem Sicherheitsparameter konfigurieren, die der Sicherheitsrichtlinie des Standorts entsprechen. Die folgenden Sicherheitsfunktionen können über die Weboberfläche, CLI oder die DSView-Software konfiguriert werden:

- Inaktivitäts-Timeout der Sitzung konfigurieren
- RPC aktivieren oder deaktivieren
- Erkennung austauschbarer Geräte, Speichergeräte und 1-Wire-Sensoren aktivieren oder deaktivieren
- Zugriff auf serielle Ports für alle Benutzer konfigurieren oder die Konfiguration von gruppen- und benutzerspezifischen Berechtigungen zulassen, um den Zugriff zu beschränken
- Sicherheitsprofil auswählen, das Folgendes definiert:
  - Aktivierte Dienste (FTP, TFTP, ICMP, IPSec, SNMP und Telnet)
  - SSH- und HTTP/HTTPS-Zugriff
  - Abruf der BOOTP-Konfiguration, BOOTP-Schnittstelle und Live-Konfigurationsabruf aktivieren oder deaktivieren

Administratoren können entweder ein vorkonfiguriertes Sicherheitsprofil auswählen oder ein benutzerdefiniertes Sicherheitsprofil erstellen.

Alle Dienste sowie die SSH- und HTTP/HTTPS-Konfigurationsoptionen, die für die einzelnen Sicherheitsprofile aktiviert bzw. deaktiviert sind, werden auf den Seiten „Assistent – Sicherheit“ und „System – Sicherheit – Sicherheitsprofil“ angezeigt.

So konfigurieren Sie ein Sicherheitsprofil:

1. Wählen Sie *System – Sicherheit – Sicherheitsprofil*.
2. Geben Sie in das Feld für das Inaktivitäts-Timeout die Anzahl von Sekunden ein, nach der das Konsolensystem geöffnete Sitzungen wegen einer Zeitüberschreitung abbricht.

HINWEIS: Dieser Wert gilt für alle Benutzersitzungen mit der Einheit über HTTP, HTTPS, SSH, Telnet oder den KONSOLEN-Port. Der Wert, der für die Berechtigungsgruppe des Benutzers konfiguriert ist, wird dadurch nicht außer Kraft gesetzt. Der neue Wert für das Inaktivitäts-Timeout gilt nur für neue Sitzungen.

3. Aktivieren oder deaktivieren Sie unter „Aktivierte Dienste“ das Kontrollkästchen *RPC*.
4. Aktivieren oder deaktivieren Sie unter „Austauschbare Geräte“ die Erkennung von austauschbaren USB- und SD-Geräten. Wenn die Option aktiviert ist, können USB-Speichergeräte deaktiviert werden, um die Art der austauschbaren Geräte aus Sicherheitsgründen einzuschränken. Die 1-Wire-Sensoren können in diesem Abschnitt ebenfalls deaktiviert werden.

HINWEIS: Diese Optionen werden für alle Konsolensystem-Modelle angezeigt, auch wenn einige Modelle nicht über Ports für SD-Karten oder 1-Wire-Sensoren verfügen. Wenn Ihr Modell nicht über diese Ports verfügt, lassen Sie diese Optionen deaktiviert.

HINWEIS: Wenn Sie die Erkennung austauschbarer Geräte deaktivieren oder die Einstellung für Speichergeräte ändern, wird dies erst nach einem Neustart wirksam.

5. Wählen Sie unter „Serielle Geräte“ eine Option aus, um festzulegen, ob der Portzugriff durch Benutzer- und Gruppenberechtigungen geregelt wird oder ob die Einstellungen für den Portzugriff für alle Benutzer gelten.
6. Aktivieren oder deaktivieren Sie unter „Abruf der BOOTP-Konfiguration“ diesen Dienst.

7. Aktivieren oder deaktivieren Sie die SSH-Authentifizierung über einen Benutzernamen und ein Kennwort.
8. Aktivieren Sie unter „Sicherheitsprofil“ das Kontrollkästchen *Benutzerdefiniert*, *Mittel*, *Offen* oder *Sicher*.
9. Klicken Sie auf *Speichern*.

FIPS-Modul

Das Konsolensystem verwendet ein eingebettetes kryptografisches Modul auf Grundlage des validierten kryptografischen FIPS 140-2-Moduls (Zertifikatsnummer 1747), das auf einer Linux ARM-Plattform ausgeführt wird.

Wenn der Administrator das FIPS-Modul aktiviert, verwendet das Konsolensystem das FIPS-Objektmodul für die Verschlüsselung. Standardmäßig ist das FIPS-Modul deaktiviert.

Wenn das FIPS-Modul aktiviert ist, zeigt die Seite „Überwachung – FIPS-Modus“, welcher Dienst (SSHV2, HTTPS, SNMPV3 und ADSAP2) sich im FIPS-Modus befindet. Alle vom Dienst verwendeten Sicherheitsfunktionen und kryptografischen Algorithmen werden im FIPS 140-2-konformen Modus ausgeführt.

So aktivieren Sie das FIPS-Modul:

1. Wählen Sie *System – Sicherheit – FIPS 140*.
2. Aktivieren Sie das Kontrollkästchen für das FIPS 140-2-Modul und klicken Sie auf *Speichern*.

Das Konsolensystem wird automatisch neu gestartet. Dabei löscht das Konsolensystem die SSH-Schlüssel, aktualisiert die Konfiguration der HTTPD-, SSHD-, ADSAP2d- und SNMPD-Dateien und testet die Integrität des FIPS-Objektmoduls. Nach dem Neustart akzeptiert das Konsolensystem SSH- und HTTPS-Verbindungen nur über eine FIPS-konforme Verschlüsselung.

Wenn FIPS aktiviert ist, gelten die folgenden Einschränkungen:

SSH-Sitzungen:

- Nur die Verschlüsselungsarten Triple-DES CBS und AES 128/192/256 werden akzeptiert.
- Nur die Integritätsalgorithmen HMAC-SHA1 und HMAC-SHA1-96 werden akzeptiert.
- Nur RSA-Schlüssel mit 1024 bis 16384 Bit werden akzeptiert.

HTTPS-Sitzungen akzeptieren nur das SSL-Protokoll V 3.1(TLSv1) mit einer der folgenden Verschlüsselungsarten zum Aufbauen des SSL-Tunnels:

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

Anforderungen über die SNMP-Version 3 werden akzeptiert, wenn die SHA-Authentifizierung und die AES-Verschlüsselungsart verwendet werden.

Sicherheit der DSView-Software

Sie können auch Sicherheitseinstellungen für die DSView-Software konfigurieren. Wenn das Konsolensystem von der DSView-Software verwaltet wird, stellt der DSView-Server das Zertifikat für das Konsolensystem bereit. Unter normalen Bedingungen verwaltet die DSView-Software das Zertifikat, und bei Bedarf wird das Zertifikat gelöscht und durch ein neues Zertifikat ersetzt. Wenn die Kommunikation mit der DSView-Software unterbrochen wird, kann der DSView-Server das Zertifikat nicht löschen. In diesem Fall kann das Konsolensystem nicht verwendet werden. Klicken Sie auf die Schaltfläche *DSView-Zertifikat löschen*, um das Konsolensystem im Modus „Allen vertrauen“ zu konfigurieren.

So konfigurieren Sie Sicherheitseinstellungen für die DSView-Software:

1. Wählen Sie *System – Sicherheit – DSView*.
2. Aktivieren Sie das Kontrollkästchen *Verwaltung der Einheit durch DSView zulassen* und klicken Sie auf *Speichern*.

Datum und Uhrzeit

Das Konsolensystem bietet zwei Optionen zum Festlegen von Datum und Uhrzeit. Datum und Uhrzeit können von einem NTP-Server (NTP = Network Time Protocol) abgerufen werden, oder Sie können das Datum und die Uhrzeit manuell festlegen. Im letzteren Fall wird die interne Uhr des Konsolensystem verwendet.

HINWEIS: Die Zeit, die auf dem Bildschirm „Datum und Uhrzeit“ unter „Aktuelle Zeit“ angegeben wird, bezieht sich auf den Zeitpunkt, zu dem der Bildschirm geöffnet wurde. Diese Zeitangabe wird nicht in Echtzeit aktualisiert.

So legen Sie Datum und Uhrzeit mithilfe von NTP fest:

1. Klicken Sie auf *System – Datum und Uhrzeit*.
2. Wählen Sie die Option *Network Time Protocol aktivieren*.
3. Geben Sie den Standort des gewünschten NTP-Servers ein und klicken Sie auf *Speichern*.

So legen Sie Datum und Uhrzeit manuell fest:

1. Klicken Sie auf *System – Datum und Uhrzeit*.
2. Wählen Sie die Option *Manuell einstellen*.
3. Wählen Sie in den Dropdown-Menüs das Datum und die Uhrzeit aus und klicken Sie dann auf *Speichern*.

So legen Sie die Zeitzone über eine vordefinierte Zeitzone fest:

1. Klicken Sie auf *System – Datum und Uhrzeit – Zeitzone*.
2. Wählen Sie die Option *Vordefiniert*.
3. Wählen Sie die gewünschte Zeitzone im Dropdown-Menü aus und klicken Sie auf *Speichern*.

So definieren Sie benutzerdefinierte Einstellungen für die Zeitzone:

1. Klicken Sie auf *System – Datum und Uhrzeit – Zeitzone*.
2. Wählen Sie die Option *Zeitzone definieren*.
3. Geben Sie den Namen und das Standardakronym für die Zeitzone ein.
4. Geben Sie den GMT-Unterschied ein.

5. Wählen Sie ggf. die Option *Sommerzeit aktivieren*.
6. Nehmen Sie die Einstellungen für die Sommerzeit vor, indem Sie die gewünschten Werte auswählen oder eingeben, und klicken Sie dann auf *Speichern*.

Hilfe und Sprache

Klicken Sie auf *System – Hilfe und Sprache* und wählen Sie dann im Dropdown-Menü die Sprache für das Konsolensystem aus.

HINWEIS: Die Sprache gilt für SSH-, Telnet- und Konsolenport-Sitzungen mit dem Konsolensystem. Die Browser-Sprache wird vom Browser bestimmt.

Online-Hilfe

Wenn die Online-Hilfe für das Konsolensystem konfiguriert ist, können Sie in jedem Formular der Weboberfläche auf die Schaltfläche *Hilfe* klicken, um ein neues Fenster zu öffnen, in dem die Produktdokumentation in Form einer Online-Hilfe angezeigt wird (auf Basis des für die Online-Hilfe konfigurierten Pfades).

Geben Sie in das Feld „URL der Online-Hilfe“ die vollständige URL der auf dem lokalen Webserver gespeicherten Online-Hilfe mit der Endung /index.html ein. Klicken Sie auf *Speichern*.

HINWEIS: Aufgrund der Firewall-Konfiguration ist es nicht immer möglich, die Online-Hilfe vom Vertiv-Server aus zu verwenden, und dies wird auch nicht empfohlen. Sie sollten im Allgemeinen das mit dem Produkt gelieferte Online-Hilfesystem verwenden oder die Online-Hilfe als ZIP-Datei herunterladen und von einem lokalen Server ausführen.

Der Systemadministrator kann die Online-Hilfe von Vertiv™ herunterladen. Weitere Informationen zum Herunterladen der Online-Hilfe erhalten Sie vom technischen Support.

Nachdem Sie die Datei für die Online-Hilfe im ZIP-Format heruntergeladen haben, müssen Sie sie in ein selbst gewähltes Verzeichnis im Stammverzeichnis des Webservers extrahieren. Der Webserver muss öffentlichen Zugriff bieten.

Allgemein

Klicken Sie auf *System – Allgemein*, um ein Anmeldebanner zu erstellen oder den Viewer-Typ auszuwählen.

Anmeldebanner:

Administratoren können ein Anmeldebanner konfigurieren, das angezeigt wird, wenn ein Benutzer eine SSHV2-, Telnet-, Konsolen- oder Weboberflächen-Sitzung beginnt.

So erstellen Sie ein Anmeldebanner:

1. Klicken Sie in der seitlichen Navigationsleiste auf *System – Allgemein*.
2. Aktivieren Sie das Kontrollkästchen für das Anmeldebanner.
3. Geben Sie den Text, der bei der Anmeldung angezeigt werden soll, in das Feld „Anmeldebanner“ ein und klicken Sie auf *Speichern*.

Serieller Viewer

Standardmäßig verwendet das Konsolensystem einen einfachen seriellen HTML5-Viewer. Es unterstützt auch einen robusteren Java-basierten seriellen Viewer. Ein Administrator kann konfigurieren, welcher serielle Viewer für die seriellen Ports und Konsolensystem verwendet werden soll.

HINWEIS: Der serielle HTML5-Viewer unterstützt maximal 10 Sitzungen pro Port bei maximal 48 Gesamtsitzungen.

So konfigurieren Sie den seriellen Viewer:

1. Klicken Sie in der seitlichen Navigationsleiste auf *System – Allgemein*.
2. Wählen Sie entweder den HTML5-Viewer oder den JNLP-Viewer aus und klicken Sie dann auf *Speichern*.

Java-basierter serieller Viewer

HINWEIS: Java 1.8.0.91 oder neuer wird empfohlen. Die 32-Bit-Version muss auf Ihrem System installiert sein, damit der serielle Viewer ausgeführt werden kann.

In der folgenden Tabelle werden die verfügbaren Schaltflächen im Java-Applet beschrieben.

Tabelle 3.2 Schaltflächen des Java-Applets zum Herstellen einer Verbindung mit dem Konsolensystem

Schaltfläche	Zweck
SendBreak	Sendet eine Unterbrechungsaufforderung an das Terminal
Disconnect	Trennt die Verbindung mit dem Java-Applet

HINWEIS: Wenn Sie den seriellen Viewer oder den Einheiten-Viewer verwenden, müssen Sie möglicherweise den Popup-Blocker des Client-Browsers deaktivieren.

HINWEIS: Wenn der Viewer ausgeführt wird, werden Sie im Browser möglicherweise gefragt, ob Sie die Ausführung der Anwendung Mindterm zulassen möchten. Sie müssen die Ausführung dieser Anwendung zulassen, damit das Viewer-Applet ausgeführt werden kann.

Startkonfiguration

Die Startkonfiguration bestimmt, von welchem Ort aus das Konsolensystem das Betriebssystem lädt. Das Konsolensystem kann von der internen Firmware oder vom Netzwerk aus starten. Standardmäßig startet das Konsolensystem von der internen Firmware im Flash-Speicher. Durch Klicken auf *System – Startkonfiguration* wird der Bildschirm „Startkonfiguration“ geöffnet.

Wenn Sie das System vom Netzwerk aus starten möchten, müssen die folgenden Voraussetzungen erfüllt werden:

- Ein TFTP-Server muss im Netzwerk verfügbar sein.
- Eine Firmware-Datei muss von Vertiv heruntergeladen und auf dem TFTP-Server zur Verfügung gestellt werden.
- Der Start-Dateiname und die IP-Adresse des TFTP-Servers müssen bekannt sein.

So konfigurieren Sie die Startkonfiguration:

1. Klicken Sie auf *System – Startkonfiguration*.

2. Wählen Sie unter „Startmodus“ die Option *Von Flash* und wählen Sie dann *Image 1* oder *Image 2*.

   – oder –

   Wählen Sie *Von Netzwerk* und geben Sie die folgenden Informationen ein:

   - IP-Adresse der Einheit: Geben Sie die feste IP-Adresse oder die von DHCP zugewiesene IP-Adresse des Konsolensystem ein.
   - TFTP-Server-IP: Geben Sie die IP-Adresse des TFTP-Startservers ein.
   - Dateiname: Geben Sie den Dateinamen der Start-Firmware ein.
3. Legen Sie über das Dropdown-Menü fest, ob der Watchdog-Timer aktiviert ist. Wenn der Watchdog-Timer aktiviert ist, wird das Konsolensystem bei einem Absturz der Software neu gestartet.
4. Wählen Sie im Dropdown-Menü die Geschwindigkeit des Konsolenports aus und klicken Sie auf *Speichern*.

Informationen

Klicken Sie auf *System – Informationen*, um die Identität des Konsolensystem sowie Informationen zu Versionen, Stromversorgung und CPU anzuzeigen.

Nutzung

Klicken Sie auf *System – Nutzung*, um Informationen zur Speicher- und Flash-Nutzung anzuzeigen.

3.3.4 Netzwerk

Klicken Sie auf *Netzwerk*, um die folgenden Netzwerkoptionen anzuzeigen und zu konfigurieren: Hostname, DNS, IPv6, Bündelung, statische IPv4- und IPv6-Routen, Hosts, Firewall, IPSec (VPN) und SNMP.

Einstellungen

Klicken Sie auf *Netzwerk – Einstellungen*, um Änderungen an den konfigurierten Netzwerkeinstellungen vorzunehmen.

Auf dieser Seite können Administratoren den Hostnamen und die DNS-Einstellungen des Konsolensystem konfigurieren. Dazu zählen primäres und sekundäres DNS, Domäne und Suchadressen. Weiterhin können Administratoren IPv6 aktivieren und so konfigurieren, dass DNS und/oder Domäne von DHCPv6 abgerufen werden.

Für eine fehlertolerante Netzwerkkonfiguration kann die Bündelung ausgewählt werden, die die Schnittstellen eth0 und eth1 zu einer einzelnen Netzwerkschnittstelle mit hoher Verfügbarkeit zusammenfasst, wobei der Bündelungsmodus „aktives Backup“ verwendet wird. Normalerweise ist die Schnittstelle eth0 aktiv, während eth1 als Backup dient. Wenn das Trägersignal auf eth0 ausfällt, wird eth1 zur aktiven Schnittstelle. Im Bündelungsmodus wird immer die MAC-Adresse von eth0 verwendet, unabhängig davon, welche Schnittstelle aktiv ist.

HINWEIS: Das Aktivieren oder Deaktivieren der Bündelung wird erst nach einem Neustart des Konsolensystem wirksam.

Routing-Typ

Das Konsolensystem unterstützt mehrere Routingtabellen und ermöglicht so das flexible Richtlinien-Routing. Mehrere Routingtabellen können nicht gleichzeitig mit dem Netzwerk-Failover oder der Bündelung aktiviert sein.

So aktivieren Sie mehrere Routingtabellen:

1. Klicken Sie auf *Netzwerk – Einstellungen*.
2. Klicken Sie unter „Mehrfach-Routing“ auf das Optionsfeld „Mehrere IPv4-Routingtabellen aktivieren“.

Netzwerk-Failover

Damit ein Konsolensystem auch während eines Netzwerkausfalls den zuverlässigen Zugriff auf kritische Geräte bieten kann, sollte es für Netzwerk-Failover konfiguriert werden. Ein Failover kann auftreten, wenn eine primäre Schnittstelle ausfällt oder wenn der Zugriff auf eine bestimmte IP-Adresse bzw. ein bestimmtes Gateway nicht mehr möglich ist. Das Failover kann über ein sekundäres Netzwerk oder eine PPP-Verbindung (Hinauswählen) aktiviert werden. Wenn das Hinauswählen konfiguriert ist, steht PPP0 als sekundäre Schnittstelle zur Verfügung, kann aber nicht als primäre Schnittstelle verwendet werden.

Durch die Verwendung der DSView-Software mit einem Konsolensystem wird sichergestellt, dass der Zugriff auf das Konsolensystem in einer Failover-Situation immer möglich ist, da das Konsolensystem „nach Hause telefoniert“ und seine IP-Adresse innerhalb der DSView-Software aktualisiert.

Administratoren können auf der Seite mit den Netzwerkeinstellungen eine sekundäre Netzwerkschnittstelle zur Verwendung mit dem Failover konfigurieren. Die primäre Schnittstelle legt das Standard-Gateway des Systems fest. Die sekundäre Schnittstelle wird verwendet, wenn die primäre Schnittstelle nicht verfügbar ist. Administratoren können auch einen von vier Auslösern zur Failover-Aktivierung auswählen:

- Primäre Schnittstelle nicht verfügbar
- Primäres Standardgateway nicht erreichbar
- DSView nicht erreichbar
- IP-Adresse nicht erreichbar

Wenn der IPSec-Tunnel konfiguriert wurde (siehe IPSec (VPN) auf Seite 34), können Administratoren ihn so konfigurieren, dass er über die sekundäre Schnittstelle, sofern verfügbar, eingerichtet wird.

So aktivieren Sie das Netzwerk-Failover:

1. Klicken Sie in der Seitenleiste der Registerkarte „Experte“ auf *Netzwerk – Einstellungen*.
2. Klicken Sie unter „Routing“ auf das entsprechende Optionsfeld, um das Netzwerk-Failover zu aktivieren.
3. Wählen Sie mithilfe der Dropdown-Menüs die primäre und die sekundäre Schnittstelle sowie den Namen der VPN-Verbindung aus.
4. Klicken Sie auf das Optionsfeld neben dem Auslöser, der das Failover einleiten soll.
5. Klicken Sie auf *Speichern*.

Bei entsprechend ausgestatteten Modellen können Sie Failover auch über das Funkmodem konfigurieren. Weitere Informationen finden Sie unter Verwenden des Funkmodems im Failover auf Seite 64.

HINWEIS: Das Funkmodem kann für Failover verwendet werden, wenn es nicht bereits als primäre Schnittstelle verwendet wird.

Geräte

Administratoren können die IP-Adressen, die den Netzwerkschnittstellen zugewiesen sind, auswählen, aktivieren und konfigurieren. Außerdem können sie die MAC-Adresse anzeigen. Die Liste der Netzwerkschnittstellen enthält außer den beiden standardmäßigen Ethernet-Schnittstellen einen Eintrag für jedes installierte USB-Ethernet-Gerät.

So konfigurieren Sie ein Netzwerkgerät:

1. Wählen Sie *Netzwerk – Geräte* aus. Daraufhin wird der Bildschirm „Geräte“ angezeigt. Auf diesem Bildschirm werden die Netzwerkschnittstellen zusammen mit ihrem jeweiligen Status (aktiviert oder deaktiviert) aufgelistet.
2. Klicken Sie auf den Namen des Netzwerkgeräts, das Sie konfigurieren möchten.
3. Aktivieren Sie das entsprechende Kontrollkästchen, wenn Sie das Netzwerkgerät als primäre Schnittstelle festlegen möchten. Standardmäßig ist eth0 als primäre Schnittstelle festgelegt.
4. Wählen Sie im Dropdown-Menü den Status aus (*Aktiviert* oder *Deaktiviert*).
5. Wählen Sie eine der folgenden Optionen für die IPv4-Methode aus:
   - Wählen Sie *DHCP* aus, damit die IPv4-Adresse vom DHCP-Server festgelegt wird.
   - Wählen Sie *Statisch* aus, wenn Sie die IPv4-Adresse, die Subnetzmaske und die Gateway-Adresse manuell eingeben möchten.
   - Wählen Sie *IPv4-Adresse nicht konfiguriert*, um IPv4 zu deaktivieren.
6. Wählen Sie eine der folgenden Optionen für die IPv6-Methode aus:
   - Wählen Sie *Zustandslos* aus, wenn die Verbindung auf die lokale IP-Adresse beschränkt ist.
   - Wählen Sie *DHCPv6* aus, damit die IPv6-Adresse vom DHCP-Server festgelegt wird.
   - Wählen Sie *Statisch* aus, wenn Sie die IPv6-Adresse und die Präfixlänge manuell eingeben möchten.
   - Wählen Sie *IPv6-Adresse nicht konfiguriert*, um IPv6 zu deaktivieren.

HINWEIS: Nach dieser Option wird die MAC-Adresse des Geräts angezeigt.

Statische IPv4- und IPv6-Routen

So fügen Sie statische Routen hinzu:

1. Wählen Sie *Netzwerk – Statische IPv4-Routen* oder *Statische IPv6-Routen*. Eventuell vorhandene statische Routen werden zusammen mit den jeweiligen Werten für Ziel-IP/Maske, Gateway, Schnittstelle und Metrik aufgelistet.
2. Klicken Sie auf *Hinzufügen*.
3. Wählen Sie *Standard* aus, um die Standardroute zu konfigurieren.

   – oder –

   Wählen Sie *Host-IP oder Netzwerk* aus, um benutzerdefinierte Einstellungen für Ziel-IP/Maske einzugeben.

Geben Sie in das Feld „Ziel-IP/Masken-Bits“ den erforderlichen Wert mit der Syntax <Ziel-IP>/<CIDR> ein.

4. Geben Sie die IP-Adresse des Gateways in das Feld „Gateway“ ein.
5. Wenn die Route nach Schnittstelle konfiguriert werden soll, geben Sie den Schnittstellennamen (Eth0, Eth1 oder PPPx) in das Feld „Schnittstelle“ ein.
6. Geben Sie die Anzahl der Hops zum Ziel in das Feld „Metrik“ ein und klicken Sie dann auf *Speichern*.

Hosts

Administratoren können eine Tabelle mit Hostnamen, IP-Adressen und Host-Aliasnamen für das lokale Netzwerk konfigurieren.

So fügen Sie einen Host hinzu:

1. Wählen Sie *Netzwerk – Hosts* aus.
2. Klicken Sie auf *Hinzufügen*, um einen neuen Host hinzuzufügen.
3. Geben Sie die IP-Adresse, den Hostnamen und den Aliasnamen für den hinzuzufügenden Host ein und klicken Sie dann auf *Speichern*.

So bearbeiten Sie einen Host:

1. Wählen Sie *Netzwerk – Hosts* aus.
2. Klicken Sie auf die IP-Adresse des Hosts, den Sie bearbeiten möchten.
3. Geben Sie einen neuen Hostnamen und ggf. einen neuen Aliasnamen ein und klicken Sie dann auf *Speichern*.

Firewall

Administratoren können das Konsolensystem so konfigurieren, dass es als Firewall fungiert. Standardmäßig akzeptieren drei integrierte Ketten alle Pakete des Typs INPUT, OUTPUT und FORWARD (eingehend, ausgehend, Weiterleitung). Durch Klicken auf die Schaltflächen *Hinzufügen*, *Löschen* oder *Richtlinie ändern* können Sie benutzerdefinierte Ketten hinzufügen oder löschen bzw. die Richtlinie der integrierten Ketten ändern. Sie können die Richtlinie von Standardketten ändern (Richtlinie ändern), um festzulegen, dass Pakete akzeptiert oder ignoriert werden; es ist jedoch nicht möglich, Standardketten zu löschen. Durch Klicken auf den *Kettennamen* können Sie Regeln für Ketten konfigurieren.

Zum Konfigurieren der Firewall klicken Sie auf *Netzwerk – Firewall*. Mit den Menüoptionen *IPv4-Filtertabelle* und *IPv6-Filtertabelle* werden separate, aber identische Konfigurationsbildschirme aufgerufen.

Für eine Standardkette kann nur die Richtlinie bearbeitet werden, wobei die Optionen AKZEPTIEREN und IGNORIEREN zur Verfügung stehen.

Wenn Sie eine Kette hinzufügen, wird nur ein benannter Eintrag für die Kette erstellt. Anschließend müssen Sie für die Kette mindestens eine Regel konfigurieren.

Konfigurieren der Firewall

Für jede Regel muss eine Aktion im Pulldown-Menü „Ziel“ ausgewählt werden (entweder *AKZEPTIEREN, IGNORIEREN, PROTOKOLLIEREN, ABLEHNEN oder ZURÜCKGEBEN*). Die ausgewählte Aktion wird für die IP-Pakete ausgeführt, die alle in der Regel angegebenen Kriterien erfüllen.

Wenn im Pulldown-Menü „Ziel“ die Option *PROTOKOLLIEREN* ausgewählt wurde, kann der Administrator eine Protokollierungsebene und ein Protokollpräfix konfigurieren.

Wenn im Pulldown-Menü „Ziel“ die Option *ABLEHNEN* ausgewählt wurde, kann der Administrator eine Option im Pulldown-Menü „Ablehnen mit“ auswählen. Das Paket wird ignoriert und ein Antwortpaket des ausgewählten Typs wird gesendet.

Protokolloptionen

Für jede Option im Pulldown-Menü „Protokoll“ sind verschiedene Felder verfügbar.

Wenn im Menü „Protokoll“ die Option *Numerisch* ausgewählt wurde, geben Sie eine Protokollnummer in das Textfeld ein.

Wenn im Menü „Protokoll“ die Option *TCP* ausgewählt wurde, können Sie im Bereich mit den TCP-Optionen die Quell- und Zielports sowie TCP-Flags eingeben.

Wenn im Menü „Protokoll“ die Option *UDP* ausgewählt wurde, können Sie im UDP-Bereich die Quell- und Zielports eingeben.

Tabelle 3.3 Firewall-Konfiguration – Felder für TCP- und UDP-Optionen

Feld/Menüoption	Definition
Quellport oder Zielport	Eine IP-Adresse oder ein IP-Adressbereich.
TCP-Flags	[Nur TCP] SYN (Synchronisieren), ACK (Bestätigen), FIN (Fertigstellen), RST (Zurücksetzen), URG (Dringend) und PSH (Push). Das Pulldown-Menü enthält für jedes Flag die folgenden Statusmöglichkeiten: Beliebig, Festlegen, Festlegung aufheben.

Wenn im Menü „Protokoll“ die Option ICMP ausgewählt wurde, steht das Pulldown-Menü „ICMP-Typ“ zur Verfügung.

Wenn der Administrator die Ethernet-Schnittstelle (eth0 oder eth1) in die Felder für die Eingabe- oder Ausgabeschnittstelle eingibt und im Pulldown-Menü „Fragmente“ eine Option auswählt (*2. und weitere Pakete, Alle Pakete und Fragmente* oder *Nicht fragmentierte Pakete und 1. Pakete*), wird die Zielaktion für Pakete ausgeführt, die von der angegebenen Schnittstelle oder an die angegebene Schnittstelle gesendet wurden, sofern sie die Kriterien der ausgewählten Menüoption „Fragmente“ erfüllen.

So fügen Sie eine Kette hinzu:

1. Wählen Sie *Netzwerk – Firewall* aus.
2. Wählen Sie entweder *IPv4-Filtertabelle* oder *IPv6-Filtertabelle* aus.
3. Klicken Sie auf *Hinzufügen*.
4. Geben Sie den Namen der hinzuzufügenden Kette ein.
5. Klicken Sie auf *Speichern*.

HINWEIS: Der Name der Kette darf keine Leerzeichen enthalten.

6. Fügen Sie mindestens eine Regel hinzu, um die Konfiguration der Kette fertigzustellen.

So ändern Sie die Richtlinie einer Standardkette:

HINWEIS: Benutzerdefinierte Ketten können nicht bearbeitet werden. Wenn Sie eine benutzerdefinierte Kette umbenennen möchten, müssen Sie sie löschen und eine neue Kette erstellen.

1. Wählen Sie *Netzwerk – Firewall* aus.
2. Wählen Sie entweder *IPv4-Filtertabelle* oder *IPv6-Filtertabelle* aus.
3. Aktivieren Sie das Kontrollkästchen neben der Kette, die Sie ändern möchten (*FORWARD, INPUT, OUTPUT*).
4. Klicken Sie auf *Richtlinie ändern* und wählen Sie dann im Dropdown-Menü entweder *Akzeptieren* oder *Ignorieren* aus.
5. Klicken Sie auf *Speichern*.

So fügen Sie eine Regel hinzu:

1. Wählen Sie *Netzwerk – Firewall* aus.
2. Wählen Sie entweder *IPv4-Filtertabelle* oder *IPv6-Filtertabelle* aus.
3. Klicken Sie in der Liste auf den Namen der Kette, der Sie eine Regel hinzufügen möchten.
4. Klicken Sie auf *Hinzufügen*, konfigurieren Sie die Regel und klicken Sie dann auf *Speichern*.

So bearbeiten Sie eine Regel:

1. Wählen Sie *Netzwerk – Firewall* aus.
2. Wählen Sie entweder *IPv4-Filtertabelle* oder *IPv6-Filtertabelle* aus.
3. Klicken Sie in der Liste auf den Namen der Kette, deren Regel Sie bearbeiten möchten.
4. Wählen Sie die Regel aus, die Sie bearbeiten möchten, und klicken Sie auf *Bearbeiten*.
5. Ändern Sie die Regel nach Bedarf und klicken Sie auf *Speichern*.

IPSec (VPN)

Ein VPN (Virtual Private Network, virtuelles privates Netzwerk) ermöglicht die sichere Kommunikation zwischen dem Konsolensystem und einem Remote-Netzwerk, indem eine sichere Verbindung zwischen dem Konsolensystem und einem Gateway hergestellt wird. Das IPSec-Protokoll wird verwendet, um den sicheren Tunnel aufzubauen. Dieses Protokoll bietet auch die Verschlüsselungs- und Authentifizierungsdienste auf IP-Ebene des Protokollstapels.

Wenn sich das Konsolensystem in einem separaten Netzwerk hinter einem Router befindet, wird ein IPSec-Tunnel mit einem X.509-Zertifikat zu einer Firewall aufgebaut. Die Zertifikate und Schlüssel werden von einer Zertifizierungsstelle (Certificate Authority, CA) an die Firewall und das Konsolensystem verteilt.

HINWEIS: Das Konsolensystem unterstützt ein Zertifikat pro Tunnel. Mehrere Zertifikate werden nicht unterstützt. IPv6-Tunnel werden ebenfalls nicht unterstützt. Zertifikate (im PKCS12-Format) können über das Menü „Systemtools“ geladen werden.

HINWEIS: Damit IPSec (VPN) ausgeführt werden kann, muss IPSec im benutzerdefinierten Sicherheitsprofil aktiviert sein.

Das Remote-Gateway ist der Remote-Host bzw. der rechte Host, während das Konsolensystem der lokale Host bzw. der linke Host ist.

Einrichten einer Zertifikatstelle

Zur Konfiguration der Fortinet Fortigate-Firewall müssen Sie einen internen CA-Server (CA = Certificate Authority, Zertifikatstelle) einrichten, der die RSA-Zertifikate erstellt, die das Konsolensystem für die Authentifizierung verwendet.

Einzelheiten zum Einrichten einer Zertifikatstelle auf einem Ubuntu-Server finden Sie unter Einrichten einer eigenen CA.

Einrichten eines Tunnels auf dem Server

So richten Sie einen Tunnel auf dem Server ein:

1. Klicken Sie auf der Registerkarte *System* der Fortigate-Weboberfläche auf die Schaltfläche *Zertifikate* und importieren Sie das CA-Zertifikat sowie das SERVER-Zertifikat, das vom Easy RSA-Server generiert wurde.
2. Klicken Sie auf der Registerkarte *Benutzer und Gerät* auf *PKI* und erstellen Sie einen neuen Benutzer namens **Benutzer1** mit einem CA namens **CA_Zert_1**. Erstellen Sie dann eine Benutzergruppe namens **Benutzergruppe1** und weisen Sie Benutzer1 dieser Gruppe zu.
3. Klicken Sie auf der Registerkarte *VPN* auf *IPSec – Tunnel* und erstellen Sie einen neuen benutzerdefinierten VPN-Tunnel mit der unten beschriebenen Konfiguration. Klicken Sie dann auf *OK*.

Tabelle 3.4 Konfigurationsparameter für den VPN-Tunnel

Parameter	Wert
Netzwerk	
Remote-Gateway	DFÜ-Benutzer
Schnittstelle	wan1
Moduskonfiguration	Aktiviert
IP-Version	IPv4
Client-Adressbereich	10.77.20.100-10.77.20.110
Subnetzmaske	255.255.255.0
System-DNS verwenden	Aktiviert
IPv4-Split-Tunnel aktivieren	Aktiviert
Erreichbare Netzwerke	local_lan
NAT-Traversal	Aktiviert
Keep-alive-Häufigkeit	300
Dead-Peer-Erkennung	Aktiviert
Authentifizierungs-	
methode	Signatur
Name des Zertifikats	server
IKE-Version	2
Peer-Optionen/Akzeptanztypen	Peer-Zertifikatgruppe
Peer-Zertifikatgruppe	Benutzergruppe1
Phase 1/Proposal	
Verschlüsselung	AES128
Authentifizierung	SHA1
Diffie-Hellman-Gruppe	14
Schlüsselgültigkeitsdauer (Sekunden)	86400
Lokale ID	C=<Land> S=<Bundesstaat/Bundesland> L=<Stadt> O=<Organisation>
Phase 2 bearbeiten	
Name	<Name>
Kommentare	<Kommentare>
Lokale Adresse/Subnetz	0.0.0.0/0.0.0.0
Remote-Adresse/Subnetz	0.0.0.0/0.0.0.0
Phase 2/Proposal	
Verschlüsselung	AES128
Authentifizierung	SHA1
Replay-Erkennung aktivieren	Aktiviert
PFS (Perfect Forward Secrecy) aktivieren	Aktiviert

Tabelle 3.4 Konfigurationsparameter für den VPN-Tunnel (Fortsetzung)

Parameter	Wert
Diffie-Hellman-Gruppe	14
Lokaler Port/Alle	Aktiviert
Remote-Port/Alle	Aktiviert
Protokoll/Alle	Aktiviert
Autokey-Keep-Alive	Aktiviert
Schlüsselgültigkeitsdauer	Sekunden
Sekunden	43200

4. Klicken Sie auf der Registerkarte *Richtlinie und Objekte* auf *Objekte – Adressen*, um einen VPN-Bereich mit den folgenden Einstellungen zu erstellen, und klicken Sie dann auf *OK*.

Tabelle 3.5 Konfiguration eines VPN-Bereichs

Parameter	Wert
Name	ipsec_vpn_range
Typ	IP-Bereich
Subnetz/IP-Bereich	10.77.20.100 - 10.77.20.110
Schnittstelle	Beliebig
In Adressliste anzeigen	Aktiviert
Kommentare	Die IP-Adresse der VPN-Clients, die eine Verbindung herstellen

5. Klicken Sie auf der Registerkarte *Richtlinie und Objekte* auf *Objekte – Adressen*, um einen lokalen LAN-Bereich mit den folgenden Einstellungen zu erstellen, und klicken Sie dann auf *OK*.

Tabelle 3.6 Konfiguration eines lokalen LAN-Bereichs

Parameter	Wert
Name	local_lan
Typ	IP/Netzmaske
Subnetz/IP-Bereich	192.168.1.0 / 255.255.255.0
Schnittstelle	Intern
In Adressliste anzeigen	Aktiviert
Kommentare	Lokales LAN – innerhalb des Netzwerks

6. Klicken Sie auf der Registerkarte *Richtlinie und Objekte* auf *Richtlinie – IPv4*, um die Firewall-Richtlinie 1 mit den folgenden Einstellungen zu erstellen, und klicken Sie dann auf *OK*.

Tabelle 3.7 Konfiguration der Firewall-Richtlinie 1

Parameter	Wert
Schnittstelle für eingehenden Datenverkehr	forti2acs
Quelladresse	ipsec_vpn_range
Schnittstelle für ausgehenden Datenverkehr	Intern
Zieladresse	local_lan
Zeitplan	Immer
Dienst	ALLE
Aktion	AKZEPTIEREN
Firewall/Netzwerkoptionen	
NAT	EIN
Schnittstellenadresse für ausgehenden Datenverkehr verwenden	Aktiviert
Sicherheitsprofile	
Anti-Virus, Webfilter, Anwendungskontrolle, SSL-Prüfung	Alle AUS
Traffic-Shaping (Verkehrsformung)	
Shared Shaper, Reverse Shaper, Per-IP Shaper	Alle AUS
Protokollierungsoptionen	
Zulässigen Datenverkehr protokollieren	EIN
Sicherheitsereignisse	Aktiviert
Kommentare	<Kommentare>
Diese Richtlinie aktivieren	Aktiviert

7. Klicken Sie auf der Registerkarte *Richtlinie und Objekte* auf *Richtlinie – IPv4*, um die Firewall-Richtlinie 2 mit den folgenden Einstellungen zu erstellen, und klicken Sie dann auf *OK*.

Tabelle 3.8 Konfiguration der Firewall-Richtlinie 2

Parameter	Wert
Schnittstelle für eingehenden Datenverkehr	Intern
Quelladresse	local_lan
Schnittstelle für ausgehenden Datenverkehr	forti2acs
Zieladresse	ipsec_vpn_range
Zeitplan	always (immer)
Dienst	ALLE
Aktion	AKZEPTIEREN
Firewall/Netzwerkoptionen	
NAT	EIN
Schnittstellenadresse für ausgehenden Datenverkehr verwenden	Aktiviert
Sicherheitsprofile	
Anti-Virus, Webfilter, Anwendungskontrolle, SSL-Prüfung	Alle AUS
Traffic-Shaping (Verkehrsformung)	
Shared Shaper, Reverse Shaper, Per-IP Shaper	Alle AUS
Protokollierungsoptionen	
Zulässigen Datenverkehr protokollieren	EIN
Sicherheitsereignisse	Aktiviert
Kommentare	<Kommentare>
Diese Richtlinie aktivieren	Aktiviert

8. Klicken Sie auf der Registerkarte *Richtlinie und Objekte* auf *Richtlinie – IPv4*, um die Firewall-Richtlinie 3 mit den folgenden Einstellungen zu erstellen, und klicken Sie dann auf *OK*.

Tabelle 3.9 Konfiguration der Firewall-Richtlinie 3

Parameter	Wert
Schnittstelle für eingehenden Datenverkehr	Beliebig
Quelladresse	Alle
Schnittstelle für ausgehenden Datenverkehr	Beliebig
Zieladresse	Alle
Aktion	VERWEIGERN
Protokollierungsoptionen	
Unzulässigen Datenverkehr protokollieren	AUS

Einrichten eines Tunnels auf dem Konsolensystem

So richten Sie einen Tunnel auf dem Konsolensystem ein:

1. Klicken Sie in der Seitenleiste der Registerkarte *Experte* auf *Netzwerk – IPSec (VPN)* und klicken Sie dann auf *Hinzufügen*.

2. Geben Sie einen Namen für die Verbindung ein.
3. Wählen Sie mithilfe der Dropdown-Menüs die Option *IKEv2* für die IKE-Version und entweder *Start*, *Hinzufügen* oder *Ignorieren* für die Startaktion.
    a. Start – lädt eine Verbindung und startet sie sofort (beim Hochfahren oder nach dem Speichern der Konfiguration).
    b. Hinzufügen – lädt eine Verbindung, ohne sie zu starten. Beispielsweise kann das VPN mit einem Skript bedingt gestartet werden.
    c. Ignorieren – ignoriert die Verbindung
4. Geben Sie für Remote-Seite (rechts) die folgenden Parameter ein:
    a. Lassen Sie das ID-Feld leer.
    b. Geben Sie die IP-Adresse des Remote-VPN in das Feld für die IP-Adresse ein.
    c. Geben Sie das Subnetz, über das das Konsolensystem eine Verbindung herstellen soll, in das Feld „Subnetz“ ein.
5. Geben Sie für lokale Seite (links) die folgenden Parameter ein:
    a. Lassen Sie das ID-Feld leer.
    b. Geben Sie die IP-Adresse der primären Schnittstelle in das Feld für die IP-Adresse ein.

HINWEIS: Die primäre Schnittstelle ist die Schnittstelle (etho oder eth1), die zur Verbindung mit der Remote-Firewall verwendet wird. Standardmäßig lautet die Einstellung eth0 und „Abruf der BOOTP-Konfiguration“ ist aktiviert. Wenn Ihre primäre Schnittstelle eth1 ist, stellen Sie sicher, dass „Abruf der BOOTP-Konfiguration“ auf der Seite „Sicherheitsprofil“ deaktiviert ist.

6. Klicken Sie auf das Optionsfeld „RSA-Zertifikat“, klicken Sie auf den Dropdown-Pfeil „Lokale PKCS12-Dateien“ und wählen Sie die PKCS12-Datei aus.

So aktivieren Sie IPSec auf dem Konsolensystem:

1. Klicken Sie in der Seitenleiste der Registerkarte *Experte* auf *System – Sicherheit – Sicherheitsprofil*.
2. Klicken Sie unter „Sicherheitsprofil“ auf das Optionsfeld „Benutzerdefiniert“.
3. Aktivieren Sie das Kontrollkästchen „IPSec aktivieren“ und klicken Sie dann auf *Speichern*.

HINWEIS: Nachdem auf die Schaltfläche „Speichern“ geklickt wurde, wird die VPN-Verbindung automatisch gestartet, wenn die Startaktion „Start“ ist. Die Informationen werden gespeichert und das VPN startet (oder startet neu).

Überprüfung

Sie können Tests ausführen, um zu überprüfen, ob die IPSec-Konfiguration erfolgreich war. Der Ping-Befehl wird zum Testen der Kommunikation verwendet.

So können Sie den IPSec-Status überprüfen und die Kommunikation testen:

1. Melden Sie sich als Stammbenutzer (root) beim Konsolensystem an.
2. Überprüfen Sie den IPSec-Status, indem Sie den Befehl *ipsec status* in die Shell-Eingabeaufforderung eingeben. Notieren Sie die VPN-DHCP-IP-Adresse.
3. Geben Sie ping in die Befehlszeile ein, drücken Sie die Leertaste, geben Sie die Adresse ein, die Sie anpingen möchten, drücken Sie dann die Eingabetaste auf Ihrer Tastatur und warten Sie auf die Ping-Ergebnisse. Testen Sie die Kommunikation vom Konsolensystem zum Ziel-Client des Remote-Subnetzes.

4. Testen Sie die Kommunikation vom Ziel-Client des Remote-Subnetzes zur VPN-DHCP-IP-Adresse des Konsolensystem.

HINWEIS: Um die Kommunikation zu testen, geben Sie ping vom Ziel-Client zur VPN-DHCP-IP-Adresse des Konsolensystem und vom Konsolensystem zum Ziel-Client des Subnetzes ein.

3.3.5 IPSec (VPN) – Erweiterte Einstellungen

Die Konfigurationsseite für IPSec (VPN) enthält die erweiterten Einstellungen für die Datei ipsec.conf. Diese in der folgenden Tabelle beschriebenen Einstellungen werden angezeigt, wenn das Kontrollkästchen „Erweiterte Einstellungen anzeigen“ aktiviert ist.

Tabelle 3.10 Erweiterte Einstellungen – Beschreibungen

Name	Beschreibung
IKE (Internet Key Exchange) Verschlüsselungs-Suite	Protokolle, die zum Austausch kryptographischer Schlüssel verwendet werden. Die Suite umfasst Algorithmen für Verschlüsselungs- (Vertraulichkeit), Hash- (Nachrichtenauthentifizierung) und DH-Gruppen-Protokolle (Schlüsselaustausch) beim Einrichten des VPN.
ESP (Encapsulating Security Payload) Verschlüsselungs-Suite	Protokolle, die zum Austausch kryptographischer Schlüssel verwendet werden. Die Suite umfasst Algorithmen für Verschlüsselungs- (Vertraulichkeit), Hash- (Nachrichtenauthentifizierung) und DH-Gruppen-Protokolle (Schlüsselaustausch) beim Einrichten des VPN. Wenn die DH-Gruppe verwendet wird, sind die höheren Gruppennummern sicherer, aber es dauert länger, den Schlüssel zu berechnen.
Security Association (SA)	Eine SA beschreibt, wie zwei oder mehr Geräte sicher miteinander kommunizieren.
Erneute Authentifizierung	Gibt an, ob sich das Gerät erneut authentifizieren soll, wenn sich eine IKE Security Association (SA) ändert.
IKE-Gültigkeitsdauer	Gibt an, wie lange der Keying-Kanal einer Verbindung (ISAKMP oder IKE SA) dauern soll, bevor sie neu ausgehandelt wird.
Schlüsselgültigkeitsdauer	Gibt an, wie lange eine bestimmte Instanz einer Verbindung (ein Satz von Verschlüsselungs-/Authentifizierungsschlüsseln für Benutzerpakete) von der erfolgreichen Verhandlung bis zum Ablauf dauern soll.
Rekey	Gibt an, ob eine Verbindung neu ausgehandelt werden soll, wenn sie kurz vor dem Ablauf steht.
Keying-Versuche	Gibt an, wie viele Versuche (eine positive ganze Zahl oder %forever) unternommen werden sollen, um eine Verbindung oder einen Ersatz für eine Verbindung auszuhandeln, bevor aufgegeben wird. Der Standardwert lautet 3.
Rekey-Begrenzung	Gibt an, wie lange vor Ablauf der Verbindung oder des Keying-Kanals versucht werden soll, einen Ersatz auszuhandeln.
DPD-Verzögerung	Gibt das Periodenzeitintervall an, mit dem R_U_THERE messages/INFORMATIONAL-Austausche an den Peer gesendet werden.

3.3.6 SNMP-Konfiguration

Administratoren können das SNMP-Protokoll konfigurieren. Dieses Protokoll wird benötigt, wenn Benachrichtigungen an eine SNMP-Verwaltungsanwendung gesendet werden sollen.

HINWEIS: Die Avocent® ACS800/8000 Advanced Console System Enterprise MIB-Textdatei ist in der Einheit an folgendem Speicherort verfügbar: /usr/local/mibs/ACS8000-MIB.asn. Die Avocent® ACS800/8000 Advanced Console System Enterprise TRAP MIB-Textdatei ist in der Einheit an folgendem Speicherort verfügbar: /usr/local/mibs/ACS8000-TRAP-MIB.asn. Beide Dateien sind auch unter www.VertivCo.com verfügbar. #

So konfigurieren Sie SNMP:

1. Klicken Sie auf *Netzwerk – SNMP*.
2. Klicken Sie auf die Schaltfläche *System*.
   a. Geben Sie die SysContact-Informationen ein (E-Mail-Adresse des Konsolensystem-Administrators, zum Beispiel acs8000_admin@vertivco.com).
   b. Geben Sie die SysLocation-Informationen ein (physischer Standort des Konsolensystem, wie zum Beispiel Avocent_ACS8000). Klicken Sie dann auf *Speichern*, um zum SNMP-Bildschirm zurückzukehren.
3. Klicken Sie auf *Hinzufügen*, um eine neue Community oder einen neuen V3-Benutzer hinzuzufügen.
4. Geben Sie in das Feld „Name“ den Community-Namen für SNMP V1/V2 bzw. den Benutzernamen für SNMP V3 ein. Geben Sie dann die OID ein.
5. Wählen Sie die gewünschte Berechtigung im Pulldown-Menü aus. Die verfügbaren Optionen sind *Lese- und Schreibzugriff* sowie *Nur Lesezugriff*.
6. Wenn SNMP V1 oder V2 erforderlich ist, klicken Sie auf die Schaltfläche *Version V1, V2* und geben Sie dann die Quelle ein (die gültige Eingabe ist die Subnetz-Adresse).

   – oder –

   Wenn SNMP V1 oder V2 mit einem IPv6-Netzwerk erforderlich ist, klicken Sie auf die Schaltfläche *Version V1,V2 für IPv6-Netzwerk* und geben Sie dann die Quelle ein (die gültige Eingabe ist die Subnetz-Adresse).

   – oder –

   Wenn SNMP V3 erforderlich ist, klicken Sie auf die Schaltfläche *Version V3*. Wählen Sie dann den Authentifizierungstyp aus (*MD5* oder *SHA*), geben Sie die Passphrase oder das Kennwort für die Authentifizierung ein, wählen Sie die Verschlüsselungsmethode aus (DES oder AES), geben Sie die Passphrase für den Datenschutz ein und wählen Sie die Mindestauthentifizierungsstufe aus (*NoAuthNoPriv*, *AuthNoPriv*, *AuthPriv*).

7. Klicken Sie auf *Speichern*.

HINWEIS: Für SNMP V1/V2c bietet das Konsolensystem dem Administrator die Möglichkeit, denselben Community-Namen mit verschiedenen Quellen (Filtern) zu konfigurieren, um den Zugriff auf spezifische Objektkennungen (OIDs) zu ermöglichen.

3.3.7 Ports

Administratoren können auf der Registerkarte „Ports“ in der seitlichen Navigationsleiste serielle Ports, Aux-Ports, das CAS-Profil und das Einwahlprofil aktivieren und konfigurieren. Auf dem Bildschirm für Aux-Ports kann das interne Modem aktiviert und konfiguriert werden.

Die seriellen Ports des Konsolensystem können mehrere unterschiedliche Rollen haben, je nach dem Profil, das für den jeweiligen Port konfiguriert wurde.

Serielle Ports

In der Tabelle „Serielle Ports“ können Sie das Verbindungsprofil (CAS, Einwahl, Strom, Hinauswählen oder Socket-Client) auf Grundlage des Typs des angeschlossenen Geräts auswählen. Außerdem können Sie den Port klonen, das System auf die werkseitigen Standardeinstellungen zurücksetzen, Ports aktivieren oder deaktivieren und eine serielle Sitzung öffnen.

Die Tabelle zeigt die Portnummer, die Geräte-ID, den Status, den Namen, das Profil, Signale und Einstellungen. Die Spalte „Einstellungen“ enthält die für den Port verwendete Pinbelegung. Dabei werden die folgenden Abkürzungen verwendet:

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

HINWEIS: Wenn kein Gerät an den Port angeschlossen ist, wird die Pinbelegung möglicherweise nicht angezeigt.

So aktivieren oder deaktivieren Sie einen oder mehrere serielle Ports:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Aktivieren Sie die Kontrollkästchen für die Ports, die Sie aktivieren oder deaktivieren möchten.
3. Klicken Sie auf die Schaltfläche *Aktivieren* oder *Deaktivieren*.

So konfigurieren oder bearbeiten Sie einen oder mehrere serielle Ports mit dem CAS-Profil:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Aktivieren Sie die Kontrollkästchen für die Ports, die Sie konfigurieren möchten.
3. Klicken Sie auf die Schaltfläche *CAS festlegen*. Verwenden Sie die Dropdown-Menüs, um den Port zu aktivieren oder zu deaktivieren und die RJ45-Pinbelegung, Geschwindigkeit, Parität, Datenbits, Stopbits und Flusssteuerung festzulegen.

HINWEIS: Wenn Sie für die RJ45-Pinbelegung die Option „Automatisch“ auswählen, wird die automatische Erkennung der Cyclades- oder Cisco-Pinbelegung für RS-232-Geräte aktiviert.

4. Klicken Sie auf *Weiter* oder auf den Link *CAS*.
    a. Geben Sie den Portnamen ein (wenn nur ein Port ausgewählt wurde) oder geben Sie das Präfix des Portnamens ein (wenn mehr als ein Port ausgewählt wurde). Der Portname lautet <Präfix des Portnamens>-p-<Portnummer>.
    b. Aktivieren Sie das Kontrollkästchen „Automatische Erkennung“. In diesem Fall wird der Portname verwendet, wenn die automatische Erkennung den Servernamen nicht erkennen kann.
    c. Aktivieren Sie das Kontrollkästchen „Automatische Geschwindigkeitserkennung aktivieren“.

HINWEIS: Für die automatische Geschwindigkeitserkennung müssen weitere Einstellungen auf dem Bildschirm „CAS-Profil – Einstellungen für die automatische Erkennung“ konfiguriert werden.

    d. Legen Sie das Protokoll und den Authentifizierungstyp über die Dropdown-Menüs fest.
    e. Geben Sie die Hotkeys für Textsitzung, Stromverwaltungssitzung und RESTful in die vorgesehenen Felder ein.

f. Geben Sie das TCP-Port-Alias für jeden Protokolltyp (Telnet, SSH und Raw-Modus) in die vorgesehenen Felder ein.

g. Geben Sie das IPv4- oder IPv6-Alias und die zugehörige Schnittstelle in das vorgesehene Feld ein.

h. Aktivieren Sie bei Bedarf die Kontrollkästchen „Sitzung nur zulassen, wenn DCD eingeschaltet ist“ und „Automatische Antwort aktivieren“.

i. Wählen Sie im Dropdown-Menü den DTR-Modus aus und geben Sie das DTR-Aus-Intervall ein.

j. Aktivieren oder deaktivieren Sie über die Dropdown-Menüs die Optionen „Unterdrückung des Zeilenvorschubs“ und „NULL nach CR-Unterdrückung“.

k. Geben Sie das Übertragungsintervall, die Unterbrechungssequenz und das Unterbrechungsintervall in die vorgesehenen Felder ein.

HINWEIS: Das Übertragungsintervall definiert die Verzögerung (in Millisekunden), bevor die Übertragung von Daten an das Ethernet über eine serielle Schnittstelle empfangen wird. Der Standardwert lautet 20 ms.

l. Aktivieren oder deaktivieren Sie über das Dropdown-Menü das Menü für eine Mehrfachsitzung. Weitere Informationen finden Sie unter Menü für Mehrfachsitzung auf Seite 51.

m. Aktivieren oder deaktivieren Sie über die Dropdown-Menüs die Optionen „Benachrichtigung für Anmelden/Abmelden bei Mehrfachsitzung“ und „Informationsbenachrichtigung“.

5. Klicken Sie auf *Weiter* oder klicken Sie auf den Link *Datenpufferung* und verwenden Sie dann die Dropdown-Menüs, um die Datenpufferung zu aktivieren und zu konfigurieren.
6. Klicken Sie auf *Weiter* oder klicken Sie auf den Link *Alarme*.
   a. Klicken Sie auf *Alarme aktivieren*, um die Erkennung von Alarmen zu aktivieren.
   b. Klicken Sie auf *Hinzufügen*, um eine Alarmzeichenfolge hinzuzufügen. Geben Sie in das Feld „Alarmzeichenfolge“ die gewünschte Zeichenfolge ein. Geben Sie in das Feld „Skript“ das Shell-Skript ein, das ausgeführt wird, wenn eine Übereinstimmung auftritt. Aktivieren Sie das Kontrollkästchen „Notfall“, wenn die LED des seriellen Ports bei jedem Auftreten dieses Alarms schnell orange blinken soll. Wenn es sich bei dem Alarm nicht um einen Notfall handelt, blinkt die LED langsam. Klicken Sie auf *Weiter*, um zum Bildschirm „Alarme“ zurückzukehren.

HINWEIS: Das Konsolensystem bietet Administratoren die Möglichkeit, der Alarmzeichenfolge ein Shell-Skript zuzuweisen. Wenn eine Übereinstimmung mit der Alarmzeichenfolge auftritt, ruft das Konsolensystem das Skript auf und übergibt die Portnummer und die Zeile, in der die Übereinstimmung aufgetreten ist, als Argumente.

   c. Aktivieren Sie das Kontrollkästchen neben einem vorhandenen Alarm und klicken Sie auf *Löschen*, um die Zeichenfolge zu löschen.
   d. Klicken Sie auf *Beliebige löschen*, um alle Zeichenfolgen zu löschen, unabhängig davon, ob sie ausgewählt sind oder nicht.

HINWEIS: Durch Klicken auf *Beliebige löschen* werden alle Alarmzeichenfolgen gelöscht. Wenn Sie alle Alarmzeichenfolgen auswählen und auf *Löschen* klicken, hat dies nicht dieselbe Wirkung, da bei dieser Methode die Alarmzeichenfolgen, die nicht in der Tabelle sichtbar sind, nicht gelöscht werden.

7. Klicken Sie auf *Weiter* oder klicken Sie auf den Link *Strom*.

a. Klicken Sie auf *Hinzufügen*, um einen neuen Ausgang hinzuzufügen. Klicken Sie auf *PDU auswählen* und wählen Sie eine PDU in der Liste der erkannten PDUs aus. Geben Sie den oder die Ausgänge in das Feld „Ausgänge“ ein und klicken Sie auf *Weiter*.

b. Aktivieren Sie das Kontrollkästchen neben einem verbundenen Ausgang und klicken Sie auf *Löschen*.

HINWEIS: Die Option „Strom“ ist nur verfügbar, wenn ein einzelner serieller Port ausgewählt ist.

8. Klicken Sie auf *Speichern*.

Tabelle 3.11 Parameter des CAS-Profils

Parameter	Beschreibung
Physisch	
Status	Definiert den Status des seriellen Ports (aktiviert oder deaktiviert). Standard: Deaktiviert.
RJ45-Pinbelegung	Definiert die Pinbelegung des seriellen Ports. Mögliche Optionen sind „Automatisch“, „Cyclades“ und „Cisco“. Für die Ports 1 und 2 werden auch die Pinbelegungen RS-422 und RS-485 unterstützt. Standard: Automatisch.
Geschwindigkeit	Definiert die Geschwindigkeit. Mögliche Werte sind 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 und 230400. Standard: 9600.
Parität	Definiert die Parität. Mögliche Werte: Gerade, Ungerade, Keine. Standard: Keine.
Datenbits	Definiert die Datenbits. Mögliche Werte sind 5, 6, 7 und 8. Standard: 8.
Stoppbits	Definiert die Stoppbits. Mögliche Werte sind 1 und 2. Standard: 1.
Flusssteuerung	Definiert die Flusssteuerung. Mögliche Werte: Keine, Hardware, Software, RxON-Software, TxON-Software. Standard: Keine.
CAS	
Portname	Der dem seriellen Port zugewiesene Name (als Alias). Standard: <Mac-Adresse der Einheit>-p-<Portnummer>.
Automatische Erkennung aktivieren	Der Zielgerät-Name wird erkannt und diesem seriellen Port zugewiesen. Wenn die automatische Erkennung fehlschlägt, wird der Portname verwendet. Standard: Deaktiviert.
Automatische Geschwindigkeitserkennung aktivieren	Versucht, die Geschwindigkeit des seriellen Ports zu erkennen. Für diese Funktion müssen weitere Einstellungen auf der Seite „CAS-Profil – Automatische Erkennung – Einstellungen“ konfiguriert werden. Standard: Deaktiviert.
Protokoll	Das Protokoll, das von autorisierten Benutzern für den Zugriff auf den seriellen Port bzw. das Ziel verwendet wird. Das Konsolensystem akzeptiert drei Protokolle für die Verbindung mit dem Ziel: Telnet für eine Telnet-Verbindung, SSH für eine sichere Verbindung und Raw-Modus für eine Raw-Socket-Verbindung. Administratoren können den Port so konfigurieren, dass er entweder einen, zwei oder alle drei Typen akzeptiert. **HINWEIS:** Für das Raw-Protokoll muss ein Raw-Modus-Portalias konfiguriert werden. Standardwert: SSH.
Authentifizierungstyp	Der Authentifizierungstyp, mit dem der Benutzer während einer Sitzung mit dem Ziel authentifiziert wird. Standard: Lokal.
Hotkey für Textsitzung	Über diesen Hotkey können Benutzer die Sitzung mit dem Ziel unterbrechen und die CLI-Eingabeaufforderung aufrufen. Im Raw-Modus nicht verfügbar. Standard: **Strg-Z**. Hinweis: Das standardmäßige Escape-Zeichen für ts_menu ist **Strg-X**.
Hotkey für Stromverwaltungssitzung	Über diesen Hotkey können Benutzer die Sitzung mit dem Ziel unterbrechen und das Menü für die Stromverwaltung aufrufen, um die Ausgänge zu steuern, die mit dem Ziel verbunden sind. Im Raw-Modus nicht verfügbar. Standard: **Strg-P**. Hinweis: Das standardmäßige Escape-Zeichen für ts_menu ist **Strg-X**.
RESTful-Hotkey	Über diesen Hotkey können Benutzer die Sitzung mit dem Ziel unterbrechen und das RESTful-Menü aufrufen, mit dem benutzerdefinierte RESTful-Aktionen ausgeführt werden können. Standard: nicht konfiguriert (leer).
TCP-Port-Alias	Telnet-Port-Alias: TCP-Port für die direkte Verbindung mit einem seriellen Port unter Verwendung des Telnet-Protokolls. SSH-Port-Alias: TCP-Port für die direkte Verbindung mit einem seriellen Port unter Verwendung des SSH-Protokolls. Raw-Modus-Portalias: TCP-Port für die direkte Verbindung mit einem seriellen Port unter Verwendung von Raw-Socket.
Port-IPv4-Alias/Port-IPv6-Alias	IPv4-/IPv6-Adresse für die direkte Verbindung mit einem seriellen Port. Standard: nicht konfiguriert (leer).
Port-IPv4-Alias-Schnittstelle/Port-IPv6-Alias-	Schnittstelle (ETH0/ETH1), die dem IPv4-/IPv6-Alias zugeordnet ist. Standard: ETH0.

Tabelle 3.11 Parameter des CAS-Profils (Fortsetzung)

Parameter	Beschreibung
Schnittstelle	
Sitzung nur zulassen, wenn DCD eingeschaltet ist	Bei ausgeschaltetem DCD verweigert die Einheit den Zugriff für diesen seriellen Port. Standard: Deaktiviert (Zugriff erlauben, wenn DCD ausgeschaltet ist).
Automatische Antwort aktivieren	Wenn die Eingabedaten einer Eingabezeichenfolge entsprechen, die für „Automatische Antwort“ konfiguriert ist, wird die Ausgabezeichenfolge an den seriellen Port übertragen. Standard: Deaktiviert.
DTR-Modus	Der DTR-Modus kann folgendermaßen eingestellt werden: „Immer ein“. „Normal“ – der DTR-Status hängt davon ab, ob eine CAS-Sitzung vorhanden ist. „Aus-Intervall“ – wenn eine CAS-Sitzung geschlossen wird, bleibt DTR während dieses Intervalls ausgeschaltet. Standard: Normal.
DTR-Aus-Intervall	Aus-Intervall für den DTR-Modus in Millisekunden. Standard: 100.
Unterdrückung des Zeilenvorschubs	Aktiviert die Unterdrückung des LF-Zeichens (LF = Line Feed, Zeilenvorschub) nach dem CR-Zeichen (CR = Carriage Return, Wagenrücklauf). Standard: Deaktiviert.
NULL nach CR-Unterdrückung	Aktiviert die Unterdrückung des NULL-Zeichens nach dem CR-Zeichen. Standard: Deaktiviert.
Übertragungsintervall	Dieses Intervall gibt in Millisekunden an, wie lange der Port wartet, bis Daten an einen Remote-Client gesendet werden. Standard: 20.
Unterbrechungssequenz	Administratoren können die Strg-Taste als Unterbrechungssequenz konfigurieren. Dazu muss vor dem Buchstaben das Zeichen ^ eingegeben werden. Im Raw-Modus nicht verfügbar. Standard: ~break.
Unterbrechungsintervall	Intervall für das Unterbrechungssignal in Millisekunden. Im Raw-Modus nicht verfügbar. Standard: 500.
Menü für Mehrfachsitzung anzeigen	Aktiviert das Menü für eine Mehrfachsitzung, wenn eine Verbindung mit einem Port hergestellt wird, auf den bereits ein anderer Benutzer zugreift. Standard: Deaktiviert.
Benachrichtigung für Anmelden/Abmelden bei Mehrfachsitzung	Aktiviert die Benachrichtigung, die an Benutzer einer Mehrfachsitzung gesendet wird, wenn sich ein neuer Benutzer anmeldet oder wenn sich ein Benutzer abmeldet. Im Raw-Modus nicht verfügbar. Standard: Deaktiviert.
Informationsbenachrichtigung	Zeigt eine Informationsmeldung an, wenn eine Sitzung mit einem Ziel geöffnet wird. Im Raw-Modus nicht verfügbar. Standard: Aktiviert.
Datenpufferung	
Status	Aktiviert oder deaktiviert die Datenpufferung. Standard: Deaktiviert.
Typ	Zeigt den Typ der Datenpufferung an: „Lokal“ – speichert die Datenpufferungsdatei im lokalen Dateisystem. „NFS“ – speichert die Datenpufferungsdatei auf dem NFS-Server. „Syslog“ – sendet die Daten an den Syslog-Server. „DSView“ – sendet die Daten an die DSView-Software. Standard: Lokal.
Lokaler Typ	Wenn der Typ auf „Lokal“ eingestellt ist, kann hier der Speicherort der Datenpufferungsdateien im lokalen Dateisystem angegeben werden. Mögliche Optionen sind der integrierte Speicher (mmcblk0) und Speicherorte auf angeschlossenen USB-Speichergeräten und SD-Karten. Standard: mmcblk0.
Zeitstempel	Wenn diese Option aktiviert ist, wird der Datenpufferungszeile in einer lokalen oder NFS-Datenbank der Zeitstempel hinzugefügt. Standard: Deaktiviert.
Nachricht bei Anmeldung/Abmeldung	Schließt besondere Benachrichtigungen zu An- und Abmeldungen in die Datenpufferung ein. Standard: Deaktiviert.
Protokollierung für serielle Sitzung	Aktiviert – Daten werden immer gespeichert. Deaktiviert – Daten werden gespeichert, wenn keine CAS-Sitzung geöffnet ist. Standard: Aktiviert.
Alarme	
Status	Wenn die Eingabedaten einer der Alarmzeichenfolgen entsprechen, wird eine besondere Ereignisbenachrichtigung generiert. Standard: Deaktiviert.

Tabelle 3.11 Parameter des CAS-Profils (Fortsetzung)

Parameter	Beschreibung
Alarmzeichenfolgen	Diese Zeichenfolgen werden zum Generieren von Ereignisbenachrichtigungen verwendet. Standard: Leer.
Skript	Name des Shell-Skripts, das aufgerufen wird, wenn eine Übereinstimmung mit der Alarmzeichenfolge in der Zeile vorliegt. Das Skript wird mit zwei Argumenten aufgerufen: mit der Portnummer und mit der Zeile, in der die Übereinstimmung aufgetreten ist.
Notfall	Wenn ein Alarm als Notfall gekennzeichnet wird, blinkt die orangefarbene LED des seriellen Ports schnell, wenn dieser Alarm auftritt. Wenn es sich nicht um einen Notfall handelt, blinkt die orangefarbene LED langsam.

So konfigurieren Sie das Einwahlprofil für einen seriellen Port, an den ein Modem angeschlossen ist:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Aktivieren Sie das Kontrollkästchen für einen seriellen Port mit angeschlossenem Modem.
3. Klicken Sie auf die Schaltfläche *Einwahl festlegen* und konfigurieren Sie dann mithilfe der Dropdown-Menüs die Einwahl-Einstellungen.
4. Konfigurieren Sie die PPP-Parameter (Adresse, Authentifizierung usw.) und klicken Sie auf *Speichern*.

Tabelle 3.12 Parameter für die Einwahl

Parameter	Beschreibung
Status	Aktiviert oder deaktiviert den Port. Standard: Deaktiviert.
Geschwindigkeit	Die Geschwindigkeit, die von mgetty zur Konfiguration des seriellen Geräts verwendet wird. Standard: 38400 bit/s.
Chat initialisieren	Chat für die Initialisierung des Modems. Standard: "" \d\d\d+++\d\d\dATZ OK.
PPP-Adresse	Konfiguriert die lokale IP-Adresse und die Remote-IP-Adresse für die PPP-Verbindung. Wenn die Option *Konfiguration von Remote-Peer akzeptieren* ausgewählt ist, sollte der Remote-Peer während der Aushandlung beide IP-Adressen (lokal und Remote) senden. Standard: keine Adresse.
Lokale IPv4-/IPv6-Adresse	Konfiguriert die lokale IPv4-/IPv6-Adresse für diese PPP-Verbindung.
Remote-IPv4-/IPv6-Adresse	Konfiguriert die Remote-IPv4-/IPv6-Adresse für diese PPP-Verbindung.
PPP-Authentifizierungsprotokoll	Über die Optionsfelder kann eine der folgenden Optionen ausgewählt werden: Keine, PAP, CHAP, EAP. Keine – keine Authentifizierung. • PAP – verwendet das PAP-Protokoll und den konfigurierten PPP-Authentifizierungstyp (gemäß Konfiguration auf der Seite „Authentifizierung – Einheitenauthentifizierung“). • CHAP – verwendet das CHAP-Protokoll. Die CHAP-Geheimfragen sollten beim Bearbeiten der Datei /etc/ppp/chap-secrets konfiguriert werden. • EAP – verwendet das EAP-Protokoll. Verfügbare Authentifizierungsmethoden: CHAP, SRP-SHA1 und TLS. Die CHAP-Geheimfragen sollten beim Bearbeiten der Datei /etc/ppp/chap-secrets konfiguriert werden. Die Geheimfragen für SRP-SHA1 sollten beim Bearbeiten der Datei /etc/ppp/srp-secrets konfiguriert werden. Hinweis: Die EAP-Authentifizierung ist nur unter Windows XP verfügbar. Standard: Keine.
CHAP	Konfigurieren Sie die Parameter „Chap-interval“, „Chap-max-challenge“ und „Chap-restart“. Standardwerte: • Chap-interval = 0. • Chap-max-challenge = 10. • Chap-restart = 3.
PPP-Inaktivitäts-Timeout	Dauer der Inaktivität in Sekunden, nach der bei PPP eine Zeitüberschreitung auftritt. Standard: 0 (kein Timeout).

So konfigurieren oder bearbeiten Sie einen oder mehrere serielle Ports mit einer angeschlossenen PDU:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Aktivieren Sie das Kontrollkästchen für einen oder mehrere serielle Ports mit angeschlossener PDU.
3. Klicken Sie auf die Schaltfläche *Strom festlegen* und konfigurieren Sie die physischen Einstellungen mithilfe der Dropdown-Menüs.
4. Klicken Sie auf *Weiter* oder klicken Sie auf den Link *Strom*.
    a. Wählen Sie den PDU-Typ im Dropdown-Menü aus.
    b. Aktivieren Sie das Kontrollkästchen „Automatische Geschwindigkeitserkennung aktivieren“.
    c. Konfigurieren Sie die Abfragerate.
    d. Geben Sie für Avocent-/Cyclades-PDUs das Intervall für das Ausschalten und erneute Einschalten ein und verwenden Sie dann die Dropdown-Menüs, um Syslog, Tonsignal und SW-Überstromschutz zu aktivieren oder zu deaktivieren.
5. Klicken Sie auf *Speichern*.

Tabelle 3.13 Parameter für den Strom

Parameter	Beschreibung
Physisch	
RJ45-Pinbelegung	Definiert die Pinbelegung des seriellen Ports. Mögliche Optionen sind „Automatisch“, „Cyclades“ und „Cisco“. Standard: Automatisch.
Status	Definiert den Status des seriellen Ports (aktiviert oder deaktiviert). Standard: Deaktiviert.
Geschwindigkeit	Definiert die Geschwindigkeit. Mögliche Werte sind 1200, 2400, 4800, 9600, 19200, 38400, 57600,115200 und 230400. Standard: 9600.
Parität	Definiert die Parität. Mögliche Werte: Gerade, Ungerade, Keine. Standard: Keine.
Datenbits	Definiert die Datenbits. Mögliche Werte sind 5, 6, 7 und 8. Standard: 8.
Stoppbits	Definiert die Stoppbits. Mögliche Werte sind 1 und 2. Standard: 1.
Flusssteuerung	Definiert die Flusssteuerung. Mögliche Werte: Keine, Hardware, Software, RxON-Software, TxON-Software. Standard: Keine.
Strom	
USV-Typ	Definiert den Typ oder den Anbieter der USV, die an den seriellen Port angeschlossen ist. Liebert GXT4 und Liebert GXT5 USV-Geräte werden unterstützt. Standard: Liebert GXT4.
PDU-Typ	Definiert den Typ oder den Anbieter der PDU, die an den seriellen Port angeschlossen ist. Standard: Automatisch. • Automatisch – Anbieter wird automatisch erkannt • Avocent-Cyclades – Avocent-Cyclades PM PDU-Familie • Vertiv – Vertiv-PDUs • SPC – Stromverwaltungsgeräte der SPC-Familie • ServerTech/Server Tech PRO2 – Server Tech-Familie • Raritan – Raritan PX G2 PDU-Familie • APC – APC rPDU2-Familie • Eaton – Eaton ePDU G3-PDUs • Geist – Geist PDU-Familie
Automatische Geschwindigkeitserkennung aktivieren	Wenn diese Option aktiviert ist, wird die Geschwindigkeit des Ports erkannt. Standard: Deaktiviert.
Abfragerate	Das Intervall (in Sekunden) für die Aktualisierung von Informationen von der PDU: Standard: 20.
Avocent-/Cyclades-PDUs	
Intervall für Ausschalten und erneutes Einschalten	Das Intervall (in Sekunden) zwischen den Aus- und Ein-Aktionen beim Befehl „Aus- und wieder einschalten“. Standard: 15.
Syslog	Wenn diese Option aktiviert ist, sendet die PDU Syslog-Nachrichten an die Einheit. Standard: Aktiviert.
Tonsignal	Aktiviert oder deaktiviert das Tonsignal der PDU. Standard: Aktiviert.
SW-Überstromschutz	Mit dieser Option wird der Überstromschutz der Software aktiviert. Standard: Deaktiviert.

So kopieren oder klonen Sie die Konfiguration eines Ports für andere Ports:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Aktivieren Sie das Kontrollkästchen des seriellen Ports, den Sie klonen möchten.
3. Klicken Sie auf die Schaltfläche *Klonen*.
4. Geben Sie die seriellen Ports, die konfiguriert werden sollen, in das Feld „Konfiguration kopieren nach“ ein und klicken Sie auf *Speichern*.

HINWEIS: Wenn der ausgewählte Port als CAS-Profil konfiguriert ist, werden die folgenden Parameter nicht kopiert: Portname, TCP-Port-Alias, IPv4-Port-Alias, IPv6-Port-Alias und Strom (verbundene Ausgänge).

So können Sie die werkseitige Konfiguration für einen oder mehrere serielle Ports wiederherstellen:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Aktivieren Sie das Kontrollkästchen für die seriellen Ports, deren werkseitige Konfiguration Sie wiederherstellen möchten, und klicken Sie dann auf die Schaltfläche *Auf Werkseinstellung zurücksetzen*.

HINWEIS: Serielle Ports sind in der werkseitigen Konfiguration auf das CAS-Profil eingestellt und deaktiviert.

Menü für Mehrfachsitzung

Administratoren können das Menü für eine Mehrfachsitzung aktivieren oder deaktivieren. Wenn das Menü aktiviert ist, können Benutzer über die Weboberfläche, die CLI oder die DSView-Software darauf zugreifen, und mehrere Benutzer können gleichzeitig eine Verbindung mit einem seriellen Port herstellen. Damit Benutzer eine Verbindung mit einem Port herstellen oder eine gemeinsame Sitzung starten können, müssen sie eine Zugriffsberechtigung für den Port besitzen. Wenn mehr als eine Sitzung mit einem seriellen Port aufgebaut wird, zeigt das Konsolensystem das Menü für eine Mehrfachsitzung an. Wenn es sich bei der Sitzung, die aufgebaut wird, um die erste Sitzung mit dem seriellen Port handelt, wird eine normale Sitzung mit dem Ziel geöffnet. Der Benutzer der ersten Sitzung kann durch Eingabe des Hotkeys (standardmäßig Strg-Z) weiterhin auf das Menü für die Mehrfachsitzung zugreifen.

So aktivieren Sie das Menü für eine Mehrfachsitzung:

1. Klicken Sie in der Seitenleiste der Registerkarte *Experte* auf *Ports – Serielle Ports*.
2. Klicken Sie auf den Port, für den Sie das Menü für eine Mehrfachsitzung aktivieren möchten.
3. Klicken Sie auf die Überschrift *CAS* und verwenden Sie dann das Dropdown-Menü im unteren Bereich der CAS-Einstellungen, um die Option *Menü für Mehrfachsitzung anzeigen* zu aktivieren.
4. Klicken Sie auf *Speichern*.

Die Optionen im Menü für eine Mehrfachsitzung richten sich nach den Zugriffsrechten des jeweiligen Benutzers. Es werden nur die Optionen angezeigt, für die der Benutzer eine Berechtigung besitzt. Beispielsweise werden für einen Benutzer, der nur zum Öffnen von schreibgeschützten Sitzungen berechtigt ist, nur die Optionen 0, 2 und 5 der folgenden Tabelle angezeigt.

Tabelle 3.14 Optionen im Menü für eine Mehrfachsitzung

Nummer	Option	Beschreibung
0	Beenden	Schließt die Clientsitzung.
1	Reguläre Sitzung einleiten	Öffnet eine Sitzung mit Lese-/Schreibzugriff.
2	Sniff-Sitzung einleiten	Öffnet eine schreibgeschützte Sitzung.
3	Nachrichten an anderen Benutzer senden	Sendet eine Nachricht an alle Benutzer, die den seriellen Port gemeinsam nutzen.
4	Sitzung(en) abbrechen	Zeigt alle Sitzungen an und fordert zum Schließen von einer oder mehreren gemeinsamen Sitzungen auf.
5	Gemeinsame Sitzung(en) auflisten	Listet alle anderen gemeinsamen Sitzungen auf.
6	Datenpufferung anzeigen	Zeigt den Inhalt der Ziel-Datenpufferungsdatei.
7	Datenpufferung löschen	Setzt den Inhalt der Ziel-Datenpufferungsdatei zurück.

Aux-Ports

Wenn auf dem Bildschirm „Aux-Ports“ der Portname ttyM1 angezeigt wird, bedeutet dies, dass das interne Modem vorhanden ist und aktiviert und konfiguriert werden kann. Wenn keine Einträge in der Tabelle der Aux-Ports vorliegen, ist kein internes Modem vorhanden und dieser Port kann nicht verwendet werden.

Bei Modellen mit Funkmodem wird der Portname als ttyM1 und der Gerätetyp als LTE angezeigt. Das Funkmodem kann nur für den Hinauswählen-Modus konfiguriert werden. Standardmäßig ist das Funkmodem deaktiviert. Weitere Informationen zur Konfiguration eines Funkmodems finden Sie unter Funkmodem auf Seite 61

So konfigurieren oder bearbeiten Sie einen Aux-Port mit einem internen Modem:

1. Wählen Sie *Ports – Aux-Ports* aus.
2. Klicken Sie auf die Schaltfläche *Einwahl festlegen* oder *Hinauswählen festlegen* und konfigurieren Sie dann mithilfe der Dropdown-Menüs die Einwahl-Einstellungen.
3. Konfigurieren Sie die PPP-Parameter (Adresse, Authentifizierung usw.).
4. Klicken Sie auf *Speichern*.

CAS-Profil

Das CAS-Profil (CAS = Console Access Server) ermöglicht den Remote-Zugriff auf die seriellen RS-232-Konsolenports Ihrer Geräte. Mithilfe eines CAS-Profils können Sie verschiedene Einstellungen konfigurieren, wie zum Beispiel Authentifizierung, Portkonfiguration (wie Geschwindigkeit und Flusssteuerung), Port-Alias, automatische Erkennung von Zielgeräten, Typ der Datenpufferung, Portalarme, Stromintegration und so weiter.

Administratoren können das CAS-Profil durch Klicken auf *Ports – CAS-Profil* konfigurieren.

Automatische Erkennung

Die automatische Erkennung erkennt den Zielgerät-Namen des Servers, der an den seriellen Port angeschlossen ist. Dieser Name wird als Aliasname des seriellen Ports verwendet.

Wenn die automatische Erkennung für ein bestimmtes serielles Gerät aktiv ist und eine Verbindung mit dem Zielgerät hergestellt wird (Ereignis DCD ON), sendet die Einheit Testzeichenfolgen und beginnt, die Antworten des Zielgeräts mithilfe von regulären Ausdrücken zu analysieren. Es gibt vordefinierte, aber auch benutzerdefinierte Test- und Übereinstimmungszeichenfolgen.

Für jede gesendete Testzeichenfolge werden alle regulären Ausdrücke, die von den Übereinstimmungszeichenfolgen definiert sind, getestet. Nach dem letzten Zyklus beginnt die Sequenz von vorne. Dieser Prozess wird so lange fortgesetzt, bis die vom Parameter „Timeout für die automatische Erkennung“ vorgegebene Zeit abgelaufen ist oder bis das Zielgerät erfolgreich erkannt wird. Wenn die automatische Erkennung fehlschlägt, wird der Zielgerät-Name auf den konfigurierten Zielgerät-Namen oder auf den entsprechenden eindeutigen Standardnamen des Zielgeräts zurückgesetzt.

HINWEIS: Der konfigurierte Zielgerät-Name wird nur verwendet, nachdem die automatische Erkennung fehlgeschlagen ist.

HINWEIS: Die automatische Erkennung beginnt, wenn sich das DCD-Signal von AUS in EIN ändert (Trennen/Anschließen des Zielgerätkabels, Aus-/Einschalten des Zielgeräts) und wenn sich die Konfiguration des seriellen Ports von „deaktiviert“ in „aktiviert“ ändert und ein Zielgerät an den Port angeschlossen ist.

Die Testzeichenfolgen dienen zur Stimulation des Servers (beispielsweise „\r“: einzelner Zeilenschalter).

Die Übereinstimmungszeichenfolgen sind reguläre Ausdrücke. Dabei ist „%H“ ein Platzhalter für den Zielgeräte-Namen, der erkannt werden soll, wie zum Beispiel %H .*meldung:

oder xxx%Hyyy

Der erste extrahiert den Zielgerät-Namen von Angaben wie MeinServer Anmeldung: und liefert als Ergebnis den Zielgerät-Namen „MeinServer“.

Der zweite extrahiert den Zielgerät-Namen von Angaben wie Server xxxZIELyyy und liefert als Ergebnis den Zielgerät-Namen „ZIEL“.

So konfigurieren Sie die Test- und Übereinstimmungszeichenfolgen für die automatische Erkennung:

Führen Sie die folgenden Schritte aus, um die Standardeinstellungen oder die Test- bzw. Übereinstimmungszeichenfolgen für die automatische Erkennung zu ändern.

1. Wählen Sie *Ports – CAS-Profil – Automatische Erkennung*. In der seitlichen Navigationsleiste werden die Optionen für die Einstellungen sowie die Test- und Übereinstimmungszeichenfolgen angezeigt.
2. So ändern Sie das standardmäßige Timeout für die automatische Erkennung oder das standardmäßige Test-Timeout:
   a. Wählen Sie *Einstellungen* aus.
   b. Geben Sie neue Werte in die Felder „Timeout für die automatische Erkennung“ und „Test-Timeout“ ein.
   c. Wählen Sie im Dropdown-Menü „Standardgeschwindigkeit bei Fehlschlagen der automatischen Erkennung“ und in der Liste der Testgeschwindigkeiten eine Geschwindigkeit aus.
   d. Klicken Sie auf *Speichern*.
3. So können Sie eine neue Test- oder Übereinstimmungszeichenfolge hinzufügen bzw. eine vorhandene Zeichenfolge löschen:
   a. Wählen Sie *Testzeichenfolgen* oder *Übereinstimmungszeichenfolgen* aus.

b. Um eine Zeichenfolge hinzuzufügen, klicken Sie auf *Hinzufügen*, geben Sie eine neue Zeichenfolge in das Feld „Neue Testzeichenfolge“ oder „Neue Übereinstimmungszeichenfolge“ ein und klicken Sie dann auf *Speichern*.

c. Um eine Zeichenfolge zu löschen, aktivieren Sie das Kontrollkästchen der Zeichenfolge und klicken Sie dann auf *Löschen*.

4. Klicken Sie auf *Speichern*.

So konfigurieren Sie die Ein- und Ausgabezeichenfolgen für die automatische Antwort:

1. Wählen Sie *Ports – CAS-Profil – Automatische Antwort*.
2. Um eine Ein- oder Ausgabezeichenfolge für die automatische Antwort hinzuzufügen, klicken Sie auf *Hinzufügen*. Geben Sie eine neue Zeichenfolge in das Feld „Eingabezeichenfolge“ oder „Ausgabezeichenfolge“ ein und klicken Sie dann auf *Speichern*.

   – oder –

   Um eine Ein- oder Ausgabezeichenfolge für die automatische Antwort zu löschen, aktivieren Sie das Kontrollkästchen neben der zu löschenden Zeichenfolge. Klicken Sie auf *Löschen* und dann auf *Speichern*.

Port-Pool

Administratoren können einen Pool mit seriellen Ports erstellen, die alle denselben Pool-Namen sowie dieselben Einstellungen für Telnet-Port-Alias, SSH-Port-Alias, Raw-Modus-Portalias, IPv4-Alias und IPv6-Alias haben. Der erste verfügbare Port im Pool wird als serieller Port für die Verbindung verwendet.

HINWEIS: Wenn ein Pool mit CAS-Ports verwendet wird, hat das Zugriffsrecht für Mehrfachsitzungen keine Wirkung. Wenn alle Ports im Pool belegt sind, wird die Verbindung mit dem Pool verweigert.

HINWEIS: Alle Ports im Pool müssen dasselbe CAS-Protokoll verwenden. Das Protokoll wird beim Herstellen der Verbindung mit dem seriellen Port validiert. Wenn das Protokoll nicht übereinstimmt, wird die Verbindung verweigert.

So konfigurieren Sie einen Pool mit CAS-Ports:

1. Klicken Sie auf *Ports – Port-Pool*.
2. Zum Erstellen eines Pools klicken Sie auf die Schaltfläche *Hinzufügen*.

   – oder –

   Zum Bearbeiten eines vorhandenen Pools klicken Sie auf den Namen des Pools.

   – oder –

   Zum Löschen eines Pools aktivieren Sie das Kontrollkästchen neben dem Pool und klicken Sie dann auf die Schaltfläche *Löschen*.

3. Geben Sie die Parameter für den Pool in die vorgesehenen Felder ein.
4. Wählen Sie auf der linken Seite des Feldes „Poolmitglieder“ die Ports aus, die Sie dem Pool hinzufügen möchten, und klicken Sie dann auf *Hinzufügen*.

   – oder –

Wählen Sie auf der rechten Seite des Feldes „Poolmitglieder“ die Ports aus, die Sie aus dem Pool entfernen möchten, und klicken Sie dann auf *Entfernen*.

5. Klicken Sie auf *Speichern*.

HINWEIS: Ein serieller Port kann nur zu einem Pool gehören, Benutzer können aber einen leeren Pool erstellen und ihm später Ports hinzufügen.

Tabelle 3.15 Parameter für CAS-Port-Pools

Parameter	Beschreibung
Poolname	Der Name des Pools. Der Poolname ist obligatorisch. Er muss den Richtlinien für Hostnamen entsprechen, maximal 64 Zeichen lang sein und mit einem Buchstaben beginnen.
Port-Alias	Der Port-Aliasname, mit dem der Pool für jedes Protokoll antwortet. • Telnet-Port-Alias für das Telnet-Protokoll. Diese Angabe ist optional. • SSH-Port-Alias für das SSH-Protokoll. Diese Angabe ist optional. • Raw-Modus-Portalias für das Raw-Modus-Protokoll. • Diese Angabe ist obligatorisch, wenn der Raw-Modus als Protokoll für die Ports konfiguriert ist.
Pool - IPv4-Alias	Die vom Pool verwendete IPv4-Adresse. Dieser Parameter ist optional.
Pool - IPv4-Alias-Schnittstelle	Die vom IPv4-Alias verwendete Schnittstelle. Standard: eth0.
Pool - IPv6-Alias	Die vom Pool verwendete IPv6-Adresse. Dieser Parameter ist optional.
Pool - IPv6-Alias-Schnittstelle	Die vom IPv6-Alias verwendete Schnittstelle. Standard: eth0.

RESTful-Client

Das Konsolensystem unterstützt eine programmierbare RESTful-Clientschnittstelle. Nach der Konfiguration von RESTful-URLs führt das Konsolensystem innerhalb einer seriellen Sitzung über ein Menü ausgewählte GET- und POST-Vorgänge für vorprogrammierte HTTP/HTTPS-URLs aus, die sich auf Serverressourcen im Netzwerk beziehen.

HINWEIS: URL-Optionen müssen über HTTP oder HTTPS mit dem RESTful-Client-Menü konfiguriert werden.

So konfigurieren Sie den RESTful-Client:

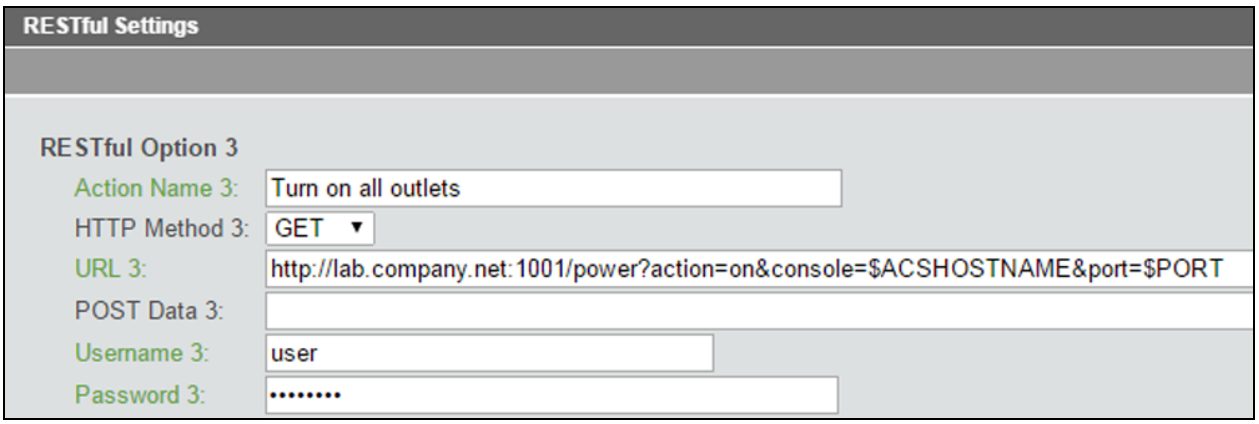
1. Klicken Sie auf *Ports – CAS-Profil – RESTful-Einstellungen*.
2. Geben Sie den Namen der Aktion, die URL, POST-Daten, den Benutzernamen und das Kennwort in die vorgesehenen Felder ein. Wählen Sie dann im Dropdown-Menü GET oder POST als HTTP-Methode für jede RESTful-Option aus. Klicken Sie abschließend auf *Speichern*.

Bei der Konfiguration von Aktionen können die folgenden Kontextvariablen verwendet werden.

Tabelle 3.16 Beschreibungen der Kontextvariablen

Kontextvariable	Beschreibung
$PORT	Identifiziert den seriellen Port (1-48) beim Aufrufen des Menüs.
$PORTNAME	Der Name des Ports.
$IPPORTALIAS	Der IPv4-Aliasname des Ports.
$TCPPORTALIAS	Der TCP-Aliasname (Telnet-Portalias) des Ports.
$ACSHOSTNAME	Der Hostname des Konsolensystem.
$ACSIPADDR	Die IP-Adresse des Konsolensystem.

Abbildung 3.3 RESTful-Client – Beispielkonfiguration



HINWEIS: HTTP-POSTs können in manchen Fällen den HTTP-Anforderungstext verwenden, um entsprechende Informationen an Server zu senden, normalerweise als XML- oder JSON-Code.

So aktivieren Sie den RESTful-Client:

1. Wenn der Portzugriff für alle Benutzer gilt, klicken Sie in der seitlichen Navigationsleiste der Registerkarte *Experte* auf *System – Sicherheit – Sicherheitsprofil*, aktivieren Sie unter „Serielle Geräte“ das Kontrollkästchen „RESTful-Menü“ und klicken Sie dann auf *Speichern*.

   – oder –

   Wenn der Portzugriff durch Berechtigungen für Benutzergruppen geregelt ist, klicken Sie in der seitlichen Navigationsleiste der Registerkarte „Experte“ auf *Benutzer – Autorisierung – Gruppen*.

   a. Klicken Sie auf die Gruppe, für die Sie den RESTful-Client aktivieren möchten.
   b. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Seriell*.
   c. Klicken Sie auf den Port, für den Sie das RESTful-Menü aktivieren möchten. Klicken Sie unter „Zugriffsrechte für Ziel“ auf „Restful-Menü“.
2. Klicken Sie in der seitlichen Navigationsleiste der Registerkarte „Experte“ auf *Ports – Serielle Ports*.
3. Klicken Sie auf den Port, für den Sie das RESTful-Menü aktivieren möchten, und klicken Sie dann oben im Fenster auf „CAS“.
4. Geben Sie in das Feld „RESTful-Hotkey“ den Hotkey ein, über den Sie den RESTful-Client aufrufen möchten, und klicken Sie auf *Speichern*.

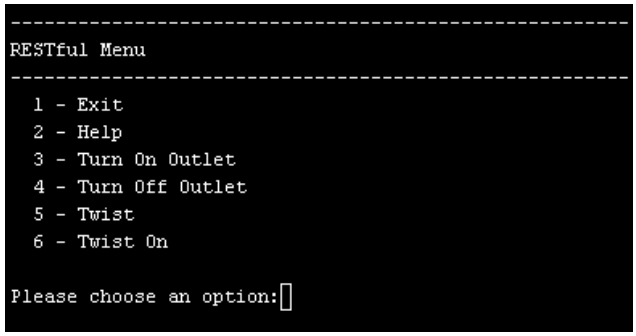
HINWEIS: Der Hotkey ist nicht standardmäßig festgelegt.

Verwenden der RESTful-Clientschnittstelle

Nachdem Sie eine serielle Sitzung geöffnet haben, drücken Sie den Hotkey, um die RESTful-Clientschnittstelle für die aktuelle Sitzung zu öffnen. Geben Sie die Nummer der RESTful-Clientanforderung ein, die Sie ausführen möchten. Standardmäßig sind „Exit“ (Beenden) und „Help“ (Hilfe) die ersten beiden Anforderungen im Menü. Sie können maximal acht weitere Anforderungen über die Weboberfläche des Konsolensystem konfigurieren.

Die folgende Abbildung zeigt ein Beispiel für das RESTful-Menü einer seriellen Sitzung.

Abbildung 3.4 Beispiel des RESTful-Clients



Einwahlprofil

Administratoren können Einstellungen für eine sichere Einwahl konfigurieren, wie beispielsweise OTP-Anmeldung, PPP-Verbindungen, PPP/PAP-Authentifizierung, Rückruf und OTP-Benutzer für PPP-Verbindungen.

HINWEIS: Wenn austauschbare Geräte für das Hinauswählen verwendet werden, sollte die Einwahl deaktiviert werden.

So konfigurieren Sie mit dem Einwahlprofil Einstellungen zur sicheren Einwahl für Ports:

1. Wählen Sie *Ports – Einwahlprofil – Einstellungen*.
2. Führen Sie die folgenden Schritte aus, um die Anmeldung beim Konsolensystem über das Modem zu ermöglichen und eine Bedingung für die zulässige Anmeldeart festzulegen.
   a. Wenn nur Rückruf-Verbindungen zulässig sein sollen, wählen Sie *Rückruf* aus.
   b. Wenn jede Verbindung zulässig sein soll, wählen Sie *Aktivieren* aus.
3. Wenn Sie die OTP-Authentifizierung aktivieren möchten, wählen Sie im Menü „OTP-Anmeldeauthentifizierung“ die Option *Aktivieren* aus.
4. Führen Sie die folgenden Schritte aus, um eine Bedingung für PPP-Verbindungen zu aktivieren und auszuwählen.
   a. Wenn nur PPP-Rückruf-Verbindungen zulässig sein sollen, wählen Sie *Rückruf* aus.
   b. Wenn jede Verbindung zulässig sein soll, wählen Sie *Aktivieren* aus.
5. Wenn das PAP-Authentifizierungsprotokoll für den Port konfiguriert ist, wählen Sie den Authentifizierungstyp im Menü „PPP/PAP-Authentifizierung“ aus.
6. Verwenden Sie das Dropdown-Menü, um den Anruferkennungsfilter zu aktivieren oder zu deaktivieren.

7. Klicken Sie auf *Speichern*.

So konfigurieren Sie mit dem Einwahlprofil Rückruf-Benutzer und -Telefonnummern für Ports:

1. Wählen Sie *Ports – Einwahlprofil – Sichere Einwahl – Rückruf-Benutzer*.
2. Klicken Sie auf *Hinzufügen*.
3. Geben Sie den Namen und die Telefonnummer für den Rückruf in die vorgesehenen Felder ein und klicken Sie dann auf *Speichern*.

So konfigurieren Sie mit dem Einwahlprofil PPP OTP-Benutzer für Ports:

1. Wählen Sie *Ports – Einwahlprofil – Sichere Einwahl – PPP OTP-Benutzer*.
2. Klicken Sie auf *Hinzufügen*.
3. Geben Sie den Benutzernamen und die Passphrase in die vorgesehenen Felder ein und klicken Sie dann auf *Speichern*.

HINWEIS: Dieser PPP OPT-Benutzer stellt nach erfolgreicher Authentifizierung eine PPP-Verbindung her.

So konfigurieren Sie mit dem Einwahlprofil EAP-TLS als PPP-Authentifizierung für Ports:

1. Wählen Sie *Ports – Aux-Ports* aus.
2. Aktivieren Sie das Kontrollkästchen des Ports, an den das Modem angeschlossen ist, und klicken Sie dann auf *Einwahl festlegen*.
3. Konfigurieren Sie die Einstellungen für die PPP-Adresse. Stellen Sie die PPP-Adresse beispielsweise auf die lokale Konfiguration ein und verwenden Sie dabei 10.0.0.1 als lokale IPv4-Adresse und 10.0.0.2 als Remote-IPv4-Adresse.
4. Wählen Sie für die PPP-Authentifizierung die Schaltfläche neben „Durch Einheit“ aus und wählen Sie dann für das Protokoll die Schaltfläche neben „EAP“ aus. Klicken Sie auf „Speichern“.
5. Wählen Sie *Ports – Einwahlprofil – Einstellungen*.
6. Aktivieren Sie die PPP-Verbindung mithilfe des Dropdown-Menüs und klicken Sie dann auf *Speichern*.
7. Kopieren Sie die Zertifikate und Schlüssel in die Datei /etc/ppp/cert. Sie müssen folgendermaßen benannt sein: server.crt (ACS800/8000-Zertifikat), ca.crt (Zertifikat der Zertifikatstelle) und server.key (asymmetrischer ACS800/8000-Schlüssel).

Anruferkennung

Sie können eingehende Anrufe anhand der Anruferkennung filtern, indem Sie den Anruferkennungsfilter in den Einstellungen zur sicheren Einwahl aktivieren. Wenn diese Option aktiviert ist, muss die Telefonnummer des eingehenden Anrufers angezeigt werden, damit der Anruf beantwortet werden kann. Standardmäßig ist die Option deaktiviert.

Sie können Telefonnummern direkt, nach Bereich oder nach Präfix hinzufügen.

Um eine Nummer direkt einzugeben, geben Sie sie ohne Symbole ein. Zum Beispiel: 8881234567.

Sie können einen Bereich eingeben, indem Sie einen Bindestrich (-) zwischen zwei Anruferkennungsnummern einfügen. Jede Nummer zwischen und einschließlich dieser beiden Nummern wird akzeptiert. Zum Beispiel: 8881234560-8881234569.

HINWEIS: Der Bereich muss unter 100 Telefonnummern liegen.

Sie können einen Präfix eingeben, indem Sie ein Sternchen (*) hinter einen Teil einer Telefonnummer setzen. Der eingehende Anruf wird beantwortet, wenn die Telefonnummer mit der angegebenen Teilnummer beginnt. Zum Beispiel: 8881234*.

Wenn der Anruferkennungsfilter aktiviert ist und keine Nummern angegeben sind, werden alle Anrufe blockiert. Blockierte Anrufe werden nicht beantwortet und klingeln bis zum Timeout. Wenn die Anruferkennungsfunktion deaktiviert ist, werden alle Anrufe beantwortet.

So geben Sie eine Liste von Telefonnummern zur Anruferkennung ein:

1. Wählen Sie *Ports – Einwahlprofil – Sichere Einwahl – Anruferkennung* aus.
2. Klicken Sie auf *Hinzufügen* und geben Sie die Telefonnummer zur Anruferkennung, den Bereich oder das Präfix ein.
3. Klicken Sie auf *Speichern*.

So löschen Sie eine Telefonnummer zur Anruferkennung aus der Liste:

1. Wählen Sie *Ports – Einwahlprofil – Sichere Einwahl – Anruferkennung* aus.
2. Markieren Sie das Kontrollkästchen neben der zu löschenden Nummer.
3. Klicken Sie auf *Löschen*.

Hinauswählen-Profil

So konfigurieren Sie das Hinauswählen-Profil für einen seriellen Port, an den ein Modem angeschlossen ist:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Aktivieren Sie das Kontrollkästchen für einen seriellen Port mit angeschlossenem Modem.
3. Klicken Sie auf die Schaltfläche *Hinauswählen festlegen*.
4. Verwenden Sie das Dropdown-Menü, um den Port zu aktivieren oder zu deaktivieren.
5. Konfigurieren Sie die Telefonnummer für das Hinauswählen bei Bedarf im vorgesehenen Feld.
6. Verwenden Sie das Dropdown-Menü, um die Modemgeschwindigkeit zu konfigurieren.
7. Konfigurieren Sie den anfänglichen Chat mit dem Modem im Feld „Chat initialisieren“.
8. Konfigurieren Sie die PPP-Parameter (Adresse, Authentifizierung usw.) und klicken Sie auf *Speichern*.

HINWEIS: Das Hinauswählen-Profil eignet sich nur zum Herstellen von PPP-Verbindungen bei Bedarf. Der Administrator muss eine statische Route konfigurieren, damit Pakete an die PPP-Schnittstelle geleitet werden.

Tabelle 3.17 Parameter für das Hinauswählen

Parameter	Beschreibung
Status	Aktiviert oder deaktiviert den Port. Standard: Deaktiviert.
Telefonnummer	Die anzuwählende Telefonnummer.
Geschwindigkeit	Die Geschwindigkeit zur Konfiguration des seriellen Geräts und zur Kommunikation mit dem angeschlossenen Modem.
Chat initialisieren	Chat für die Initialisierung des Modems.
Lokale IPv4-/IPv6-Adresse	Konfiguriert die lokale IPv4-/IPv6-Adresse für diese PPP-Verbindung. Falls dies leer bleibt, akzeptiert PPP die Adresse vom Remote-Peer.
Remote-IPv4-/IPv6-Adresse	Konfiguriert die Remote-IPv4-/IPv6-Adresse für diese PPP-Verbindung. Falls dies leer bleibt, akzeptiert PPP die Adresse vom Remote-Peer.
PPP-Authentifizierungsprotokoll	Konfiguriert, welches Ende der Verbindung diese PPP-Authentifizierung steuert und wählt die zu verwendende Methode aus.
PPP-Inaktivitäts-Timeout	Dauer der Inaktivität in Sekunden, nach der bei PPP eine Zeitüberschreitung auftritt. Standard: 0 (kein Timeout).
CHAP	Konfiguriert die CHAP-spezifischen PPP-Authentifizierungseinstellungen.

Socket-Client-Profil

So konfigurieren Sie das Socket-Client-Profil für einen seriellen Port, an den ein Gerät angeschlossen ist:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Aktivieren Sie das Kontrollkästchen für einen seriellen Port mit angeschlossenem Gerät.
3. Klicken Sie auf *Socket-Client festlegen* und konfigurieren Sie über die Dropdown-Menüs die physischen Einstellungen.
4. Konfigurieren Sie die Socket-Client-Einstellungen (Adresse des Remote-Servers, TCP-Port und Ereignisauslöser) und klicken Sie auf *Speichern*.

Tabelle 3.18 Socket-Client-Parameter

Parameter	Beschreibung
RJ45-Pinbelegung	Definiert die Pinbelegung des seriellen Ports.
Status	Definiert den Status des seriellen Ports (aktiviert oder deaktiviert). Standard: Deaktiviert.
Geschwindigkeit	Definiert die Geschwindigkeit. Mögliche Werte sind 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 und 230400. Standard: 9600.
Parität	Definiert die Parität. Mögliche Werte: Gerade, Ungerade, Keine. Standard: Keine.
Datenbits	Definiert die Datenbits. Mögliche Werte sind 5, 6, 7 und 8. Standard: 8.
Stoppbits	Definiert die Stoppbits. Mögliche Werte sind 1 und 2. Standard: 1.
Flusssteuerung	Definiert die Flusssteuerung. Mögliche Werte: Keine, Hardware, Software, RxON-Software, TxON-Software. Standard: Keine.
Remote-Server	IPv4- oder IPv6-Adresse des Remote-Servers.
Remote-TCP-Port	TCP-Port, über den die Verbindung mit einem Remote-Server hergestellt werden soll.
Verbindung herstellen	Konfiguriert das Ereignis, das das Herstellen der Verbindung auslöst: DCD-Schwellenpegel oder Immer.

3.3.8 Funkmodem

Die Konfigurationsoberfläche für das Avocent® ACS800/8000 Advanced Console SystemFunkmodem ähnelt der für das interne 56k-Modem. Das Funkmodem wird über den Aux-Port des Konsolensystem konfiguriert.

So konfigurieren oder bearbeiten Sie einen Aux-Port mit einem Funkmodem:

1. Wählen Sie *Ports – Aux-Ports* aus.
2. Klicken Sie auf den Link *ttyM1*, um die Konfigurationsseite des Modems zum Hinauswählen zu öffnen.

HINWEIS: Das Funkmodem kann nur für den Hinauswählen-Modus konfiguriert werden.

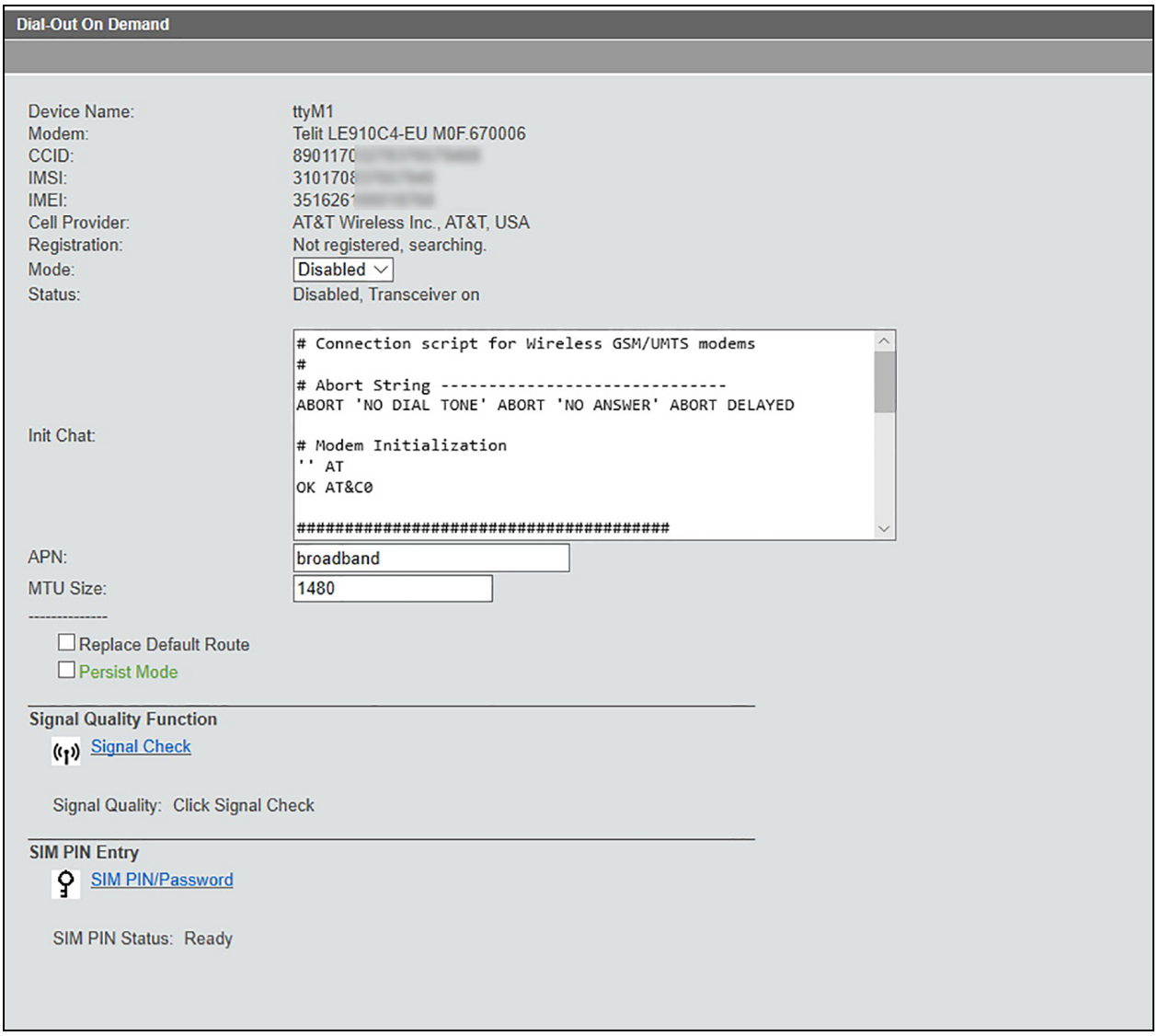
3. Aktivieren Sie das Modem im Dropdown-Menü.Wenn diese Option aktiviert ist, wird das Modem nach jedem Neustart eingeschaltet.
4. Das Chat-Skript ist ein verwendbarer Standard für den Anbieter. Falls gewünscht, können Sie Änderungen am Chat-Skript über das Fenster „Chat initialisieren“ vornehmen.
5. Das APN-Feld listet den Standardnamen des Zugangspunkts auf. Sie können den APN hier ändern, ohne das Chat-Skript bearbeiten zu müssen.

HINWEIS: Wenn Sie den APN ändern, gehen alle Änderungen am Chat-Skript verloren.

6. Aktivieren oder deaktivieren Sie die Option zum Ersetzen der Standardroute.
7. Aktivieren oder deaktivieren Sie den Persist-Modus.

Weitere Informationen zur Konfiguration des Funkmodems finden Sie in den folgenden Abschnitten.

Abbildung 3.5 Konfigurationsseite zum Hinauswählen für das Funkmodem



Oben auf dem Bildschirm werden die von der SIM-Karte gelesenen CCID- und IMSI-Nummern angezeigt. Wenn diese Nummern nicht vorhanden sind oder eine ungültige Nummer angezeigt wird, dann ist ein Problem beim Lesen der SIM-Karte aufgetreten. Überprüfen Sie, ob die SIM-Karte richtig installiert ist. Die IMEI-Nummer stammt aus dem Chipsatz des Funkmodems.

Modus

Standardmäßig ist die Modusauswahl deaktiviert. Wenn Sie sie aktivieren, wird der Point-to-Point Protocol Daemon (PPPD) gestartet und das Funkmodem eingeschaltet. Wenn diese Option aktiviert ist, wird das Funkmodem nach jedem Neustart eingeschaltet.

Im Failover-Modus schaltet sich das Funkmodem ein, auch wenn es deaktiviert ist. Failover-Bedingungen sind weiterhin aktiviert.

Status

Die Statuszeile zeigt den aktuellen Status an:

- Deaktiviert oder Aktiviert – Zeigt an, ob das Funkmodem aktiviert oder deaktiviert ist. Das Modem kann manuell oder per Failover aktiviert werden.
- Sender-Empfänger aus – Die Standardeinstellung. Der Sender-Empfänger ist ausgeschaltet, wenn das Modem deaktiviert ist.
- Sender-Empfänger an – Der Sender-Empfänger ist eingeschaltet, wenn das Modem entweder manuell oder per Failover aktiviert wurde.
- Failover: nein – Bei Konfiguration als Failover-Gerät zeigt diese Option an, ob sich das Funkmodem im Failover-Modus befindet.
- Oben oder unten – gibt an, ob die Schnittstelle des Funkmodems eingeschaltet ist.

Chat initialisieren

Das Chat-Skript in einem Editor-Fenster. Sie können in diesem Fenster individuelle Änderungen am Chat-Skript vornehmen. Das Standard-Chat-Skript stammt vom Dienstanbieter.

HINWEIS: Für die meisten Benutzer sollte das Standard-Chat-Skript verwendet werden.

APN

Der im Chat-Skript aufgeführte Name des Zugangspunkts. In diesem Feld können Sie den APN ändern, ohne das Chat-Skript direkt bearbeiten zu müssen. Wenn Sie den APN hier ändern, gehen alle anderen im Chat-Skript vorgenommenen Änderungen verloren.

Standardroute ersetzen

Sendet eine Konfigurationsoption an den PPP Daemon, um das Funkmodem als Standard-Gateway festzulegen. Das Gateway wird wiederhergestellt, wenn das Funkmodem abgeschaltet wird. Dies ähnelt der Eingabe einer statischen Route, ist aber nützlich, um das Funkmodem als Standard-Gateway für Failover festzulegen.

Persist-Modus

Wenn der Persist-Modus aktiviert ist, versucht das Konsolensystem, das Funkmodem wieder zu starten, falls der PPP Daemon aus irgendeinem Grund herunterfährt. Wenn er deaktiviert ist, bleibt das Funkmodem ausgeschaltet, wenn der PPP Daemon herunterfährt (z. B. bei Verlust des Funkdiensts).

Signalqualitätsfunktion

Ermöglicht das Abrufen von Messwerten des Rohsignalpegels und der Bitfehlerrate, um die Diagnose eines Problems bei der Verbindung zum Funknetzwerk oder einer langsamen Verbindung zu ermöglichen. Klicken Sie auf *Signalprüfung*, um eine Antwort abzurufen.

Der Signalpegel kann von höchstens –113 db bis mindestens –51 db reichen. Die Bitfehlerrate reicht von weniger als 1 % bis 12,8 % oder mehr.

Sie können keine Signalqualitätsprüfung abrufen, während das Modem in Betrieb ist. Der Sender-Empfänger des Modems ist eingeschaltet, aber das Chat-Skript wird nicht ausgeführt. Während der Sitzung ist die serielle Schnittstelle des Funkmodems mit dem PPP Daemon verbunden.

SIM PIN-Eingabe

Klicken Sie auf *SIM PIN/Kennwort*, um Ihre PIN zur Aktivierung des Funkdiensts mit einer SIM-Karte einzugeben.

Überprüfen der Funkverbindung

Die Statuszeile auf dem Hinauswählen-Bildschirm zeigt an, ob das Funkmodem eingeschaltet ist. Die IP-Adresse des Funkmodems können Sie auf der Seite „Überwachung“ abrufen. Gehen Sie zu *Überwachung - Netzwerk - Geräte*.

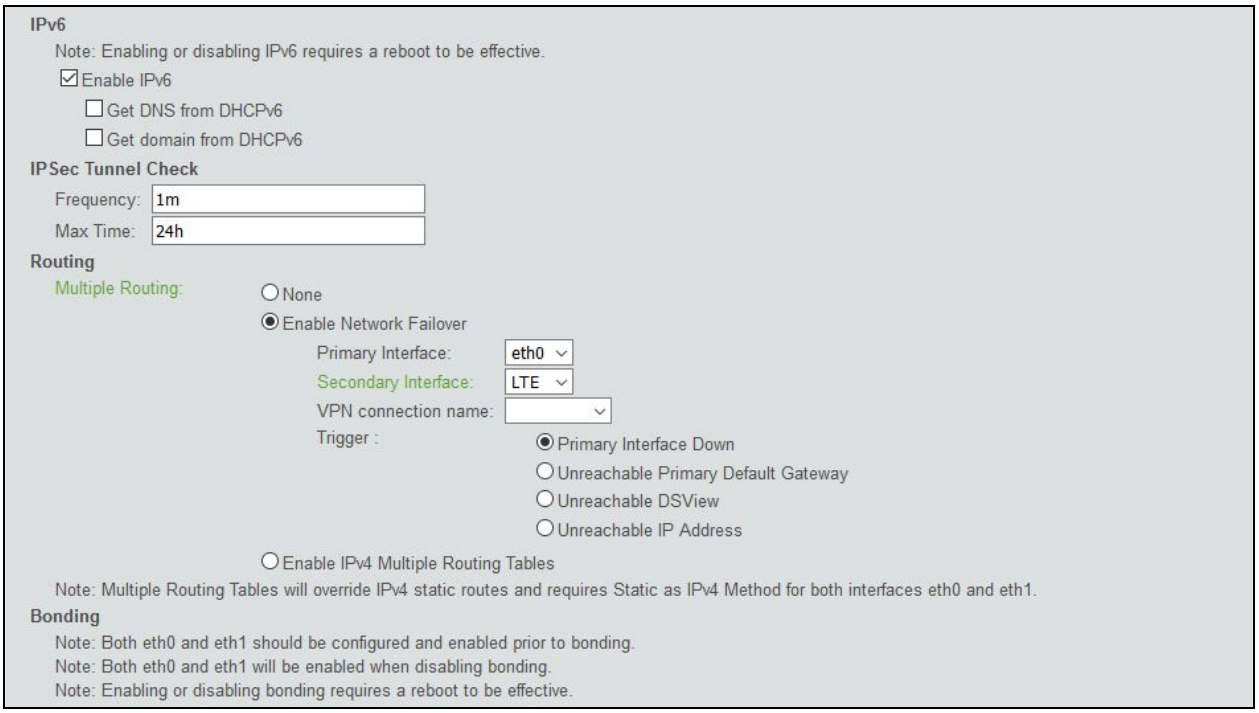
Auf der Seite „Geräte“ ist das Gerät ppp0-LTE das Modem. Wenn das Modem aktiviert ist, wird die IPv4-Adresse angezeigt, und der Verbindungsstatus ist aktiv. Die IP-Adresse wird für den privaten Netzwerkdienst benötigt. Die IPv4-Adresse ist nicht statisch und ändert sich jedes Mal, wenn Sie die Funknetzverbindung neu starten oder neu aufbauen.

HINWEIS: Fortgeschrittene Benutzer können ein Skript für weitere Debug-Informationen ausführen.

Verwenden des Funkmodems im Failover

Navigieren Sie zu *Netzwerk - Einstellungen* und wählen Sie *Routing - Netzwerk-Failover aktivieren* aus. Wählen Sie in der Liste „Sekundäre Schnittstelle“ das Gerät ppp0 (oder lte0) aus. Dies ist bei aktiviertem und deaktiviertem Modem möglich.

Abbildung 3.6 Konfigurieren des Funkmodems als Failover-Gerät



Die Failover-Bedingung ist in diesem Fall, dass die primäre Schnittstelle ausgefallen ist. Bei aktiviertem Failover wird bei einem Ausfall von eth0 das Funkmodem gestartet. Beim Dienstanbieter wird dadurch nur der Internetzugang zur Verfügung gestellt. Ein Server im Internet kann sich nicht direkt anmelden. Eine andere Dienstleistungsart oder ein anderer Dienstanbieter kann den Zugang möglicherweise bereitstellen.

Die andere Alternative ist die Nutzung eines VPN-Dienstes. Konfigurieren Sie das VPN so, dass es eine Verbindung über IPsec zu einem sicheren Gateway mit einer öffentlichen IP-Adresse herstellt. Anschließend können Sie über den IPsec-Tunnel auf das Konsolensystem zugreifen.

So konfigurieren Sie IPsec:

1. Schalten Sie den IPsec-Dienst ein. Gehen Sie zur Seite *System - Sicherheit - Sicherheitsprofil*, scrollen Sie nach unten und wählen Sie das Kontrollkästchen zur Aktivierung von IPsec aus.
2. Gehen Sie auf die Seite *Netzwerk – IPSec (VPN)* und fügen Sie ein neues VPN-Profil hinzu.
3. Geben Sie die VPN-Parameter ein. Das folgende Bild ist ein Beispiel. Wenn Sie fertig sind, klicken Sie auf *Speichern*.
4. Navigieren Sie zurück zum Failover-Bildschirm auf *Netzwerk – Einstellungen* und wählen Sie das VPN für Failover aus.

Abbildung 3.7 IPsec VPN-Beispiel

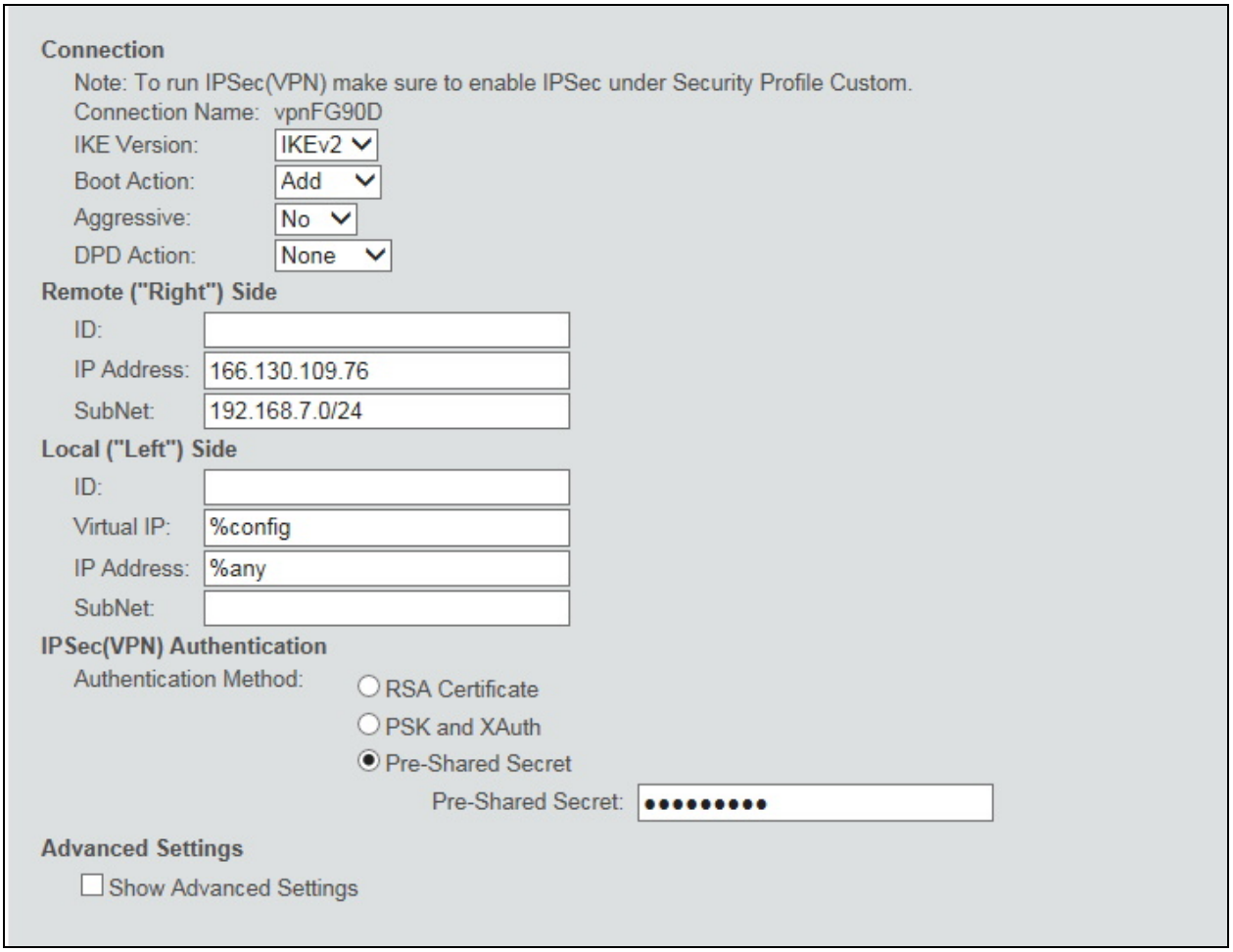
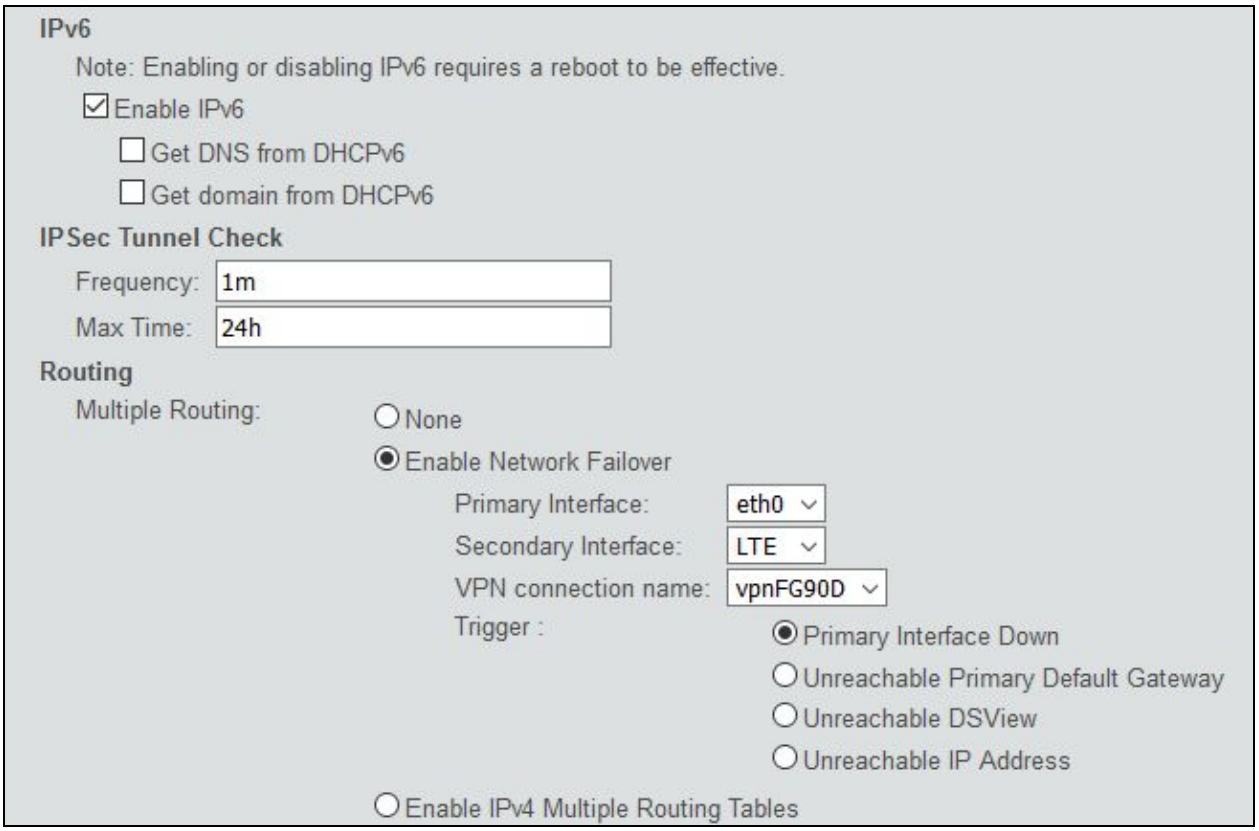


Tabelle 3.19 IPsec Beschreibungen

Element	Beschreibung
IKE-Version	Normalerweise IKEv2, es sei denn, das Gateway, zu dem die Verbindung hergestellt wird, ist alt.
Aktion beim Hochfahren	Aktivieren Sie die Einstellung „Für Failover hinzufügen“. Bei der Starteinstellung versucht das VPN zu starten, sobald das Konsolensystem hochfährt.
Aggressiv	Sollte auf „Nein“ gestellt werden.
DPD-Aktion	Keine. Konnte nicht auf „Neustart“ gestellt werden. Bedeutet „Dead-Peer-Erkennung“.
ID	Leer gelassen, weil das Remote-Gateway anhand der IP-Adresse identifiziert werden soll.
Subnetz	Das Subnetz, auf das wir hinter dem sicheren Remote-Gateway zugreifen. In diesem Fall wird ein Fortigate und dessen LAN-Subnetz verwendet.
Lokale linke Seite	
ID	IDs werden verwendet, um jede Seite zu identifizieren, aber wenn sie leer gelassen werden, wird nur die IP-Adresse verwendet.
Virtuelle IP	Weist die IP-Adresse für den Tunnel zu.Die Einstellung **%config** bedeutet, dass eine Adresse vom sicheren Remote-Gateway abgerufen wird.
IP-Adresse	Die am Tunnel beteiligte IP-Adresse des Konsolensystems. Für ein normales Ethernet kann dies auf eine feste IP-Adresse eingestellt werden. Für das Funkmodem weist der Anbieter die IP-Adresse zu, und beim AT&T-Dienst ändert sie sich. Die Einstellung **%any** bedeutet, dass eine beliebige Schnittstelle oder aktive IP-Adresse verwendet wird.
IPsec (VPN) Authentifizierung	Setzen Sie die Einstellung auf „Pre-shared secret“, um einen für den Tunnel eindeutigen Passcode/Kennwort zu verwenden. Jede Seite dieses IPsec-Tunnels muss das gleiche Kennwort/Geheimwort verwenden. Natürlich können Sie alternativ auch X509/RSA-Zertifikate verwenden.
Erweiterte Einstellungen	Behalten Sie hier die Standardeinstellungen bei, sodass IPsec die Verschlüsselungs-Suite aushandelt.

Abbildung 3.8 Beispiel eines für Failover ausgewählten VPN



Wenn „Standardroute ersetzen“ aktiviert ist, wird bei einem Failover-Ereignis (eth0 fällt aus) das Funkmodem hochgefahren und dann das VPN gestartet. Die LAN-Clients auf dem Remote-Gateway können über die virtuelle IP-Adresse des Tunnels auf das Konsolensystem zugreifen.

3.3.9 Austauschbare Geräte

Das Konsolensystem unterstützt verschiedene austauschbare Geräte, die an die USB-Ports angeschlossen werden können. Außerdem unterstützen einige Modelle eine einzelne SD-Karte im SD-Kartensteckplatz.

HINWEIS: Wenn ein austauschbares Gerät nicht in der aktuellen Liste der unterstützten austauschbaren Geräte enthalten ist, versucht das Konsolensystem möglicherweise, das Gerät mit Standardeinstellungen zu konfigurieren, sodass es ordnungsgemäß funktioniert. Wenn ein austauschbares Gerät nicht in der internen Datenbank vorhanden ist, wird in der Spalte „Geräte-Info“ womöglich gar kein Text angezeigt, oder der angezeigte Text variiert je nach dem Typ der Karte. Ein Beispiel ist „Unbekanntes Gerät f024 (Rev 01)“.

So können Sie ein austauschbares Gerät installieren und vom System erkennen lassen:

1. Wählen Sie in der seitlichen Navigationsleiste *Austauschbare Geräte*.
2. Klicken Sie auf *Erkennung austauschbarer Geräte aktivieren*, damit die angeschlossenen austauschbaren Geräte erkannt werden. Wenn diese Option bereits auf der Seite „System – Sicherheit“ aktiviert wurde, müssen Sie sie hier nicht noch einmal aktivieren.
3. Schließen Sie ein Gerät an einen USB-Port an oder stecken Sie eine SD-Karte in den SD-Kartensteckplatz des Konsolensystem ein.

4. In der Tabelle „Austauschbare Geräte“ werden alle austauschbaren Geräte aufgelistet, die erkannt wurden.

HINWEIS: Wenn Sie die Erkennung austauschbarer Geräte deaktivieren möchten, klicken Sie auf *Erkennung austauschbarer Geräte deaktivieren*.

So können Sie ein austauschbares Gerät auswerfen oder löschen:

1. Wählen Sie in der seitlichen Navigationsleiste *Austauschbare Geräte*.
2. Aktivieren Sie das Kontrollkästchen neben dem austauschbaren Gerät, das Sie auswerfen oder löschen möchten.
3. Klicken Sie auf *Auswerfen* oder *Löschen*. Klicken Sie dann auf *Speichern*.

HINWEIS: Werfen Sie austauschbare Geräte immer über die Weboberfläche aus, bevor Sie sie physisch entfernen.

Gerätekonfiguration

Speichergeräte werden nach der Erkennung durch das Konsolensystem automatisch bereitgestellt und konfiguriert, es sei denn, die Unterstützung für Speichergeräte ist deaktiviert. Ethernet-Karten, Modems und USB-Konsolengeräte müssen konfiguriert werden.

HINWEIS: Die Konfiguration von Drahtlosgeräten wird erst wirksam, nachdem das jeweilige Gerät ausgeworfen und erneut eingesteckt wurde.

So konfigurieren Sie ein austauschbares Gerät:

1. Klicken Sie in der seitlichen Navigationsleiste auf *Austauschbare Geräte*.
2. Klicken Sie bei einem Netzwerkgerät auf seinen Namen, um die Netzwerkparameter zu konfigurieren.

   – oder –

   Klicken Sie bei einem Modem (V.92) auf das Kontrollkästchen neben seinem Namen und dann entweder auf *Einwahl festlegen* oder *Hinauswählen festlegen*, um die Parameter für das Einwählen bzw. Hinauswählen zu konfigurieren.

   – oder –

   Klicken Sie bei einem USB-Konsolengerät auf das Kontrollkästchen neben seinem Namen und dann auf *Konsole festlegen*, um es dem System als weiteren Port hinzuzufügen. Sie können entweder die Standard-Portzuweisung akzeptieren oder einen unbenutzten Port in das Feld „Port“ eingeben und auf *Zuweisen* klicken. Wechseln Sie dann zur Seite *Ports – Serielle Ports*, um den neu hinzugefügten Port zu konfigurieren und zu aktivieren.

Zuweisung der USB-Konsole

USB-Konsolengeräte werden standardmäßig auf einen Port basierend auf der Anzahl der seriellen Ports des Konsolensystems eingestellt. Die folgende Tabelle zeigt die Standard-Portzuweisungen.

Tabelle 3.20 Zuweisung der ACS80X USB-Konsole

	USB-Ports			
MODELL	Oben links	Unten links	Oben rechts	Unten rechts
ACS802	3	4	5	6
ACS804	5	6	7	8
ACS808	9	10	11	12

Tabelle 3.21 Zuweisung der ACS80XX USB-Konsole

	Hintere USB-Ports						Vordere USB-Ports	
Modell	Oben links	Unten links	Oben Mitte	Unten Mitte	Oben rechts	Unten rechts	Oben	Unten
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

Wenn der standardmäßig zugewiesene Port bereits verwendet wird oder wenn das USB-Gerät nicht direkt an das Konsolensystem angeschlossen ist, wird der nächste verfügbare Port nach den reservierten Ports verwendet. Beispielsweise ist bei einem ACS808 Konsolensystem Port 13 der nächste verfügbare Port.

Hotplugging

Serielle Konsolengeräte können getrennt und wieder an denselben USB-Port angeschlossen werden, ohne offene serielle Sitzungen zu unterbrechen. In den meisten Fällen erhält das USB-Gerät den gleichen, von Linux zugewiesenen Gerätenamen. In einigen Fällen wird ein anderer Gerätename zugewiesen, wenn der ursprüngliche Name offenbar verwendet wird.

HINWEIS: Das Gerät muss wieder mit dem gleichen Port verbunden werden, um Hotplugging zu ermöglichen.

3.3.10 Authentifizierung

Die Authentifizierung kann auf verschiedene Weise erfolgen: lokal, über Einmalkennwörter (One Time Passwords, OTP) oder über einen Remote-Authentifizierungsserver auf Grundlage von LDAP, Radius, Kerberos oder TACACS+. Wenn das Konsolensystem von einem DSView-Server verwaltet wird, wird auch die DSView-Authentifizierung unterstützt. Das Konsolensystem unterstützt auch Remote-Gruppenautorisierungen für die Authentifizierungsmethoden LDAP, Radius, Kerberos und TACACS+.

Die folgenden Ausweichmechanismen (Fallback) sind verfügbar:

Zunächst kann eine lokale Authentifizierung versucht werden; wenn diese fehlschlägt, wird eine Remote-Authentifizierung versucht (Local/Remote_Method).

– oder –

Zunächst kann eine Remote-Authentifizierung versucht werden, gefolgt von einer lokalen Authentifizierung (Remote_Method/Local).

– oder –

Die lokale Authentifizierung kann nur versucht werden, wenn kein Remote-Authentifizierungsserver verfügbar ist (Remote_Method_Down_Local).

Administratoren können die Authentifizierung über das CLI-Dienstprogramm und die Weboberfläche konfigurieren. Die standardmäßige Authentifizierungsmethode für das Konsolensystem und die seriellen Ports ist „Lokal“. Die Authentifizierungsmethode, die für das Konsolensystem oder die Ports konfiguriert ist, wird für die Authentifizierung aller Benutzer verwendet, die versuchen, sich über Telnet, SSH oder die Weboberfläche anzumelden.

Einheiten-Authentifizierung

Das Konsolensystem nimmt die Authentifizierung für das Konsolensystem und die Ports entweder nach Gruppen oder individuell vor.

HINWEIS: Bei Verwendung der Gruppenautorisierung sollten Sie dieselbe Authentifizierung für das Konsolensystem und alle seriellen Ports vewenden. Alternativ können Sie die SSO-Authentifizierung (SSO = Single Sign-On, einmalige Anmeldung) nutzen, um die Gruppenautorisierung zu ermöglichen.

Wenn die SSO-Authentifizierung deaktiviert ist, verwendet das Konsolensystem die individuelle Konfiguration auf Grundlage des Zugriffsziels: das Konsolensystem selbst oder jeder einzelne serielle Port. Benutzer müssen bei jedem Zugriff auf einen individuellen Port ihr Kennwort eingeben. Wenn die SSO-Authentifizierung aktiviert ist, verwendet sie für alle Zugriffe den Authentifizierungsserver, den Sie im Pulldown-Menü auswählen. In diesem Fall ist keine weitere Authentifizierung erforderlich.

HINWEIS: Wenn Sie im Pulldown-Menü die Option *nicht konfiguriert* auswählen, können die Ports auch weiterhin individuelle Authentifizierungsserver verwenden. In diesem Fall müssen Sie beim ersten Zugriff auf die Ports immer Ihr Kennwort eingeben. Anschließend ist für die Ports keine Authentifizierung über ein Kennwort mehr erforderlich, sofern die SSO-Authentifizierung aktiviert ist.

So legen Sie die Authentifizierung für das Konsolensystem fest:

1. Klicken Sie auf *Authentifizierung – Einheiten-Authentifizierung*.
2. Wählen Sie im Dropdown-Menü „Authentifizierungstyp“ den gewünschten Authentifizierungsserver aus.
3. Wählen Sie die Option *Ausweichen auf den Typ „Lokal“ für den Stammbenutzer im Konsolenport der Einheit aktivieren*, wenn die Remote-Authentifizierung fehlschlägt und der Administrator als Stammbenutzer (root) über den Konsolenport auf die Einheit zugreifen möchte.
4. Wählen Sie die Option *SSO aktivieren* aus, um die SSO-Authentifizierung zu aktivieren, und wählen Sie dann den gewünschten Authentifizierungsserver im Dropdown-Menü „Authentifizierungstyp“ aus.
5. Klicken Sie auf *Speichern*.

Authentifizierungsserver

Bevor Sie einen Authentifizierungsserver verwenden können, müssen Sie seine IP-Adresse und in den meisten Fällen noch weitere Parameter konfigurieren. Für die folgenden Authentifizierungsserver ist eine Konfiguration erforderlich: RADIUS-, TACACS+-, LDAP(S)|AD-, Kerberos-, - und DSView-Server.

So konfigurieren Sie einen RADIUS-Authentifizierungsserver:

1. Wählen Sie *Authentifizierung – Authentifizierungsserver – RADIUS*.

2. Geben Sie die IP-Adressen des ersten Authentifizierungsservers und des ersten Abrechnungsservers ein.
3. Geben Sie ggf. die IP-Adressen des zweiten Authentifizierungsservers und des zweiten Abrechnungsservers ein.
4. Geben Sie Ihr Geheimwort oder Ihre Passphrase in das Feld „Geheimfrage“ ein (gilt für die ersten und zweiten Authentifizierungs- und Abrechnungsserver). Wiederholen Sie die Eingabe dann im Feld „Geheimfrage bestätigen“.
5. Geben Sie die gewünschte Anzahl von Sekunden für das Server-Timeout in das Feld „Timeout“ ein.
6. Geben Sie die gewünschte Anzahl von Neuversuchen in das Feld „Neuversuche“ ein.
7. Wenn Sie das Kontrollkästchen *Diensttyp-Attribut aktivieren, um Autorisierungsgruppe anzugeben* aktiviert haben, geben Sie den Namen der Autorisierungsgruppe für jeden der folgenden Diensttypen ein: Anmeldung, Rahmen, Rückruf/Anmeldung, Rückruf/Rahmen, Ausgehend, Administrativ.
8. Klicken Sie auf *Speichern*.

So konfigurieren Sie einen TACACS+-Authentifizierungsserver:

1. Wählen Sie *Authentifizierung – Authentifizierungsserver – TACACS+*.
2. Geben Sie die IP-Adressen des ersten Authentifizierungsservers und des ersten Abrechnungsservers ein.
3. Geben Sie ggf. die IP-Adressen des zweiten Authentifizierungsservers und des zweiten Abrechnungsservers ein.
4. Wählen Sie im Dropdown-Menü „Service“ den gewünschten Dienst aus (PPP oder raccess).
5. Geben Sie Ihr Geheimwort oder Ihre Passphrase in das Feld „Geheimfrage“ ein (gilt für die ersten und zweiten Authentifizierungs- und Abrechnungsserver). Wiederholen Sie die Eingabe dann im Feld „Geheimfrage bestätigen“.
6. Geben Sie die gewünschte Anzahl von Sekunden für das Server-Timeout in das Feld „Timeout“ ein.
7. Geben Sie die gewünschte Anzahl von Neuversuchen in das Feld „Neuversuche“ ein.
8. Wenn Sie das Kontrollkästchen *Shell-Attribut der Benutzerebene und raccess-Dienste aktivieren, um die Autorisierungsgruppe anzugeben* aktiviert haben, geben Sie den Namen der Autorisierungsgruppe für bis zu 15 Benutzerebenen ein.
9. Klicken Sie auf *Speichern*.

So konfigurieren Sie einen LDAP(S)|AD-Authentifizierungsserver:

1. Wählen Sie *Authentifizierung – Authentifizierungsserver – LDAP(S)|AD*.
2. Geben Sie die IP-Adresse des Servers ein.
3. Geben Sie die Basis ein.
4. Wählen Sie im Dropdown-Menü „Sicher“ entweder *Aus, Ein* oder *Start_TLS*.
5. Geben Sie den Datenbank-Benutzernamen ein.
6. Geben Sie Ihr Datenbank-Kennwort ein und wiederholen Sie die Eingabe dann im Feld „Kennwort bestätigen“.
7. Geben Sie die gewünschten Anmeldeattribute ein.
8. Klicken Sie auf *Speichern*.

So konfigurieren Sie einen Kerberos-Authentifizierungsserver:

1. Wählen Sie *Authentifizierung – Authentifizierungsserver – Kerberos*.
2. Geben Sie die IP-Adresse (den Bereich) des Servers ein.
3. Geben Sie den Domänennamen des Bereichs ein (Beispiel: AVOCENT.com).
4. Geben Sie den Domänennamen ein (Beispiel: .avocent.com).
5. Klicken Sie auf *Speichern*.

So konfigurieren Sie einen DSView-Authentifizierungsserver:

1. Wählen Sie *Authentifizierung – Authentifizierungsserver – DSView*.
2. Geben Sie die IP-Adressen 1 bis 4 für die DSView-Server in die vorgesehenen Felder ein.
3. Klicken Sie auf *Speichern*.

3.3.11 Benutzerkonten und Benutzergruppen

Der Zugriff auf Ports und andere Rechte können auf Grundlage von Berechtigungen verwaltet werden, die Administratoren benutzerdefinierten Benutzergruppen und einzelnen Benutzerkonten zuweisen können.

Gruppen und Benutzer können auch berechtigt sein, den Strom zu verwalten, während sie mit Geräten verbunden sind. Das Konsolensystem umfasst zwei Standardbenutzer (admin und root) sowie vier vordefinierte Benutzergruppen (admin, appliance-admin, shell-login-profile und user).

Für jeden Benutzer muss ein Benutzerkonto auf dem Konsolensystem oder auf einem Authentifizierungsserver eingerichtet werden. Die Admin- und Stammbenutzer (admin und root) verfügen standardmäßig über Konten. Administratoren können Konten für andere Benutzer hinzufügen und konfigurieren. Jedes lokale Benutzerkonto wird mindestens einer Benutzergruppe zugewiesen.

HINWEIS: Wenn ein Benutzer aus allen Gruppen entfernt wird, werden seine Berechtigungen auf die der Standardbenutzergruppe zurückgesetzt. Aus diesem Grund wird empfohlen, benutzerdefinierte Gruppen zu verwenden und der Standardbenutzergruppe keine zusätzlichen Berechtigungen zu erteilen.

Standardmäßig verfügen alle Benutzer über Zugriff auf alle Ports des Konsolensystem. Wenn der Zugriff bestimmten Benutzergruppen erteilt werden soll, muss der Administrator festlegen, dass der Portzugriff über Berechtigungen gesteuert wird, die Benutzergruppen zugewiesen sind.

So legen Sie fest, dass der Portzugriff über Berechtigungen gesteuert wird, die Benutzergruppen zugewiesen sind:

1. Klicken Sie in der seitlichen Navigationsleiste auf der Registerkarte „Experte“ auf *System – Sicherheit – Sicherheitsprofil*.
2. Klicken Sie unter „Serielle Geräte“ auf die Schaltfläche „Durch Zugriffsrechte gesteuert, die Benutzergruppen und bestimmten Benutzern zugewiesen sind“. Klicken Sie dann auf *Speichern*.

Lokale Konten

Gemäß den werkseitigen Standardeinstellungen verfügt das Konsolensystem über zwei lokale Benutzerkonten:

- admin: Dieser Benutzer führt die erstmalige Netzwerkkonfiguration durch. Der Admin-Benutzer ist Mitglied der Admin-Gruppe und kann das Konsolensystem und die Ports sowie Benutzer- und Gruppenberechtigungen konfigurieren.
- root: Der Root-Benutzer (Stammbenutzer) hat dieselben Administrationsberechtigungen wie der Admin-Benutzer, zusätzlich aber auch uneingeschränkte Shell-Berechtigungen. Der Root-Benutzer ist Mitglied der Gruppen „admin“ und „shell-login-profile“. Wenn sich ein Root-Benutzer über den KONSOLEN-Port, über SSH oder über Telnet anmeldet, gibt das Anmeldeprofil vor, dass die Sitzung direkt zur Shell wechselt. Das Anmeldeprofil kann so angepasst werden, dass kein direkter Wechsel zur Shell erfolgt.

So zeigen Sie die Zugriffsrechte der Benutzer für die Einheit an:

1. Klicken Sie auf *Benutzer – Lokale Konten – Benutzernamen*. Die Benutzernamen werden im Inhaltsbereich aufgelistet.
2. Klicken Sie unter „Benutzername“ auf einen Benutzernamen. Im Inhaltsbereich werden Informationen zum ausgewählten Benutzer angezeigt.

HINWEIS: Wenn Sie einen Benutzernamen auswählen, ändern sich der Inhaltsbereich und die seitliche Navigationsleiste. In der seitlichen Navigationsleiste werden bestimmte Menüoptionen für Mitglieder und Zugriffsrechte angezeigt (darunter Rechte für „Seriell“, „Strom“ und „Einheit“).

3. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Seriell* oder *Zugriffsrechte – Strom*, um Bildschirme aufzurufen, in denen die festen Zugriffsrechte und Berechtigungen für den ausgewählten Benutzer angezeigt werden.

HINWEIS: Die Bildschirme „Seriell“ und „Strom“ sind schreibgeschützt und können daher nicht geändert werden.

4. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Einheit*. Der Bildschirm „Zugriffsrechte für Einheit“ wird geöffnet. Er enthält eine Liste aller Zugriffsrechte, die dem Benutzer zur Verfügung stehen. Folgende Zugriffsrechte für die Einheit sind verfügbar:
   - Informationen zur Einheit anzeigen
   - Sitzungen trennen
   - Einheit neu starten
   - Flash-Upgrade für Einheit durchführen und Einheit neu starten
   - Einstellungen der Einheit konfigurieren
   - Benutzerkonten konfigurieren
   - Konfiguration sichern/wiederherstellen
   - Shell-Zugriff
   - Dateien übertragen
   - DFÜ-Zugriff

So fügen Sie neue Benutzer hinzu:

1. Klicken Sie auf *Benutzer – Lokale Konten – Benutzernamen*. Der Bildschirm „Benutzernamen“ wird mit einer Liste aller Benutzer angezeigt.
2. Klicken Sie auf *Hinzufügen*. Der Bildschirm „Lokale Benutzerinformationen“ wird angezeigt.
3. Geben Sie den neuen Benutzernamen und ein Kennwort ein. Geben Sie dann das Kennwort zur Bestätigung noch einmal ein.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Benutzer muss das Kennwort bei der nächsten Anmeldung ändern*.
5. Wenn Sie den Benutzer einer verfügbaren Benutzergruppe hinzufügen möchten, wählen Sie den Namen der Benutzergruppe im Feld auf der linken Seite aus und klicken Sie auf *Hinzufügen*. Die Standardgruppe lautet „user“ (Benutzer). Sie können eine Benutzergruppe aus dem Feld auf der rechten Seite entfernen, indem Sie sie auswählen und auf *Entfernen* klicken.
6. Geben Sie die gewünschten Parameter für „Kennwortablauf“ ein.
   - Min. Tage: Geben Sie an, wie viele Tage mindestens zwischen einer Kennwortänderung liegen müssen. Frühere Versuche, das Kennwort zu ändern, werden abgelehnt. Lassen Sie dieses Feld leer, wenn die Einschränkung, dass eine Kennwortänderung erst nach einer bestimmten Anzahl Tage möglich ist, nicht gelten soll.
   - Max. Tage: Geben Sie die maximale Anzahl von Tagen für die Gültigkeit des Kennworts an. Nach diesem Zeitraum muss das Kennwort zwingend geändert werden. Lassen Sie dieses Feld leer, wenn die Einschränkung, dass ein Kennwort nur eine bestimmte Anzahl Tage gültig ist, nicht gelten soll.
   - Warntage: Geben Sie die Anzahl von Tagen an, an denen der Benutzer vor dem Ablauf des Kennworts eine Warnung erhält. Wenn Sie 0 eingeben, wird die Warnung am Ablaufdatum ausgegeben. Lassen Sie dieses Feld leer, wenn die Warnung nicht ausgegeben werden soll.
7. Geben Sie das gewünschte Datum für den Kontoablauf ein (JJJJ-MM-TT).
8. Klicken Sie auf *Speichern*.

So konfigurieren Sie Kennwortregeln:

1. Klicken Sie auf *Benutzer – Lokale Konten – Kennwortregeln*.
2. Wenn Sie die Kennwortkomplexität festlegen möchten (empfohlen), stellen Sie sicher, dass die Option *Kennwortkomplexität überprüfen* aktiviert ist.
3. Wenn Sie die Kennwortkomplexität aktiviert haben, geben Sie die gewünschten Werte ein.
4. Geben Sie die gewünschten Werte für „Standardablauf“ ein.
5. Klicken Sie auf *Speichern*.

Benutzergruppen

Benutzergruppen verfügen entweder über standardmäßige oder von einem Administrator zugewiesene Zugriffsrechte und Berechtigungen. Administratoren können die Berechtigungen und Zugriffsrechte der Benutzer ändern, die den Gruppen „appliance-admin“ oder „user“ angehören. Außerdem können sie weitere Gruppen mit benutzerdefinierten Berechtigungen und Zugriffsrechten erstellen. Administratoren können Berechtigungen und Zugriffsrechte der Benutzer in allen Gruppen jederzeit hinzufügen, löschen oder ändern.

Wenn ein Administrator das Konsolensystem so konfiguriert, dass der Zugriff der Benutzer auf Ports eingeschränkt ist, kann er Benutzer bestimmten Gruppen zuweisen, die zum Zugriff auf Ports berechtigt sind. Außerdem kann der Administrator Gruppen die Berechtigung zur Stromverwaltung und zur Datenpufferverwaltung erteilen.

In diesem Dokument und in der Software werden Benutzer, deren Konten auf Remote-Authentifizierungsservern konfiguriert sind, als Remote-Benutzer bezeichnet. Remote-Benutzer benötigen keine lokalen Konten.

HINWEIS: Wenn ein Benutzer aus allen Gruppen entfernt wird, werden seine Berechtigungen auf die der Standardbenutzergruppe zurückgesetzt. Aus diesem Grund wird empfohlen, benutzerdefinierte Gruppen zu verwenden und der Standardbenutzergruppe keine zusätzlichen Berechtigungen zu erteilen.

Die Radius-, TACACS+- und LDAP-Authentifizierungsdienste bieten die Möglichkeit der Gruppenkonfiguration. Wenn ein Remote-Benutzer Mitglied einer Remote-Gruppe ist, meldet der Authentifizierungsserver bei der Authentifizierung des Benutzers den Gruppennamen an das Konsolensystem. Eine lokale Gruppe mit demselben Namen muss auch auf dem Konsolensystem konfiguriert sein. Wenn ein Authentifizierungsserver bei der Authentifizierung eines Remote-Benutzers keine Gruppe zurückgibt, wird der Remote-Benutzer standardmäßig der Gruppe „user“ zugewiesen.

Gruppe „admin“

Mitglieder der Gruppe „admin“ verfügen über uneingeschränkte Administrationsberechtigungen, die nicht geändert werden können. Sie haben dieselben Zugriffs- und Konfigurationsberechtigungen wie der standardmäßige Admin-Benutzer. Administratoren können Ports konfigurieren, Benutzer hinzufügen und die an das Konsolensystem angeschlossenen Stromversorgungsgeräte verwalten.

So zeigen Sie die Zugriffsrechte der Benutzergruppe „admin“ für die Einheit an:

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*. Daraufhin wird der Bildschirm „Gruppennamen“ angezeigt. Auf diesem Bildschirm werden die drei Standard-Benutzergruppen sowie alle weiteren Gruppen aufgelistet, die erstellt wurden.
2. Klicken Sie unter „Gruppenname“ auf *admin*. Im Inhaltsbereich wird der Bildschirm „Mitglieder“ angezeigt, auf dem alle Mitglieder der Gruppe „admin“ aufgelistet werden. Die Standardmitglieder sind Admin- und Stammbenutzer (admin und root).

HINWEIS: Wenn Sie einen Gruppennamen auswählen, ändern sich der Inhaltsbereich und die seitliche Navigationsleiste. In der seitlichen Navigationsleiste werden bestimmte Menüoptionen für Mitglieder und Zugriffsrechte angezeigt (darunter Rechte für „Seriell“, „Strom“ und „Einheit“).

3. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Seriell* oder *Zugriffsrechte – Strom*, um die Bildschirme aufzurufen, in denen die festgelegten Zugriffsrechte und Berechtigungen angezeigt werden, die Mitglieder der Gruppe „admin“ für serielle Ports bzw. Stromverwaltungsfunktionen besitzen.

HINWEIS: Die Bildschirme „Seriell“ und „Strom“ sind schreibgeschützt und können daher nicht geändert werden.

4. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Einheit*. Der Bildschirm „Zugriffsrechte für Einheit“ wird geöffnet. Er enthält eine Liste aller Zugriffsrechte, die Mitgliedern der Gruppe „admin“ zur Verfügung stehen. Alle Zugriffsrechte für die Einheit sind aktiviert. Folgende Zugriffsrechte für die Einheit sind verfügbar:
   - Informationen zur Einheit anzeigen
   - Sitzungen trennen
   - Einheit neu starten
   - Flash-Upgrade für Einheit durchführen und Einheit neu starten
   - Einstellungen der Einheit konfigurieren
   - Benutzerkonten konfigurieren
   - Konfiguration sichern/wiederherstellen
   - Shell-Zugriff

- Dateien übertragen
- DFÜ-Zugriff

HINWEIS: Der Bildschirm „Zugriffsrechte für Einheit“ für die Benutzergruppen „admin“ und „appliance-admin“ ist schreibgeschützt und kann daher nicht geändert werden. Wenn Sie ein Kontrollkästchen deaktivieren und dann auf *Speichern* klicken, wird eine Fehlermeldung eingeblendet. Alle ausgewählten Rechte werden im Konsolensystem beibehalten.

Gruppe „appliance-admin“

Die Mitglieder der Benutzergruppe „appliance-admin“ haben Zugriff auf serielle Ports und Optionen für die Stromverwaltung, sofern diese Zugriffsberechtigungen nicht durch das Sicherheitsprofil eingeschränkt werden. Außerdem haben Mitglieder der Gruppe alle Administrator-Zugriffsberechtigungen für die Einheit, mit Ausnahme der Berechtigungen „Benutzerkonten konfigurieren“ und „Shell-Zugriff“, die für diese Gruppe dauerhaft deaktiviert sind.

Gruppe „user“

Die Mitglieder der Gruppe „user“ haben Zugriff auf Zielgeräte, sofern dieser Zugriff nicht von einem Administrator eingeschränkt wurde. Wenn der Portzugriff global durch ein Sicherheitsprofil eingeschränkt wird, kann der Administrator den Mitgliedern der Gruppe „user“ den Zugriff auf Ports gewähren. Mitglieder der Gruppe „user“ haben keine Zugriffsrechte für das Konsolensystem.

Administratoren können Einheiten-Zugriffsrechte und Berechtigungen hinzufügen. Außerdem haben Administratoren die Möglichkeit, Benutzer verschiedenen benutzerdefinierten Benutzergruppen hinzuzufügen, um nach Bedarf Berechtigungen und Zugriffsrechte zu erteilen. Standardmäßig sind alle Optionen auf dem Bildschirm „Zugriffsrechte für Einheit“ deaktiviert.

HINWEIS: Der Bildschirm „Zugriffsrechte für Einheit“ für die Gruppe „user“ kann jederzeit von einem Administrator geändert werden. Dadurch werden die Zugriffsrechte für alle Mitglieder der Gruppe „user“ des Konsolensystem geändert.

Gruppe „shell-login-profile“

Mitglieder der Gruppe „shell-login-profile“ haben nach der Anmeldung Zugriff auf die Shell. Standardmäßig gehört der Stammbenutzer (root) zu dieser Gruppe. Diese Gruppe ist nicht geschützt und kann daher gelöscht werden.

Verwalten von Benutzergruppen

Administratoren und Mitglieder der Gruppe „admin“ können benutzerdefinierte Benutzergruppen erstellen und ihnen beliebige Benutzer zuweisen.

So erstellen Sie eine benutzerdefinierte Benutzergruppe:

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*. Daraufhin wird der Bildschirm „Gruppen“ angezeigt. Auf diesem Bildschirm werden die drei Standard-Benutzergruppen sowie alle weiteren benutzerdefinierten Benutzergruppen aufgelistet, die erstellt wurden.
2. Klicken Sie im Inhaltsbereich auf *Hinzufügen*.
3. Geben Sie den Namen der neuen Benutzergruppe ein.
4. Klicken Sie auf *Speichern*.

So fügen Sie einer Benutzergruppe Mitglieder hinzu:

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*.
2. Klicken Sie auf den Namen der Benutzergruppe.
3. Klicken Sie auf *Hinzufügen*. Der Bildschirm „Mitgliedszuweisung“ wird geöffnet. Die verfügbaren Benutzer werden im linken Bereich dieses Bildschirms aufgelistet, während der rechte Bereich leer ist.
4. Verschieben Sie Benutzer aus dem linken Bereich „Verfügbare Benutzer“ in den rechten Bereich, indem Sie auf den Benutzernamen doppelklicken oder indem Sie den Benutzernamen auswählen und dann auf die Schaltfläche *Hinzufügen* klicken. Sie können Benutzernamen aus dem rechten Bereich entfernen, indem Sie auf den Namen doppelklicken oder indem Sie den Namen auswählen und dann auf die Schaltfläche *Entfernen* klicken.
5. Wenn Sie der neuen Benutzergruppe Remote-Benutzer hinzufügen möchten, geben Sie sie in das Feld „Neue Remote-Benutzer“ ein (dabei muss es sich um gültige Namen auf dem Remote-Authentifizierungsserver handeln).
6. Klicken Sie auf *Speichern*.

So entfernen Sie Mitglieder aus einer Benutzergruppe:

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*.
2. Klicken Sie auf den Namen der Benutzergruppe.
3. Aktivieren Sie die Kontrollkästchen neben den Mitgliedern, die Sie entfernen möchten. Klicken Sie auf *Löschen*, um die ausgewählten Mitglieder zu löschen.

So konfigurieren Sie ein Inaktivitäts-Timeout für Sitzungen und/oder ein Anmeldeprofil für eine Gruppe:

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*.
2. Klicken Sie auf den Namen der Gruppe, für die Sie ein Inaktivitäts-Timeout für Sitzungen und/oder ein Anmeldeprofil konfigurieren möchten. Klicken Sie in der seitlichen Navigationsleiste auf *Anmeldeprofil*.
3. Wählen Sie ein Optionsfeld aus, um festzulegen, ob Sie die globalen Einstellungen für das Sitzungs-Timeout oder benutzerdefinierte Einstellungen für die Benutzergruppe verwenden möchten. Wenn Sie benutzerdefinierte Einstellungen verwenden möchten, geben Sie den gewünschten Wert für das Sitzungs-Timeout (in Sekunden) in das vorgesehene Feld ein.
4. Aktivieren Sie das Kontrollkästchen *Anmeldeprofil aktivieren*.
5. Klicken Sie auf *ts_menu*, um die ts_menu-Anwendung zu verwenden, wenn ein Mitglied der ausgewählten Benutzergruppe eine Sitzung auf dem Konsolensystem öffnet. Geben Sie die ts-menu-Optionen in das Feld „Optionen“ ein.

   – oder –

   Klicken Sie auf *CLI*, um beim Öffnen einer Sitzung die CLI zu verwenden. Geben Sie den CLI-Befehl in das vorgesehene Feld ein und aktivieren Sie das Kontrollkästchen, wenn das System nach dem Ausführen des Befehls beendet werden soll.
6. Klicken Sie auf *Speichern*.

HINWEIS: Wenn der Benutzer zu mehreren Gruppen gehört, wird das erste aktivierte Anmeldeprofil in alphabetischer Reihenfolge der Gruppe verwendet.

Tabelle 3.22 ts_menu-Optionen

Befehl	Beschreibung
-p	Zeigt den TCP-Port an.
-i	Zeigt die lokale IPv4-Adresse an, die dem seriellen Port zugewiesen ist.
-i6	Zeigt die lokale IPv6-Adresse an, die dem seriellen Port zugewiesen ist.
-u <Name>	Der in der Sitzung mit dem Ziel zu verwendende Benutzername.
-e <[^]Zeichen>	Escape-Zeichen, mit dem die Sitzung mit dem Ziel geschlossen wird. Standardwert: Strg-X.
-l	Sortiert die Ports in einer Liste und beendet das System.
-ro	Schreibgeschützter Modus.
<Portname>	Stellt eine direkte Verbindung mit einem seriellen Port her.
-t	Inaktivitäts-Timeout in Sekunden für das Ziel.

So weisen Sie einer Benutzergruppe Zugriffsrechte für serielle Ports zu:

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*.
2. Klicken Sie auf den Namen der neuen Benutzergruppe.
3. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte*.
4. Klicken Sie im Inhaltsbereich auf *Hinzufügen*.
5. Verschieben Sie serielle Zielgeräte aus dem linken Bereich „Verfügbares Ziel“ in den rechten Bereich, indem Sie auf den Namen des seriellen Zielgeräts doppelklicken

   – oder –

   indem Sie das Zielgerät auswählen und dann auf die Schaltfläche *Hinzufügen* klicken. Sie können Zielgeräte aus dem rechten Bereich entfernen, indem Sie auf das Zielgerät doppelklicken oder indem Sie das Zielgerät auswählen und dann auf die Schaltfläche *Entfernen* klicken.
6. Wählen Sie die gewünschten Zugriffsrechte aus.
7. Klicken Sie auf *Speichern*. Der Bildschirm „Seriell“ wird eingeblendet. Auf diesem Bildschirm werden die seriellen Zielgeräte, für die Sie der Benutzergruppe Zugriffsrechte erteilt haben, sowie die konfigurierten Berechtigungen aufgelistet.
8. Bearbeiten Sie die Zugriffsrechte, indem Sie das Kontrollkästchen für ein oder mehrere Zielgeräte aktivieren und dann auf *Bearbeiten* klicken. Der Bildschirm „Zugriffsrechte für Ziel“ wird mit einer Liste der Zugriffsrechte eingeblendet. Wählen Sie die gewünschten Zugriffsrechte aus und klicken Sie auf *Speichern*.

So weisen Sie einer Benutzergruppe Zugriffsrechte für PDUs zu:

HINWEIS: Wenn Sie einer Benutzergruppe Zugriffsrechte für eine PDU zuweisen, verfügen die Mitglieder dieser Benutzergruppe über uneingeschränkten Zugriff auf alle Stromverwaltungsfunktionen für die jeweilige PDU. Wenn Sie der Benutzergruppe nur Zugriffsrechte für Ausgänge zuweisen möchten, befolgen Sie die Schritte weiter unten im Abschnitt *So weisen Sie einer neuen benutzerdefinierten Benutzergruppe Zugriffsrechte für Ausgänge zu*.

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*.
2. Klicken Sie auf den Namen der Benutzergruppe.
3. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Strom*.

4. Klicken Sie im Inhaltsbereich auf *Hinzufügen*. Der Bildschirm „PDU-Zuweisung“ wird eingeblendet. Die verfügbaren PDUs werden im linken Bereich des Bildschirms aufgelistet.
5. Verschieben Sie PDU-Geräte aus dem linken Bereich „Verfügbare PDUs“ in den rechten Bereich, indem Sie auf den PDU-Namen doppelklicken oder indem Sie die PDU auswählen und dann auf die Schaltfläche *Hinzufügen* klicken. Sie können PDUs aus dem rechten Bereich entfernen, indem Sie auf den PDU-Namen doppelklicken oder indem Sie die PDU auswählen und dann auf die Schaltfläche *Entfernen* klicken.
6. Im Feld unten können Sie eine benutzerdefinierte PDU-ID festlegen.

HINWEIS: Über die benutzerdefinierte PDU-ID werden Benutzergruppen die Verwaltungsberechtigungen für PDUs zugewiesen, die noch nicht an das Konsolensystem angeschlossen wurden.

7. Klicken Sie auf *Speichern*.

So weisen Sie einer neuen benutzerdefinierten Benutzergruppe Zugriffsrechte für Ausgänge zu:

HINWEIS: Wenn Sie einer Benutzergruppe Zugriffsrechte für Ausgänge zuweisen, können die Mitglieder der Gruppe Ausgänge ein- und ausschalten sowie Funktionen zum Sperren und zum Aus- und Wiedereinschalten für kompatible PDUs aktivieren.

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*.
2. Klicken Sie auf den Namen der neuen Benutzergruppe.
3. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Strom – Ausgänge*.
4. Klicken Sie auf *Hinzufügen*. Der Bildschirm „Ausgang hinzufügen“ wird eingeblendet.
5. Klicken Sie für verbundene PDUs auf die Schaltfläche *PDU auswählen*, um die Felder „Verbundene PDUs“ und „Ausgänge“ zu aktivieren.
6. Wählen Sie *Verbundene PDU* im Pulldown-Menü aus.
7. Geben Sie die Ausgänge ein, die der Benutzergruppe zugewiesen sind.

HINWEIS: Sie können Ausgänge individuell (zum Beispiel 1,3,6,8) oder als Bereich (zum Beispiel 1-4) angeben. Auch eine Kombination ist möglich (zum Beispiel 1-4,6,8 – hiermit werden Zugriffsrechte für die Ausgänge 1, 2, 3, 4, 6 und 8 erteilt).

8. Wenn eine benutzerdefinierte PDU-ID zur späteren Verwendung erstellt wurde und Sie die Ausgänge vorab zuweisen möchten, klicken Sie auf die Schaltfläche *Benutzerdefiniert*, um die benutzerdefinierte PDU-ID einzugeben. Geben Sie dann die Ausgänge an.
9. Klicken Sie auf *Speichern*.

So weisen Sie einer Benutzergruppe Zugriffsrechte für USVs zu:

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*.
2. Klicken Sie auf den Namen der Benutzergruppe.
3. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Strom – USV*.
4. Klicken Sie im Inhaltsbereich auf *Hinzufügen*. Der Bildschirm „USV-Zuweisung“ wird eingeblendet. Die verfügbaren USV-Geräte werden im linken Bereich des Bildschirms aufgelistet.

5. Verschieben Sie USV-Geräte aus dem linken Bereich „Verfügbare USV“ in den rechten Bereich, indem Sie auf den USV-Namen doppelklicken oder indem Sie das USV-Gerät auswählen und dann auf die Schaltfläche *Hinzufügen* klicken. Sie können USV-Geräte aus dem rechten Bereich entfernen, indem Sie auf den USV-Namen doppelklicken oder indem Sie das USV-Gerät auswählen und dann auf die Schaltfläche *Entfernen* klicken.
6. Im Feld unten auf der Seite können Sie eine benutzerdefinierte USV-ID festlegen.

HINWEIS: Über die benutzerdefinierte USV-ID werden Benutzergruppen die Verwaltungsberechtigungen für USV-Geräte zugewiesen, die noch nicht an das Konsolensystem angeschlossen wurden.

So weisen Sie benutzerdefinierten Benutzergruppen Zugriffsrechte für Einheiten zu:

1. Klicken Sie auf *Benutzer – Autorisierung – Gruppen*.
2. Klicken Sie auf den Namen der neuen Benutzergruppe.
3. Klicken Sie in der seitlichen Navigationsleiste auf *Zugriffsrechte – Einheit*.
4. Wählen Sie die gewünschten Zugriffsrechte für die Einheit aus und klicken Sie auf *Speichern*.

So konfigurieren Sie eine Gruppe auf einem TACACS+-Authentifizierungsserver:

1. Fügen Sie auf dem Server den raccess-Dienst zur Benutzerkonfiguration hinzu.
2. Definieren Sie im raccess-Dienst die Gruppe(n), zu denen der Benutzer gehört. Verwenden Sie dazu die folgende Syntax:

Gruppenname = <Gruppe1>[,<Gruppe2,...,GruppeN>];

Zum Beispiel:

Konfigurieren Sie auf dem Konsolensystem eine neue Autorisierungsgruppe namens TACACS_1 und konfigurieren Sie dann die Zugriffsrechte für diese Gruppe. Konfigurieren Sie auf dem TACACS+-Server den Benutzer „regina“ mit dem folgenden Attribut: `raccess = Gruppenname=TACACS_1;`

Konfigurieren Sie dann den Benutzer „special“ mit dem folgenden Attribut: `raccess = Gruppenname=admin;`

Während der Authentifizierungsphase erhält das Konsolensystem das raccess-Attribut vom TACACS+-Server. Der Benutzer „regina“ gehört zur Autorisierungsgruppe TACACS_1 und der Benutzer „special“ gehört zur Autorisierungsgruppe „admin“.

So konfigurieren Sie eine Gruppe auf einem RADIUS-Authentifizierungsserver:

Definieren Sie im Attribut FRAMED_FILTER_ID die Gruppe(n), zu denen der Benutzer gehört. Verwenden Sie dazu die folgende Syntax:

```
[:Gruppenname=]<acs800/8000_Gruppe1>[,<acs800/8000_Gruppe2>];
```

HINWEIS: Die Gruppennamen müssen durch ein Komma getrennt werden und mit einem Semikolon enden.

HINWEIS: Das ACS 800/8000 akzeptiert mehrere Attribute FRAMED_FILTER_ID.

Zum Beispiel:

Konfigurieren Sie auf dem Konsolensystem die neuen Autorisierungsgruppen RADIUS_1 und RADIUS_2 und konfigurieren Sie dann die Zugriffsrechte für diese Gruppen. Konfigurieren Sie auf dem RADIUS-Server den Benutzer „regina“ mit dem folgenden Attribut:

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

– oder –

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

– oder –

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

Konfigurieren Sie dann den Benutzer „special“ mit dem folgenden Attribut:

```
FramedFilterID = Gruppenname=admin;
```

Während der Authentifizierungsphase erhält das Konsolensystem das Attribut FramedFilterID vom RADIUS-Server. Der Benutzer „regina“ gehört zu den Autorisierungsgruppen RADIUS_1 und RADIUS_2. Der Benutzer „special“ gehört zur Autorisierungsgruppe „admin“.

So konfigurieren Sie eine Gruppe auf einem LDAP-Authentifizierungsserver:

Bearbeiten Sie auf dem LDAP-Server das Attribut „info“ für den Benutzer und fügen Sie die folgende Syntax hinzu.

```
info: Gruppenname=<Gruppe1>[,<Gruppe2>,...,<GruppeN>];
```

Zugriffsrechte für die DSView-Software

Administratoren können konfigurieren, wie die Viewer-Sitzungsrechte der DSView-Software den Zugriffsrechten des Konsolensystem zugeordnet werden, wenn ein Benutzer über den seriellen Viewer der DSView-Software auf ein Zielgerät zugreift.

So konfigurieren Sie die Zuordnung zwischen den Zugriffsrechten der DSView-Software und den Zugriffsrechten des Konsolensystem:

1. Klicken Sie auf *Benutzer – Autorisierung – DSView-Zugriffsrechte*.
2. Wählen Sie die gewünschten Zugriffsrechte aus und klicken Sie auf *Speichern*.

3.3.12 Ereignisbenachrichtigungen

Das Konsolensystem generiert Benachrichtigungen für verschiedene Ereignisse. Sie können das Konsolensystem so konfigurieren, dass diese Ereignisbenachrichtigungen zur sofortigen Verwendung oder zur späteren Analyse an ein bestimmtes Ziel gesendet oder an einem bestimmten Ort gespeichert werden.

Ereignisliste

Auf dem Bildschirm „Ereignisliste“ werden Ereignisse des Konsolensystem aufgeführt, die jeweils für SNMP-Traps, Syslog, DSView-Software, E-Mail und SMS konfiguriert werden können.

So konfigurieren Sie Ereignisse:

1. Klicken Sie auf *Ereignisse und Protokolle – Ereignisse*.
2. Suchen Sie die Ereignisse, für die Sie Benachrichtigungen senden möchten, und aktivieren Sie die Kontrollkästchen neben den zugehörigen Ereignisnummern.
3. Klicken Sie auf *Bearbeiten*.
4. Wenn für einen konfigurierten Ereigniszieltyp eine Ereignisbenachrichtigung gesendet werden soll, aktivieren Sie das entsprechende Kontrollkästchen *Senden*.
5. Klicken Sie auf *Speichern*. Die Seite „Ereignisse“ wird angezeigt. Die Spalte unter dem Zieltyp enthält ein X, wenn das Kontrollkästchen „Senden“ auf dem Bildschirm „Ereigniseinstellungen“ aktiviert wurde.

Ereignisziele

So konfigurieren Sie Ereignisziele:

1. Klicken Sie auf *Ereignisse und Protokolle – Ereignisziele*.
2. Wählen Sie unter „Syslog“ im Dropdown-Menü die Einrichtung aus.

   Wählen Sie *Remote-Server – IPv4* aus, damit Syslog-Nachrichten an einen oder mehrere Remote-IPv4-Syslog-Server gesendet werden. Geben Sie dann die IPv4-Adresse oder den Hostnamen sowie den UDP-Port für jeden Remote-Syslog-Server ein.

   – oder –

   Wählen Sie *Remote-Server – IPv6* aus, damit Syslog-Nachrichten an einen oder mehrere Remote-IPv6-Syslog-Server gesendet werden können. Geben Sie dann die IPv6-Adresse oder den Hostnamen sowie den UDP-Port für jeden Remote-Syslog-Server ein.
3. Wählen Sie *Einheiten-Konsole* aus, damit Nachrichten an die Konsole des Konsolensystem gesendet werden.
4. Wählen Sie *Stammsitzung* aus, damit Syslog-Nachrichten an alle Sitzungen gesendet werden, bei denen Sie als Stammbenutzer (root) angemeldet sind.
5. Geben Sie unter „SNMP-Trap“ in das Feld „Community“ den Namen der Community ein, die auf einem oder mehreren SNMP-Trap-Servern definiert ist. Geben Sie dann die IP-Adressen von maximal fünf Servern in die Server-Felder ein.
6. Geben Sie unter „SMS“ den SMS-Server, den Port und die Pager-Nummer in die vorgesehenen Felder ein.
7. Geben Sie unter „E-Mail“ den Server, den Port und die Ziel-E-Mail in die vorgesehenen Felder ein.
8. Geben Sie unter „DSView“ die IP-Adresse des DSView-Servers, an den die Ereignisbenachrichtigungen gesendet werden sollen, in das Feld „DSView Server“ ein. Geben Sie die Syslog-Server-Portnummer für den DSView-Server, die SSH-Informationen und die Pufferwarnungen in die vorgesehenen Felder ein.
9. Klicken Sie auf *Speichern*.

Trap-Weiterleitung

Das Konsolensystem empfängt SNMP-Traps und leitet sie an einen Remote-SNMP-Trap-Server weiter.

So fügen Sie einen SNMP-Trap-Server für die Trap-Weiterleitung hinzu:

1. Klicken Sie auf *Ereignisse und Protokolle – Trap-Weiterleitung*.
2. Klicken Sie auf *Hinzufügen*.
3. Geben Sie die IP-Adresse des Remote-Servers und den UDP-Port ein.
4. Geben Sie die OID ein, um die an diesen Server zu sendenden Traps zu filtern (optional).

So bearbeiten Sie die Konfiguration eines SNMP-Trap-Servers:

1. Klicken Sie auf *Ereignisse und Protokolle – Trap-Weiterleitung*.
2. Klicken Sie auf den Index des zu bearbeitenden Servers.
3. Ändern Sie den UDP-Port und/oder die OID und klicken Sie auf *Speichern*.

Datenpufferung

Wenn die Datenpufferung an einer oder mehreren seriellen Schnittstelle(n) aktiviert ist, werden die Einstellungen auf der Seite „Ereignisse und Protokolle – Datenpufferung“ auf den Typ (das Ziel) der Pufferung angewendet. Die Segmentgröße, die in Kilobyte angegeben wird, bestimmt die Größe jeder gespeicherten Datenpufferdatei. Freie Segmente legen fest, wie viele zusätzliche historische Pufferdateien der Segmentgröße beibehalten und mit dem Suffix .1, .2 usw. benannt werden.

So konfigurieren Sie die Datenpufferung:

1. Wählen Sie *Ereignisse und Protokolle – Datenpufferung*.
2. Geben Sie die Segmentgröße in kB und die freien Segmente in den Bereich „Einstellungen für die lokale Datenpufferung“ ein.
3. Geben Sie im Bereich „Einstellungen für die NFS-Datenpufferung“ die folgenden Informationen ein: NFS-Server, NFS-Pfad, Segmentgröße (KB) und freie Segmente.

HINWEIS: Der RPC-Dienst muss auf dem Bildschirm „Sicherheitsprofil“ aktiviert werden, bevor die Einstellungen für die NFS-Datenpufferung konfiguriert werden können.

4. Um die Datenpufferungsdateien jeden Tag nach Stunde zu segmentieren, geben Sie die Zeit in das Feld „Protokolldateien schließen und neue öffnen zur Uhrzeit (HH:MM)“ ein. Diese Einstellung gilt für die lokale und die NFS-Datenpufferung.
5. Zum Konfigurieren des Datenpufferspeichers auf einem Syslog-Server wählen Sie im Bereich „Einstellungen für die Syslog-Datenpufferung“ eine Einrichtungsnummer im Dropdown-Menü aus: Log Local 0, Log Local 1, Log Local 2, Log Local 3, Log Local 4 oder Log Local 5.
6. Klicken Sie auf *Speichern*.

So aktivieren Sie die Datenpufferung:

1. Wählen Sie *Ports – Serielle Ports* aus.
2. Klicken Sie auf den Port, an dem Sie die Datenpufferung aktivieren möchten.
3. Verwenden Sie auf der Registerkarte „Datenpufferung“ das Dropdown-Menü neben „Status“ aus, um die Datenpufferung zu *aktivieren*.

Protokollierung für die Einheit

Wenn die Protokollierung für die Einheit aktiviert ist, werden die Befehle (Eingabe) und die Ausgabe von SSH- und Telnet-Sitzungen an die Einheit zu Prüfungszwecken aufgezeichnet.

So konfigurieren Sie die Protokollierung für die Einheit:

1. Klicken Sie auf *Datenprotokollierung für Einheitensitzung aktivieren*.
2. Wählen Sie das Ziel für die Datenprotokolle der Einheitensitzung im Pulldown-Menü aus. Die verfügbaren Optionen sind *Lokal*, *NFS*, *Syslog* und *DSView*.
    a. Wenn Sie „Lokal“ als Ziel ausgewählt haben, wählen Sie im Dropdown-Menü das gewünschte lokale Ziel aus. Das Ziel *mmcblk0* ist der integrierte Flash-Speicher. Die SD-Karte (sofern vorhanden und aktiviert) ist *mmcblk1*. USB-Geräte (sofern vorhanden und aktiviert) sind *sda1*, *sda2* und so weiter.

HINWEIS: Wenn das lokale Ziel auf mmcblk0 eingestellt ist, lautet das Protokollverzeichnis auf der Einheit /mnt/hdUser/db. Wenn das lokale Ziel auf mmcblk1 oder auf ein USB-Gerät eingestellt ist, entspricht das Protokollverzeichnis dem Stammverzeichnis (oberste Ebene) dieses Geräts.

3. Aktivieren oder deaktivieren Sie den Zeitstempel für die Datenprotokolle der Einheitensitzung.
4. Klicken Sie auf *Datenprotokollierungsalarme für Einheitensitzung aktivieren*.
5. Geben Sie die gewünschten Alarmzeichenfolgen (maximal 10) in die vorgesehenen Felder ein.
6. Klicken Sie auf *Speichern*.

3.3.13 Stromverwaltung

Angeschlossene Stromversorgungsgeräte können für die Remote-Stromverwaltung verwendet werden. Mithilfe des Konsolensystems können Benutzer, die zur Stromverwaltung berechtigt sind, Geräte, die an eine verbundene PDU angeschlossen sind, einschalten, ausschalten oder zurücksetzen. Außerdem können autorisierte Benutzer ein angeschlossenes Liebert GXT4 oder GXT5 USV-Gerät überwachen und steuern (USV = unterbrechungsfreie Stromversorgung).

Die folgenden PDU-Typen können an jeden seriellen Port angeschlossen werden.

- Avocent Power Management Power Distribution Unit (PM PDU).
- Vertiv MPH2-Rack-PDUs sowie MPX- und MPH-Rack-PDUs mit installierten RPC2-Karten.
- Cyclades PM Intelligent Power Distribution Units (IPDUs). Bei Cyclades PM-IPDUs können bis zu 128 Ausgänge verkettet und über einen einzelnen seriellen Port verwaltet werden.
- Avocent SPC-Stromverwaltungsgeräte.
- Server Technology Sentry Familie der geschalteten Cabinet Power Distribution Units (CDUs), Smart Cabinet Power Distribution Units (Smart CDUs) und geschaltete CDU Expansion Module (CW/CX)-Stromversorgungsgeräte. Eine zusätzliche Ebene mit Stromversorgungsgeräten kann mit ServerTech Expansion-Modulen verkettet werden.
- Server Technology Sentry Power Tower XL (PTXL)- und Power Tower Expansion Module (PTXM)-Stromversorgungsgeräte.
- Eaton ePDU G3-PDUs. Bis zu acht ePDUs können verkettet und über einen einzelnen seriellen Port verwaltet werden.
- Raritan PX G2-PDUs.
- APC rPDU2-PDUs.
- Geist GU2 und R-Series Rack PDUs mit Firmware 5.3 oder neuer werden unterstützt.

HINWEIS: Der Begriff „PDU“ bezieht sich auf alle diese Stromversorgungsgeräte.

Liebert RPC2-Karten, Avocent PM-PDUs, Cyclades PM-PDUs, Raritan-PDUs, Eaton-ePDUs, APC-PDUs und Avocent SPC-Geräte werden vom Konsolensystem automatisch erkannt und unterstützt, wenn der entsprechende serielle Port für die Stromverwaltung konfiguriert ist.

PDUs

So verwalten Sie eine PDU:

1. Wählen Sie *Stromverwaltung – PDUs*.
2. Aktivieren Sie das Kontrollkästchen neben der PDU, die Sie verwalten möchten.
3. Klicken Sie wahlweise auf *Ein, Aus, Aus- und wieder einschalten, PDU neu starten, HW-Überstromschutz zurücksetzen* oder *Werkseitige Standardeinstellungen*. Eine Bestätigung wird angezeigt. Klicken Sie auf *OK*.

HINWEIS: Die Stromsteuerungsfunktionen (Ein, Aus, Aus- und wieder einschalten) werden auf alle Ausgänge der PDU angewendet.

4. Wenn Sie die ID der PDU ändern möchten, klicken Sie auf *Umbenennen* und geben Sie den gewünschten Namen in das Feld „Neue PDU-ID“ ein.
5. Klicken Sie auf *Speichern*.

So führen Sie ein Firmware-Upgrade durch:

1. Aktivieren Sie das Kontrollkästchen neben der PDU, deren Firmware Sie aktualisieren möchten, und klicken Sie auf die Schaltfläche *Firmware-Upgrade durchführen*.

HINWEIS: Sie können ein Firmware-Upgrade für mehrere PDUs gleichzeitig durchführen. Dies ist jedoch nur für Avocent PM-PDUs und Vertiv-PDUs (MPH2, MPH und MPX mit installierten RPC2-Karten) möglich. Wenn Sie ein Upgrade von PDUs in einer Verkettung durchführen, wählen Sie nur die erste PDU in der Kette aus, da die Upgrades der restlichen PDUs in der Kette automatisch durchgeführt werden.

2. Wählen Sie *Remote-Umgebung* aus und geben Sie die Remote-Serverinformationen ein.

   – oder –

   Wählen Sie *Eigener Computer* aus und navigieren Sie zu dem Speicherort der Firmware-Datei.

3. Klicken Sie auf *Download*, um die Firmware auf das Konsolensystem herunterzuladen.
4. Wenn der Download abgeschlossen wurde, zeigt das Konsolensystem die aktuelle und die heruntergeladene Firmwareversion an. Wenn die heruntergeladenen Versionsinformationen korrekt sind, klicken Sie auf *Upgrade jetzt durchführen*, um das Firmware-Upgrade für die PDU zu starten.
5. Klicken Sie nach dem Start des Upgrades auf *Fertigstellen*. Es wird eine Meldung angezeigt, die besagt, dass das Upgrade erfolgreich gestartet wurde. Auf der Seite „PDU-Übersicht“ wird der Upgrade-Status angezeigt. Die PDU wird neu gestartet, wenn das Upgrade abgeschlossen ist.

So können Sie die Informationen einer PDU anzeigen und Ausgänge verwalten:

1. Wählen Sie *Stromverwaltung – PDUs*.
2. Klicken Sie auf den Namen der PDU, die Sie anzeigen oder verwalten möchten.

3. Daraufhin wird ein Fenster mit einer Tabelle der Ausgänge und Stromsteuerungsfunktionen angezeigt. In der seitlichen Navigationsleiste des Fensters werden die verfügbaren Optionen aufgelistet.
4. So verwalten Sie die Ausgänge einer PDU:
   a. Aktivieren Sie die Kontrollkästchen neben den Nummern der Ausgänge, die Sie verwalten möchten.
   b. Klicken Sie auf *Ein*, *Aus*, *Aus- und wieder einschalten*, *Sperren* oder *Entsperren*, um die jeweilige Funktion für die ausgewählten Ausgänge auszuführen.
5. Klicken Sie in der seitlichen Navigationsleiste auf *Informationen*, um die Informationen einer PDU anzuzeigen.
6. Klicken Sie in der seitlichen Navigationsleiste auf *Übersicht*, um Informationen zur Datenüberwachung anzuzeigen.
7. Klicken Sie in der seitlichen Navigationsleiste auf *Strom*, *Spannung*, *Stromverbrauch*, *Energieverbrauch* oder *Umgebung*, um eine Tabelle mit den entsprechenden Informationen anzuzeigen. Klicken Sie auf *Werte zurücksetzen*, um die Max.-, Min.- und die Durchschnittswerte zu löschen.

So konfigurieren Sie eine PDU:

1. Klicken Sie auf *Einstellungen*, um die seitliche Navigationsleiste einzublenden.
2. Klicken Sie auf *Ausgänge*.
3. Klicken Sie auf die Nummer eines Ausgangs, um seine Einstellungen zu ändern. Klicken Sie auf *Speichern* und dann auf *Schließen*.

   – oder –

   Aktivieren Sie zwei oder mehr Kontrollkästchen neben den Ausgängen, deren Einstellungen Sie ändern möchten. Klicken Sie auf *Bearbeiten*, um die Einstellungen für die ausgewählten Ausgänge zu ändern. Klicken Sie auf *Speichern*.
4. Klicken Sie auf *PDU*, um die PDU-Einstellungen anzuzeigen und zu konfigurieren. Klicken Sie abschließend auf *Speichern*.
5. Klicken Sie auf *Phasen* oder *Leisten*.
   a. Klicken Sie auf den Namen der Phase oder Leiste, deren Einstellungen Sie ändern möchten, oder aktivieren Sie die Kontrollkästchen der Phase(n) oder Leiste(n), die Sie ändern möchten.
   b. Klicken Sie auf *Speichern*, um die Einstellungen zu speichern, und klicken Sie dann auf *Schließen*, um zum Bildschirm „Phase“ zurückzukehren.

HINWEIS: Das PDU-Modell bestimmt, welche Parameter im Fenster „Einstellungen“ verfügbar sind.

USV

So verwalten Sie eine USV:

1. Wählen Sie *Stromverwaltung – USV*.
2. Aktivieren Sie das Kontrollkästchen neben der USV, die Sie verwalten möchten.

3. Klicken Sie wahlweise auf *Ausgabe ausschalten*, *Ausgabe einschalten* oder *Ausgabe aus- und wieder einschalten*. Daraufhin wird eine Option angezeigt, mit der Sie die gewünschte Verzögerungszeit vor dem Ausführen des Vorgangs festlegen können. Klicken Sie auf die Schaltfläche, um den Vorgang auszuführen.
4. Wenn Sie die ID der USV ändern möchten, klicken Sie auf *Umbenennen* und geben Sie den gewünschten Namen in das Feld „Neue USV-ID“ ein.
5. Klicken Sie auf *Speichern*.

So zeigen Sie Informationen zu einem USV-Gerät an:

1. Wählen Sie *Stromverwaltung – USV*.
2. Klicken Sie auf den Namen der USV, die Sie anzeigen oder verwalten möchten.
3. Klicken Sie in der seitlichen Navigationsleiste auf die Optionen, um Informationen zur USV anzuzeigen.

So konfigurieren Sie eine USV:

1. Klicken Sie auf *Einstellungen*, um die seitliche Navigationsleiste einzublenden.
2. Klicken Sie in der seitlichen Navigationsleiste auf die Optionen, um die USV zu konfigurieren.

Anmeldung

Administratoren können das Anmeldekennwort für einen unterstützten PDU-Typ ändern. Dieses Kennwort wird vom Konsolensystem für die Kommunikation mit der PDU verwendet. (Nur ein Kennwort wird für alle PDUs desselben Typs unterstützt.)

So ändern Sie ein PDU-Kennwort:

1. Wählen Sie *Stromverwaltung – Anmeldung*.
2. Geben Sie das neue Kennwort für jeden PDU-Typ ein, für den Sie das Kennwort ändern möchten.
3. Klicken Sie auf *Speichern*.

Ausgangsgruppen

Auf der Registerkarte *Ausgangsgruppen* können Sie Ausgangsgruppen konfigurieren und ihren Status, die Ausgänge und den Stromverbrauch anzeigen. Außerdem können Sie ausgewählte Ausgangsgruppen einschalten, ausschalten sowie aus- und wieder einschalten.

So verwalten Sie Ausgangsgruppen:

1. Wählen Sie *Stromverwaltung – Ausgangsgruppen*.
2. Aktivieren Sie das Kontrollkästchen neben der Ausgangsgruppe, die Sie verwalten möchten.
3. Klicken Sie ggf. auf das Optionsfeld *Ein*, *Aus* oder *Aus- und wieder einschalten*.

   – oder –

4. Klicken Sie auf *Hinzufügen*, um eine Ausgangsgruppe hinzuzufügen. Der Bildschirm „Gruppe hinzufügen“ wird angezeigt. Geben Sie den Namen in das Feld „Gruppenname“ ein.
5. Klicken Sie auf *Speichern*.

So können Sie Informationen zur Ausgangsgruppe anzeigen und ändern:

1. Wählen Sie *Stromverwaltung – Ausgangsgruppen*.
2. Klicken Sie auf den Namen der Ausgangsgruppe, die Sie anzeigen oder verwalten möchten.
3. Wenn Sie der Gruppe einen neuen Ausgang hinzufügen möchten, klicken Sie auf *Hinzufügen*. Füllen Sie die Felder aus und klicken Sie dann auf *Speichern*, um zur Tabelle „Details der Ausgangsgruppe“ zurückzukehren.
4. Wenn Sie Ausgänge aus der Gruppe entfernen möchten, aktivieren Sie ihre Kontrollkästchen. Klicken Sie auf *Löschen* und dann auf *Schließen*.

Netzwerk-PDUs

Stromversorgungsgeräte, die mit dem Netzwerk verbunden sind und für die SNMP (Lesen/Schreiben) aktiviert ist, können für die Remote-Stromverwaltung verwendet werden. Autorisierte Benutzer können über das Konsolensystem die Stromversorgung für Geräte, die an die Netzwerk-PDU angeschlossen sind, ein- oder ausschalten.

HINWEIS: SNMP muss für die PDU aktiviert sein und eine Community mit Schreibberechtigungen bieten.

Durch Auswahl des Knotens *Netzwerk-PDUs* können Administratoren neue Netzwerk-PDUs hinzufügen oder die Konfiguration von vorhandenen Netzwerk-PDUs bearbeiten.

Die folgenden Funktionen werden für Netzwerk-PDUs unterstützt: Stromsteuerung von Ausgängen (einschalten, ausschalten, aus- und wieder einschalten, neu starten) sowie Umbenennen der PDU und der Ausgänge.

So fügen Sie eine Netzwerk-PDU hinzu:

1. Wählen Sie *Stromverwaltung – Netzwerk-PDUs*.
2. Klicken Sie auf *Hinzufügen*.
3. Geben Sie die IP-Adresse der Netzwerk-PDU ein.
4. Wählen Sie den PDU-Typ aus.
5. Geben Sie das Intervall an, in dem der Status der Ausgänge von der PDU abgefragt werden soll.
6. Geben Sie den Namen der Community ein, die in der PDU über die Schreibberechtigung verfügt.

Netzwerk-USV

Liebert GXT4 und GXT5 USV-Geräte, die über installierte Liebert Intellislot Unity-Karten verfügen, mit dem Netzwerk verbunden sind und für die SNMP (Lesen/Schreiben) aktiviert ist, können überwacht und gesteuert werden. Autorisierte Benutzer können über das Konsolensystem Informationen zu Batterien sowie zu Eingängen und Ausgängen des Systems überwachen und Anschlussdosen der Ausgänge steuern.

HINWEIS: SNMP muss für das USV-Gerät aktiviert sein und eine Community mit Schreibberechtigungen bieten.

Durch Auswahl des Knotens „Netzwerk-USV“ können Administratoren neue Netzwerk-USV-Geräte hinzufügen oder die Konfiguration von vorhandenen Netzwerk-USV-Geräten bearbeiten.

3.3.14 Sensoren

Intern

Das Konsolensystem verfügt über Sensoren, die die interne Temperatur überwachen. Sie können einen Betriebstemperaturbereich angeben, der für die Umgebungsbedingungen des Konsolensystems geeignet ist. Zwei interne Temperatursensoren können Ereignisbenachrichtigungen generieren: der Sensor für die CPU-Temperatur und der Sensor für die Platinentemperatur.

VORSICHT: Verwenden Sie keine Werte, die die Höchst- und die Mindesttemperatur überschreiten bzw. unterschreiten. **Anhänge auf Seite 93.**

So konfigurieren Sie die Temperatursensoren:

1. Klicken Sie auf *Sensoren – Einheit – Intern*, um die Seite „Intern“ zu öffnen, auf der die Temperatursensoren für die CPU und die Platine angezeigt werden.
2. Geben Sie in das Feld für die Höchsttemperatur der CPU oder der Platine die Höchsttemperatur in Grad Celsius ein. Bei Überschreiten dieses Wertes wird eine Ereignisbenachrichtigung generiert.
3. Geben Sie in das Feld für die Höchsttemperatur-Schwelle der CPU oder der Platine die Höchsttemperatur-Schwelle unter der Höchsttemperatur in Grad Celsius ein.

HINWEIS: Das Feld für die Höchsttemperatur-Schwelle definiert einen Bereich etwas ober- und unterhalb der Höchsttemperatur. Wenn die Temperatur einen Wert erreicht, der höher als die Höchsttemperatur zuzüglich der Schwelle ist, wird eine Ereignisbenachrichtigung generiert. Wenn die Temperatur auf einen Wert fällt, der unterhalb der Höchsttemperatur abzüglich der Schwelle liegt, wird eine Ereignisbenachrichtigung generiert, die Sie darüber informiert, dass das Konsolensystem wieder eine normale Betriebstemperatur erreicht hat. Dasselbe Prinzip gilt auch für die Mindesttemperatur-Schwelle.

4. Geben Sie in das Feld für die Mindesttemperatur einen Wert in Grad Celsius ein. Wenn die Temperatur des Konsolensystems diesen Wert unterschreitet, wird eine Ereignisbenachrichtigung generiert.
5. Geben Sie in das Feld für die Mindesttemperatur-Schwelle einen Wert in Grad Celsius ein, um die Schwelle oberhalb der Mindesttemperatur festzulegen.
6. Klicken Sie auf *Speichern*.

Externe 1-Wire-Sensoren

Ein externer 1-Wire-Sensor kann über ein CAT 5-Kabel an den SENSOR-Port an der Vorderseite des Konsolensystems angeschlossen werden. Die Unterstützung von 1-Wire-Sensoren ist standardmäßig aktiviert. Sie kann über die Seite „Sicherheitsprofil“ deaktiviert werden.

So konfigurieren Sie einen 1-Wire-Sensor:

Klicken Sie in der seitlichen Navigationsleiste auf *Sensoren – Einheit – 1-Wire*. Erkannte Sensoren werden zusammen mit dem Sensortyp und Informationen zu vorhandenen Werten in einer Tabelle angezeigt.

HINWEIS: Diese Option wird für alle Konsolensystem-Modelle angezeigt, auch wenn einige Modelle nicht über Ports für SD-Karten oder 1-Wire-Sensoren verfügen. Wenn Ihr Modell nicht über einen SENSOR-Port verfügt, lassen Sie diese Option deaktiviert.

HINWEIS: Wenn ein angeschlossener Sensor nicht angezeigt wird, klicken Sie auf *Liste aktualisieren*, um die Seite zu aktualisieren.

HINWEIS: Die Optionen für die Sensorkonfiguration richten sich nach dem Typ des Sensors. Sensoren haben gemeinsame Konfigurationseinstellungen für den Namen und den Standort.

Kontaktsensoren (SN-2D/SN-3C)

Dieser Sensortyp kann eine Ereignisbenachrichtigung generieren, wenn sich der Status eines Eingangs ändert. Ein Eingang kann den Status *Deaktiviert*, *Alarm wenn offen* oder *Alarm wenn geschlossen* haben.

Externe Temperatur

Dieser Sensortyp kann eine Ereignisbenachrichtigung generieren, wenn die Temperatur einen benutzerdefinierten Schwellenwert unter- oder überschreitet. Als Maßeinheit kann *Celsius* oder *Fahrenheit* konfiguriert werden. Die Schwellenwerte „Niedrig – Warnung“, „Niedrig – Kritisch“, „Hoch – Warnung“ und „Hoch – Kritisch“ müssen eingestellt werden, damit Ereignisse generiert werden können. Außerdem muss der Alarmstatus auf *Aktiviert* eingestellt werden, damit ein Alarm generiert wird.

Externe Luftfeuchtigkeit

Dieser Sensortyp kann eine Ereignisbenachrichtigung generieren, wenn die Luftfeuchtigkeit einen benutzerdefinierten Schwellenwert unter- oder überschreitet. Die Schwellenwerte „Niedrig – Warnung“, „Niedrig – Kritisch“, „Hoch – Warnung“ und „Hoch – Kritisch“ müssen eingestellt werden, damit Ereignisse generiert werden können. Außerdem muss der Alarmstatus auf *Aktiviert* eingestellt werden, damit ein Alarm generiert wird.

Differenzialdruck (SN-DP)

Dieser Sensortyp kann eine Ereignisbenachrichtigung generieren, wenn der Differenzialdruck einen benutzerdefinierten Schwellenwert unter- oder überschreitet. Die Schwellenwerte „Niedrig – Warnung“, „Niedrig – Kritisch“, „Hoch – Warnung“ und „Hoch – Kritisch“ müssen eingestellt werden, damit Ereignisse generiert werden können. Außerdem muss der Alarmstatus auf *Aktiviert* eingestellt werden, damit ein Alarm generiert wird.

Lecksensor (SN-L)

Dieser Sensortyp kann zwei Alarmarten generieren: einen Leckalarm, wenn ein Leck erkannt wird, und einen Kabelfehleralarm, wenn ein Verkabelungsproblem erkannt wird. Ein verfügbarer Konfigurationsparameter ist die Filterzeit in Sekunden. Dieser Parameter gibt an, wie lange das Leck bestehen muss, bevor ein Ereignis generiert wird.

Sensoren für digitale Eingänge

Ein externer Sensor für digitale Eingänge kann über ein CAT 5-Kabel an den DIGITAL IN-Port an der Vorderseite des Konsolensystems angeschlossen werden.

So konfigurieren Sie einen Sensor für digitale Eingänge:

1. Klicken Sie in der seitlichen Navigationsleiste auf *Sensoren – Einheit – Digitaler Eingang*. Die erkannten digitalen Eingänge werden in einer Tabelle angezeigt.
2. Klicken Sie auf die Nummer, die der Position des Sensors entspricht, um die Seite mit den Einstellungen zu öffnen.

3. Geben Sie den Namen und den Standort des Sensors ein und wählen Sie im Dropdown-Menü den Sensortyp aus.
4. Sie können einen Sensor für digitale Eingänge so konfigurieren, dass er ein Ereignis generiert. Dazu müssen Sie den Alarm-Parameter konfigurieren. Wählen Sie im Dropdown-Menü für den Alarm die Option *Alarm wenn offen*, *Alarm wenn geschlossen* oder *Deaktivieren*.

HINWEIS: Diese Option wird für alle Konsolensystem-Modelle angezeigt, auch wenn einige Modelle nicht über einen DIGITAL IN-Port verfügen. Wenn Ihr Modell nicht über einen DIGITAL IN-Port verfügt, lassen Sie diese Option deaktiviert.

Sensoren für digitale Ausgänge

Das ACS800 Advanced Console System unterstützt zwei digitale Ausgänge. Die digitalen Ausgänge sind ferngesteuerte Relais-Ports, die zum Öffnen und Schließen eines Stromkreises verwendet werden können.

HINWEIS: Digitale Ausgänge werden vom ACS8000 Advanced Console System nicht unterstützt.

So konfigurieren Sie einen Sensor für digitale Ausgänge:

1. Klicken Sie in der seitlichen Navigationsleiste auf „Digitaler Ausgang“.
2. Klicken Sie auf die Nummer, die der Position des Sensors entspricht, um die Seite mit den Einstellungen zu öffnen.
3. Geben Sie ggf. einen Namen für den Sensor ein.
4. Verwenden Sie das Dropdown-Menü, um einen Stromkreis *EIN* oder *AUS* zu schalten, und klicken Sie dann auf *Speichern*.

3.3.15 Aktive Sitzungen

Mehrere Benutzer können beim Konsolensystem angemeldet sein und gleichzeitig Sitzungen ausführen. Mit der Funktion „Aktive Sitzungen“ können Sie alle aktiven Sitzungen anzeigen und unerwünschte Sitzungen beenden. Klicken Sie auf *Aktive Sitzungen*, um alle Sitzungen anzuzeigen, die auf dem Konsolensystem geöffnet sind.

HINWEIS: Wenn Sie eine weitere Sitzung mit dem Konsolensystem starten, während dieser Bildschirm angezeigt wird, erscheint die neue Sitzung erst dann auf dem Bildschirm, wenn Sie oben im Fenster der Weboberfläche auf *Aktualisieren* klicken.

So beenden Sie eine aktive Sitzung:

1. Klicken Sie auf *Aktive Sitzungen*. Der Bildschirm „Aktive Sitzungen“ wird geöffnet. Auf diesem Bildschirm werden alle Sitzungen, die auf dem Konsolensystem geöffnet sind, nach der IP-Adresse der Workstation des Benutzers aufgelistet.
2. Aktivieren Sie das Kontrollkästchen neben der Sitzung, die Sie beenden möchten, und klicken Sie dann auf die Schaltfläche *Sitzung beenden*. Nach ein paar Sekunden werden auf dem Bildschirm „Aktive Sitzungen“ wieder alle geöffneten Sitzungen angezeigt, ohne die Sitzung, die Sie gerade beendet haben.

3.3.16 Überwachung

Durch Klicken auf *Überwachung* können Sie verschiedene Informationen zum Netzwerk und zum Konsolenport anzeigen. Diese Bildschirme dienen nur zur Anzeige und ermöglichen dem Benutzer keine Interaktivität. Die folgende Tabelle zeigt, welche Informationen verfügbar sind.

Tabelle 3.23 Bildschirme für die Überwachung

Bildschirmname	Definition
Netzwerk – Geräte	Zeigt Ethernet-Ports und USB-Netzwerkadapter, Status (aktiviert/deaktiviert), IPv4-Adresse, IPv4-Maske und IPv6-Adresse.
Netzwerk – IPv4-Routingtabelle	Zeigt Ziel, Gateway, Genmask, Flags, Metrik, Ref, Nutzung und Schnittstelle.
Netzwerk – IPv6-Routingtabelle	Zeigt Ziel, nächsten Hop, Flags, Metrik, Ref, Nutzung und Schnittstelle.
Serielle Ports	Zeigt Gerätename, Profil, Einstellungen, Signale, TX-Byte, RX-Byte, Rahmenfehler, Paritätsfehler, Unterbrechung und Überlauf. Durch Klicken auf die Schaltfläche „Zähler zurücksetzen“ können Administratoren die Statistikzähler für ausgewählte Ports zurücksetzen.
FIPS-Modus	Zeigt Dienstname und Modusanzeige.
Interaktionsloses Protokoll	Zeigt die Protokolldatei für die interaktionslose Bereitstellung und ermöglicht dem Administrator, den Inhalt des Protokolls zu löschen.
Anruferkennungsprotokoll	Zeigt die letzten 20 Anrufe an.
IPSec Tunnel-Status	Zeigt die IPSec-Verbindungsdetails an, einschließlich Tunnelstatus, Remote-IP-Adresse, IKE-Gültigkeitsdauer, Einrichtungszeit, Phasenalgorithmen und Zertifikatsname.

3.3.17 Kennwort ändern

Auf diesem Bildschirm können Administratoren oder Benutzer ihr eigenes Kennwort ändern.

So ändern Sie Ihr eigenes Kennwort:

1. Wählen Sie *Kennwort ändern*.
2. Geben Sie das alte und das neue Kennwort in die vorgesehenen Felder ein.
3. Bestätigen Sie das neue Kennwort und klicken Sie dann auf *Speichern*.

3.4 Weboberfläche für reguläre Benutzer – Übersicht

Tabelle 3.24 Optionen der Weboberfläche für reguläre Benutzer

Menüoption	Beschreibung
Zugriff	Hier werden alle Geräte angezeigt, auf die der Benutzer zugreifen kann. Klicken Sie in der Spalte „Aktion“ eines Geräts auf *Serieller Viewer*, um eine Terminalsitzung mit diesem Gerät zu starten.
Stromverwaltung – PDUs – Ausgangsgruppen	Durch Klicken auf *PDUs* können Sie PDUs, die an das Konsolensystem angeschlossen sind, einschalten, ausschalten, aus- und wieder einschalten, neu starten oder umbenennen, den HW-Überstromschutz zurücksetzen oder die werkseitigen Standardeinstellungen der PDUs wiederherstellen. Klicken Sie auf *Ausgangsgruppen*, um Gruppen mit Ausgängen an angeschlossenen PDUs zu verwalten. Klicken Sie auf „USV“, um angeschlossene USV-Geräte zu überwachen und zu steuern.
Kennwort ändern	Mit dieser Option können Sie Ihr eigenes Kennwort ändern.

Anhänge

Anhang A: Technische Daten

Tabelle A.1 Technische Daten der Hardware für das ACS8000 Advanced Console System

Kategorie	Wert
Allgemeine Informationen	
CPU	Dual Core ARM Cortex-A9 mit 766 MHz
Arbeitsspeicher	1 GB DDR3L/16 GB eMMC FLASH
Schnittstellen	• Zwei Dual-Media-Ports, 1000 Base-TX-Kupfer/1 Gbit/s SFP-Glasfaser • 48 serielle Ports mit automatischer Erkennung und Switching-Unterstützung für Cyclades- und Cisco-Pinbelegungen • Zwei der seriellen Ports unterstützen RS232/422/485-Multiprotokoll mit automatischer Erkennung und Switching-Unterstützung für Cyclades- und Cisco-Pinbelegungen im RS232-Modus • 1 serieller Konsolenport • Acht USB 2.0-Hostports (die vorderen Ports sind bei manchen Modellen nicht verfügbar) • Ein SD-Kartensteckplatz (nicht bei allen Modellen verfügbar) • Optionaler V.92/56K MODEM-Port • 1-Wire-Schnittstelle für externe Sensoren (nicht bei allen Modellen verfügbar) • RJ45-Einzelanschluss mit vier digitalen Eingängen für externe Kontaktsensoren (nicht bei allen Modellen verfügbar)
Informationen zur Stromversorgung	
Stromversorgung	Interne, redundante Stromversorgung, 100-240 VAC, 50/60 Hz , Doppeleingang optional, -48 VDC optional erhältlich
Stromverbrauch	Nennspannung 120 VAC: Typisch: 0,17 A, 20 W; max. 0,25 A, 30 W Nennspannung 230 VAC: Typisch: 0,1 A, 23 W; max. 0,15 A, 35 W Nennspannung -48 VDC (20 % Toleranz), typisch: 0,5 A
Umgebungsbedingungen	
Betriebstemperatur	0 ° C bis 50 °C (mit DC-Stromversorgung) -10 ° C bis 70 °C (mit AC-Stromversorgung)
Lagertemperatur	-20 °C bis 70 °C
Luftfeuchtigkeit	20 % bis 80 % relative Luftfeuchtigkeit (nicht kondensierend) für den gesamten Betriebstemperaturbereich
Maße	
Höhe x Breite x Tiefe	4,318 x 43,434 x 24,13 cm
Gewicht	2,722-3,175 kg je nach Modell

Tabelle A.2 Technische Daten der Hardware für das ACS800 Advanced Console System

Kategorie	Wert
Allgemeine Informationen	
CPU	Dual Core ARM Cortex-A9 mit 766 MHz
Arbeitsspeicher	1 GB DDR3L/16 GB eMMC FLASH
Schnittstellen	• Zwei Dual-Media-Ports, 1000 Base-TX-Kupfer • Acht serielle Ports mit automatischer Erkennung und Switching-Unterstützung für Cyclades- und Cisco-Pinbelegungen • Alle acht Ports unterstützen RS232/422/485-Multiprotokoll mit automatischer Erkennung und Switching-Unterstützung für Cyclades- und Cisco-Pinbelegungen im RS232-Modus • 1 serieller Konsolenport • Vier USB 2.0-Hostports • Analoger V.92/56K MODEM-Port • 1-Wire-Schnittstelle für externe Sensoren • RJ45-Einzelanschluss mit vier digitalen Eingängen für externe Kontaktsensoren • Digitale Ausgangsanschlüsse mit vier Ausgangssignalen.
Informationen zur Stromversorgung	
Stromversorgung	Intern: 100-240 VAC, 50/60 Hz
Stromverbrauch	Nennspannung 120 VAC: Typisch: 80,5 mA/3,5 W; max. 306 mA/17 W Nennspannung 240 VAC:Typisch: 60 mA/3,75 W; max. 191 mA/17 W
Umgebungsbedingungen	
Betriebstemperatur	-20 °C bis 70 °C
Lagertemperatur	-20 °C bis 70 °C
Luftfeuchtigkeit	20 % bis 80 % relative Luftfeuchtigkeit (nicht kondensierend) für den gesamten Betriebstemperaturbereich
Maße	
Höhe x Breite x Tiefe	3,302 x 21,2852 x 18,1864 cm
Gewicht	1,72365 kg

Anhang B: Interaktionslose Bereitstellung

Die interaktionslose Bereitstellung erweitert die Funktionalität des Konsolensystems zum Abruf der BOOTP-Konfiguration. Mithilfe der interaktionslosen Bereitstellung können zahlreiche Konsolensysteme in einer Umgebung eingerichtet werden. Wenn Sie die interaktionslose Bereitstellung verwenden möchten, benötigen Sie gültige DHCP- und TFTP-Server. Sie können Ihre DHCP-Server so konfigurieren, dass sie neue Konsolensysteme dazu anweisen, eine Vorlagenkonfiguration herunterzuladen sowie ein Upgrade/Downgrade der Firmware auszuführen.

Die Einrichtung der DHCP-/TFTP-Server sowie der Konfigurationsdateien dauert im Normalfall nur wenige Minuten, kann Ihnen aber viele Stunden Zeit sparen, die sonst für die Konfiguration erforderlich wären, wenn Sie Ihrem Netzwerk später weitere Konsolensysteme hinzufügen. Nach Abschluss der Bereitstellung können Sie auf die einzelnen Konsolensysteme zugreifen, um ihre Konfiguration bei Bedarf anzupassen (beispielsweise können Sie eine statische IP-Adresse und einen Hostnamen zuweisen).

Mithilfe der interaktionslosen Bereitstellung können Konsolensysteme nach dem Starten und Initialisieren automatisch konfiguriert und aktualisiert werden. Dies vereinfacht die Eingliederung und Installation des Konsolensystems im vorhandenen Netzwerk.

Administratoren können ein Protokoll der interaktionslosen Konfigurationen anzeigen, indem sie in der Seitenleiste der Registerkarte „Experte“ auf *Interaktionsloses Protokoll* klicken.

B.1 Konfigurationsdatei für die interaktionslose Bereitstellung

Damit die interaktionslose Bereitstellung verwendet werden kann, muss der Administrator zunächst die Konfigurationsdatei des Konsolensystems auf einem Remote-Server speichern. Die Konfigurationsdatei wird von der Setup-Datei verwendet, die für die interaktionslose Bereitstellung erstellt wird. Weitere Informationen zum Erstellen und Speichern einer Konfigurationsdatei finden Sie unter Konfigurationsdateien auf Seite 20.

HINWEIS: Die Parameter in der Konfigurationsdatei gelten für alle Konsolensysteme, die die Datei empfangen. Wenn ein bestimmter Parameter, wie beispielsweise der Hostname, nicht für alle Konsolensysteme gelten soll, müssen Sie ihn auskommentieren, indem Sie ihm das Rautenzeichen (#) voranstellen.

B.2 Setup-Datei

Nachdem die Konfigurationsdatei auf einem Remote-Server gespeichert und der DHCP-Server konfiguriert wurde, muss der Administrator eine Setup-Datei erstellen. Anhand der Setup-Datei identifiziert das Konsolensystem Konfigurationsparameter und wichtige Bereitstellungsinformationen, wie den Dateinamen für das Firmware-Image, den Namen der Konfigurationsdatei und die IP-Adresse des Remote-Servers, auf dem die Konfigurationsdatei gespeichert wurde. Die erstellte Setup-Datei muss auf einem TFTP-, FTP- oder SFTP-Server gespeichert werden. Die IP-Adresse des TFTP-, FTP- oder SFTP-Servers wird im DHCP-Angebot gesendet.

HINWEIS: Wenn Sie die Setup-Datei auf einem TFTP-Server speichern, wird als Speicherort der Stammordner empfohlen.

Im Folgenden finden Sie ein Beispiel für die Setup-Datei.

```
ONE_TIME_CONFIG=YES
FIRMWARE_VERSION=1.0.1
FIRMWARE_FILENAME=/var/tftp/acs8000/acs8000_1.0.1.bin

FIRMWARE_SERVER_IP=192.168.100.2
FIRMWARE_SERVER_USERNAME=required username
FIRMWARE_SERVER_PASSWORD=required password
FIRMWARE_SERVER_PROTOCOL=SFTP
CONFIG_FILENAME=/tftp/config-xml
CONFIG_SERVER_IP=192.168.100.2
CONFIG_SERVER_USERNAME=
CONFIG_SERVER_PASSWORD=
CONFIG_SERVER_PROTOCOL=SFTP
```

Tabelle B.1 Beschreibungen der Setup-Datei

Parameter	Beschreibung
ONE_TIME_CONFIG	Wenn dieser Parameter auf YES (Ja) eingestellt ist, ruft das Konsolensystem die Konfigurationsdatei beim ersten Start ab. Bei weiteren Startvorgängen wird die Konfigurationsdatei nicht gesendet. Wenn der Parameter auf NO (Nein) eingestellt ist, ruft das Konsolensystem die Konfigurationsdatei bei jedem Start ab.
FIRMWARE_VERSION	Die Version der Firmware, die an die Einheit gesendet werden soll.
FIRMWARE_FILENAME	Der Pfad und der Dateiname der Firmware.
FIRMWARE_SERVER_IP	Die IP-Adresse oder der Hostname des Servers, auf dem die Firmware gehostet wird.
FIRMWARE_SERVER_USERNAME	Falls die Firmware auf einem sicheren Server gehostet wird, geben diese Parameter die Anmeldedaten für den Zugriff auf den Server an.
FIRMWARE_SERVER_PASSWORD	
FIRMWARE_SERVER_PROTOCOL	Das Protokoll des Servers, auf dem die Firmware gehostet wird. Folgende Protokolle werden unterstützt: TFTP, FTP, SFTP, SCP und WGET.
CONFIG_FILENAME	Der Pfad und der Dateiname der Konfigurationsdatei.
CONFIG_SERVER_IP	Die IP-Adresse oder der Hostname des Servers, auf dem die Konfigurationsdatei gehostet wird.
CONFIG_SERVER_USERNAME	Falls die Konfigurationsdatei auf einem sicheren Server gehostet wird, geben diese Parameter die Anmeldedaten für den Zugriff auf den Server an. Die Anmeldedaten sind in den meisten Fällen erforderlich. Beim Benutzernamen handelt es sich um einfachen Text, während das Kennwort verschlüsselt sein muss.
CONFIG_SERVER_PASSWORD	
CONFIG_SERVER_PROTOCOL	Das Protokoll des Servers, auf dem die Konfigurationsdatei gehostet wird. Folgende Protokolle werden unterstützt: FTP, SFTP, SCP und WGET.

Kennwortverschlüsselung

Für die Parameter FIRMWARE_SERVER_PASSWORD oder CONFIG_SERVER_PASSWORD sollte ein verschlüsseltes Kennwort mit Hash-Funktion erstellt werden. Der Hash-Wert muss in einer Linux-Umgebung generiert werden, in der OpenSSL ausgeführt wird. Geben Sie die folgenden Befehle wie gezeigt in eine Linux-Befehlszeile oder eine Konsolensystem-Shell ein. Geben Sie dann das resultierende Hash-Kennwort in die Setup-Datei für den definierten Servertyp ein.

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

HINWEIS: Ersetzen Sie im Beispiel oben den Text <MyPassword> durch ein gültiges Kennwort.

B.3 Kopieren der Setup-Datei auf einen Server

Die erstellte Setup-Datei muss auf einen TFTP-Server kopiert werden. Das folgende Beispiel zeigt, was Sie in das System eingeben müssen, um die Dateien auf Ihren Server zu kopieren und anschließend zu überprüfen, ob das Konsolensystem die Datei herunterladen kann.

Kopieren der Setup-Datei auf einen TFTP-Server:

```
Beispiel: tftpd-hpa
Standardmäßiges TFTP-Stammverzeichnis /var/lib/tftpboot
~$ sudo cp zerotouch.setup /var/lib/tftpboot
```

B.4 Abrufen der Setup-Datei

Nach dem Abruf der IP-Adressen für das Konsolensystem und den TFTP- bzw. -Server, auf den die Setup-Datei hochgeladen wurde, wird im Rahmen der interaktionslosen Bereitstellung versucht, die Setup-Datei herunterzuladen. Wenn das Konsolensystem die Setup-Datei heruntergeladen hat, verwendet es die in der Datei enthaltenen Informationen, um das Image abzurufen und/oder die Konfiguration des Konsolensystem durchzuführen.

B.5 Konfiguration eines DHCP-Servers

Beim Start fordert das Konsolensystem möglicherweise die Zuweisung einer IP-Adresse an. Während dieses Vorgangs fragt der DHCP-Server vom DNS-Server den Standort des TFTP- oder HTTP-Servers ab, auf dem sich die Setup-Datei befindet. Administratoren können wahlweise auf dem DHCP-Server einen Eintrag erstellen, der ein bestimmtes Konsolensystem oder einen Konsolensystem-Bereich eindeutig identifiziert. Dieser Eintrag dient bei der Bereitstellung des Konsolensystems als Filter.

Der Administrator muss zwei Optionen konfigurieren. Option 66 definiert den Hostnamen oder die IP-Adresse des TFTP-Servers, auf dem sich die Setup-Datei befindet. Option 67 definiert den Namen der Setup-Datei (zum Beispiel acszero.cfg).

So konfigurieren Sie die Optionen 66 und 67:

1. Verwenden Sie den Windows Server Manager oder das DHCP-Snap-In in der Microsoft Management Console (MMC), um die DHCP-Serverkonsole zu öffnen.
2. Klicken Sie im linken Bereich des DHCP-Server-Fensters auf *IPv4*.
3. Klicken Sie mit der rechten Maustaste auf *Server Options* (Serveroptionen) und klicken Sie dann auf *Configure Options* (Optionen konfigurieren), um einen globalen Bereich zu konfigurieren.

   – oder –

   Klicken Sie mit der rechten Maustaste auf *Scope Options* (Bereichsoptionen) und klicken Sie dann auf *Configure Options* (Optionen konfigurieren), um einen einzelnen Bereich zu konfigurieren.
4. Klicken Sie auf die Option *066*, um den Standort des Servers einzugeben, der als Host für die Setup-Datei dient.
5. Geben Sie den Hostnamen des TFTP-Servers ein.
6. Klicken Sie auf die Option *067*, um den Namen der Setup-Datei einzugeben.

Administratoren können mithilfe von zwei weiteren DHCP-Optionen einen Filter für die interaktionslose Bereitstellung ausgewählter Konsolensysteme definieren. Option 60 definiert die Herstellerklasse, Avocent_ACS800/8000<Seriennummer des Konsolensystems>. Option 61 definiert die MAC-Adresse des Konsolensystems.

So richten Sie die Optionen 60 und 61 ein (optional):

1. Verwenden Sie den Windows Server Manager oder das DHCP-Snap-In in der MMC, um die DHCP-Serverkonsole zu öffnen.
2. Klicken Sie im linken Bereich des DHCP-Fensters auf *IPv4*.
3. Klicken Sie in der Registerkartenleiste auf *Action* (Aktion) und dann im Pulldown-Menü auf *Set Predefined Options* (Vordefinierte Optionen einstellen).
4. Wählen Sie unter der Optionenklasse *DHCP Standard Options* (DHCP-Standardoptionen) und klicken Sie dann auf *Add* (Hinzufügen).
5. Geben Sie einen Namen für die Option in das Feld „Name“ ein, wählen Sie im Dropdown-Menü „Data type“ (Datentyp) den Eintrag *String* (Zeichenfolge) aus, geben Sie 060 in das Feld „Code“ ein und geben Sie eine Beschreibung für die Option ein. Klicken Sie auf *OK*.
6. Wiederholen Sie Schritt 5 und geben Sie dabei 061 in das Feld „Code“ ein.

DNS-Server

Wenn die Option für den DNS-Bereich noch nicht auf Ihrem DHCP-Server konfiguriert ist und wenn es sich bei dem Eintrag für Option 66 um einen Hostnamen anstelle einer IP-Adresse handelt, können Sie den DNS-Server konfigurieren.

So konfigurieren Sie den DNS-Server:

1. Verwenden Sie den Windows Server Manager oder das DHCP-Snap-In in der MMC, um die DHCP-Serverkonsole zu öffnen.
2. Klicken Sie im linken Bereich des DHCP-Fensters auf *IPv4*.
3. Klicken Sie mit der rechten Maustaste auf *Server Options* (Serveroptionen) und klicken Sie dann auf *Configure Options* (Optionen konfigurieren).
4. Klicken Sie auf Option *006*, um die DNS-Server zu definieren.
5. Geben Sie die IP-Adresse in das vorgesehene Feld ein und klicken Sie auf *Add* (Hinzufügen).

HINWEIS: Wenn Sie den Servernamen eingeben, wird er vom DNS-Server aufgelöst.

Reservierungen

Sie können IP-Adressen für jedes zu aktualisierende Konsolensystem reservieren. Eine Reservierung ist eine IP-Adresse, die immer für ein bestimmtes Konsolensystem vergeben wird, wenn es das DHCP-Lease verlängert.

So reservieren Sie eine IP-Adresse:

1. Verwenden Sie den Windows Server Manager oder das DHCP-Snap-In in der Microsoft Management Console (MMC), um die DHCP-Serverkonsole zu öffnen.
2. Klicken Sie im linken Bereich des DHCP-Fensters auf *IPv4*.
3. Klicken Sie mit der rechten Maustaste auf *Reservations* (Reservierungen) und klicken Sie dann auf *New Reservation* (Neue Reservierung).

4. Geben Sie die folgenden Einzelheiten in die vorgesehenen Felder ein: einen Namen für die Reservierung, die IP-Adresse, die dem Konsolensystem zugewiesen werden soll, die MAC-Adresse für das Konsolensystem und eine Beschreibung.

HINWEIS: Sie finden die MAC-Adresse des Konsolensystems unten auf dem Konsolensystem.

5. Wählen Sie unter „Supported types“ (Unterstützte Typen) über das Optionsfeld entweder „Both“ (Beide) oder nur „DHCP“ aus.
6. Klicken Sie auf *Add* (Hinzufügen). Die reservierte IP-Adresse wird in der Reservierungstabelle angezeigt.

Im Folgenden finden Sie ein Beispiel für die Konfiguration eines Linux DHCP-Servers.

```
Beispiel: ISC DHCP Server für Linux
Bearbeiten: /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 Aktivieren der interaktionslosen Bereitstellung

Administratoren können die interaktionslose Bereitstellung über die Weboberfläche oder das CLI aktivieren. Sobald die interaktionslose Bereitstellung aktiviert ist, müssen Sie den Inhalt des interaktionslosen Bereitstellungsprotokolls löschen.

So aktivieren Sie die interaktionslose Bereitstellung über die Weboberfläche:

1. Klicken Sie in der Seitenleiste der Weboberfläche auf *System – Sicherheit – Sicherheitsprofil*.
2. Aktivieren Sie unter „Abruf der BOOTP-Konfiguration“ die Kontrollkästchen für den Abruf der BOOTP-Konfiguration und den Live-Konfigurationsabruf.
3. Wählen Sie *eth0* als BOOTP-Schnittstelle im Dropdown-Menü aus.
4. Klicken Sie auf *Speichern*.
5. Klicken Sie in der Seitenleiste der Weboberfläche auf *Überwachung – Interaktionsloses Protokoll* und klicken Sie dann auf *Protokollinhalt löschen*.

So aktivieren Sie die interaktionslose Bereitstellung über das CLI:

1. Melden Sie sich als **Stammbenutzer (root)** beim Konsolensystem an.
2. Geben Sie **cd system/security/security_profile/** ein, um zur Sicherheitsprofilebene zu navigieren.
3. Geben Sie set **bootp_enabled=yes**. ein und drücken Sie dann die **Eingabetaste**.
4. Geben Sie set **bootp_interface=eth0**. ein und drücken Sie dann die **Eingabetaste**.
5. Geben Sie set **enable_live_configuration_retrieval_(any_time_dhcp_renews)=yes** ein und drücken Sie dann die **Eingabetaste**.
6. Geben Sie **commit** ein, um die Konfiguration zu speichern.
7. Geben Sie **cd /monitoring/zero-touch_log/** ein, um zur Ebene des interaktionslosen Protokolls zu navigieren.

8. Geben Sie **clear_log** ein. Geben Sie bei entsprechender Aufforderung **Yes** ein, um das interaktionslose Bereitstellungsprotokoll zu löschen.

Anhang C: Abruf der BOOTP-Konfiguration

Sie können festlegen, dass das Konsolensystem beim Start oder bei der Verlängerung der IP-Adresse neu konfiguriert wird.

So generieren Sie die abzurufende Konfiguration:

1. Klicken Sie auf *Systemtools – Konfiguration speichern* und speichern Sie die Konfiguration lokal oder auf einer FTP-Site.

   – oder –

   Rufen Sie mit dem Befehl „list_configuration“ die CLI-Vorlagenskripts ab, bearbeiten Sie die Konfiguration des Konsolensystems und speichern Sie sie als Textdatei.

   – oder –

   Bearbeiten Sie eine Datei mit CLI-Befehlen und speichern Sie die Datei.

2. Übertragen Sie die gespeicherte Datei an einen DHCP-Server.
3. Konfigurieren Sie den DHCP-Server so, dass die Konfigurationsdatei an das Konsolensystem übertragen wird.

So können Sie ein Konsolensystem mit BOOTP neu konfigurieren:

1. Klicken Sie auf *System – Sicherheit – Sicherheitsprofil*. Stellen Sie unter „Abruf der BOOTP-Konfiguration“ sicher, dass das Kontrollkästchen *Aktiviert* ausgewählt ist.
2. Deaktivieren Sie das Kontrollkästchen *Live-Konfigurationsabruf aktivieren (bei jeder DHCP-Verlängerung)*. Die gespeicherte Konfiguration wird beim nächsten Neustart abgerufen und angewendet.

   – oder –

   Stellen Sie sicher, dass das Kontrollkästchen *Live-Konfigurationsabruf aktivieren (bei jeder DHCP-Verlängerung)* aktiviert ist. Die gespeicherte Konfiguration wird bei der nächsten Verlängerung der IP-Adresse abgerufen und angewendet.

HINWEIS: Sie müssen den DHCP-Server konfigurieren, damit die Konfigurationsdatei an das Konsolensystem übertragen wird.

Anhang D: Wiederherstellen des Kennworts für ein Konsolensystem

1. Stellen Sie eine direkte Verbindung mit dem KONSOLEN-Port des Konsolensystems her.
2. Schalten Sie das Konsolensystem aus und dann wieder ein.
3. Drücken Sie die **Leertaste**, um auf die uboot-Eingabeaufforderung zuzugreifen.
4. Geben Sie **hw_boot single** ein und drücken Sie die **Eingabetaste**.
5. Das Konsolensystem wird im Einzelbenutzer-Modus gestartet. Geben Sie **passwd** ein und drücken Sie die **Eingabetaste**.
6. Geben Sie das neue Kennwort ein und bestätigen Sie es.
7. Geben Sie **reboot** ein und lassen Sie das Konsolensystem einen normalen Startvorgang ausführen.

Anhang E: SSH-Einrichtung mit zulässiger RSA Keypair-Authentifizierung anstatt über einen Benutzernamen und ein Kennwort

So richten Sie ein Client-Linux-System ein, um auf das ACS800/8000 Advanced Console System zuzugreifen:

1. Erstellen Sie einen neuen Admin-Benutzer auf dem Konsolensystem. Zum Beispiel: acsadmin.
2. Fügen Sie den neuen Benutzer zu den Gruppen „admin“ und „shell-login-profile“ hinzu.
3. Erzeugen Sie auf Ihrem Linux-Client-System ein Schlüsselpaar für den ssh-Zugriff auf Ihr Konsolensystem.

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

4. Drücken Sie zweimal die Eingabetaste, um für dieses Schlüsselpaar auf Ihrem Server keine Passphrase zu installieren.

   – oder –

   Geben Sie eine Passphrase ein.

HINWEIS: Hinweis: Diese beiden Dateien werden durch das obige ssh-keygen erstellt:

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

5. Fügen Sie auf Ihrem Linux-Client-System Zeilen wie im folgenden Beispiel zu Ihrer Datei $HOME/.ssh/config hinzu:

```
Host acsadmin132
HostName <IP-Adresse des Konsolensystems>, zum Beispiel 10.207.24.132
Benutzer acsadmin
IdentityFile ~/.ssh/acsadmin-id_rsa
```

6. Melden Sie sich über SSH als Benutzer acsadmin (der neue Benutzer) beim Konsolensystem an.
7. Verwenden Sie die vier folgenden Befehle, um den öffentlichen Schlüssel für das acsadmin-Konto auf dem Konsolensystem zu installieren.

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

Zum Beispiel für den ssh-Befehl

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

8. Wählen Sie auf der Registerkarte *System - Sicherheit - Sicherheitsprofil* der Weboberfläche das Kontrollkästchen ab, um *SSH-Authentifizierung über einen Benutzernamen und ein Kennwort* zu deaktivieren. Die nächste SSH-Anmeldung von Ihrem Linux-Client-System beim Konsolensystem gelingt mit dem Schlüsselpaar und Sie werden nicht nach einem Kennwort gefragt.

HINWEIS: Die Deaktivierung dieser Funktion verhindert, dass sich ein Benutzer, der weder auf dem Client noch auf dem Konsolensystem ein Schlüsselpaar eingerichtet hat, über SSH beim Konsolensystem anmelden kann. Sie werden auch nicht in der Lage sein, serielle Sitzungen von der Weboberfläche aus zu starten, da diese eine Authentifizierung per Benutzername/Kennwort erfordern.

Ein Beispiel für einen ssh-Anmeldebefehl unter Verwendung des Host-Eintrags given.ssh/config lautet: ssh acsadmin@acsadmin132.

Anhang F: Portinformationen für die Kommunikation mit der DSView-Software

Die folgenden Ports eines Avocent® ACS800/8000 Advanced Console Systems können Verbindungen von der DSView-Managementsoftware akzeptieren:

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

Die folgenden Ports der DSView-Software können Verbindungen vom Konsolensystem akzeptieren:

- TCP-Port 4122 (Standard: SSH-Server)
- TCP-Port 4514 (Standard: Datenprotokollierung oder Syslog-Server)

Anhang G: Zugriff auf ein Konsolensystem mit einer DSView-Softwareinstallation per DFÜ

Wenn ein Benutzer der DSView-Software eine serielle Sitzung einleitet, treten die folgenden Ereignisse auf:

- Der Benutzer wählt den seriellen Port aus, auf den zugegriffen werden soll.
- Ein Viewer wird vom DSView-Server auf die Workstation des Benutzers heruntergeladen.
- Die DSView-Software übergibt verschiedene Informationen an den Viewer, darunter einen Autorisierungsschlüssel sowie die IP-Adresse und den seriellen Port des Konsolensystems.
- Der Viewer greift dann über eine SSH-Sitzung auf den seriellen Port des Konsolensystems zu, indem er den vom DSView-Server empfangenen Autorisierungsschlüssel übergibt.
- Die serielle Sitzung beginnt.

Zur Gewährleistung einer unterbrechungsfreien Konnektivität kann der DSView-Server mit Out-of-Band-Zugriff konfiguriert werden, der es ihm ermöglicht, ein Konsolensystem über ein Modem zu erreichen, falls das Netzwerk oder das Internet nicht verfügbar ist.

G.1 Installation der DSView-Software mit Out-of-Band-Zugriff

Der DSView-Server muss auf Hardware ausgeführt werden, an die ein Modem angeschlossen ist. Das Konsolensystem muss über ein integriertes Modem verfügen oder über einen USB-Anschluss oder einen seriellen Port Zugriff auf ein Modem haben.

Für diese Installation muss der DSView-Server die zentrale Empfangsstelle für die Pakete sein, die den heruntergeladenen Viewer und das Konsolensystem verlassen. Um dies zu gewährleisten, muss der Proxy-Modus in der DSView-Software konfiguriert werden. Der Viewer richtet sich dann zum Herstellen der SSH-Verbindung an den DSView-Server (nicht an das Konsolensystem). Der DSView-Server bestimmt dann die Route der Pakete, indem er sowohl die Quell-IP-Adresse als auch die Ziel-IP-Adresse ändert, wobei er als Kommunikationsvermittler dient.

Unter normalen Betriebsbedingungen werden Pakete, die vom seriellen Viewer empfangen werden, per Ethernet über den DSView-Server geleitet. In einem Fehlerzustand erkennt der DSView-Server, dass der normale Kommunikationsweg zum Konsolensystem unterbrochen ist. Er wählt zum Konsolensystem hinaus, durchläuft die Authentifizierung und stellt eine PPP-Verbindung her. Pakete, die normalerweise über Ethernet übertragen werden, werden stattdessen über PPP geleitet.

Aufgrund des Unterschieds zwischen der Ethernet- und der DFÜ-Geschwindigkeit fällt die Leistung dabei merklich schlechter aus. Verbindungen mit mehreren Benutzern beeinträchtigen die Leistung zusätzlich und werden daher nicht empfohlen. Das DFÜ-Verfahren sollte deshalb nur als Notfallmechanismus verwendet werden.

G.2 DFÜ-Konfiguration für ein Konsolensystem

So konfigurieren Sie in der DSView-Software eine DFÜ-Verbindung für ein Konsolensystem:

1. Wählen Sie in einem Einheiten-Fenster das ACS Konsolensystem aus, das Sie konfigurieren möchten. Für die Einwahl mit Rückruf müssen Sie zunächst auf der Registerkarte „System“ die Optionen *DSView-Server – Eigenschaften – DSView-Modemsitzungen* auswählen und dann die Telefonnummer, die dem DSView-Server zugewiesen ist, in das Feld für die Analogtelefonnummer eingeben.
2. Wählen Sie *DSView-Einstellungen – DFÜ* aus und klicken Sie auf *DFÜ aktivieren*.
3. Wählen Sie *Modemtyp – Analog* aus.
4. Geben Sie die Telefonnummer für das Konsolensystem ein.
5. Geben Sie den PPP-Benutzer in das vorgesehene Feld ein und wählen Sie das PPP-Authentifizierungsprotokoll aus.
6. Aktivieren Sie für die Einwahl mit Rückruf das Kontrollkästchen für die Rückwahl.
7. Wählen Sie *DSView-Einstellungen – DFÜ – PPP-Kennwort*, geben Sie das Kennwort für den Zugriff auf das ACS 800/8000 Konsolensystem ein und wiederholen Sie die Kennworteingabe zur Bestätigung.
8. Wählen Sie *DSView-Einstellungen – DFÜ – IP-Adressen*.
9. Klicken Sie auf *Automatisch generieren*, wenn die IP-Adresse automatisch festgelegt werden soll, oder geben Sie die lokale PPP-IP-Adresse und die IP-Adresse der Einheit manuell ein.
10. Wählen Sie DSView-Einstellungen – DFÜ aus und klicken Sie auf Speichern.
11. So konfigurieren Sie das Konsolensystem in der DSView-Software so, dass es die DFÜ-Verbindung empfängt:
12. Wählen Sie in einem Einheiten-Fenster das ACS Konsolensystem aus, das Sie konfigurieren möchten.
13. Für das interne Modem wählen Sie *Ports – Aux-Ports* und dann das Modem aus.
14. Wählen Sie DSView-Einstellungen – DFÜ und klicken Sie dann auf *Konfiguration per Push übertragen*.

HINWEIS: Der folgende Schritt ist nur erforderlich, wenn in den DFÜ-Einstellungen der DSView-Software die Option *CHAP* im Feld „PPP-Authentifizierungsprotokoll“ ausgewählt wurde.

15. Melden Sie sich bei der CLI des Konsolensystems an und greifen Sie auf die Linux-Shell zu. Bearbeiten Sie den Abschnitt /etc/ppp/chap-secrets und fügen Sie eine Zeile hinzu, wobei die erste Spalte den PPP-Benutzer und die dritte Spalte das PPP-Kennwort enthält, wie im folgenden Beispiel gezeigt:

    pppuser * "ppppassword" *

Anhang H: Internes Modem

Einige Modelle des Konsolensystems sind mit einem internen Modem ausgestattet. Dieses Modem wird verwendet, um Telefonanrufe einzuleiten und anzunehmen und um die Kommunikation mit anderen Modems herzustellen, damit Daten übertragen werden können.

Die Modem-Funktionen werden mithilfe von AT-Befehlen gesteuert. Mit diesen Befehlen wird das Modem angewiesen, bestimmte Funktionen auszuführen, wie beispielsweise Wählen einer Nummer oder Annehmen von Anrufen. Normalerweise werden die Befehle automatisch von der Kommunikationssoftware ausgegeben. Für einige Anwendungen muss jedoch möglicherweise spezielle Software entwickelt werden, da kein normales Betriebssystem vorhanden ist.

Das Modem akzeptiert und verarbeitet AT-Befehle automatisch bei den meisten standardmäßigen DTE-Geschwindigkeiten (DTE = Data Terminal Equipment, Datenendeinrichtung) und Paritätseinstellungen. Auf jeden ausgegebenen Befehl antwortet das Modem mit einem Ergebniscode, der Ihnen den Status des Modems mitteilt. Das Format eines einfachen AT-Befehls und Ergebniscodes wird unten gezeigt:

AT<Befehl><CR>

OK

AT = Attention (Achtung)

<Befehl> = ein gültiger Befehl

<CR> = Carriage Return (Zeilenschalter) oder Eingabetaste

OK = Ergebniscode

Tabelle H.1 Beispiel für eine Befehlszeichenfolge

Befehl	Beschreibung
ATDT7678900<CR>	Weist das Modem an, die Nummer 7678900 zu wählen und zu versuchen, eine Verbindung mit dem Remote-Gerät herzustellen.
ATS0=2<CR>	Aktiviert die Option „Automatische Antwort“. Wenn das Modem einen Klingelton erkennt, versucht es, den Anruf nach zwei Klingeltönen anzunehmen.

Tabelle H.2 Grundlegende AT-Befehle

Befehl	Beschreibung
ATA/	Wiederholt den zuletzt ausgeführten Befehl.
ATA	Antworten.
ATB0	CCITT-Vorgang mit 300 oder 1200 bit/s.
ATB1	Bell-Vorgang bei 300 oder 1200 bit/s (Standard).
ATD	Wählen.
ATD0-9	Wählen der DTMF-Ziffern 0 bis 9.
ATDA-D	Wählen der DTMF-Zeichen A, B, C und D.
ATDP	Auswahl des Impulswahlverfahrens; wirkt sich auf den aktuellen Wählvorgang und auf nachfolgende Wählvorgänge aus.
ATDT	Auswahl des Tonwahlverfahrens; wirkt sich auf den aktuellen Wählvorgang und auf nachfolgende Wählvorgänge aus.
ATD!	Flash: Wechselt nach der von S29 definierten Zeit in den Status „Frei“ (aufgelegt).
ATDW	Wartet vor dem Wählen einer Nummer auf Erkennung des Wähltons. Wenn innerhalb der von S7 angegebenen Zeit kein Wählton erkannt wird, bricht das Modem den Rest der Sequenz ab, wechselt in den Status „Frei“ und generiert eine Fehlermeldung.
ATD@	Wartet fünf Sekunden Stille ab, bevor mit der nächsten Wählzeichenfolge fortgefahren und dann die Handshake-Sequenz abgeschlossen wird.
ATD,	Pause. Das Modem legt eine Pause ein, bevor es die Nummer wählt. Die Länge der Pause wird von S8 festgelegt. Wird meist verwendet, wenn über eine private Telefonanlage eine externe Leitung angewählt wird.
ATD;	Kehrt nach dem Ausführen des Befehls zum Befehlsmodus zurück.
ATE0	Deaktiviert das Befehlsecho.
ATE1	Aktiviert das Befehlsecho (Standard).
ATH0	Auflegen.
ATH1	Zwingt das Modem zum Abheben (Wechsel in den Status „Besetzt“).
ATI0	Meldet den Produktcode.
ATI2	Meldet OK (für die Softwarekompatibilität).
ATI3	Meldet die Firmware-Version des Modems. Zum Beispiel: CX810801-V90.
ATL0	Schaltet den Lautsprecher stumm.
ATL1	Stellt den Lautsprecher auf niedrige Lautstärke ein (Standard).
ATL2	Stellt den Lautsprecher auf mittlere Lautstärke ein.
ATL3	Stellt den Lautsprecher auf hohe Lautstärke ein.
ATM0	Der Lautsprecher ist immer ausgeschaltet.
ATM1	Der Lautsprecher ist beim Verbinden des Anrufs eingeschaltet, wird aber ausgeschaltet, wenn das Trägersignal erkannt wird (Standard).
ATM2	Der Lautsprecher ist immer eingeschaltet.
ATM3	Der Lautsprecher ist beim Wählen und beim Empfang des Trägersignals ausgeschaltet, aber beim Antworten eingeschaltet.
ATQ0	Aktiviert Ergebniscodes an die Datenendeinrichtung (DTE) (Standard).
ATQ1	Deaktiviert Ergebniscodes an die Datenendeinrichtung (DTE).
ATSr	Legt das S-Register „r“ als Standardregister fest.
ATSr=n	Stellt das S-Register „r“ auf den Wert „n“ ein.

Tabelle H.2 Grundlegende AT-Befehle (Fortsetzung)

Befehl	Beschreibung
ATSr?	Meldet den Wert des S-Registers „r“.
ATV0	Aktiviert Ergebniscodes in Kurzform.
ATV1	Aktiviert Ergebniscodes in Langform.
ATW0	Beim Herstellen der Verbindung meldet das Modem nur die DTE-Geschwindigkeit (zum Beispiel CONNECT 9600). Weitere Antworten sind deaktiviert (Standard).
ATW1	Beim Herstellen der Verbindung meldet das Modem die Modulationsart, die Leitungsgeschwindigkeit, das Fehlerkorrekturprotokoll und die DTE-Geschwindigkeit. Weitere Antworten sind deaktiviert.
ATW2	Beim Herstellen der Verbindung meldet das Modem die DCE-Geschwindigkeit (zum Beispiel CONNECT 2400). Weitere Antworten sind deaktiviert.
ATX0	Wähl- und Besetztton werden ignoriert. Sendet eine CONNECT-Meldung, wenn eine Verbindung durch Wählen ohne Wähltonerkennung hergestellt wird.
ATX1	Deaktiviert die Überwachung von Besetzttönen. Sendet nur die Meldungen OK, CONNECT, RING, NO CARRIER und ERROR. Wenn die Erkennung des Besetzttons erzwungen wird und der Besetztton erkannt wird, wird NO CARRIER anstelle von BUSY gemeldet. Wenn die Erkennung des Wähltons erzwungen wird oder ausgewählt ist, aber kein Wählton erkannt wird, wird NO CARRIER anstelle von NO DIALTONE gemeldet.
ATX2	Deaktiviert die Überwachung von Besetzttönen. Sendet nur OK, CONNECT, RING, NO CARRIER, ERROR, NO DIALTONE und CONNECT XXXX. Wenn die Erkennung des Besetzttons erzwungen wird und der Besetztton erkannt wird, wird NO CARRIER anstelle von BUSY gemeldet. Wenn die Erkennung des Wähltons erzwungen wird oder ausgewählt ist, aber kein Wählton erkannt wird, wird NO CARRIER anstelle von NO DIALTONE gemeldet.
ATX3	Aktiviert die Überwachung von Besetzttönen. Sendet nur OK, CONNECT, RING, NO CARRIER, ERROR, NO DIALTONE und CONNECT oder CARRIER XXXX. Wenn die Erkennung des Wähltons erzwungen wird, aber kein Wählton erkannt wird, wird NO CARRIER gemeldet.
ATX4	Aktiviert die Überwachung von Besetzttönen. Sendet alle Meldungen (Standard).
ATZ0	Warmstart.
AT&C0	DCD bleibt immer eingeschaltet.
AT&C1	DCD folgt dem Status des Trägersignals (Standard).
AT&D0	DTR wird ignoriert.
AT&D1	Wechselt in den Escape-Modus, wenn ein Übergang von EIN zu AUS für DTR erkannt wird.
AT&D2	Wechselt in den Status „Frei“ (Auflegen), nimmt den Befehlsstatus an und deaktiviert die Option „Automatische Antwort“, wenn ein Übergang von EIN zu AUS für DTR erkannt wird (Standard).
AT&D3	Bei einem Übergang von EIN zu AUS führt das Modem einen Warmstart aus. Dies entspricht der Ausgabe eines ATZ-Befehls.
AT&F	Stellt die werkseitige Konfiguration wieder her.
AT&G0	Deaktiviert den Schutzton (Standard).
AT&G1	Aktiviert den 550-Hz-Schutzton.
AT&G2	Aktiviert den 1800-Hz-Schutzton.
AT&K0	Deaktiviert die Flusssteuerung.
AT&K3	Aktiviert die RTS/CTS-Flusssteuerung (Standard für Datenmodi).
AT&K4	Aktiviert die XON/XOFF-Flusssteuerung.
AT&K5	Unterstützt die transparente XON/XOFF-Flusssteuerung.
AT&P0	Verhältnis Öffnen/Schließen von 39/61 bei 10 Impulsen pro Sekunde (Standard).
AT&P1	Verhältnis Öffnen/Schließen von 33/67 bei 10 Impulsen pro Sekunde.

Tabelle H.2 Grundlegende AT-Befehle (Fortsetzung)

Befehl	Beschreibung
AT&P2	Verhältnis Öffnen/Schließen von 39/61 bei 20 Impulsen pro Sekunde.
AT&P3	Verhältnis Öffnen/Schließen von 33/67 bei 20 Impulsen pro Sekunde.
AT&Q0	Wählt den direkten synchronen Betrieb aus.
AT&Q5	Das Modem versucht, eine Verbindung mit Fehlerkorrektur herzustellen.
AT&Q6	Wählt den asynchronen Betrieb im Normalmodus aus (ermöglicht die Geschwindigkeitspufferung und die Flusssteuerung, aber keine Fehlerkorrektur).
AT&V	Zeigt die aktuelle Konfiguration des Modems an. Bei Eingabe dieses Befehls zeigt das Modem den aktuellen Befehl und die geltenden Registereinstellungen an.
AT%C0	Deaktiviert die Datenkomprimierung.
AT%C1	Aktiviert die MNP 5-Datenkomprimierung.
AT%C2	Aktiviert die V.42bis-Datenkomprimierung (stellt S46 Bit 1 ein).
AT%C3	Aktiviert die V.42bis- und MNP 5-Datenkomprimierung (Standard).
AT%E0	Deaktiviert die Überwachung der Leitungsqualität und die Auto-Retrain-Funktion zur Neukonfiguration.
AT%E1	Aktiviert die Überwachung der Leitungsqualität und die Auto-Retrain-Funktion zur Neukonfiguration.
AT%E2	Aktiviert die Überwachung der Leitungsqualität und die Fallback/Fall-Forward-Funktion zur Geschwindigkeitsanpassung (Standard).
AT%L	Signalpegel der Leitung. Gibt einen Wert zurück, der den Pegel des empfangenen Signals angibt. Zum Beispiel: 009 = -9 dBm.
AT%Q	Signalqualität der Leitung. Meldet die Signalqualität der Leitung (DAA-abhängig). Gibt das Byte der höheren Ordnung des EQM-Werts zurück. Je nach dem EQM-Wert werden die Retrain- oder Fallback/Fall-Forward-Funktionen eingeleitet, sofern sie über die Befehle AT%E1 bzw. AT%E2 aktiviert wurden.
AT+MS	Modulation auswählen/erzwingen.

H.1 AT+MS-Modulationsauswahl

Dieser zusammengesetzte Parameter im erweiterten Format steuert die Betriebsart der Modulationsfähigkeiten des Modems. Er akzeptiert sechs Unterparameter:

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

Zum Ablesen der aktuellen Einstellungen geben Sie AT+MS?<CR> ein.

Tabelle H.3 Unterstützte Geschwindigkeiten beim +MS-Befehl

Modulation	Trägersignal	Beschreibung
Bell 103	B103	300
Bell 212	B212	1200
V.21	V21	300
V.22	V22	1200
V.22 bis	V22	2400 oder 1200
V.23	V23C	1200rx/75tx oder 75rx/1200tx
V.32	V32	9600 oder 4800
V.32 bis	V32B	14400, 12000, 9600, 7200 oder 4800
V.34	V34	33600, 31200, 28800, 26400, 19200, 16800, 14400, 12000, 9600, 7200, 4800 oder 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 Festlegen der Option für Nebenstellen

Dieser Befehl aktiviert oder deaktiviert die Optionen „Leitung besetzt“ und „Nebenstelle abnehmen“.

Tabelle H.4 Festlegen der Optionen für Nebenstellen

Wert für -STE=n	Nebenstelle abnehmen	Leitung besetzt
0 (Standard)	Deaktiviert	Deaktiviert
1	Deaktiviert	Aktiviert
2	Aktiviert	Deaktiviert
3	Aktiviert	Aktiviert

Wenn die Leitung belegt ist und das Modem einen ATDT-Befehl zum Hinauswählen empfängt, wechselt das Modem nicht in den Status „Besetzt“ und zeigt den Ergebniscode „LINE-IN-USE“ an. Wenn sich das Modem im Status „Besetzt“ befindet und die Nebenstelle abgenommen wird, unterbricht das Modem die Verbindung und zeigt den Ergebniscode „OFF-HOOK INTRUSION“ an.

H.3 AT S-Register

Die S-Register verwenden das folgende Format: ATSr = n<CR>. Dabei ist „r“ die Nummer des S-Registers und „n“ der Parameter, auf den es eingestellt wird. Zum Lesen des aktuellen Inhalts eines S-Registers geben Sie den Befehl ATSr?<CR> ein, wobei „r“ das jeweilige Register ist. Das Modem zeigt dann den Wert des S-Registers an.

Tabelle H.5 AT S-Register

Register	Bereich	Einheiten	Standard	Beschreibung
S0	0-255	Klingeltöne	0	Anzahl der Klingeltöne bis Rufannahme. ATS0=1<CR> bedeutet, dass der Anruf beim ersten erkannten Klingelton angenommen wird.
S1	0-255	Klingeltöne	0	Anzahl der gezählten Klingeltöne.
S2	0-127	ASCII	43	Code des Escape-Zeichens.
S3	0-127	ASCII	13	Abbruch-Zeichen für Befehlsmodus <CR>.
S4	0-127	ASCII	10	Zeichen für Zeilenvorschub.
S5	0-127	ASCII	8	Zeichen für Rücktaste.
S6	2-255	Sekunden	2	Wartezeit für Erkennung des Wähltons.
S7	1-255	Sekunden	50	Wartezeit für Trägersignal.
S8	0-255	Sekunden	2	Wartezeit für Komma in der Wählzeichenfolge.
S10	1-255	0,1 s	14	Zeit zwischen Verlust des Trägersignals und Verbindungsende.
S11	50-255	0,01 s	85	Tondauer bei Tonwahl.
S12	0-127	1/50 s	50	Schutzzeit für Escape-Code.
S24	0-255	1 s	0	Inaktivitäts-Timer für Ruhemodus.
S29	0-255	10 ms	70	Zeit für Hook Flash-Modifikator.
S30	0-255	10 s	0	Timer zum Trennen bei Inaktivität.
S95			0	Ergebniscode-Steuerung.

H.4 Grundlegende Modem-Ergebniscodes

Als Antwort auf die Verarbeitung eines AT-Befehls gibt das Modem verschiedene Codes aus. Über den Vn-Befehl können Ergebniscodes entweder als Wort (V1) oder im numerischen Format (V0) angezeigt werden. Der Qn-Befehl steuert, ob Ergebniscodes ausgegeben werden (Q0) oder nicht ausgegeben werden (Q1). Die Xn- und Wn-Befehle sowie das S95-Register bestimmen, in welchem Ergebniscode-Format das Modem den Typ der hergestellten Verbindung anzeigt. Es gibt mehr als 300 Codes. Die am häufigsten verwendeten Codes werden in der folgenden Tabelle aufgelistet.

Tabelle H.6 Liste grundlegender Ergebniscodes

Numerisch	Wortform	Beschreibung
0	OK	Das Modem hat den Befehl empfangen und bestätigt.
1	CONNECT	Verbindung mit 300 bit/s hergestellt oder erweiterte Ergebniscodes sind deaktiviert (X0).
2	RING	Der Klingelton eines eingehenden Anrufs wurde erkannt.
3	NO CARRIER	Dieser Ergebniscode weist entweder auf ein beabsichtigtes Trennen oder auf einen Fehler beim Herstellen der Verbindung hin.
4	ERROR	Ein ungültiger Befehl wurde an das Modem ausgegeben.
5	CONNECT 1200	Geschwindigkeit der Leitung oder der DTE-Verbindung beträgt 1200 bit/s.
6	NO DIALTONE	
7	BUSY	Das Modem hat ein Besetztzeichen erkannt.
8	NO ANSWER	Der Remote-Server hat nach Ablauf der S7-Zeit nicht geantwortet.
10	CONNECT 2400	Geschwindigkeit der Leitung oder der DTE-Verbindung beträgt 2400 bit/s.
12	CONNECT 9600	Geschwindigkeit der Leitung oder der DTE-Verbindung beträgt 9600 bit/s.
15	CONNECT 14400	Geschwindigkeit der Leitung oder der DTE-Verbindung beträgt 14400 bit/s.
16	CONNECT 19200	Geschwindigkeit der Leitung oder der DTE-Verbindung beträgt 19200 bit/s.
17	CONNECT 38400	Geschwindigkeit der Leitung oder der DTE-Verbindung beträgt 38400 bit/s.
18	CONNECT 57600	Geschwindigkeit der Leitung oder der DTE-Verbindung beträgt 57600 bit/s.

H.5 Digitaler Leitungsschutz

Das Modem verfügt über einen optionalen digitalen Leitungsschutz-Stromkreis, der automatisch Überstrom auf den T- und R-Pins erkennt. Wenn das Modem in den Status „Besetzt“ wechselt, überprüft es sofort den Strom an den T- und R-Pins. Wenn der Strom 150 mA überschreitet, zeigt das Modem den Ergebniscode „DIGITAL LINE DETECTED“ (DIGITALE LEITUNG ERKANNT) an und wechselt dann wieder in den Status „Frei“. Das Modem zeigt diesen Ergebniscode so lange an, bis im Status „Besetzt“ wieder Normalstrom auf den T- und R-Pins erkannt wird. Der digitale Leitungsschutz schützt das Modem, falls es versehentlich an eine digitale Telefonleitung angeschlossen wird.

H.6 Ruhemodus

Das Modem kann über die Einstellung ATS24=n in den Ruhemodus mit geringem Stromverbrauch versetzt werden. Dabei gibt „n“ in Sekunden an, wie lange das Modem im Normalmodus bleibt, wenn keine Aktivität auf der Telefonleitung oder DTE-Leitung erkannt wird, bevor es in den Ruhemodus mit geringem Stromverbrauch wechselt. Der Timer wird zurückgesetzt, wenn eine Aktivität auf der DTE- oder Telefonleitung auftritt. Wenn S24 auf 0 eingestellt ist, wechselt das Modem nie in den Ruhemodus.

H.7 Trennen eines Anrufs

Es gibt mehrere Möglichkeiten, einen Anruf zu trennen. Im Folgenden werden diese Methoden beschrieben.

Wenn Sie die Stromversorgung des Modems zurücksetzen oder Pin-Nr. 12 (Leitung zurücksetzen) umschalten, wird die Verbindung getrennt und das Modem wechselt in den Offline-Status.

Wenn das DTR-Signal (Pin-Nr. 4) von EIN zu AUS wechselt, wird das Modem ebenfalls getrennt. Bei Verwendung dieser Methode muss sichergestellt werden, dass der DTR-Befehl auf &D2 oder &D3 eingestellt ist und nicht auf &D0 (erzwungen).

Auch das Remote-Gerät kann das Trennen des Modems verursachen. Wenn die Verbindung mit dem Remote-Modem getrennt wird, erkennt Ihr Modem automatisch den Verlust des Trägersignals und kehrt in den Offline-Status zurück.

Sie können auch den ATH- oder den ATZ-Befehl verwenden, um einen Anruf zu trennen. Damit Sie einen Befehl an das Modem ausgeben können, wenn es sich im Online-Status befindet, muss das Modem in den Online-Befehlsstatus versetzt werden. Dies wird durch Ausgabe einer besonderen Escape-Sequenz erreicht. Der Standardwert dieser dreistelligen Escape-Sequenz ist das Pluszeichen „+“ (zum Ändern siehe S2). Die Sequenz „+++“ wird durch eine Verzögerung von einer Sekunde vor und nach dem Senden geschützt (zum Ändern der Schutzzeit siehe S12). Wenn das Modem die Escape-Sequenz erkennt, wird der Ergebniscode OK angezeigt und das Modem befindet sich im Online-Befehlsstatus. Nun kann der ATH- oder der ATZ-Befehl zum Trennen des Anrufs ausgegeben werden.

H.8 Auswählen von Länderkennungen

Die Länderkennung des Modems wird über den +GCI-Befehl eingestellt. Wenn Sie zu einem der 30 verfügbaren Länder wechseln möchten, geben Sie den Befehl AT+GCI=n aus, wobei „n“ eine der zweistelligen Länderkennungen ist. Dieser Befehl muss bei jedem Einschalten des Modems ausgegeben werden. Die jeweilige Einstellung wird nicht automatisch gespeichert oder beibehalten. Sie sollte Teil der Initialisierungszeichenfolge sein.

Zum Beispiel: AT+GCI=00<CR> Bedeutung: Länderkennung auf „Japan“ ändern.

OK Bedeutung: Das Modem hat den Befehl akzeptiert und ist

nun für den Betrieb in Japan konfiguriert.

AT+GCI?<CR> Bedeutung: Aktuelle Länderkennung anzeigen.

+GCI:00 Bedeutung: (Japan ist derzeit als Land ausgewählt.)

OK

Um zu sehen, welche Länder in der Modem-Firmware verfügbar sind, geben Sie AT+GCI=?<CR> ein.

Das Modem zeigt alle verfügbaren zweistelligen Länderkennungen an.

Tabelle H.7 Liste der Länderkennungen

Land	Kennung	Land	Kennung	Land	Kennung
Australien	09	Hongkong	50	Polen	8A
Österreich	0A	Indien	53	Portugal	8B
Belgien	0F	Irland	57	Südafrika	9F
Brasilien	16	Italien	59	Singapur	9C
China	26	Japan	00	Spanien	A0
Dänemark	31	Korea	61	Schweden	A5
Finnland	3C	Mexiko	73	Schweiz	A6
Frankreich	3D	Niederlande	7B	Taiwan	Fe
Deutschland	42	Norwegen	82	TBR21	FD
USA	B5	Vereinigtes Königreich	B4		

H.9 Anruferkennung

Das Modem kann bestimmte Informationen über eingehende Telefonanrufe anzeigen. Das Modem kann das Datum, die Uhrzeit, die Telefonnummer und den Namen für eingehende Anrufe anzeigen. Wenn die Option für die Anruferkennung aktiviert ist, werden die entsprechenden Informationen zwischen dem ersten und dem zweiten Klingelton angezeigt. Damit diese Funktion korrekt funktioniert, muss der Anruferkennungsdienst für die Telefonleitung, an die das Modem angeschlossen ist, bei der örtlichen Telefongesellschaft abonniert worden sein. Es folgt ein Beispiel für die Informationen, die angezeigt werden:

RING

DATE = 1305

TIME = 1346

NMBR = 408 767 8900

NAME = RADICOM RESEARCH

RING

Die Informationen zur Anruferkennung können entweder wie oben formatiert oder auch unformatiert angezeigt werden. Die Option für die Anruferkennung des Modems wird über die Befehle +VCID und +VRID gesteuert.

Tabelle H.8 Informationen bei Verwendung der Anruferkennung

Befehl	Parameter	Beschreibung
+VCID?	n. z.	Zeigt die aktuelle +VCID-Einstellung an (0-2).
+VCID=	0	Deaktiviert die Anruferkennung (Standard).
+VCID=	1	Aktiviert die Anruferkennung mit formatierter Darstellung auf der Datenendeinrichtung (DTE).
+VCID+	2	Aktiviert die Anruferkennung mit unformatierter Darstellung auf der Datenendeinrichtung (DTE).
+VRID=	0	Zeigt die formatierten Informationen der Anruferkennung für den zuletzt empfangenen Anruf an.
+VRID+	1	Zeigt die unformatierten Informationen der Anruferkennung für den zuletzt empfangenen Anruf an.

Anhang I: Behördliche Vorschriften in Bezug auf das in diesem Produkt installierte Analogmodem

I.1 Sicherheitswarnungen zu analogen Telekommunikationsgeräten

Vor der Wartung muss dieses Produkt von der Stromversorgung und dem Telefonnetz getrennt werden. Beachten Sie auch folgende Hinweise:

- Die Telefonverkabelung darf nie während eines Gewitters installiert werden.
- Telefonbuchsen dürfen nicht in nassen oder feuchten Umgebungen installiert werden, sofern sie nicht speziell für derartige Umgebungen vorgesehen sind.
- Berühren Sie niemals unisolierte Telefondrähte oder Abschlusswiderstände, wenn die Telefonleitung nicht an der Netzwerkschnittstelle getrennt wurde.
- Gehen Sie beim Installieren oder Modifizieren von Telefonleitungen vorsichtig vor.

I.2 Avertissements de sécurité concernant les télécommunications analogiques

Avant l'entretien, débranchez ce produit de la source d'alimentation et du réseau téléphonique. Par ailleurs :

- Ne raccordez jamais les câbles téléphoniques pendant un orage.
- Ne raccordez jamais les prises téléphoniques dans des endroits humides à moins que la prise ne soit spécialement conçue pour ce type d'endroit.
- Ne touchez jamais les câbles ou terminaux téléphoniques non isolés à moins que la ligne téléphonique n'ait été déconnectée de l'interface réseau.
- Faites preuve de prudence lors du raccordement ou de la modification des lignes téléphoniques.

I.3 Einschränkungen für internationale Modems

Bei internationalen Modems variieren möglicherweise einige Standardeinstellungen für das Wählen und Antworten oder es gelten unterschiedliche Einschränkungen. Das Ändern von Einstellungen kann dazu führen, dass ein Modem die behördlichen Vorschriften bestimmter Länder nicht mehr erfüllt. Beachten Sie auch, dass in einigen Softwarepaketen möglicherweise Funktionen vorhanden sind oder Einschränkungen fehlen, die dazu führen, dass das Modem maßgebliche Vorschriften nicht erfüllt.

USA, 47 CFR Part 68 Telecom

1. Dieses Gerät erfüllt die Vorschriften des US-amerikanischen Regelwerks „Title 47 CFR Part 68" und die Vorschriften gemäß ACTA (Administrative Council for Terminal Attachments). Auf diesem Gerät befindet sich ein Etikett, das unter anderem die Registrierungsnummer und den Anschlusswert (Ringer Equivalence Number, REN) dieses Geräts oder eine Produktkennung im folgenden Format angibt:

   Für aktuelle Produkte: US:AAAEQ##Txxxx.

   Für Altprodukte: AU7USA-xxxxx-xx-x.

   Diese Nummer muss auf Anfrage der Telefongesellschaft mitgeteilt werden.

2. Der Stecker und die Buchse, mit denen dieses Gerät an die Gebäudeverkabelung und das Telefonnetz angeschlossen wird, müssen die entsprechenden Vorschriften des Regelwerks „Title 47 CFR Part 68“ und die Vorschriften gemäß ACTA erfüllen. Für den Anschluss muss eine ebenfalls regelkonforme Modularbuchse verwendet werden.
3. Anhand des Anschlusswertes (Ringer Equivalence Number, REN) lässt sich ermitteln, wie viele Geräte an eine Telefonleitung angeschlossen werden können. Wenn zu viele Geräte an eine Telefonleitung angeschlossen sind, klingeln die Geräte bei einem eingehenden Anruf möglicherweise nicht. In den meisten Regionen (jedoch nicht in allen) darf die Summe der Anschlusswerte nicht mehr als fünf (5,0) betragen. Erkundigen Sie sich ggf. bei Ihrer Telefongesellschaft, wie viele Geräte (gemäß Summe der Anschlusswerte) an die Telefonleitung angeschlossen werden dürfen. Bei Produkten, die nach dem 23. Juli 2001 zugelassen wurden, ist die REN Teil der Produktkennung, die folgendes Format hat: US:AAAEQ##Txxxx. Die durch ## dargestellten Ziffern entsprechen der REN ohne Dezimalzeichen (beispielsweise entspricht 03 der REN 0,3). Bei älteren Produkten wird die REN separat auf dem Etikett angezeigt.
4. Wenn dieses Gerät die Funktionsweise des Telefonnetzes beeinträchtigt, werden Sie von der Telefongesellschaft im Voraus benachrichtigt, dass möglicherweise eine Dienstunterbrechung erforderlich ist. Sollte keine Vorabbenachrichtigung möglich sein, informiert die Telefongesellschaft den Kunden so bald wie möglich. Sie werden auch über Ihr Recht in Kenntnis gesetzt, eine Beschwerde bei der FCC einzureichen, sollten Sie dies als notwendig erachten.
5. Die Telefongesellschaft kann Änderungen an ihren Anlagen, Geräten, Betriebsabläufen oder Prozeduren vornehmen, die sich auf den Betrieb des Geräts auswirken können. In diesem Fall werden Sie vorab von der Telefongesellschaft informiert, damit Sie die für einen unterbrechungsfreien Dienst erforderlichen Maßnahmen ergreifen können.
6. Sollten bei der Verwendung dieses Geräts Probleme auftreten, wenden Sie sich bitte unter der nachfolgend angegebenen Adresse an Vertiv, um Einzelheiten zum Reparaturverfahren zu erhalten. Wenn das Gerät Störungen am Telefonnetz verursacht, werden Sie möglicherweise von Ihrer Telefongesellschaft aufgefordert, das Gerät vom Telefonnetz zu trennen, bis das Problem behoben ist.
7. Herstellungsinformationen zum Telekommunikationsgerät (Modem):

   Hersteller: Multi-Tech Systems, Inc.

   Handelsname: Socket Modem SocketModem SocketModem

   Modellnummer: MT5692SMI

   Registrierungsnummer:US:AU7MM01BMT5692SMI

   Anschlusswert (REN): 0,1B

   Modularbuchse (USOC): RJ11C oder RJ11W oder RJ45 (Einzelleitung)

   Vertiv

   4991 Corporate Drive

   Huntsville, AL 35805 USA

   1-888-793-8763

I.4 MT5692SMI-Zulassung in Thailand

Dieses Telekommunikationsgerät entspricht den Vorgaben von NTC1.

1NTC (National Telecommunications Commission) ist die thailändische Aufsichtsbehörde für die Telekommunikation.

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

I.5 Warnhinweis der Telecom in Neuseeland

1. Die Erteilung einer Telepermit-Genehmigung für ein Endgerät bedeutet lediglich, dass Telecom anerkennt, dass das Gerät die Mindestvoraussetzungen für den Anschluss an das Telecom-Netz erfüllt. Sie stellt keine Billigung des Produkts durch Telecom dar und erteilt keinerlei Gewährleistung. Insbesondere stellt die Erteilung einer Telepermit-Genehmigung keine Garantie dar, dass das jeweilige Gerät in jeder Hinsicht korrekt mit Geräten anderer Hersteller oder Fabrikate funktioniert, die über eine Telepermit-Genehmigung verfügen. Die Erteilung der Genehmigung impliziert auch nicht, dass das jeweilige Produkt mit allen Netzwerkdiensten der Telecom kompatibel ist.

   Dieses Gerät kann nicht unter allen Betriebsbedingungen mit einer höheren Geschwindigkeit als vorgegeben betrieben werden. In einigen Telefonnetzen sind Verbindungen mit einer Geschwindigkeit von 33,6 kbit/s und 56 kbit/s wahrscheinlich auf niedrigere Bitraten beschränkt. Telecom übernimmt keine Verantwortung für Schwierigkeiten, die dadurch entstehen.

2. Wenn dieses Produkt beschädigt wird, muss es sofort vom Netz getrennt werden. Ergreifen Sie dann die erforderlichen Maßnahmen zur Reparatur oder Entsorgung.
3. Dieses Modem darf nicht auf eine Art und Weise verwendet werden, die zu einer Störung oder Belästigung anderer Telecom-Kunden führen kann.
4. Dieses Gerät arbeitet mit der Impulswahl, während der Telecom-Standard das DTMF-Tonwahlverfahren ist. Es besteht keine Garantie, dass Telecom-Leitungen auch in Zukunft das Impulswahlverfahren unterstützen werden.

   Wenn dieses Gerät an dieselbe Leitung wie andere Geräte angeschlossen ist, kann die Impulswahl zu Klingel- oder anderen Störgeräuschen führen oder eine Fehlantwort verursachen. Solche Probleme sollten NICHT an den technischen Kundendienst der Telecom gemeldet werden.

   Das DTMF-Tonwahlverfahren wird empfohlen, da es schneller als die Impulswahl (dekadisch) ist und in fast allen Vermittlungsstellen in Neuseeland unterstützt wird.

5. Warnhinweis: Bei einem Ausfall des Stromnetzes können keine 111- oder andere Anrufe von diesem Gerät getätigt werden.
6. Dieses Gerät ist möglicherweise nicht in der Lage, einen Anruf ordnungsgemäß an ein anderes Gerät zu übergeben, das an dieselbe Leitung angeschlossen ist.
7. Einige Parameter, die für die Erfüllung der Telepermit-Voraussetzungen der Telecom erforderlich sind, hängen von dem mit diesem Produkt verbundenen Gerät (PC) ab. Das verbundene Gerät muss innerhalb der folgenden Grenzwerte betrieben werden, damit die Vorgaben der Telecom erfüllt werden:

Wiederholte Anrufe an dieselbe Nummer:

- Innerhalb eines Zeitraums von 30 Minuten dürfen nicht mehr als 10 Anrufversuche an dieselbe Nummer für jede einzelne manuelle Einleitung eines Anrufs erfolgen.
- Zwischen dem Ende eines Versuchs und dem Beginn des nächsten Versuchs muss das Gerät mindestens 30 Sekunden lang aufgelegt werden.
- Automatische Anrufe an unterschiedliche Nummern:

- Das Gerät muss so eingerichtet werden, dass bei automatischen Anrufen an unterschiedliche Nummern ein Abstand eingehalten wird, sodass zwischen dem Ende eines Anrufversuchs und dem Beginn des nächsten Anrufversuchs mindestens 5 Sekunden vergehen.

8. Voraussetzung für den ordnungsgemäßen Betrieb ist, dass die Summe der Anschlusswerte der an eine Leitung angeschlossenen Geräte niemals 5 übersteigt.

I.6 Voraussetzungen für Japan

Das Modem erfüllt die JATE-Vorschriften (Japan Approval Institute for Telecommunications Equipment, japanische Zulassungsbehörde für Telekommunikationsgeräte):

MT5692SMI – JATE-Zulassung 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

590-1536-503H