Sistema de consola avanzada ACS800/8000 de Avocent®

Guía de uso e instalación

La información que contiene este documento está sujeta a cambios sin previo aviso, y es posible que no sirva para todas las aplicaciones. Aunque se han tomado todas las precauciones para garantizar la exactitud y la integridad del presente documento, Vertiv no asume ninguna responsabilidad, y rechaza toda responsabilidad legal, por daños resultantes del uso de esta información o causados por cualquier error u omisión. Consulte otros códigos de construcción y prácticas locales según corresponda para los métodos, herramientas y materiales correctos que se usen al ejecutar procedimientos no descritos específicamente en este documento.

Los productos contemplados en este manual de instrucciones están fabricados y/o comercializados por Vertiv. Este documento pertenece a Vertiv y contiene información confidencial y exclusiva propiedad de Vertiv. Está terminantemente prohibida cualquier copia, uso o difusión del mismo sin el permiso por escrito de Vertiv.

Los nombres de empresas y productos son marcas comerciales o marcas comerciales registradas de sus respectivas empresas. Cualquier pregunta relativa al uso de nombres de marcas comerciales debe dirigirse al fabricante original.

Sitio de asistencia técnica

Si experimenta cualquier problema de instalación o funcionamiento con el producto, consulte la sección pertinente de este manual para intentar resolver el problema mediante los procedimientos descritos.

Visite https://www.vertiv.com/en-us/support/ para obtener ayuda adicional.

CONTENIDO

1 Introducción

El sistema de consola avanzada ACS800/8000 de Avocent® actúa como punto único para el acceso y la administración de dispositivos conectados como, por ejemplo, consolas serie, módems y dispositivos de alimentación. El sistema de consola permite la gestión segura y remota de centros de datos y la gestión fuera de banda de activos informáticos desde cualquier lugar del mundo.

NOTA: A menos que se indique lo contrario, las menciones a un sistema de consola hacen referencia a todos los modelos de la serie del 800/8000.

El sistema de consola proporciona un acceso seguro tanto local (puerto de consola) como remoto (IP y acceso telefónico). El sistema de consola ejecuta el sistema operativo Linux® con un sistema de archivos persistente en memoria Flash que se puede actualizar con un archivo local en un equipo informático conectado al sistema de consola.

Varios administradores pueden iniciar sesión en el sistema de consola al mismo tiempo y pueden usar la interfaz de usuario web, la interfaz de línea de comandos (utilidad CLI) o el software de gestión DSView ™ 4 para acceder al sistema de consola y configurarlo.

NOTA: A menos que se indique lo contrario, todas las menciones al software DSView en este documento hacen referencia a la versión 4 o superior.

En función del modelo, el sistema de consola cuenta con cuatro u ocho puertos USB que admiten módems, dispositivos de almacenamiento, adaptadores de red, concentradores USB y dispositivos de consola USB. Algunos modelos están equipados con una ranura para tarjetas SD que permite la conexión de un dispositivo de almacenamiento adicional.

Dos puertos de red admiten conexiones a más de una red, o se pueden configurar para enlace Ethernet para disfrutar de redundancia y de una mayor fiabilidad o soporte en la conmutación por error en red.

Para el marcado de entrada y un retorno de llamada seguro con el protocolo punto a punto (PPP), un módem interno opcional se puede instalar en fábrica o se puede utilizar un módem externo conectado a un puerto serie o USB.

Algunos modelos también están equipados con una antena para conectividad móvil.

1.1 Características y beneficios

1.1.1 Opciones de acceso

El acceso seguro está disponible mediante las siguientes opciones locales (puerto de consola analógica) y remotas (IP digital y acceso telefónico):

- Conexión de red IP LAN/WAN.
- Acceda de forma telefónica a un módem interno configurado en fábrica (opcional) o un módem conectado a uno de los puertos serie o USB.
- Algunos modelos también incorporan una antena para conectividad móvil.
- Conexión con dispositivos de destino. Un usuario autorizado puede establecer una conexión Telnet, SSH v2 o sin procesar con un dispositivo de destino. Para que se utilice Telnet o SSH para conexiones de dispositivos de destino, el servicio Telnet o SSH debe configurarse en el perfil de seguridad que esté en vigor.

- Conexión de consola del sistema de consola. Un administrador puede iniciar sesión desde un terminal local o desde un equipo informático con un programa de emulación de terminal que esté conectado al puerto de consola y puede utilizar la utilidad CLI. La pantalla de la utilidad CLI (--:- cli->) se muestra en el inicio de sesión.

Más de un administrador puede iniciar sesión en el sistema de consola y establecer una sesión CLI o de interfaz de usuario web activa. Todas las sesiones reciben el siguiente mensaje de advertencia cuando otro administrador o el sistema modifica la configuración: *La configuración del equipo se ha alterado desde fuera de su sesión*. Al recibir este mensaje, cada administrador debe verificar que se hayan guardado los cambios realizados durante la sesión.

1.1.2 Interfaz de usuario web (IU web)

Los usuarios y administradores pueden realizar la mayoría de tareas mediante la interfaz de usuario web (IU web), a la que se puede acceder con HTTP o HTTPS. La IU web funciona en Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome y Apple Safari o en cualquier equipo informático compatible que tenga acceso de red al sistema de consola. La lista de navegadores cliente compatibles y sus versiones está disponible en las notas de la versión.

NOTA: Cuando acceda al sistema de consola a través de la interfaz de usuario web, no desactive los cuadros de diálogo adicionales si se lo solicita su navegador. Si desactiva los cuadros de diálogo, desactivará también ciertas funcionalidades de la interfaz de usuario web.

1.1.3 Compatibilidad con IPv4 y IPv6

El sistema de consola es compatible con protocolos IPv4 e IPv6 de doble pila. El administrador puede usar la interfaz de usuario web o CLI para configurar la compatibilidad solo con direcciones IPv4 o con direcciones tanto IPv4 como IPv6. En la siguiente lista se describe la compatibilidad con IPv6 que se proporciona en el sistema de consola:

- DHCP
- Sesiones de marcado de entrada y marcado de salida (enlaces PPP)
- Integración con el software DSView
- Interfaces Ethernet eth0 y eth1
- Firewall (tablas IP)
- HTTP/HTTPs
- Kernel de Linux
- Autenticación remota: Servidores Radius, Tacacs+, LDAP y Kerberos
- SNMP
- Acceso SSH y Telnet
- Servidor Syslog

NOTA: IPSec no es compatible con IPv6.

1.1.4 Usuarios y grupos flexibles

Se puede definir una cuenta para cada usuario en el sistema de consola o en un servidor de autenticación. El administrador y los usuarios raíz tienen cuentas de forma predeterminada y pueden añadir y configurar otras cuentas de usuario. El acceso a los puertos puede restringirse de forma opcional según las autorizaciones que un administrador puede asignar a grupos de usuarios personalizados o a usuarios individuales. Para obtener más información, consulte Cuentas de usuarios y grupos de usuarios en la página 70.

1.1.5 Seguridad

Los perfiles de seguridad determinan qué servicios de red están activados en el sistema de consola. Los administradores pueden permitir que todos los usuarios accedan a los puertos activados o permitir la configuración de las autorizaciones de grupos y usuarios para restringir el acceso. También puede seleccionar un perfil de seguridad que defina qué servicios (FTP, TFTP, ICMP, IPSec y Telnet) están activados y el acceso SSH y HTTP/HTTPS. El administrador puede seleccionar un perfil de seguridad preconfigurado o crear un perfil personalizado. Para obtener más información, consulte Seguridad en la página 23.

1.1.6 Autenticación

La autenticación se puede realizar de forma local, con contraseñas de un solo uso (OTP), un servidor de autenticación Kerberos, LDAP, RADIUS o TACACS+ remoto o un servidor de DSView. El sistema de consola también admite las autorizaciones de grupos remotos para los métodos de autenticación LDAP, RADIUS y TACACS+. También hay disponibles mecanismos de reserva.

Cualquier método de autenticación configurado para el sistema de consola o los puertos se utiliza para la autenticación de cualquier usuario que intente iniciar sesión mediante Telnet, SSH o la interfaz de usuario web. Para obtener más información, consulte Autenticación en la página 67.

1.1.7 VPN basadas en IPSec con NAT traversal

Si IPSec se activa en el perfil de seguridad seleccionado, un administrador puede usar la función VPN para activar conexiones seguras. Para obtener más información, consulte IPSec (VPN) en la página 34.

1.1.8 Filtrado de paquetes

Un administrador puede configurar un sistema de consola para filtrar paquetes como un firewall. El filtrado de paquetes está controlado por cadenas, que son perfiles con nombre con reglas definidas por el usuario. La tabla de filtros del sistema de consola contiene varias cadenas integradas que se pueden modificar pero no eliminar. Un administrador también puede crear y configurar cadenas nuevas.

1.1.9 SNMP

Si SNMP está activado en el perfil de seguridad seleccionado, un administrador puede configurar el agente de protocolo simple de administración de redes (SNMP) en el sistema de consola para responder a las solicitudes enviadas por una aplicación de gestión de SNMP.

El agente SNMP del sistema de consola es compatible con SNMP v1/v2 y v3, MIB-II y MIB empresarial. Para obtener más información, consulte Configuración SNMP en la página 40.

NOTA: Los archivos de texto con la MIB empresarial (ACS8000-MIB.asn) y la MIB de CAPTURAS (ACS8000-TRAP-MIB.asn) están disponibles en el equipo, en el directorio /usr/local/mibs.

1.1.10 Registro de datos, notificaciones, alarmas y almacenamiento en búfer de datos

Un administrador puede configurar el registro de datos, notificaciones y alarmas para alertar a administradores sobre problemas con notificaciones de correo electrónico, SMS, captura de SNMP o software DSView. Un administrador también puede almacenar datos almacenados en búfer de forma local, de forma remota o con el software de gestión DSView. También se pueden enviar mensajes sobre el sistema de consola y los servidores o dispositivos conectados a servidores Syslog.

1.1.11 Gestión de alimentación

El sistema de consola permite que los usuarios con autorización para la gestión de alimentación enciendan, apaguen y restablezcan los dispositivos conectados a una unidad de distribución de la alimentación (PDU). Los dispositivos de alimentación se pueden conectar a cualquier puerto serie. Los usuarios autorizados también pueden supervisar y controlar una fuente de alimentación ininterrumpida (UPS) conectada. Para obtener más información, consulte Gestión de alimentación en la página 82.

1.1.12 Detección automática

Un administrador puede activar la detección automática para buscar el nombre de host de un dispositivo de destino conectado a un puerto serie. Las cadenas de sondeo y respuesta predeterminadas de la función de detección automática tienen un alcance amplio. Un administrador puede configurar cadenas de sondeo y respuesta específicas para un sitio. La detección automática también se puede configurar mediante el software DSView.

1.1.13 Módulo FIPS

La serie 140 de estándares federales de procesamiento de información (FIPS, por sus siglas en inglés) son estándares de seguridad informática del gobierno de EE. UU. que especifican los requisitos para los módulos de criptografía.

El sistema de consola incorpora un módulo criptográfico basado en el módulo criptográfico validado por FIPS 140-2 (número de certificado 1747) que se ejecuta en una plataforma ARM de Linux. Para obtener más información, consulte Módulo FIPS en la página 25.

1.2 Ejemplos de configuración

En el gráfico y en la tabla siguientes se muestra una configuración del sistema de consola avanzada ACS800/8000 de Avocent® con todas las opciones posibles. Las opciones pueden variar según el modelo y no existe ningún modelo que cuente con todas las opciones mostradas.

Figura 1.1 Configuración del sistema de consola avanzada ACS8000 mostrando todas las opciones

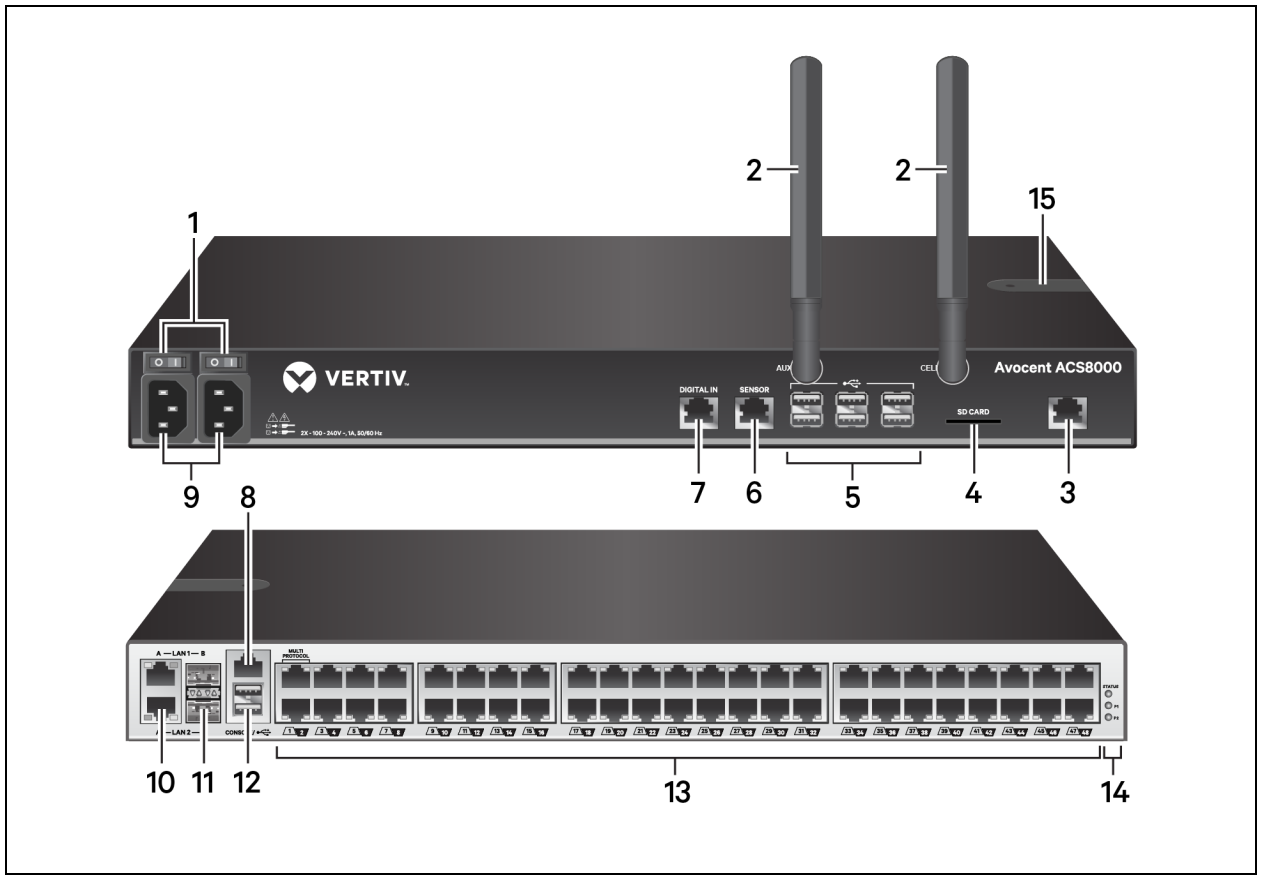


Tabla 1.1 Descripciones de la configuración del sistema de consola avanzada ACS8000

Número	Descripción
1	Botones de alimentación (se muestra una fuente de alimentación doble).
2	Antenas móviles para el módem móvil (no disponibles en algunos modelos).
3	Conecte una línea telefónica al puerto de módem del módem interno.
4	Ranura para tarjetas SD (no disponible en algunos modelos).
5	Puertos USB para dispositivos USB compatibles (no disponibles en algunos modelos).
6	Puerto de sensor para un sensor ambiental de 1 cable (no disponible en algunos modelos).
7	Puertos de entrada digital para sensores de humo, fugas, presión o contacto seco de un cable (no disponibles en algunos modelos).
8	Puerto de la consola para conectar un terminal o estación de trabajo. El sistema de consola se configura mediante un terminal o un emulador de terminal con los siguientes ajustes de sesión: 9600, 8, N y 1, sin ningún control de flujo.
9	Fuente de alimentación (se muestra una fuente de alimentación doble).
10/11	Puertos LAN. Los puertos de la izquierda son para conexiones de interfaz de cobre. Los puertos de la derecha son para conexiones de interfaz de fibra. Puede conectarse a uno o a ambos puertos de red para redundancia; sin embargo, solo se puede utilizar un puerto LAN1 y LAN2 al mismo tiempo. Si ambos puertos LAN1 o LAN2 están conectados, la conexión de fibra tiene prioridad.
12	Dos puertos USB en la parte posterior del sistema de consola para dispositivos USB adicionales.
13	Puertos serie. Use cables CAT 5e o CAT 6 y adaptadores de consola DB9 o DB25 para conectar los dispositivos serie y de alimentación adecuados a los puertos serie del sistema de consola.
14	LED de estado.
15	Ranura para tarjetas SIM.

En el gráfico y en la tabla siguientes se muestran los puertos multiprotocolo y los LED.

Figura 1.2 Puertos multiprotocolo y LED del sistema de consola avanzada ACS8000 de Avocent®

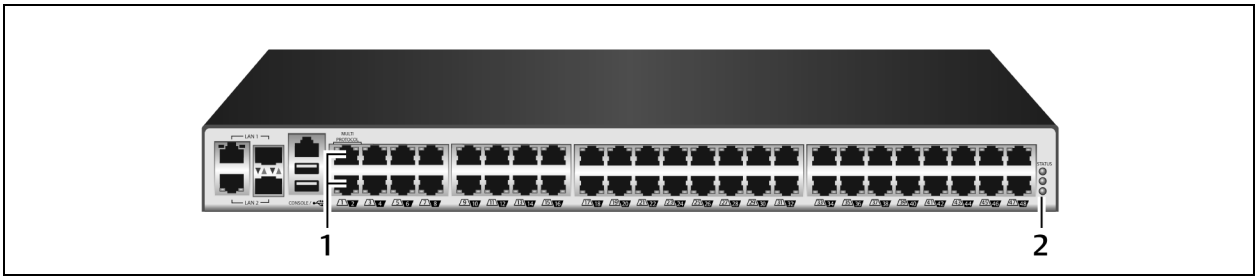


Tabla 1.2 Descripciones de los puertos multiprotocolo y los LED

Número	Descripción
1	Puertos multiprotocolo. Estos dos puertos pueden aceptar contactos RS422 y RS485, además de contactos Cyclades y Cisco.
2	LED.El LED de estado está verde cuando el sistema de consola se ha inicializado por completo. Los LED P1 y P2 indican una fuente de alimentación activa. P1 está verde cuando la fuente de alimentación 1 está activada. P2 está verde cuando la fuente de alimentación 2 está activada.

Figura 1.3 Inserción de la tarjeta SIM

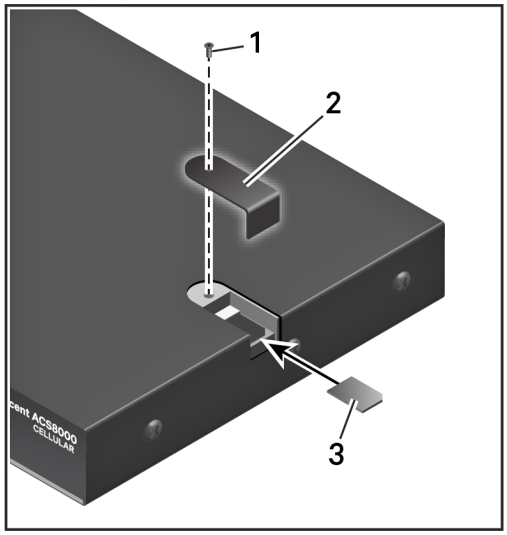


Tabla 1.3 Descripción para la inserción de la tarjeta SIM

Elemento	Descripción
1	Retire el tornillo para sacar la tapa. Una vez que haya insertado la tarjeta, vuelva a colocar la tapa y el tornillo.
2	Retire la tapa para dejar a la vista la ranura de la tarjeta SIM. Vuelva a colocar la tapa una vez que haya insertado la tarjeta.
3	Introduzca la tarjeta.

Figura 1.4 Configuración habitual del sistema de consola avanzada ACS800

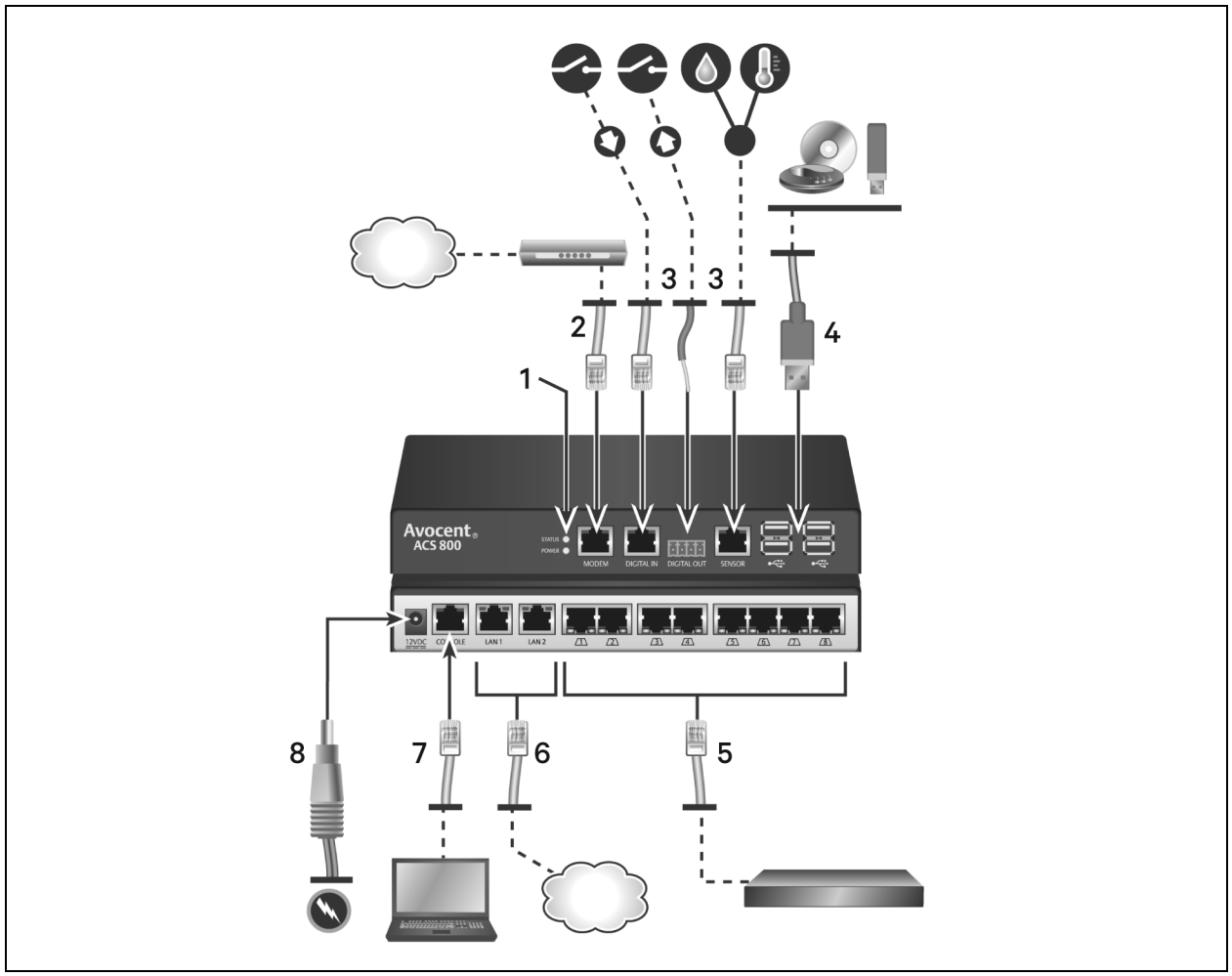


Tabla 1.4 Descripciones de la configuración habitual del sistema de consola avanzada ACS800

Número	Descripción
1	LED. El LED de estado está verde cuando el sistema de consola se ha inicializado por completo. El LED de alimentación está verde cuando se está suministrando alimentación al sistema de consola.
2	Conecte una línea telefónica al puerto de módem del módem interno.
3	Puertos de sensores para sensores de 1 cable ambientales, de humo, fugas, presión o contacto seco.
4	Puertos USB para dispositivos USB compatibles.
5	Puertos serie. Use cables CAT 5e o CAT 6 y adaptadores de consola DB9 o DB25 para conectar los dispositivos serie y de alimentación adecuados a los puertos serie del sistema de consola. Todos los puertos serie son multiprotocolo y seleccionables por el usuario con contactos RS485, RS422 y RS232.
6	Puertos LAN de cobre. Puede conectarse a uno o a ambos puertos de red para redundancia.
7	Puerto de consola.
8	Fuente de alimentación.

1.2.1 Estados de los LED de los puertos serie

En cada puerto serie hay dos LED que se encienden en verde o amarillo. Los LED verdes indican el estado de la conexión física con un puerto serie, la conectividad remota (cuando sea pertinente) y la transferencia de datos. Los LED amarillos indican si se está supervisando un puerto serie junto con el nivel de alerta (emergencia, alerta o ninguno) de un destino supervisado. En la siguiente tabla se describe el significado de todos los estados de los LED.

Tabla 1.5 Descripción del estado de los LED

Estado	Descripción para LED verdes	Descripción para LED amarillos
Apagado	No hay conexión física	No hay almacenamiento en búfer de datos
Encendido (verde o amarillo constante)	El dispositivo está físicamente conectado al puerto serie	El almacenamiento en búfer de datos está activado para el puerto serie
Parpadeo lento	Telnet, SSH o una sesión sin procesar están activos	Hay una alerta activa
Parpadeo rápido	Actividad de transmisión o recepción de datos	Emergencia

Esta página se ha dejado en blanco de forma intencionada

2 Introducción

2.1 Instalación

Para obtener información sobre la instalación del sistema de consola, consulte la guía de instalación rápida del sistema ACS800 o ACS8000 que se incluye con el producto.

2.2 Encendido del sistema de consola

En función del modelo, el sistema de consola recibe alimentación a partir de fuentes de alimentación únicas o dobles de CA o CC.

¡ADVERTENCIA! Ejecute siempre el comando de apagado desde la interfaz de usuario web, CLI o el software DSView en el nodo Información general/Herramientas antes de apagar el sistema de consola y volver a encenderlo. De este modo se asegurará de que el restablecimiento no se produce mientras se está accediendo al sistema de archivos de la memoria Flash y ayuda a evitar daños en la memoria Flash.

2.2.1 Alimentación de CA

Para encender un sistema de consola con alimentación de CA:

1. Asegúrese de que el sistema de consola está apagado.
2. Conecte el cable de alimentación en el sistema de consola y en una fuente de alimentación.
3. Encienda el sistema de consola.
4. Encienda los interruptores de alimentación de los dispositivos conectados.

2.2.2 Alimentación de CC

La alimentación de CC se conecta a un sistema de consola con alimentación de CC mediante tres cables: Retorno (RTN), tierra (GND) y -48 V de CC. Para disponer de redundancia, hay dos conjuntos de cables que se pueden conectar a dos fuentes de alimentación separadas.

¡ADVERTENCIA! Es vital que la fuente de alimentación cumpla los requisitos de alimentación de CC del sistema de consola. Asegúrese de que la fuente de alimentación sea del tipo correcto y que los cables de alimentación de CC están en buenas condiciones antes de continuar. De lo contrario, podrían provocarse lesiones personales o daños en el equipo.

En el diagrama siguiente se muestra la configuración de los conectores de alimentación de CC.

NOTA: La alimentación de CC solo está disponible en el sistema de consola ACS8000.

Figura 2.1 Bloque de terminales de conexión de alimentación de CC

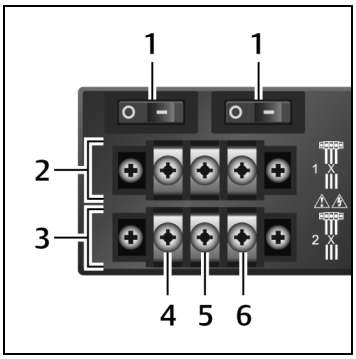


Tabla 2.1 Detalles de la conexión de alimentación de CC

Número	Descripción	Número	Descripción
1	Interruptor de encendido, uno para cada fuente de alimentación	4	RTN (retorno)
2	Conexiones para la primera fuente de alimentación	5	GND (tierra)
3	Conexiones para la segunda fuente de alimentación	6	-48 V de CC

Para encender un sistema de consola con alimentación de CC:

1. Asegúrese de que el sistema de consola está apagado.
2. Asegúrese de que los cables de alimentación de CC no estén conectados a una fuente de alimentación.
3. Retire la cubierta protectora del bloque de alimentación de CC; para ello, deslícela hacia la izquierda o hacia la derecha.
4. Afloje los tres tornillos del terminal de conexión de alimentación de CC.
5. Conecte el cable de retorno al terminal RTN, el cable de tierra al terminal GND y el cable de -48 V de CC al terminal de -48 V de CC y apriete los tornillos.
6. Vuelva a colocar la cubierta protectora en su lugar sobre el bloque de terminales de CC.
7. Si el sistema de consola dispone de terminales de CC de doble entrada, repita los pasos 3-6 para el segundo terminal.
8. Conecte los cables de alimentación de CC a la fuente de alimentación de CC y encienda la fuente de alimentación de CC.
9. Encienda el sistema de consola.
10. Encienda los interruptores de alimentación de los dispositivos conectados.

2.3 Configuración de un sistema de consola

El sistema de consola se puede configurar al nivel del equipo mediante la interfaz de línea de comandos a la que se accede a través del puerto CONSOLE o Ethernet. Se puede acceder a todos los comandos de terminal a través de un terminal o un equipo informático que ejecute un software de emulación de terminal.

NOTA: Para configurar el sistema de consola con el software DSView, consulte la guía de uso e instalación del software de gestión DSView 4.5 de Avocent®. Para configurar el sistema de consola mediante la interfaz de usuario web, consulte Información general sobre la interfaz de usuario web para administradores en la página 18. Para configurar el sistema de consola mediante Telnet o SSH, consulte la guía de referencia de comandos del sistema de consola avanzada ACS 800/8000 de Avocent®.

Para conectar un terminal al sistema de consola:

1. Utilice un cable de módem nulo para conectar un terminal o un equipo informático que ejecute software de emulación de terminal (como por ejemplo HyperTerminal) al puerto CONSOLE del panel posterior del sistema de consola. Se proporciona un adaptador cruzado RJ-45 a DB9 (hembra).

   El terminal está configurado a 9600 bits por segundo (bps), 8 bits de datos, 1 bit de parada, sin paridad y sin control de flujo.

2. Encienda el sistema de consola. Cuando el sistema de consola finalice la inicialización, en el terminal se mostrará la pancarta de inicio de sesión y el mensaje de inicio de sesión.

2.3.1 Uso de Telnet o SSH

Un usuario autorizado puede utilizar un cliente de Telnet o SSH para realizar una conexión directamente a la consola de un dispositivo si se cumplen todas las condiciones siguientes:

Telnet o SSH:

- Este protocolo se activa en el perfil de seguridad seleccionado
- El cliente está disponible y está activado en el equipo informático desde el que se realiza la conexión

Para usar Telnet para conectarse a un dispositivo a través de un puerto serie:

Para este procedimiento, necesita el nombre de usuario configurado para acceder al puerto serie, el nombre del puerto (por ejemplo, 14-35-60-p-1), el nombre del dispositivo (por ejemplo, ttyS1), el alias de puerto TCP (por ejemplo, 7001) o el alias de puerto IP (por ejemplo, 100.0.0.100) y el nombre de host del sistema de consola o su dirección IP.

Para utilizar un cliente Telnet, introduzca la información en los cuadros de diálogo del cliente.

-O bien-

Para usar Telnet en un shell, introduzca el siguiente comando:

```
#telnet [nombre de host | dirección IP]
inicio de sesión: nombre de usuario:[nombre del puerto | nombre del dispositivo | alias de puerto TCP]
-O bien-
#telnet [nombre de host | dirección IP] alias de puerto TCP
inicio de sesión: nombre de usuario
-O bien-
#telnet alias de puerto IP
inicio de sesión: nombre de usuario
```

Para cerrar una sesión Telnet:

Pulse la tecla de acceso rápido de Telnet definida para el cliente. La predeterminada es **Ctrl]** + **q** para salir.

-O bien-

Pulse la tecla de acceso rápido de la sesión de texto para la pantalla de CLI y, a continuación, escriba **exit**.

Para usar SSH para conectarse a un dispositivo a través de un puerto serie:

Para este procedimiento, necesita el nombre de usuario configurado para acceder al puerto serie, el nombre del puerto (por ejemplo, 14-35-60-p-1), el alias de puerto TCP (por ejemplo, 7001), el nombre del dispositivo (por ejemplo, ttyS1) y el nombre de host del sistema de consola, la dirección IP o el alias de puerto IP (por ejemplo, 100.0.0.100).

Para usar un cliente de SSH:

Introduzca la información en los cuadros de diálogo del cliente.

-O bien-

Para usar SSH en un shell, introduzca el siguiente comando:

```
ssh -l  nombre de usuario:nombre del puerto  [nombre de host | dirección IP]
-O bien-
ssh -l nombre de usuario:nombre del dispositivo[nombre de host | dirección IP]
-O bien-
ssh -l nombre de usuario:alias de puerto TCP[nombre de host | dirección IP]
-O bien-
ssh -l nombre de usuario alias_puerto_IP
```

Para cerrar una sesión SSH:

Al principio de una línea, pulse la tecla de acceso rápido definida para el cliente de SSH seguida de un punto. El valor predeterminado es **~**.

-O bien-

Pulse la tecla de acceso rápido de la sesión de texto para la pantalla de CLI y, a continuación, escriba **exit**.

3 Acceso al sistema de consola mediante la interfaz de usuario web

Una vez que haya conectado el sistema de consola avanzada ACS800/8000 de Avocent® a una red, puede acceder al sistema de consola con su interfaz de usuario web. La interfaz de usuario web proporciona acceso directo al sistema de consola mediante una interfaz gráfica de usuario en lugar de una interfaz basada en comandos.

NOTA: Para un sistema de consola nuevo en el que se utilicen los valores predeterminados de fábrica, LAN1 intenta obtener una dirección IP mediante DHCP y LAN2 cuenta con una dirección IP estática de 192.168.161.10. Use LAN2 para la configuración inicial o utilice el puerto de consola para detectar la dirección IPv4 asignada por DHCP de LAN1.

NOTA: Para obtener instrucciones sobre cómo acceder al sistema de consola mediante la CLI o el software DSView, consulte la guía de referencia de comandos del sistema de consola avanzada ACS800/8000 de Avocent® o la guía de uso e instalación del software de gestión DSView 4.5 de Avocent®.

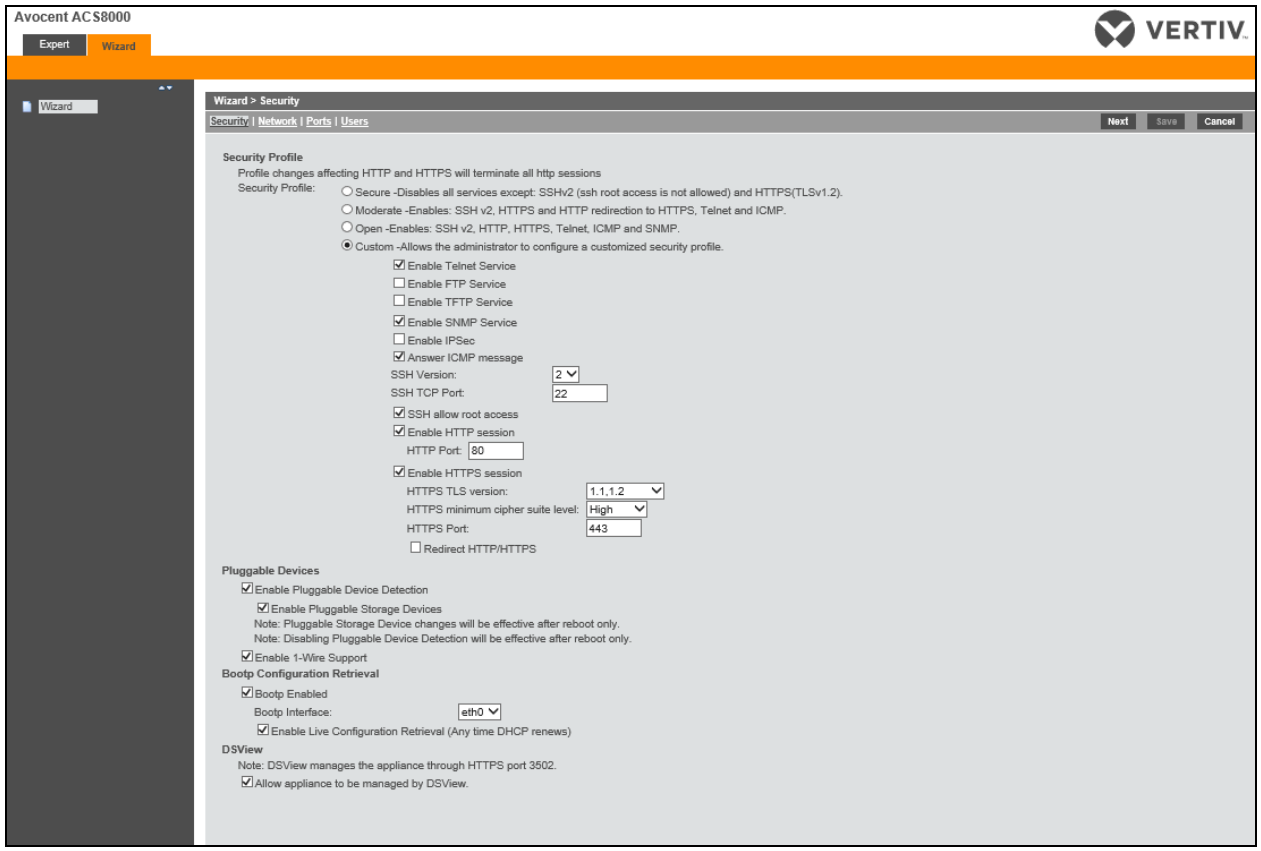
3.1 Modo de asistente

El modo de asistente se ha diseñado para simplificar el proceso de instalación y configuración y para ello se guía al administrador por los pasos de configuración. Los administradores pueden configurar todos los puertos en el perfil CAS y definir los ajustes de perfil de seguridad, red y usuarios mediante el asistente.

De forma predeterminada, el asistente se muestra la primera vez que un administrador accede al sistema de consola a través de la interfaz de usuario web. Los inicios de sesión subsiguientes se abren en el modo Experto y, una vez que se ha configurado el sistema de consola, el modo Experto se convierte en el modo predeterminado. Los administradores puede alternar entre los modos Experto y de asistente si hacen clic en la barra de pestañas de la pantalla del administrador de la interfaz de usuario web.

En la imagen siguiente se muestra una pantalla habitual cuando un administrador se encuentra en modo de asistente.

Figura 3.1 Pantalla Asistente



Los procedimientos siguientes describen cómo configurar el sistema de consola desde el asistente.

Para configurar los parámetros de seguridad y seleccionar un perfil de seguridad:

1. Seleccione el enlace *Seguridad* en la zona de contenido.
2. Seleccione el perfil de seguridad deseado. Si utiliza un perfil de seguridad personalizado, haga clic en las casillas de verificación e introduzca los valores necesarios para configurar los servicios, SSH y las opciones de HTTP y HTTPS para que se ajusten a su política de seguridad del sitio.
3. Los dispositivos conectables, entre los que se incluyen dispositivos conectados a la ranura para tarjetas SD y a los puertos USB, están desactivados de forma predeterminada. Para activarlos, marque la casilla Activar detección de dispositivos conectables. Los dispositivos de almacenamiento (tarjeta SD y almacenamiento USB) están activados de forma predeterminada cuando la detección de dispositivos conectables está activada. Para desactivar este subconjunto de dispositivos conectables, desmarque la casilla Activar dispositivos de almacenamiento conectables. Los dispositivos conectables también incluyen el puerto para sensor de 1 cable, que está activado de forma predeterminada. Para desactivar el puerto del sensor de 1 cable, desmarque la casilla Activar compatibilidad con 1 cable.

NOTA: Estas opciones aparecen en todos los modelos de sistema de consola, aunque algunos modelos no disponen de tarjeta SD ni puertos para sensor de 1 cable. Si su modelo no dispone de estos puertos, deje estas opciones desactivadas.

4. En el encabezado Recuperación de la configuración de Bootp, desmarque la(s) casilla(s) para desactivar la recuperación de la configuración de Bootp y/o la recuperación de la configuración en vivo.
5. Si no usa el software DSView para gestionar el equipo, desmarque la casilla *Permitir que el equipo esté gestionado por DSView*.
6. Haga clic en *Siguiente* para configurar la red o haga clic en el enlace *Red*, *Puertos* o *Usuarios* para abrir la pantalla adecuada.

Para configurar los parámetros de red:

1. Seleccione el enlace *Red* en la zona de contenido.
2. Introduzca el nombre de host, el DNS primario y el dominio en los campos correspondientes.
3. Seleccione el método IPv4 o IPv6 para la interfaz ETH0. Si usa la opción Estático, introduzca la dirección, la máscara y la puerta de enlace en los campos correspondientes.
4. Active o desactive LLDP (protocolo de detección de nivel de vínculo).
5. Activar o desactivar compatibilidad con IPv6.
6. Haga clic en *Siguiente* para configurar puertos o haga clic en el enlace *Seguridad*, *Puertos* o *Usuarios* para abrir la pantalla adecuada.

Para configurar puertos:

1. Seleccione el enlace *Puertos* en la zona de contenido.
2. Marque la casilla para activar todos los puertos.
3. Use los menús desplegables adecuados para seleccionar los valores de los campos Contactos RJ45, Velocidad, Paridad, Bits de datos, Bits de parada, Control de flujo, Protocolo, Tipo de autenticación y Estado de almacenamiento en búfer de datos, y Marca de hora de almacenamiento en búfer de datos.
4. Seleccione el tipo de almacenamiento en búfer de datos. Si usa NFS, introduzca la información sobre el servidor NFS y la ruta NFS en los campos correspondientes.
5. Haga clic en *Siguiente* para configurar usuarios o haga clic en el enlace *Red*, *Seguridad* o *Usuarios* para abrir la pantalla adecuada.

Para configurar usuarios y cambiar las contraseñas de usuario :

1. Seleccione el enlace *Usuarios* en la zona de contenido.
2. Haga clic en un nombre de usuario (*administrador* o *raíz*) e introduzca la nueva contraseña en los campos Contraseña y Confirmar contraseña.

   -O bien-

3. Haga clic en *Añadir* para añadir un usuario. Introduzca el nuevo nombre de usuario y contraseña en los campos correspondientes.
4. (Opcional) Para obligar al usuario a cambiar su contraseña predeterminada la próxima vez que inicie sesión, seleccione la casilla de verificación *El usuario debe cambiar la contraseña en el siguiente inicio de sesión*.
5. Asigne el usuario a uno o más grupos.
6. (Opcional) Configure la caducidad de la cuenta y de la contraseña.
7. Haga clic en *Siguiente*.

8. Repita los pasos 3-7 según sea necesario para configurar nuevas cuentas de usuario y asignarlas a grupos predeterminados.

NOTA: De forma predeterminada, todos los usuarios configurados pueden acceder a todos los puertos activados. Se necesita configuración adicional si su política de seguridad del sitio requiere que restrinja el acceso de los usuarios a los puertos.

9. Haga clic en *Guardar* y luego en *Finalizar*.

3.2 Información general sobre la interfaz de usuario web para administradores

NOTA: Para ver información general sobre la interfaz de usuario web para usuarios normales, consulte Información general sobre la interfaz de usuario web para usuarios normales en la página 90.

Para iniciar sesión en la interfaz de usuario web:

1. Abra un navegador web e introduzca la dirección IP del sistema de consola en el campo de dirección.
2. Inicie sesión con su nombre de usuario y contraseña. El nombre de usuario predeterminado es admin. La primera vez que inicie sesión como admin, deje el campo de contraseña en blanco. Se le solicitará que cree una nueva contraseña.

NOTA: De forma predeterminada, el usuario raíz está desactivado. Un usuario admin puede activar el usuario raíz desde la página Usuarios - Cuentas locales - Nombres de usuario.

En la figura siguiente se muestra una pantalla habitual de la interfaz de usuario web para un administrador.

Figura 3.2 Pantalla de la interfaz de usuario web para administradores

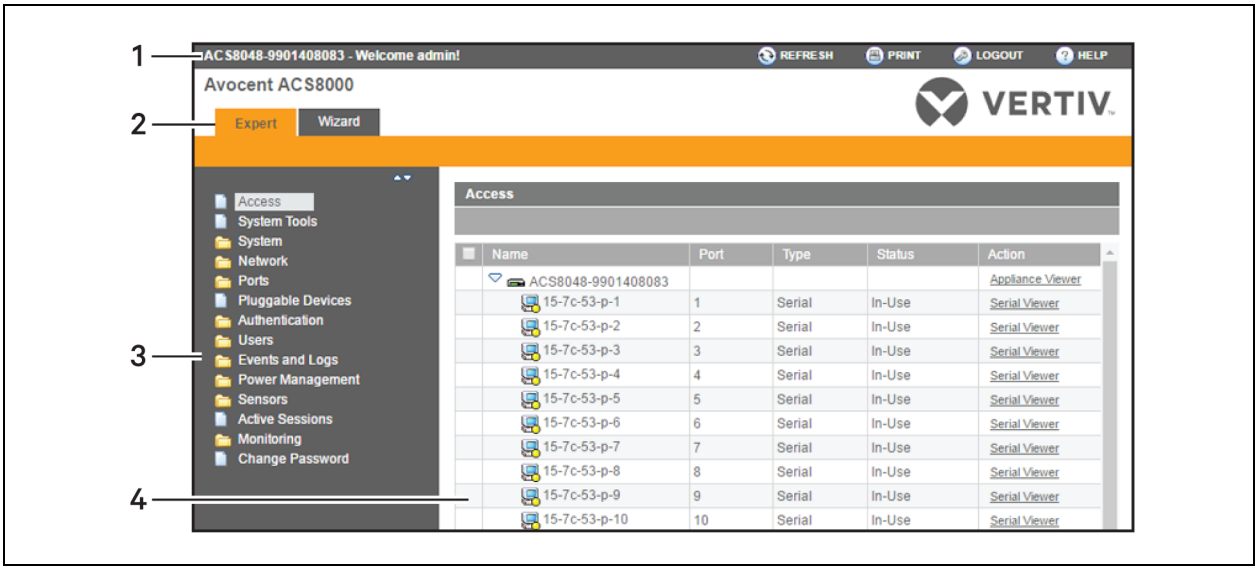


Tabla 3.1 Zonas de la pantalla de la interfaz de usuario web

Número	Descripción
1	Barra de opciones superior. El nombre del equipo y del usuario que ha iniciado sesión aparecen en el lado izquierdo. Los botones Actualizar, Imprimir, Cerrar sesión y Ayuda aparecen a la derecha.
2	Barra de pestañas. Muestra si el administrador se encuentra en modo Experto o Asistente.
3	Barra de navegación lateral. Opciones de menú para la configuración, la visualización de información del sistema y el acceso a dispositivos. Las opciones cambian según los derechos de usuario.
4	Zona de contenido. El contenido cambia en función de las opciones seleccionadas en la barra de navegación lateral.

3.3 Modo Experto

Las siguientes pestañas están disponibles en la barra de navegación lateral de la interfaz de usuario web cuando un administrador se encuentra en modo Experto.

3.3.1 Acceso

Todos los dispositivos conectados al sistema de consola se pueden ver desde el icono de Acceso.

Para ver y conectarse a dispositivos mediante la interfaz de usuario web:

1. Seleccione *Acceso* en la barra de navegación lateral. En la zona de contenido se muestra el nombre del sistema de consola y una lista de nombres o alias para todos los dispositivos instalados y configurados a los que el usuario está autorizado a acceder.
2. Seleccione *Visor serie* en la columna Acción para abrir una conexión con el puerto serie seleccionado.

   -O bien-

   Seleccione *Visor del equipo* en la columna Acción para abrir una conexión al sistema de consola.

NOTA: El visor HTML5 es el que se abre de forma predeterminada; sin embargo, si un administrador ha seleccionado el visor JNLP, aparecerá el visor de applets de Java.

3. Si no inicia sesión automáticamente, inicie sesión cuando se le solicite.

3.3.2 Herramientas del sistema

Haga clic en *Herramientas del sistema* para mostrar los iconos en los que se puede hacer clic para reiniciar o apagar el sistema de consola, actualizar el firmware del sistema de consola, guardar o restaurar su configuración o abrir una sesión de terminal con el sistema de consola.

Actualización del firmware

El sistema de consola permite el almacenamiento de dos imágenes de firmware. A medida que se actualiza el firmware, la imagen que no se está ejecutando actualmente se sobrescribirá con el nuevo firmware. El firmware más reciente se puede descargar desde el sitio web de Vertiv y el sistema de consola puede acceder a él mediante un servidor de protocolo de transferencia de archivos (FTP), de protocolo de transferencia segura de archivos (SFTP) o de protocolo de copia segura (SCP). El firmware también se puede descargar con un navegador web desde el equipo informático local del usuario.

Para ver la versión actual del firmware del sistema de consola, en la barra lateral de la pestaña Experto, haga clic en *Sistema - Información*.

Para actualizar el firmware de un sistema de consola:

1. En http://www.VertivCo.com, acceda a la sección de actualizaciones del producto y busque el firmware correspondiente para su sistema de consola.
2. Guarde el nuevo firmware en un servidor accesible mediante FTP, SFTP o SCP o en el escritorio.
3. En la barra lateral de la interfaz de usuario web del sistema de consola, haga clic en *Herramientas del sistema* y, a continuación, en *Actualizar firmware*.
4. Descargue el archivo desde el servidor que ha seleccionado en el paso 2.
    a. Haga clic en el botón de opción situado junto a la opción Servidor remoto y, a continuación, utilice el menú desplegable para seleccionar el protocolo del servidor en el que ha guardado el archivo.
    b. Introduzca la dirección IP del servidor en el que se ha guardado el firmware en el campo correspondiente.
    c. Introduzca el nombre de usuario y la contraseña para el servidor en los campos correspondientes.
    d. Introduzca el directorio de archivos en el que se ha guardado el firmware y el nombre de archivo del firmware en los campos adecuados.

    -O bien-

    Seleccione *Mi PC* para descargar el archivo desde su escritorio.

    a. Escriba el nombre de archivo del nuevo firmware o haga clic en *Examinar* para abrir una ventana y acceder al archivo.
5. Haga clic en *Descargar*. El sistema de consola descargará el firmware desde el sitio especificado y se mostrará un mensaje cuando la descarga haya finalizado.
6. Haga clic en *Instalar*.
7. Una vez que el nuevo firmware se haya instalado, reinicie el sistema de consola.

Archivos de configuración

Los administradores pueden crear una imagen de copia de seguridad de la configuración del sistema de consola. Durante la creación, no se deben realizar cambios en la configuración. La copia de seguridad del archivo de configuración puede cargarse en un servidor remoto, almacenarse en un archivo local del sistema de consola o guardarse en el equipo informático del usuario web. Los archivos de configuración se pueden guardar como un archivo comprimido, una secuencia de comandos CLI o un archivo XML.

Para guardar el archivo de configuración actual:

1. En la barra lateral de la pestaña Experto, haga clic en *Herramientas del sistema*.

2. Haga clic en *Guardar configuración*.
3. Utilice el menú desplegable para seleccionar el formato de archivo.
4. Cargue el archivo en un servidor remoto.
    a. Haga clic en el botón de opción Servidor remoto y, a continuación, use el menú desplegable para seleccionar el protocolo del servidor en el que desee guardar el archivo.
    b. Introduzca la dirección IP del servidor en el que se guardará el archivo en el campo correspondiente.
    c. Introduzca el nombre de usuario y la contraseña para el servidor en los campos correspondientes.
    d. Introduzca el directorio de archivos en el que se guardará el archivo de configuración y el nombre de archivo en los campos apropiados.

    -O bien-

    Guarde el archivo de forma local; para ello, haga clic en el botón de opción Archivo local y, a continuación, introduzca el nombre de archivo.

NOTA: El nombre de archivo puede incluir la ruta completa de la ubicación en la que se guardará el archivo. Si se especifica la ruta completa se permite que el archivo se guarde en un dispositivo de almacenamiento USB que se haya montado, por ejemplo /media/sda1/nombre de archivo. Si no se especifica la ruta completa, el archivo se guarda en /mnt/hdUser/backup/<nombre de archivo>.

    -O bien-

    Guarde el archivo en su equipo informático; para ello, haga clic en el botón de opción Mi PC. El archivo se guardará en la carpeta Descargas.

5. Haga clic en *Guardar*.

Para restaurar una configuración anterior:

1. En la barra lateral de la pestaña Experto, haga clic en *Herramientas del sistema*.
2. Haga clic en *Restaurar configuración*.
3. Restaure el archivo desde un servidor remoto.
    a. Haga clic en el botón de opción Servidor remoto y, a continuación, utilice el menú desplegable para seleccionar el protocolo del servidor en el que se guardará el archivo de configuración.
    b. Introduzca la dirección IP del servidor en el que se guardará el archivo en el campo correspondiente.
    c. Introduzca el nombre de usuario y la contraseña para el servidor en los campos correspondientes.
    d. Introduzca la ruta y el nombre de archivo del archivo de configuración.

    -O bien-

    Restaure desde un archivo local; para ello, haga clic en el botón de opción Local e introduzca el nombre del archivo.

    -O bien-

Restaure el archivo desde su equipo informático; para ello, haga clic en el botón de opción Mi PC, acceda a la ubicación en la que se guarda el archivo en el equipo informático y haga clic en *Abrir*.

4. Haga clic en *Restaurar*.

Integridad de configuración

Para garantizar la integridad de configuración, el sistema de consola permite que los administradores generen y verifiquen una firma digital (MD5) de la configuración del sistema de consola. El sistema de consola compara su valor de suma de comprobación MD5 con un valor de suma de comprobación MD5 conocido para verificar su configuración y mantenerlo protegido contra daños.

Los administradores pueden especificar una configuración en ejecución como de confianza e instruir al sistema de consola que genere una etiqueta MD5 para dicha configuración de confianza. Los administradores también pueden verificar la configuración mediante su comparación con otra configuración conocida o de confianza. El sistema de consola declarará la configuración como Sin cambiar o Modificada una vez finalizada la verificación.

La integridad de configuración funciona y se basa en los archivos de configuración guardados y restaurados del sistema de consola. También depende de la función de aprovisionamiento sin necesidad de intervención.

NOTA: Para poder utilizar la integridad de configuración, debe guardar la configuración con la opción de archivo comprimido. El formato de archivo comprimido captura más datos de configuración para garantizar la exactitud de los resultados de integridad de configuración. Si la configuración se guarda en los formatos de secuencia de comandos CLI o de archivo XML, se producirán resultados de integridad de configuración no válidos.

El sistema de consola genera una notificación de evento cada vez que se genera una etiqueta MD5. Para obtener más información sobre los eventos, consulte Lista de eventos en la página 79.

Para generar una etiqueta MD5:

1. En la barra lateral de la interfaz de usuario web del sistema de consola, haga clic en *Herramientas del sistema* y, a continuación, haga clic en *Integridad de configuración*.
2. Haga clic en el botón de opción Generar etiqueta MD5 para la configuración en ejecución y haga clic en *Ejecutar*.
3. La etiqueta MD5 generada se muestra en la pantalla como un valor hexadecimal de 32 caracteres y también se guarda en el sistema de consola como el valor con el que realizar comparaciones posteriores. Los administradores pueden cortar y pegar esta cadena para usarla en otros sistemas.

Para verificar una etiqueta MD5:

1. En la barra lateral de la interfaz de usuario web del sistema de consola, haga clic en *Herramientas del sistema* y, a continuación, haga clic en *Integridad de configuración*.
2. Haga clic en el botón de opción Verificar configuración en ejecución.
3. Deje el campo MD5 en blanco para verificar la configuración en ejecución.

   -O bien-

   Introduzca una cadena de suma de comprobación MD5 para verificar una configuración conocida.

4. Haga clic en *Ejecutar*.

Certificado HTTPS

Puede generar un certificado autofirmado nuevo o descargar un certificado firmado al dispositivo desde un servidor FTP o desde su escritorio.

Para generar un nuevo certificado autofirmado:

1. En la barra lateral de la pestaña Experto, haga clic en *Herramientas del sistema*.
2. Haga clic en *Generar/descargar certificado*.
3. Para generar un nuevo certificado, haga clic en el botón de opción situado que hay al lado de Generar certificado autofirmado e introduzca la información deseada en los campos del certificado autofirmado: País, Estado/Provincia, Ciudad/Localidad, Organización, Unidad de organización, Nombre común, Dirección de correo electrónico y Comentario de Netscape.

   -O bien-

   Para descargar un certificado firmado desde un servidor FTP, SFTP o SCP, haga clic en el botón de opción que hay al lado de Servidor remoto e introduzca toda la información sobre el servidor: Dirección IP, nombre de usuario, contraseña, directorio de archivos y nombre de archivo.

   -O bien-

   Para descargar un certificado desde su escritorio, haga clic en el botón de opción junto a Descargar certificado desde mi equipo informático, haga clic en *Elegir archivo* o *Examinar* para acceder a la ubicación en la que se ha guardado el archivo y haga clic en *Abrir*.
4. Haga clic en *Generar/descargar*. Se mostrará la información del certificado.
5. Haga clic en *Aplicar*. Aparece el mensaje *Al aplicar el certificado nuevo finalizarán todas las sesiones HTTP/HTTPS. Será necesario reiniciar el navegador. ¿Está seguro de que desea continuar?*
6. Haga clic en *Aceptar* para continuar. El certificado se guardará y el navegador se reiniciará para poder usar el nuevo certificado.

NOTA: Se cerrarán todas las sesiones http/https y el usuario deberá restablecer la conexión.

3.3.3 Sistema

Haga clic en *Sistema* para mostrar información sobre el sistema de consola y permitir que los administradores configuren los parámetros de sistema del sistema de consola. Las siguientes pestañas se muestran en Sistema, en la barra de navegación lateral.

Seguridad

Perfil de seguridad

Un perfil de seguridad determina qué servicios están activados en el sistema de consola.

Durante la configuración inicial, el administrador del sistema de consola debe configurar los parámetros de seguridad para que se ajusten a la política de seguridad del sitio. Las siguientes características de seguridad se pueden configurar en la interfaz de usuario web, la CLI o el software DSView:

- Configurar el tiempo de espera de inactividad de la sesión
- Activar o desactivar RPC
- Activar o desactivar la detección de dispositivos conectables, dispositivos de almacenamiento y sensores de 1 cable
- Posibilidad de configurar el acceso de puerto serie para todos los usuarios, o permitir la configuración de autorizaciones para grupos y para usuarios específicos para restringir el acceso
- Seleccione un perfil de seguridad, que defina:
  - Los servicios activados (FTP, TFTP, ICMP, IPSec, SNMP y Telnet)
  - El acceso SSH y HTTP/HTTPS
  - La activación o desactivación de la recuperación de la configuración de Bootp, la interfaz de Bootp y la activación o desactivación de la configuración en vivo

El administrador puede seleccionar un perfil de seguridad preconfigurado o crear un perfil personalizado.

Todos los servicios y las opciones de configuración de SSH y HTTP/HTTPS que están activadas y desactivadas para cada perfil de seguridad se muestran en las páginas Asistente - Seguridad y Sistema - Seguridad - Perfil de seguridad.

Para configurar un perfil de seguridad:

1. Seleccione *Sistema - Seguridad - Perfil de seguridad*.
2. En el campo Tiempo de espera de inactividad, introduzca el número de segundos que deben transcurrir antes de que se agote el tiempo de espera de las sesiones abiertas en el sistema de consola.

NOTA: Este valor se aplica a cualquier sesión de usuario hacia el equipo a través de HTTP, HTTPS, SSH, Telnet o el puerto CONSOLE. No sobrescribirá el valor configurado para el grupo de autorización del usuario. El nuevo tiempo de espera de inactividad se aplicará únicamente a las nuevas sesiones.

3. En la sección Servicios activados, active o desactive la casilla de verificación *RPC*.
4. En la sección Dispositivos conectables, active o desactive la detección de dispositivos conectables para dispositivos USB y SD. Si están activados, el almacenamiento USB y la tarjeta SD se pueden desactivar para restringir el tipo de dispositivos conectables por motivos de seguridad. Los sensores de 1 cable también se pueden desactivar en esta sección.

NOTA: Estas opciones aparecen en todos los modelos de sistema de consola, aunque algunos modelos no disponen de tarjeta SD ni puertos para sensor de 1 cable. Si su modelo no dispone de estos puertos, deje estas opciones desactivadas.

NOTA: La desactivación de la detección de dispositivos conectables o el cambio del ajuste del dispositivo de almacenamiento solo serán efectivos después de reiniciar.

5. En el encabezado Dispositivos serie, seleccione si el acceso a los puertos está controlado por la autorización de los usuarios y de los grupos o si la configuración de acceso a los puertos se aplica a todos los usuarios.
6. En el encabezado Recuperación de la configuración de Bootp, active o desactive el servicio.
7. Active/desactive la autenticación SSH mediante nombre de usuario/contraseña.
8. Seleccione la casilla de verificación *Personalizado*, *Moderado*, *Abierto* o *Seguro* en el encabezado Perfil de seguridad.
9. Haga clic en *Guardar*.

Módulo FIPS

El sistema de consola incorpora un módulo criptográfico basado en el módulo criptográfico validado por FIPS 140-2 (número de certificado 1747) que se ejecuta en una plataforma ARM de Linux.

Si un administrador activa el módulo FIPS, el sistema de consola utilizará el módulo de objetos FIPS para realizar operaciones de cifrado. El módulo FIPS está desactivado de forma predeterminada.

Cuando el módulo FIPS esté activado, en la página Supervisión - Modo FIPS se mostrará qué servicio (SSHv2, HTTPS, SNMPv3 y ADSAP2) se encuentra en modo FIPS. Todas las funciones de seguridad y algoritmos criptográficos usados por el servicio se realizan en modo aprobado FIPS 140-2.

Para activar el módulo FIPS:

1. Seleccione *Sistema - Seguridad - FIPS 140*.
2. Marque la casilla para activar el módulo FIPS 140-2 y haga clic en *Guardar*.

El sistema de consola se reiniciará automáticamente. Durante el reinicio, el sistema de consola borrará las claves SSH, actualizará la configuración de los archivos HTTPD, SSHD, ADSAP2d y SNMPD y comprobará la integridad del módulo de objetos FIPS. Una vez que se haya completado el reinicio, el sistema de consola solo aceptará las conexiones SSH y HTTPS que usen cifrados aprobados por FIPS.

Cuando FIPS está activado, se aplican las siguientes restricciones:

Para sesiones SSH:

- Triple-DES CBS y AES 128/192/256 son los únicos cifrados que se aceptarán.
- HMAC-SHA1 y HMAC-SHA1-96 son los únicos algoritmos de integridad de mensajes que se aceptarán.
- Solo se aceptarán claves RSA de 1024 a 16384 bits.

Las sesiones HTTPS solo aceptarán el protocolo SSL v 3.1(TLSv1) para establecer el túnel SSL con uno de los siguientes cifrados:

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

Las solicitudes de SNMP versión 3 se aceptarán cuando la autenticación sea SHA y el cifrado sea AES.

Seguridad del software DSView

También puede configurar los ajustes de seguridad del software DSView. Cuando el sistema de consola esté gestionado por el software DSView, el servidor de DSView suministrará el certificado al sistema de consola. En condiciones normales, el software DSView gestionará el certificado para borrarlo y sustituirlo por un nuevo certificado, según sea necesario. Si se interrumpe la comunicación con el software DSView, el servidor de DSView no podrá borrar el certificado y no se podrá utilizar el sistema de consola. Haga clic en el botón *Borrar certificado de DSView* para configurar el sistema de consola en modo Confiar en todos.

Para configurar los ajustes de seguridad del software DSView:

1. Seleccione *Sistema - Seguridad - DSView*.
2. Haga clic en la casilla de verificación *Permitir que el equipo esté gestionado por DSView* y en *Guardar*.

Fecha y hora

El sistema de consola ofrece dos opciones para configurar la fecha y la hora. Puede recuperar la fecha y la hora a partir de un servidor de protocolo de tiempo de redes (NTP) o puede configurar la fecha y hora manualmente para que se utilice el reloj interno del sistema de consola para proporcionar información de fecha y hora.

NOTA: La hora actual que se muestra en la pantalla Fecha y hora solo indica la hora a la que se abrió la pantalla. No se sigue actualizando en tiempo real.

Para configurar la hora y la fecha con NTP:

1. Haga clic en *Sistema - Fecha y hora*.
2. Seleccione *Activar protocolo de tiempo de redes*.
3. Acceda al sitio del servidor NTP que desee y haga clic en *Guardar*.

Para configurar la hora y la fecha manualmente:

1. Haga clic en *Sistema - Fecha y hora*.
2. Seleccione *Definir manualmente*.
3. Use los menús desplegables para seleccionar la fecha y la hora necesarias y haga clic en *Guardar*.

Para definir la zona horaria mediante una zona horaria predefinida:

1. Haga clic en *Sistema - Fecha y hora - Zona horaria*.
2. Seleccione *Predefinida*.
3. Seleccione la zona horaria necesaria en el menú desplegable y haga clic en *Guardar*.

Para definir ajustes de zona horaria predefinidos:

1. Haga clic en *Sistema - Fecha y hora - Zona horaria*.
2. Seleccione *Definir zona horaria*.
3. Introduzca el nombre de la zona horaria y el acrónimo de hora estándar que desee.
4. Introduzca el desplazamiento de GMT.
5. Seleccione *Activar horario de verano*, si es necesario.
6. Seleccione o introduzca los valores necesarios de configuración de horario de verano y haga clic en *Guardar*.

Ayuda e idioma

Haga clic en *Sistema - Ayuda e idioma* y utilice el menú desplegable para seleccionar el idioma del sistema de consola.

NOTA: La opción de idioma se aplica a las sesiones SSH, Telnet y de puerto de consola hacia el sistema de consola. El idioma del navegador viene determinado por el propio navegador.

Ayuda en línea

Cuando la función de ayuda en línea se ha configurado para el sistema de consola, al hacer clic en el botón *Ayuda* desde cualquier formulario de la interfaz de usuario web, se abre una nueva ventana y su contenido se redirige a la ruta configurada para la documentación del producto de ayuda en línea.

Introduzca la URL completa de la ayuda en línea, acabada en /index.html, en el servidor web local en el campo URL de la ayuda en línea. Haga clic en *Guardar*.

NOTA: No siempre es posible usar la función de ayuda en línea desde el servidor de Vertiv debido a las configuraciones de firewall, ni tampoco se recomienda. Por norma general, es recomendable que utilice el sistema de ayuda en línea que se proporciona con el producto o que descargue el archivo .zip de la ayuda en línea y que lo ejecute desde un servidor local.

El administrador del sistema puede descargar la ayuda en línea desde Vertiv™. Para obtener más información sobre la descarga de la ayuda en línea, póngase en contacto con el servicio de asistencia técnica.

Una vez que se ha obtenido el archivo de la ayuda en línea (en formato zip), los archivos deben extraerse y colocarse en un directorio seleccionado por el usuario en el directorio raíz del servidor web. El servidor web debe ser accesible públicamente.

General

Haga clic en *Sistema - General* para crear una pancarta de inicio de sesión o seleccionar el tipo de visor.

Pancarta de inicio de sesión:

Los administradores pueden configurar una pancarta de inicio de sesión para que se muestre cuando un usuario inicie una sesión SSHv2, Telnet, de consola o de la interfaz de usuario web.

Para crear una pancarta de inicio de sesión:

1. *Haga clic en Sistema - General* en la barra de navegación lateral.
2. Marque la casilla para activar la pancarta de inicio de sesión.
3. Introduzca el texto que desee que se muestre al iniciar sesión en el campo Pancarta de inicio de sesión y haga clic en *Guardar*.

Visor serie

De forma predeterminada, el sistema de consola utiliza un visor serie HTML5 básico. También es compatible con un visor serie Java más robusto. Un administrador puede configurar qué visor serie se usará para los puertos serie y el sistema de consola.

NOTA: El visor serie HTML5 admite un máximo de 10 sesiones por puerto con un límite de 48 sesiones en total.

Para configurar el visor serie:

1. Haga clic en *Sistema - General* en la barra de navegación lateral.
2. Seleccione el visor HTML5 o el visor JNLP y, a continuación, haga clic en *Guardar*.

Visor serie Java

NOTA: Se recomienda Java 1.8.0.91 o posterior. Debe tener la versión de 32 bits instalada para poder ejecutar el visor serie.

En la siguiente tabla se describen los botones disponibles en el applet Java.

Tabla 3.2 Botones del applet Java para conectarse al sistema de consola

Botón	Función
Enviar interrupción	Para enviar una interrupción al terminal
Desconectar	Para desconectarse del applet Java

NOTA: Puede que sea necesario desactivar el bloqueador de ventanas emergentes del navegador del cliente para poder usar los visores serie o del equipo.

NOTA: Cuando se ejecute el visor, puede que el navegador pida permiso para ejecutar la aplicación Mindterm. Es necesario conceder este permiso para que se ejecute el applet del visor.

Configuración de arranque

La configuración de arranque define la ubicación desde la cual el sistema de consola carga el sistema operativo. El sistema de consola puede arrancar desde su firmware interno o desde la red. De forma predeterminada, el sistema de consola arranca desde el firmware interno presente en la memoria Flash. Si hace clic en *Sistema - Configuración de arranque*, aparecerá la pantalla Configuración de arranque.

Si necesita arrancar desde la red, asegúrese de que se cumplan los siguientes prerrequisitos:

- Debe haber un servidor TFTP disponible en la red
- Se debe descargar un archivo de firmware desde Vertiv y dicho archivo debe estar disponible en el servidor TFTP
- Se conoce el nombre de archivo de arranque y la dirección IP del servidor TFTP

Para configurar la configuración de arranque:

1. Haga clic en *Sistema - Configuración de arranque*.
2. En Modo de arranque, seleccione *Desde la flash*y, a continuación, *Imagen 1* o *Imagen 2*.

   -O bien-

   Seleccione *Desde la red* e introduzca la información siguiente:

   - Dirección IP del equipo: Introduzca la dirección IP fija o una dirección IP asignada por DHCP al sistema de consola.
   - Dirección IP del servidor TFTP: Introduzca la dirección IP del servidor de arranque TFTP.
   - Nombre de archivo: Introduzca el nombre de archivo del firmware de arranque.
3. Use el menú desplegable para seleccionar si el temporizador de vigilancia está activado. Si el temporizador de vigilancia está activado, el sistema de consola se reinicia si se produce un bloqueo del software.
4. Use el menú desplegable para seleccionar la velocidad del puerto de consola y haga clic en *Guardar*.

Información

Haga clic en *Sistema - Información* para ver la información sobre la identidad, las versiones, la alimentación y la CPU del sistema de consola.

Uso

Haga clic en *Sistema - Uso* para ver el uso de memoria y flash.

3.3.4 Red

Haga clic en *Red* para ver y configurar las opciones de red de nombre de host, DNS, IPv6, vinculación, rutas estáticas de IPv4 e IPv6, hosts, firewall, IPSec (VPN) y SNMP.

Ajustes

Haga clic en *Red - Ajustes* para modificar los ajustes de red configurados.

En esta página, un administrador puede configurar el nombre de host y la configuración de DNS del sistema de consola, lo que incluye el DNS principal y secundario, el dominio y las direcciones de búsqueda. Los administradores también pueden activar IPv6 y configurarlo para obtener el DNS y/o el dominio desde DHCPv6.

Para disponer de una configuración de red tolerante a fallos, se puede seleccionar la opción Vinculación para combinar eth0 y eth1 en una sola interfaz de red de alta disponibilidad mediante el uso del modo de vinculación de reserva activa. La interfaz eth0 es la interfaz activa normal con eth1 como reserva; si la señal portadora se interrumpe en eth0, eth1 se convierte en la interfaz activa. La dirección MAC de eth0 se usa siempre en modo de vinculación, independientemente de la interfaz que esté activa.

NOTA: Después de activar o desactivar la vinculación, debe reiniciar el sistema de consola para que el cambio surta efecto.

Tipo de enrutamiento

El sistema de consola admite tablas de enrutamiento múltiple para un enrutamiento de políticas flexible. Las tablas de enrutamiento múltiple no se pueden activar al mismo tiempo que la conmutación por error de red o si la vinculación está activa.

Para activar tablas de enrutamiento múltiple:

1. Haga clic en *Red - Ajustes*.
2. En Enrutamiento múltiple, haga clic en el botón de opción Activar tablas de enrutamiento múltiples IPv4.

Conmutación por error de la red

Para garantizar que un sistema de consola se pueda utilizar para proporcionar acceso a dispositivos vitales durante una interrupción de la red, dicho sistema se debe configurar para la función de conmutación por error de la red. La conmutación por error se puede producir cuando una interfaz primaria se vuelve inactiva o cuando una IP/puerta de enlace determinada se vuelve inaccesible. La función de conmutación por error se puede activar mediante una conexión de red secundaria o PPP (marcado de salida). Si el marcado de salida se ha configurado, PPP0 estará disponible como interfaz secundaria pero no se podrá utilizar como la interfaz primaria.

El uso del software DSView con un sistema de consola garantizará que el sistema de consola siempre pueda estar accesible cuando se encuentre en una situación de conmutación por error, ya que el sistema de consola "llamará a casa" y actualizará su dirección IP en el software DSView.

En la página Red - Ajustes, los administradores pueden configurar una interfaz de red secundaria que se utilizará para la función de conmutación por error. La interfaz primaria establece la puerta de enlace predeterminada del sistema, mientras que la interfaz secundaria se usa cuando la interfaz primaria no está disponible. Los administradores también pueden seleccionar uno de los cuatro desencadenadores que activan la función de conmutación por error:

- Interfaz primaria inactiva
- Puerta de enlace predeterminada primaria inaccesible
- DSView inaccesible
- Dirección IP inaccesible

Si el túnel IPSec se ha configurado (consulte IPSec (VPN) en la página 34), los administradores pueden configurar el túnel IPSec que se establecerá a través de la interfaz secundaria cuando esté activa.

Para activar la conmutación por error de la red:

1. En la barra lateral de la pestaña Experto haga clic en *Red - Ajustes*.
2. En el encabezado Enrutamiento, haga clic en el botón de opción para activar la conmutación por error de la red.
3. Utilice los menús desplegables para seleccionar las interfaces primarias y secundarias, además del nombre de la conexión VPN.
4. Haga clic en el botón de opción situado junto al desencadenador que desee utilizar para iniciar la conmutación por error.
5. Haga clic en *Guardar*.

También puede configurar la conmutación por error mediante el módem móvil, en los modelos que incorporan uno. Para obtener más información, consulte Uso del módem móvil en la conmutación por error en la página 62.

NOTA: Puede usarse la opción móvil para una conmutación por error si no está ya siendo usada como interfaz primaria.

Dispositivos

Un administrador puede seleccionar, activar y configurar las direcciones IP asignadas a las interfaces de red y ver la dirección MAC. Además de las dos interfaces Ethernet estándar, en la lista de interfaces de red se incluye una entrada para cualquier dispositivo Ethernet USB que pueda haberse instalado.

Para configurar un dispositivo de red:

1. Seleccione *Red - Dispositivos*. Aparecerá la pantalla Dispositivos con una lista de interfaces de red y su estado (activado o desactivado).
2. Haga clic en el nombre del dispositivo de red que desee configurar.
3. Marque la casilla si desea configurar el dispositivo de red como interfaz primaria. De forma predeterminada, eth0 se configura como interfaz primaria.
4. Seleccione el estado (*Activado* o *Desactivado*) en el menú desplegable.
5. Seleccione una de las siguientes opciones de método IPv4:
   - Seleccione *DHCP* para que el servidor DHCP defina la dirección IP IPv4.

- Seleccione *Subred* para introducir la dirección IPv4, la máscara de subred y la dirección de puerta de enlace manualmente.
- Seleccione *Dirección IPv4 no configurada* para desactivar IPv4.

6. Seleccione una de las siguientes opciones de método IPv6:
   - Seleccione *Sin estado* si el enlace está restringido a la dirección IP local.
   - Seleccione *DHCPv6* para que el servidor DHCP defina la dirección IP IPv6.
   - Seleccione *Estático* para introducir la dirección IPv6 y la longitud del prefijo manualmente.
   - Seleccione *Dirección IPv6 no configurada* para desactivar IPv6.

NOTA: La dirección MAC del dispositivo se mostrará después de esta opción.

Rutas estáticas IPv4 y IPv6

Para añadir rutas estáticas:

1. Seleccione *Red - Rutas estáticas IPv4* o *Rutas estáticas IPv6*. Se muestran todas las rutas estáticas existentes con sus valores de IP de destino/máscara, puerta de enlace, interfaz y métrica.
2. Haga clic en *Añadir*.
3. Seleccione *Predeterminado* para configurar la ruta predeterminada.

   -O bien-

   Seleccione *IP de host o red* para introducir ajustes personalizados para la opción IP de destino/máscara.

   Introduzca la información necesaria sobre IP de destino/bits de máscara con la sintaxis <IP de destino>/<CIDR> en el campo IP de destino/bits de máscara.
4. Introduzca la dirección IP de la puerta de enlace en el campo Puerta de enlace.
5. Introduzca el nombre de la interfaz (Eth0, Eth1 o PPPx) en el campo Interfaz cuando la ruta sea por interfaz.
6. Introduzca el número de saltos al destino en el campo Métrica y, a continuación, haga clic en *Guardar*

Hosts

Los administradores pueden configurar una tabla de nombres de host, direcciones IP y alias de host para la red local.

Para añadir un host:

1. Seleccione *Red - Hosts*.
2. Haga clic en *Añadir* para añadir un nuevo host.
3. Introduzca la dirección IP, el nombre de host y el alias del host que desee añadir y, a continuación, haga clic en *Guardar*.

Para editar un host:

1. Seleccione *Red - Hosts*.

2. Haga clic en la dirección IP del nombre de host que desee editar.
3. Introduzca un nuevo nombre y alias de host, si es pertinente y, a continuación, haga clic en *Guardar*.

Firewall

Los administradores pueden configurar el sistema de consola para que actúe como un firewall. De forma predeterminada, tres cadenas incorporadas aceptan todos los paquetes de ENTRADA, REENVÍO y SALIDA. Seleccione los botones *Añadir*, *Eliminar* o *Cambiar política* para añadir una cadena de usuario, eliminar cadenas añadidas por el usuario y cambiar la política de cadenas integrada. La política de las cadenas predeterminadas se puede modificar (Cambiar política) para aceptar o prohibir, pero dichas cadenas no se pueden eliminar. Si hace clic en el *Nombre de cadena* podrá configurar las reglas de las cadenas.

La configuración del firewall está disponible al hacer clic en *Red - Firewall*. Se accede a pantallas de configuración separadas pero idénticas desde las opciones de menú *Tabla de filtros IPv4* o *Tabla de filtros IPv6*.

En las cadenas predeterminadas solo se puede editar su política; las opciones de política de las cadenas predeterminadas son ACEPTAR y PROHIBIR.

Cuando se añade una cadena, solo se crea una entrada con nombre para dicha cadena. Se deben configurar una o más reglas para una cadena después de que esta se haya añadido.

Configuración del firewall

Para cada regla, se debe seleccionar una acción (*ACEPTAR, PROHIBIR, REGISTRAR, RECHAZAR o VOLVER*) en el menú desplegable Destino. La acción seleccionada se realiza en un paquete IP que coincida con todos los criterios especificados en la regla.

Si la opción *REGISTRO* se selecciona en el menú desplegable Destino, el administrador puede configurar un nivel de registro y un prefijo de registro.

Si se selecciona *RECHAZAR* en el menú desplegable Destino, el administrador puede seleccionar una opción en el menú desplegable Rechazar con; el paquete se prohíbe y se envía un paquete de respuesta del tipo seleccionado.

Opciones de protocolo

Se activan diferentes campos para cada opción del menú desplegable Protocolo.

Si se selecciona *Numérico* en el menú Protocolo, introduzca un Número de protocolo en el campo de texto.

Si se selecciona *TCP* en el menú Protocolo, se activa una sección de opciones de TCP en la que se pueden introducir puertos de origen y de destino e indicadores TCP.

Si se selecciona *UDP* en el menú Protocolo, se activa la sección UDP en la que se pueden introducir puertos de origen y de destino.

Tabla 3.3 Configuración del firewall - Campos de opciones de TCP y UDP

Campo/opción de menú	Definición
Puerto de origen o Puerto de destino	Una sola dirección IP o un intervalo de direcciones IP.
Indicadores TCP	[Solo TCP] SYN (sincronizar), ACK (confirmar), FIN (finalizar), RST (restablecer), URG (urgente) y PSH (insertar). Las condiciones en el menú desplegable para cada indicador son: Cualquiera, Definir o Sin definir.

Si se selecciona ICMP en el menú Protocolo, se activa el menú desplegable Tipo de ICMP.

Si un administrador introduce la interfaz Ethernet (eth0 o eth1) en los campos de interfaz de entrada o de salida y selecciona una opción (*Segundos paquetes y posteriores*, *Todos los paquetes y fragmentos* o *Paquetes no fragmentados y primeros paquetes*) en el menú desplegable Fragmentos, la acción de destino se realiza en paquetes desde o hacia la interfaz especificada si cumplen los criterios de la opción seleccionada del menú Fragmentos.

Para añadir una cadena:

1. Seleccione *Red - Firewall*.
2. Seleccione *Tabla de filtros IPv4* o *Tabla de filtros IPv6* según sea necesario.
3. Haga clic en *Añadir*.
4. Introduzca el nombre de la cadena que desee añadir.
5. Haga clic en *Guardar*.

NOTA: No se permiten espacios en el nombre de la cadena.

6. Agregue una o más reglas para completar la configuración de la cadena.

Para cambiar la política de una cadena predeterminada:

NOTA: Las cadenas definidas por el usuario no se pueden editar. Para cambiar el nombre de una cadena añadida por el usuario, elimínela y cree una cadena nueva.

1. Seleccione *Red - Firewall*.
2. Seleccione *Tabla de filtros IPv4* o *Tabla de filtros IPv6* según sea necesario.
3. Seleccione la casilla de verificación situada al lado del nombre de la cadena que desee cambiar (*REENVÍO*, *ENTRADA*, *SALIDA*).
4. Haga clic en *Cambiar política* y seleccione *Aceptar* o *Prohibir* en el menú desplegable.
5. Haga clic en *Guardar*.

Para añadir una regla:

1. Seleccione *Red - Firewall*.
2. Seleccione *Tabla de filtros IPv4* o *Tabla de filtros IPv6* según sea necesario.
3. En la lista de cadenas, haga clic en el nombre de la cadena a la que desea añadir una regla.
4. Haga clic en *Añadir* y configure la regla según sea necesario; a continuación, haga clic en *Guardar*.

Para editar una regla:

1. Seleccione *Red - Firewall*.

2. Seleccione *Tabla de filtros IPv4* o *Tabla de filtros IPv6* según sea necesario.
3. En la lista de cadenas, haga clic en el nombre de la cadena con la regla que desee editar.
4. Seleccione la regla que desee editar y haga clic en *Editar*.
5. Modifique la regla según sea necesario y haga clic en *Guardar*.

IPSec (VPN)

Una red privada virtual (VPN) permite una comunicación segura entre el sistema de consola y una red remota por medio del uso de una puerta de enlace y la creación de una conexión segura entre el sistema de consola y la puerta de enlace. El protocolo IPSec se utiliza para establecer el túnel seguro y proporciona servicios de cifrado y autenticación en el nivel IP de la pila de protocolo.

Con un sistema de consola ubicado en una red separada detrás de un enrutador, se establece un túnel IPSec con un certificado x.509 para un firewall. Una autoridad de certificación (CA) se encarga de distribuir los certificados y claves al firewall y al sistema de consola.

NOTA: El sistema de consola admite un certificado por túnel. No se admiten varios certificados. No se admiten túneles IPv6. Los certificados (en formato PKCS 12) se pueden cargar desde el menú Herramientas del sistema.

NOTA: Para ejecutar IPSec (VPN), debe activar IPSec en el perfil de seguridad personalizado.

La puerta de enlace remota se conoce como el host remoto o derecho y el sistema de consola se conoce como el host local o izquierdo.

Creación de un certificado de autorización

Para configurar el firewall Fortigate de Fortinet, debe crear un servidor de certificado de autorización (CA) interno que genere certificados de RSA que el sistema de consola utiliza para la autenticación.

Para obtener información sobre la creación de un CA en un servidor Ubuntu®, consulte Creación de un CA.

Creación de un túnel en el servidor

Para crear un túnel en el servidor:

1. En la pestaña *Sistema* de la interfaz de usuario web de Fortigate, haga clic en *Certificados* e importe el certificado de CA y el certificado de SERVIDOR que se generó desde el servidor easy-rsa.
2. En la pestaña *Usuario y dispositivo*, haga clic en *PKI* y cree un nuevo usuario con el nombre usuario1 con un CA con el nombre CA_Cert_1. A continuación, cree un grupo de usuarios con el nombre grupo_usuarios1 y coloque al usuario1 en ese grupo.
3. En la pestaña *VPN* , haga clic en *IPSec - Túneles* y cree un nuevo túnel VPN personalizado con la configuración siguiente; a continuación, haga clic en *Aceptar*.

Tabla 3.4 Parámetros de configuración del túnel VPN

Parámetro	Valor
Red	
Puerta de enlace remota	Usuario de acceso telefónico
Interfaz	wan1
Configuración de modo	Activado
Versión de IP	IPv4
Intervalo de direcciones de cliente	10.77.20.100-10.77.20.110
Máscara de subred	255.255.255.0
Usar DNS del sistema	Activado
Activar túnel dividido de IPv4	Activado
Redes accesibles	lan_local
NAT Traversal	Activado
Frecuencia de Keepalive	300
Detección de pares muertos	Activado
Autenticación	
Método	Firma
Nombre del certificado	servidor
Versión de IKE	2
Tipos de aceptación de opciones de pares	Grupo de certificados de pares
Grupo de certificados de pares	grupo_usuarios1
Propuesta de fase 1	
Cifrado	AES128
Autenticación	SHA1
Grupo Diffie-Hellman	14
Duración de la clave (segundos)	86400
Identificador local	C=<país> S=<estado> L=<ciudad> O=<organización>
Fase 2 de edición	
Nombre	<nombre>
Comentarios	<comentarios>
Subred de dirección local	0.0.0.0/0.0.0.0
Subred de dirección remota	0.0.0.0/0.0.0.0
Propuesta de fase 2	
Cifrado	AES128
Autenticación	SHA1
Activar detección de reproducción	Activado
Activar confidencialidad directa total (PFS)	Activado

Tabla 3.4 Parámetros de configuración del túnel VPN (continuación)

Parámetro	Valor
Grupo Diffie-Hillman	14
Todos los puertos locales	Activado
Todos los puertos remotos	Activado
Todos los protocolos	Activado
Función Keep Alive de Autokey	Activado
Duración de la clave	Segundos
Segundos	43200

4. En la pestaña *Política y objetos*, haga clic en *Objetos - Direcciones* para crear un intervalo de VPN con los ajustes siguientes; a continuación, haga clic en *Aceptar*.

Tabla 3.5 Configuración de intervalo de VPN

Parámetro	Valor
Nombre	intervalo_vpn_ipsec
Tipo	Intervalo IP
Subred/intervalo IP	10.77.20.100 - 10.77.20.110
Interfaz	Cualquiera
Mostrar en lista de direcciones	Activado
Comentarios	La dirección IP que se proporciona a los clientes de VPN que se conectan.

5. En la pestaña *Política y objetos*, haga clic en *Objetos - Direcciones* para crear un intervalo de LAN local con los ajustes siguientes; a continuación, haga clic en *Aceptar*.

Tabla 3.6 Configuración de intervalo de LAN local

Parámetro	Valor
Nombre	lan_local
Tipo	IP/máscara de red
Subred/intervalo IP	192.168.1.0 / 255.255.255.0
Interfaz	Interno
Mostrar en lista de direcciones	Activado
Comentarios	Lan local - Dentro de la red

6. En la pestaña *Política y objetos*, haga clic en *Política - IPv4* para crear una política de firewall 1 con los ajustes siguientes; a continuación, haga clic en *Aceptar*.

Tabla 3.7 Configuración de la política de firewall 1

Parámetro	Valor
Interfaz entrante	forti2acs
Dirección de origen	intervalo_vpn_ipsec
Interfaz saliente	Interno
Dirección de destino	lan_local
Programa	Siempre
Servicio	TODOS
Acción	ACEPTAR
Opciones de red/firewall	
NAT	ACTIVADO
Usar la dirección de la interfaz saliente	Activado
Perfiles de seguridad	
Antivirus, filtro web, control de aplicaciones e inspección SSL	Todos DESACTIVADOS
Conformación del tráfico	
Conformador compartido, conformador inverso y conformador por IP	Todos DESACTIVADOS
Opciones de registro	
Registrar tráfico permitido	ACTIVADO
Eventos de seguridad	Activado
Comentarios	<Comentarios>
Activar esta política	Activado

7. En la pestaña *Política y objetos*, haga clic en *Política - IPv4* para crear una política de firewall 2 con los ajustes siguientes; a continuación, haga clic en *Aceptar*.

Tabla 3.8 Configuración de la política de firewall 2

Parámetro	Valor
Interfaz entrante	Interno
Dirección de origen	lan_local
Interfaz saliente	forti2acs
Dirección de destino	intervalo_vpn_ipsec
Programa	Siempre
Servicio	TODOS
Acción	ACEPTAR
Opciones de red/firewall	
NAT	ACTIVADO
Usar la dirección de la interfaz saliente	Activado
Perfiles de seguridad	
Antivirus, filtro web, control de aplicaciones e inspección SSL	Todos DESACTIVADOS
Conformación del tráfico	
Conformador compartido, conformador inverso y conformador por IP	Todos DESACTIVADOS
Opciones de registro	
Registrar tráfico permitido	ACTIVADO
Eventos de seguridad	Activado
Comentarios	<Comentarios>
Activar esta política	Activado

8. En la pestaña *Política y objetos*, haga clic en *Política - IPv4* para crear una política de firewall 3 con los ajustes siguientes; a continuación, haga clic en *Aceptar*.

Tabla 3.9 Configuración de la política de firewall 3

Parámetro	Valor
Interfaz entrante	Cualquiera
Dirección de origen	Todos
Interfaz saliente	Cualquiera
Dirección de destino	Todos
Acción	DENEGAR
Opciones de registro	
Registrar tráfico de infracciones	DESACTIVADO

Creación de un túnel en el sistema de consola

Para crear un túnel en el sistema de consola:

1. En la barra lateral de la pestaña *Experto* , haga clic en *Red - IPSec (VPN)* y, a continuación, en *Añadir*.

2. Introduzca un nombre para la conexión.
3. Use los menús desplegables para seleccionar *IKEv2* para la versión de IKE e *Iniciar*, *Añadir*o *Ignorar* para la Acción de inicio.
    a. Iniciar: Carga una conexión y la pone en marcha de inmediato (arranque o tras guardar la configuración).
    b. Añadir: Carga una conexión sin iniciarla. Por ejemplo, la VPN puede iniciarse de forma condicional con una secuencia de comandos.
    c. Ignorar: Ignora la conexión.
4. Para el lado remoto (derecho), introduzca los siguientes parámetros:
    a. Deje el campo Identificador en blanco.
    b. Introduzca la dirección IP de la VPN remota en el campo Dirección IP.
    c. En el campo Subred, introduzca la subred que el sistema de consola utilizará para conectarse.
5. Para el lado local (izquierdo), introduzca los siguientes parámetros:
    a. Deje el campo Identificador en blanco.
    b. Introduzca la dirección IP de la interfaz primaria en el campo Dirección IP.

NOTA: La interfaz primaria es la interfaz (eth0 o eth1) empleada para conectar con el firewall remoto. De forma predeterminada, el ajuste es eth0 y está activada la Recuperación de la configuración de Bootp. Su interfaz primaria es eth1; compruebe que la opción Recuperación de la configuración de Bootp de la página Perfil de seguridad esté desactivada.

6. Haga clic en el botón de opción Certificado RSA, haga clic en la flecha desplegable de los archivos locales de PKCS12 y seleccione el archivo PKCS12.

Para activar IPSec en el sistema de consola:

1. En la barra lateral de la pestaña *Experto* , haga clic en *Sistema - Seguridad - Perfil de seguridad*.
2. Haga clic en el botón de opción Personalizado en Perfil de seguridad.
3. Marque la casilla Activar IPSec y, a continuación, haga clic en *Guardar*.

NOTA: Después de hacer clic en el botón Guardar, la conexión de la VPN se inicia automáticamente si la acción de inicio es Iniciar. La información se guarda y se inicia la VPN (o se reinicia).

Verificación

Se pueden realizar pruebas de verificación para asegurarse de que la configuración de IPSec se haya realizado correctamente. El comando ping se usa para comprobar la comunicación.

Para verificar el estado de IPSec y comprobar la comunicación:

1. Inicie sesión en el sistema de consola como raíz.
2. Compruebe el estado de IPSec. Para ello, introduzca el comando *ipsec status* en el símbolo del sistema del shell. Anote la dirección IP DHCP de VPN.
3. Introduzca ping en la ventana de comando, pulse la barra de espacio, introduzca la dirección a la que desea hacer el ping y, a continuación, pulse la tecla Entrar de su teclado y espere los resultados del ping. Pruebe la comunicación desde el sistema de consola hacia el cliente objetivo de la subred remota.

4. Compruebe la comunicación desde el cliente de destino de la subred remota a la dirección IP DHCP de VPN sistema de consola.

NOTA: Para comprobar la comunicación, introduzca ping desde el cliente de destino a la dirección IP VPN DHCP del sistema de consola y desde el sistema de consola al cliente de destino de subred.

3.3.5 Ajustes avanzados de IPSec (VPN)

La página de configuración de IPSec (VPN) incluye los ajustes avanzados del archivo ipsec.conf. Estos ajustes, descritos en la tabla siguiente, se muestran cuando la casilla de verificación Mostrar ajustes avanzados está activada.

Tabla 3.10 Descripciones de los ajustes avanzados

Nombre	Descripción
Conjunto de cifrado IKE (Internet Key Exchange)	Protocolo del servidor utilizado para intercambiar claves criptográficas. Este conjunto incluye algoritmos para protocolos de cifrado (confidencialidad), hash (autenticación de mensajes) y grupo DH (intercambio de claves) al configurar la VPN.
Conjunto de cifrado ESP (Encapsulating Security Payload)	Protocolo del servidor utilizado para intercambiar claves criptográficas. Este conjunto incluye algoritmos para protocolos de cifrado (confidencialidad), hash (autenticación de mensajes) y grupo DH (intercambio de claves) al configurar la VPN. Si se utiliza grupo DH, los grupos de números más elevados son los más seguros, aunque tardan más en computar la clave.
Asociación de seguridad (SA)	Una SA describe cómo se comunicarán dos o más dispositivos de forma segura.
Reautenticación	Especifica si el dispositivo debe reautenticar cuando cambia una asociación de seguridad IKE (SA).
Vigencia de IKE	Especifica cuánto debe durar un canal de claves de una conexión (ISAKMP o SA de IKE) antes de que sea renegociado.
Duración de la clave	Especifica cuánto debe durar una instancia concreta de una conexión (un conjunto de claves de cifrado/autenticación para paquetes de usuario) desde la correcta negociación hasta su caducidad.
Regenerar claves	Especifica si se debe renegociar una conexión cuando está a punto de caducar.
Intentos de generación de claves	Especifica cuántos intentos (un entero positivo o %forever) se realizarán para negociar una conexión, o para sustituir una, antes de abandonar. El valor predeterminado es 3.
Margen para regenerar claves	Especifica cuánto tiempo antes de que caduque una conexión o un canal de claves se debe intentar negociar el inicio de una sustitución.
Retraso DPD	Especifica el intervalo del período de tiempo con el que los mensajes R_U_ THERE/INFORMATIONAL se envían al par.

3.3.6 Configuración SNMP

Los administradores pueden configurar SNMP, que es necesario si se deben enviar notificaciones a una aplicación de gestión SNMP.

NOTA: El archivo de texto de Enterprise MIB del sistema de consola avanzada ACS800/8000 de Avocent® está disponible en el equipo en: /usr/local/mibs/ACS8000-MIB.asn. El archivo de texto de Enterprise TRAP MIB del sistema de consola avanzada ACS800/8000 de Avocent® está disponible en el equipo en: /usr/local/mibs/ACS8000-TRAP-MIB.asn. Ambos archivos también están disponibles en www.VertivCo.com.

Para configurar SNMP:

1. Haga clic en *Red - SNMP*.

2. Haga clic en el botón *Sistema*.
    a. Introduzca la información de SysContact (dirección de correo electrónico del administrador del sistema de consola, por ejemplo acs8000_admin@vertivco.com).
    b. Introduzca la información de SysLocation (ubicación física del sistema de consola, por ejemplo Avocent_ACS8000) y, a continuación, haga clic en *Guardar* para volver a la pantalla SNMP.
3. Haga clic en *Añadir* para añadir una comunidad o un usuario v3 nuevos.
4. Introduzca el nombre de comunidad para SNMP v1/v2 o el nombre de usuario para SNMP v3 en el campo Nombre e introduzca el OID.
5. Seleccione el permiso que desee en el menú desplegable. Las opciones son *Lectura y escritura* o *Solo lectura*.
6. Si la versión de SNMP necesaria es v1 o v2, haga clic en el botón *Versión v1, v2* y, acto seguido, introduzca el origen (la entrada válida es la dirección de subred).

    -O bien-

    Si la versión de SNMP necesaria es v1 o v2 con una red IPv6, haga clic en el botón *Versión v1,v2 para red IPv6* y, a continuación, introduzca el origen (la entrada válida es la dirección de subred).

    -O bien-

    Si la versión de SNMP necesaria es v3, haga clic en el botón *Versión v3*, a continuación seleccione el tipo de autenticación (*MD5* o *SHA*), introduzca la frase de contraseña o la contraseña de autenticación, seleccione el método de cifrado (DES o AES), introduzca la frase de contraseña de privacidad y seleccione el nivel de autenticación mínimo (*NoAuthNoPriv*, *AuthNoPriv*, *AuthPriv*).
7. Haga clic en *Guardar*.

NOTA: Para SNMP v1/v2c, el sistema de consola permitirá a un administrador que configure el mismo nombre de comunidad con diferentes orígenes (filtros) para tener acceso a identificadores de objeto específicos (OID).

3.3.7 Puertos

Los administradores pueden activar y configurar los puertos serie, los puertos auxiliares, el perfil CAS y el perfil de marcado de entrada en la pestaña Puertos de la barra de navegación lateral. En la pantalla Puertos auxiliares, puede activar y configurar el módem interno.

Los puertos serie del sistema de consola pueden desempeñar varias funciones distintas, en función del perfil configurado para un puerto.

Puertos serie

En la tabla Puertos serie, puede especificar el perfil de conexión (CAS, Marcado de entrada, Alimentación, Marcado de salida o Cliente de socket) en función del tipo de dispositivo conectado y puede clonar el puerto, restablecer los valores predeterminados de fábrica, activar/desactivar puertos o abrir una sesión serie.

En la tabla se muestra el número de puerto, el identificador del dispositivo, el estado, el nombre, el perfil, las señales y los ajustes. La columna Ajustes contiene los contactos que se utilizan para el puerto con las siguientes abreviaturas:

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

NOTA: Es posible que los contactos no se muestren si no hay ningún dispositivo conectado al puerto.

Para activar o desactivar uno o más puertos serie:

1. Seleccione *Puertos - Puertos serie*.
2. Haga clic en la casilla de verificación para cada puerto que desee activar o desactivar.
3. Haga clic en el botón *Activar* o *Desactivar*.

Para configurar o editar uno o más puertos serie con el perfil CAS:

1. Seleccione *Puertos - Puertos serie*.
2. Haga clic en la casilla de verificación para cada puerto que desee configurar.
3. Haga clic en el botón *Definir CAS*. Use los menús desplegables para activar o desactivar el puerto y configurar los contactos RJ-45, la velocidad, la paridad, los bits de datos, los bits de parada y el control de flujo.

NOTA: Si se selecciona AUTO para los contactos RJ-45, se activa la detección automática de contactos Cyclades o Cisco para dispositivos RS-232.

4. Haga clic en *Siguiente* o en el enlace *CAS*.
    a. Introduzca el nombre del puerto (cuando solo se ha seleccionado un puerto) o el prefijo del nombre del puerto (cuando se ha seleccionado más de un puerto). El nombre del puerto será <prefijo del nombre del puerto>-p-<número de puerto>.
    b. Marque la casilla para activar la detección automática. En este caso, el nombre del puerto se utilizará cuando la función de detección automática no detecte el nombre del servidor.
    c. Marque la casilla para activar la velocidad de detección automática.

NOTA: Para la detección de velocidad automática se necesita una configuración adicional en la pantalla Perfil CAS - Ajustes de detección automática.

    d. Utilice los menús desplegables apropiados para establecer el protocolo y el tipo de autenticación.
    e. Introduzca la sesión de texto, la sesión de alimentación y las teclas de acceso rápido RESTful en los campos apropiados.
    f. Introduzca el alias del puerto TCP para cada tipo de protocolo (Telnet, SSH y Modo sin procesar) en el campo correspondiente.
    g. Introduzca el alias IPv4 o IPv6 y su interfaz en el campo apropiado.
    h. Para permitir una sesión solo si DCD está activado y para activar la respuesta automática, marque las casillas correspondientes.
    i. Use el menú desplegable para seleccionar el modo DTR e introduzca el intervalo de desactivación de DTR.

j. Utilice los menús desplegables para activar o desactivar la supresión de avance de línea y la opción Suprimir NULL después de CR.

k. Introduzca el intervalo de transmisión, la secuencia de interrupción y el intervalo de interrupción en los campos apropiados.

NOTA: El intervalo de transmisión define el retardo (en milisegundos) antes de que se reciba la transmisión de datos a Ethernet a través de un puerto serie. El valor predeterminado es 20 ms.

l. Utilice el menú desplegable para activar o desactivar el menú de multisesión. Para obtener más información, consulte Menú de multisesión en la página 49.

m. Use los menús desplegables para activar o desactivar la notificación de multisesión de inicio/cierre de sesión y la notificación de mensaje informativo.

5. Haga clic en *Siguiente* o en el enlace *Almacenamiento en búfer de datos* y utilice los menús desplegables para activar y configurar el almacenamiento en búfer de datos.

6. Haga clic en *Siguiente* o en el enlace *Alertas*.

a. Haga clic en *Activar alertas* para activar la detección de alertas.

b. Haga clic en *Añadir* para añadir una cadena de alerta. En el campo Cadena de alerta, introduzca la cadena. En el campo Secuencia de comandos, introduzca la secuencia de comandos de shell que se ejecutará cuando se produzca la coincidencia. Marque la casilla Emergencia para que el LED del puerto serie parpadee rápidamente en ámbar siempre que se produzca esta alerta. Una alarma que no sea de emergencia parpadea lentamente. Haga clic en *Siguiente* para volver a la pantalla Alertas.

NOTA: El sistema de consola permite que los administradores asocien una secuencia de comandos de shell a la cadena de alerta. Cuando hay una coincidencia con la cadena de alerta, el sistema de consola llamará a la secuencia de comandos y pasará el número de puerto y la línea en los que se produce la coincidencia como argumentos.

c. Marque la casilla junto a una alerta existente y haga clic en *Eliminar* para eliminar la cadena.

d. Haga clic en *Eliminar cualquiera* para eliminar todas las cadenas, tanto si están seleccionadas como si no.

NOTA: Si se hace clic en *Eliminar cualquiera*, se eliminarán todas las cadenas de alerta. Seleccionar todas las cadenas de alerta y hacer clic en *Eliminar* no constituye la misma función, ya que no se eliminarán las cadenas de alerta que no se muestren en la tabla.

7. Haga clic en *Siguiente* o haga clic en el enlace *Alimentación*.

a. Haga clic en *Añadir* para añadir una nueva toma. Haga clic en *PDU seleccionada* y seleccione una PDU en la lista de PDU detectadas. Introduzca la(s) toma(s) en el campo Tomas y haga clic en *Siguiente*.

b. Marque la casilla junto a una toma combinada existente y haga clic en *Eliminar* para eliminarla.

NOTA: La opción Alimentación solo está disponible cuando se selecciona un único puerto serie.

8. Haga clic en *Guardar*.

Tabla 3.11 Parámetros del perfil CAS

Parámetro	Descripción
Físico	
Estado	Define el estado del puerto serie como activado o desactivado. Predeterminado: Desactivado.
Contactos RJ-45	Define los contactos del puerto serie como automático, Cyclades o Cisco. Los puertos 1 y 2 también admiten contactos RS-422 y RS-485. Predeterminado: Automático.
Velocidad	Define la velocidad como 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 o 230400. Predeterminado: 9600.
Paridad	Define la paridad como Par, Impar o Ninguno. Predeterminado: Ninguno.
Bits de datos	Define los bits de datos como 5, 6, 7 u 8. Predeterminado: 8.
Bits de parada	Define los bits de parada como 1 o 2. Predeterminado: 1.
Control de flujo	Define el control de flujo como ninguno, hardware, software, software RxON o software TxON. Predeterminado: Ninguno.
CAS	
Nombre del puerto	Nombre asociado con el puerto serie (como alias). Predeterminado: <dirección mac del equipo>-p-<número de puerto>.
Activar detección automática	El nombre del destino se detectará y se asociará a este puerto serie. Si falla, se utilizará el nombre del puerto. Predeterminado: Desactivado.
Activar velocidad de detección automática	Intenta detectar la velocidad del puerto serie. Para esta función se necesita una configuración adicional en la página Perfil CAS - Detección automática - Ajustes. Predeterminado: Desactivado.
Protocolo	El protocolo que los usuarios autorizados utilizarán para acceder al puerto serie/destino. El sistema de consola acepta tres protocolos para la conexión al destino: Telnet para una conexión Telnet, SSH para una conexión segura y modo sin procesar para una conexión de socket sin procesar. Un administrador puede configurar el puerto para aceptar uno, dos o los tres tipos. **NOTA:** Para el protocolo sin procesar es necesaria la configuración del alias de puerto de modo sin procesar. Valor predeterminado: SSH.
Tipo de autenticación	Tipo de autenticación que se utilizará para autenticar al usuario durante la sesión de destino. Predeterminado: Local.
Tecla de acceso rápido de sesión de texto	Tecla de acceso rápido para suspender la sesión de destino e ir a la pantalla de CLI. No disponible para modo sin procesar. Predeterminado: **Ctrl-Z**. Nota: El carácter de escape predeterminado para ts_menu es **Ctrl-X**.
Tecla de acceso rápido de sesión de administración de energía	Tecla de acceso rápido para suspender la sesión de destino y mostrar el menú de gestión de alimentación para controlar las tomas combinadas con el destino. No disponible para modo sin procesar. Predeterminado: **Ctrl-P**. Nota: El carácter de escape predeterminado para ts_menu es **Ctrl-X**.
Tecla de acceso rápido RESTful	Tecla de acceso rápido para suspender la sesión de destino y mostrar el menú RESTful, que se utiliza para realizar acciones RESTful definidas por el usuario. Valor predeterminado: Sin configurar (en blanco).
Alias de puerto TCP	Alias de puerto Telnet: Puerto TCP para conectarse directamente a un puerto serie mediante el uso del protocolo Telnet para la conexión. Alias de puerto SSH: Puerto TCP para conectarse directamente a un puerto serie mediante el uso del protocolo SSH para la conexión. Alias de puerto de modo sin procesar: Puerto TCP para conectarse directamente a un puerto serie mediante el uso de socket sin procesar para la conexión.
Alias de puerto IPv4/IPv6	Dirección IPv4/IPv6 usada para conectarse directamente a un puerto serie. Valor predeterminado: Sin configurar (en blanco).
Interfaz de alias IPv4/IPv6 de puerto	Interfaz (ETH0/ETH1) asociada al alias IPv4/IPv6. Predeterminado: ETH0.

Tabla 3.11 Parámetros del perfil CAS (continuación)

Parámetro	Descripción
Permitir sesión solo si DCD está activado	Cuando el DCD esté desactivado, el equipo denegará el acceso para este puerto serie. Predeterminado: Desactivado (permitir acceso si DCD está desactivado).
Activar respuesta automática	Cuando los datos de entrada coincidan con una cadena de entrada configurada en Respuesta automática, la cadena de salida se transmitirá al puerto serie. Predeterminado: Desactivado.
Modo DTR	El modo DTR se pude configurar con los valores siguientes: Siempre activado. Normal: El estado de DTR dependerá de la existencia de una sesión CAS. Intervalo de desactivación: Cuando se cierre una sesión de CAS, el DTR se mantendrá inactivo durante este intervalo. Predeterminado: Normal.
Intervalo de desactivación de DTR	Intervalo en segundos usado por el intervalo de desactivación del modo DTR en milisegundos. Predeterminado: 100.
Supresión de avance de línea	Permite la supresión del carácter LF después del carácter CR. Predeterminado: Desactivado.
Suprimir NULL después de CR	Permite la supresión del carácter NULL después del carácter CR. Predeterminado: Desactivado.
Intervalo de transmisión	El intervalo que el puerto espera para enviar datos a un cliente remoto en milisegundos. Predeterminado: 20.
Secuencia de interrupción	Un administrador puede configurar la tecla de control como la secuencia de interrupción si introduce ^ antes de la letra. No disponible para modo sin procesar. Predeterminado: ~interrupción.
Intervalo de desactivación	Intervalo de la señal de interrupción en milisegundos. No disponible para modo sin procesar. Predeterminado: 500.
Mostrar menú de multisesión	Activa el menú de multisesión al conectarse a un puerto al que ya accede otro usuario. Predeterminado: Desactivado.
Notificación de inicio/cierre de sesión de multisesión	Activa la notificación a los usuarios de multisesión cuando un nuevo usuario inicia sesión o un usuario cierra su sesión. No disponible para modo sin procesar. Predeterminado: Desactivado.
Notificación de mensaje informativo	Muestra un mensaje de información cuando se abre una sesión de destino. No disponible para modo sin procesar. Predeterminado: Activado.
Almacenamiento en búfer de datos	
Estado	Activa o desactiva el almacenamiento en búfer de datos. Predeterminado: Desactivado.
Tipo	Muestra el tipo de almacenamiento en búfer de datos: Local: Almacena el archivo de almacenamiento en búfer de datos en el sistema de archivos local. NFS: Almacena el archivo de almacenamiento en búfer de datos en el servidor NFS. Syslog: Envía los datos al servidor Syslog. DSView: Envía los datos al software DSView. Predeterminado: Local.
Tipo local	Cuando el tipo se establece como local, especifica la ubicación del sistema local en la que se almacenan los archivos de almacenamiento en búfer de datos. Las opciones son la memoria integrada (mmcblk0) o ubicaciones de almacenamiento USB o de tarjetas SD conectadas. Predeterminado: mmcblk0.
Marca de hora	Cuando está activado, añade la marca de hora a la línea de almacenamiento en búfer de datos para una base de datos local o NFS. Predeterminado: Desactivado.
Mensaje de inicio/cierre de sesión	Incluye notificación especial para los inicios de sesión y los cierres de sesión en el almacenamiento en búfer de datos. Predeterminado: Desactivado.
Registro de la sesión serie	Activado: Almacena los datos en todo momento. Desactivado: Almacena datos cuando no se abre una sesión CAS. Predeterminado: Activado.

Tabla 3.11 Parámetros del perfil CAS (continuación)

Parámetro	Descripción
Alertas	
Estado	Se generará una notificación de evento especial cuando los datos de entrada coincidan con una de las cadenas de alerta. Predeterminado: Desactivado.
Cadenas de alerta	Cadenas utilizadas para generar notificaciones de eventos. Predeterminado: Vacío.
Secuencia de comandos	Nombre de la secuencia de comandos del shell que se llamará cuando haya coincidencia de la cadena de alerta en la línea. La secuencia de comandos se llamará con dos argumentos: El número de puerto y la línea en la que se produjo la coincidencia.
Emergencia	Al marcar una alerta como una emergencia, el LED del puerto serie parpadea rápidamente en ámbar cuando se produce esta alerta en lugar de parpadear lentamente para una situación que no sea de emergencia.

Para configurar el Perfil de marcado de entrada para un puerto serie con un módem conectado:

1. Seleccione *Puertos - Puertos serie*.
2. Haga clic en la casilla de verificación de un puerto serie con un módem conectado.
3. Haga clic en el botón *Definir marcado de entrada* y utilice los menús desplegables para configurar los ajustes de marcado de entrada.
4. Configure los parámetros PPP (dirección, autenticación, etc.) y haga clic en *Guardar*.

Tabla 3.12 Parámetros de marcado de entrada

Parámetro	Descripción
Estado	Activa o desactiva el puerto. Predeterminado: Desactivado.
Velocidad	La velocidad que mgetty usará para configurar el dispositivo serie. Predeterminado: 38400 bps.
Iniciar chat	Chat para la inicialización del módem. Predeterminado: "" \d\d\d+++\d\d\dATZ OK.
Dirección PPP	Configura la dirección IP local y remota para el enlace PPP. Si se selecciona *Aceptar configuración del equipo remoto del mismo nivel*, el equipo remoto del mismo nivel debe enviar ambas direcciones IP (local y remota) durante la negociación. Predeterminado: No hay dirección.
Dirección IPv4/IPv6 local	Configura la dirección IPv4/IPv6 local para esta conexión PPP.
Dirección IPv4/IPv6 remota	Configura la dirección IPv4/IPv6 remota para esta conexión PPP.
Protocolo de autenticación PPP	Utiliza el botón de opción para seleccionar: Ninguno, PAP, CHAP o EAP. Ninguno: No hay autenticación. • PAP: Use el protocolo PAP y el tipo de autenticación configurado en el tipo de autenticación PPP (se configura en la página Autenticación/Autenticación de unidad). • CHAP: Se usa el protocolo CHAP. La configuración de los secretos de CHAP se debe realizar al editar el archivo /etc/ppp/chap-secrets. • EAP: Se usa el protocolo EAP. Autenticaciones disponibles: CHAP, SRP-SHA1 y TLS. La configuración de los secretos de CHAP se debe realizar al editar el archivo /etc/ppp/chap-secrets. La configuración de los secretos de SRP-SHA1 se debe realizar al editar el archivo /etc/ppp/srp-secrets. Nota: La autenticación EAP solo está disponible en los sistemas operativos Windows XP. Predeterminado: Ninguno.
CHAP	Configure CHAP-interval, CHAP-max-challenge y CHAP-restart. Valores predeterminados: • Intervalo de CHAP = 0. • Desafío máx. de CHAP = 10. • Reinicio de CHAP = 3.
Tiempo de espera de inactividad PPP	Número de segundos de inactividad antes de que se agote el tiempo de espera de PPP. Predeterminado: 0 (no hay tiempo de espera).

Para configurar o editar uno o más puertos serie con una PDU conectada:

1. Seleccione *Puertos - Puertos serie*.
2. Haga clic en la casilla de verificación de uno o más puertos serie con una PDU conectada.
3. Haga clic en el botón *Definir alimentación* y use los menús desplegables para configurar los ajustes físicos.
4. Haga clic en *Siguiente* o haga clic en el enlace *Alimentación*.
    a. Utilice el menú desplegable para seleccionar el tipo de PDU.
    b. Marque la casilla para activar la velocidad de detección automática.
    c. Configure la tasa de sondeo.
    d. Para PDU de Avocent/Cyclades, introduzca el intervalo de apagar y encender y, a continuación, use los menús desplegables para activar o desactivar las opciones de Syslog, Zumbador y Protección contra sobrecorriente de software.
5. Haga clic en *Guardar*.

Tabla 3.13 Parámetros de alimentación

Parámetro	Descripción
Físico	
Contactos RJ-45	Define los contactos del puerto serie como automático, Cyclades o Cisco. Predeterminado: Automático.
Estado	Define el estado del puerto serie como activado o desactivado. Predeterminado: Desactivado.
Velocidad	Define la velocidad como 1200, 2400, 4800, 9600, 19200, 38400, 57600,115200 o 230400. Predeterminado: 9600.
Paridad	Define la paridad como Par, Impar o Ninguno. Predeterminado: Ninguno.
Bits de datos	Define los bits de datos como 5, 6, 7 u 8. Predeterminado: 8.
Bits de parada	Define los bits de parada como 1 o 2. Predeterminado: 1.
Control de flujo	Define el control de flujo como ninguno, hardware, software, software RxON o software TxON. Predeterminado: Ninguno.
Alimentación	
Tipo de UPS	Define el tipo o el proveedor del UPS conectado al puerto serie. Son compatibles los UPS Liebert GXT4 y Liebert GXT5. Predeterminado: Liebert GXT4.
Tipo de PDU	Define el tipo o el proveedor de la PDU conectada al puerto serie. Predeterminado: Automático. • Automático: Se detecta el proveedor. • Avocent-Cyclades: Gama de PDU PM de Avocent-Cyclades. • Vertiv: PDU de Vertiv • SPC: Gama de dispositivos de control de la alimentación SPC. • Server Tech/Server Tech PRO2: Gama de Server Tech. • Raritan: Gama de PDU PX G2 de Raritan. • APC: Gama rPDU2 de APC. • Eaton: PDU G3 ePDU de Eaton. • Geist: Gama de PDU de Geist.
Activar velocidad de detección automática	Cuando está activado, detecta la velocidad del puerto. Predeterminado: Desactivado.
Tasa de sondeo	El intervalo en segundos para actualizar la información de la PDU. Predeterminado: 20.
Para PDU de Avocent/Cyclades	
Intervalo de ciclo de apagado/encendido	El intervalo en segundos entre las acciones de apagado y encendido del comando de apagar y encender. Predeterminado: 15.
Syslog	Cuando está activado, la PDU enviará mensajes de Syslog al equipo. Predeterminado: Activado.
Zumbador	Activa o desactiva el zumbador de la PDU. Predeterminado: Activado.
Protección contra sobrecorriente de software	Cuando está activado, la protección contra sobrecorriente de software está activada. Predeterminado: Desactivado.

Para copiar/clonar la configuración de un puerto a otros puertos:

1. Seleccione *Puertos - Puertos serie*.
2. Haga clic en la casilla de verificación del puerto serie que desee clonar.
3. Haga clic en el botón *Clonar*.
4. Introduzca el (los) puerto(s) serie que se va(n) a configurar en el campo Copiar configuración a y haga clic en *Guardar*.

NOTA: Si el puerto seleccionado está configurado como un perfil CAS, los siguientes parámetros no se copiarán: Nombre de puerto, alias de puerto TCP, alias IPv4 de puerto, alias IPv6 de puerto y alimentación (tomas combinadas).

Para restablecer uno o más puertos serie a su configuración de fábrica:

1. Seleccione *Puertos - Puertos serie*.
2. Haga clic en la casilla de verificación de uno o más puertos serie que desee restablecer a su configuración de fábrica y, a continuación, haga clic en el botón *Restablecer a valores de fábrica*.

NOTA: Los puertos serie se configuran según el perfil CAS y están desactivados en la configuración de fábrica.

Menú de multisesión

Los administradores pueden activar o desactivar el menú de multisesión. Cuando esté activado, los usuarios pueden acceder al menú desde la interfaz de usuario web, la CLI o el software DSView, y varios usuarios pueden conectarse a un puerto serie de forma simultánea. Para conectarse a un puerto o iniciar una sesión compartida, el usuario debe tener permiso para acceder al puerto. Si se establece más de una sesión en un puerto serie, el sistema de consola muestra el menú de multisesión. Si la sesión que se establece es la primera con el puerto serie, se abrirá una sesión normal con el destino. Un usuario de la primera sesión todavía puede acceder al menú de multisesión si pulsa la tecla de acceso rápido textual (Ctrl-Z de forma predeterminada).

Para activar el menú de multisesión:

1. En la barra lateral de la pestaña *Experto* , haga clic en *Puertos - Puertos serie*.
2. Haga clic en el puerto para el que desee activar el menú de multisesión.
3. Haga clic en el encabezado *CAS* y, cerca de la parte inferior de la sección Ajustes de CAS, use el menú desplegable para *activar* la opción *Mostrar menú de multisesión*.
4. Haga clic en *Guardar*.

En el menú de multisesión hay opciones que dependen de los derechos de acceso del usuario. Si un usuario no tiene derechos para una opción, esa opción no se muestra. Por ejemplo, las opciones 0, 2 y 5 de la tabla siguiente se muestran para un usuario que solo tiene permiso para abrir sesiones de solo lectura.

Tabla 3.14 Opciones del menú de multisesión

Número	Opción	Descripción
0	Salir	Cierra la sesión del cliente.
1	Iniciar una sesión normal	Abre una sesión de lectura/escritura.
2	Iniciar una sesión de prueba	Abre una sesión de solo lectura.
3	Enviar mensajes a otro usuario	Envía un mensaje a todos los usuarios que comparten el puerto serie.
4	Terminar sesión(es)	Muestra todas las sesiones y solicita el cierre de una o más sesiones compartidas.
5	Enumerar sesión(es) compartida(s)	Enumera todas las demás sesiones compartidas.
6	Mostrar almacenamiento en búfer de datos	Muestra el contenido del archivo de almacenamiento en búfer de datos del destino.
7	Borrar almacenamiento en búfer de datos	Restablece el contenido del archivo de almacenamiento en búfer de datos del destino.

Puertos auxiliares

En la pantalla Puertos auxiliares, si el nombre del puerto aparece como ttyM1, el módem interno está presente y se puede activar y configurar. Si no hay entradas en la tabla Puerto auxiliar, el módem interno no está presente y este puerto no se puede usar.

En los modelos con módem móvil, el nombre del puerto aparece como ttyM1 y el tipo de dispositivo aparece como LTE. El módem móvil solo se puede configurar para el modo de marcado de salida. De forma predeterminada, el módem móvil está desactivado: Para obtener más información sobre la configuración de un módem móvil, consulte Módem móvil en la página 59

Para configurar o editar un puerto auxiliar con un módem interno:

1. Seleccione *Puertos - Puertos auxiliares*.
2. Haga clic en el botón *Definir marcado de entrada* o *Definir marcado de salida* y utilice los menús desplegables para configurar los ajustes de marcado de entrada.
3. Configure los parámetros de PPP (dirección, autenticación, etc.).
4. Haga clic en *Guardar*.

Perfil CAS

El perfil CAS (servidor de acceso a consola) proporciona acceso remoto a puertos de consola RS-232 serie en sus dispositivos. Con un perfil CAS, puede configurar la autenticación, la configuración de puertos (como, por ejemplo, la velocidad y el control de flujo), la creación de alias de puertos, la detección automática de destinos, el tipo de almacenamiento en búfer de datos, las alertas de puertos, la integración de alimentación, etc.

Un administrador puede configurar el perfil CAS si hace clic en *Puertos - Perfil CAS*.

Detección automática

La función de detección automática detectará el nombre del destino del servidor conectado al puerto serie. Este nombre se usará como alias del puerto serie.

Cuando la detección automática está activa para un dispositivo serie determinado, al conectarse el destino (evento DCD activado), el equipo enviará cadenas de sondeo y comenzará a analizar las respuestas del dispositivo de destino mediante expresiones regulares. Habrá cadenas de sondeo y coincidencia predefinidas, así como cadenas definidas por el cliente.

Para cada cadena de sondeo enviada, se probarán todas las expresiones regulares definidas por las cadenas de coincidencia. Después del último ciclo, la secuencia se reinicia. Este procedimiento se ejecutará durante un período determinado (especificado por el parámetro de tiempo de espera de detección automática) o hasta que el destino se detecte correctamente. Si la detección automática falla, el nombre del destino se restablecerá al nombre del destino configurado o al nombre del destino predeterminado exclusivo correspondiente.

NOTA: El nombre del destino configurado solo se usará después de que el proceso de detección automática haya fallado.

NOTA: El proceso de detección automática se inicia cuando hay variación en la señal DCD de desactivada a activada (desconecte/conecte el cable del destino, apague/encienda el destino) y cuando la configuración del puerto serie va de desactivado a activado y hay un destino conectado en el puerto.

Las cadenas de sondeo se utilizarán para estimular el servidor (por ejemplo "\r": un solo retorno de carro).

Las cadenas de coincidencia son expresiones regulares en las que "%H" es un marcador de posición para el nombre del destino que desee detectar como, por ejemplo, %H .*ogin:

O xxx%Hyyy

El primero extraerá el nombre del destino de elementos como, por ejemplo: Inicio de sesión de Mi servidor: y dará como resultado el nombre del destino Mi servidor.

Y el segundo, de elementos como: Servidor xxxDESTINOyyy y dará como resultado el nombre del destino DESTINO.

Para configurar las cadenas de sondeo/coincidencia usadas por la función de detección automática:

Realice este procedimiento para cambiar los ajustes predeterminados o las cadenas de sondeo o coincidencia que se utilizan en la detección automática.

1. Seleccione *Puertos - Perfil CAS - Detección automática*. Las opciones Ajustes, Cadenas de sondeo y Cadenas de coincidencia aparecen en la barra de navegación lateral.
2. Para cambiar el tiempo de espera de detección automática o de sondeo predeterminado, realice los pasos siguientes.
    a. Seleccione *Ajustes*.
    b. Introduzca un nuevo valor en los campos Tiempo de espera de detección automática y Tiempo de espera de sondeo.
    c. Seleccione una velocidad en el menú desplegable Velocidad predeterminada en fallo de detección automática y Lista de velocidades de sondeo.
    d. Haga clic en *Guardar*.
3. Para añadir una cadena de sondeo o de coincidencia nueva o eliminar una cadena ya existente, realice los pasos siguientes.
    a. Seleccione *Cadenas de sondeo* o *Cadenas de coincidencia*.
    b. Para añadir una cadena, haga clic en *Añadir*, introduzca una cadena nueva en el campo Nueva cadena de sondeo o Nueva cadena de coincidencia y haga clic en *Guardar*.

c. Para eliminar una cadena, seleccione la casilla de verificación correspondiente a la cadena y haga clic en *Eliminar*.

4. Haga clic en *Guardar*.

Para configurar las cadenas de entrada/salida utilizadas por la función de respuesta automática:

1. Seleccione *Puertos - Perfil CAS - Respuesta automática*.
2. Para añadir una cadena de entrada y salida de respuesta automática, haga clic en *Añadir*. Introduzca una cadena nueva en los campos Cadena de entrada o Cadena de salida y haga clic en *Guardar*.

   -O bien-

   Para eliminar una cadena de entrada y salida de respuesta automática, seleccione la casilla de verificación situada junto a la cadena que desee eliminar. Haga clic en *Eliminar* y, a continuación, en *Guardar*.

Grupo de puertos

Los administradores pueden crear un grupo de puertos serie en el que cada puerto serie del grupo comparte un nombre de grupo, un alias de puerto Telnet, un alias de puerto SSH, un alias de puerto de modo sin procesar, un alias IPv4 y un alias IPv6. El primer puerto disponible del grupo se utiliza como puerto serie para la conexión.

NOTA: El derecho de acceso a múltiples sesiones no tiene ningún efecto cuando se usa un grupo de puertos CAS. Cuando todos los puertos del grupo se están utilizando, se deniega la conexión al grupo.

NOTA: Todos los puertos del grupo deben compartir el mismo protocolo CAS. El protocolo se valida durante la conexión al puerto serie. Si el protocolo no coincide, la conexión se denegará.

Para configurar un grupo de puertos CAS:

1. Haga clic en *Puertos - Grupo de puertos*.
2. Para crear un grupo, haga clic en el botón *Añadir*.

   -O bien-

   Para editar un grupo existente, haga clic en el nombre del grupo que desee editar.

   -O bien-

   Para eliminar un grupo, marque la casilla situada junto al grupo que desee eliminar y haga clic en el botón *Eliminar*.

3. Introduzca los parámetros del grupo en los campos correspondientes.
4. En el lado izquierdo del campo Miembros del grupo, seleccione los puertos que se van a añadir al grupo y haga clic en *Añadir*.

   -O bien-

   En el lado derecho del campo Miembros del grupo, seleccione los puertos que se van a eliminar del grupo y haga clic en *Eliminar*.

5. Haga clic en *Guardar*.

NOTA: Un puerto serie solo puede pertenecer a un grupo a la vez, pero un usuario puede crear un grupo vacío y añadir puertos al mismo más adelante.

Tabla 3.15 Parámetros del grupo de puertos CAS

Parámetro	Descripción
Nombre del grupo	El nombre del grupo. El nombre del grupo es obligatorio y debe seguir las directrices de nombre de host, no superar los 64 caracteres y comenzar con una letra.
Alias de puerto	El alias de puerto por el que el grupo responde para cada protocolo. • Alias de puerto Telnet para protocolo Telnet. Es opcional. • Alias de puerto SSH para protocolo SSH. Es opcional. • Alias de puerto de modo sin procesar para protocolo de modo sin procesar. • Es obligatorio cuando el modo sin procesar está configurado como protocolo para los puertos.
Alias IPv4 de grupo	La dirección IPv4 usada por el grupo. Este parámetro es opcional.
Interfaz de alias IPv4 de grupo	La interfaz usada por el alias IPv4. Predeterminado: Eth0.
Alias IPv6 de grupo	La dirección IPv6 usada por el grupo. Este parámetro es opcional.
Interfaz de alias IPv6 de grupo	La interfaz usada por el alias IPv6. Predeterminado: Eth0.

Cliente RESTful

El sistema de consola es compatible con una interfaz de cliente RESTful programable. Tras la configuración de las URL RESTful, el sistema de consola realiza, desde una sesión serie, operaciones GET y POST seleccionadas desde menú a URL HTTP/HTTPS preprogramadas para recursos de servidor en la red.

NOTA: Las opciones de URL se deben configurar mediante HTTP o HTTPS con el menú del cliente RESTful.

Para configurar el cliente RESTful:

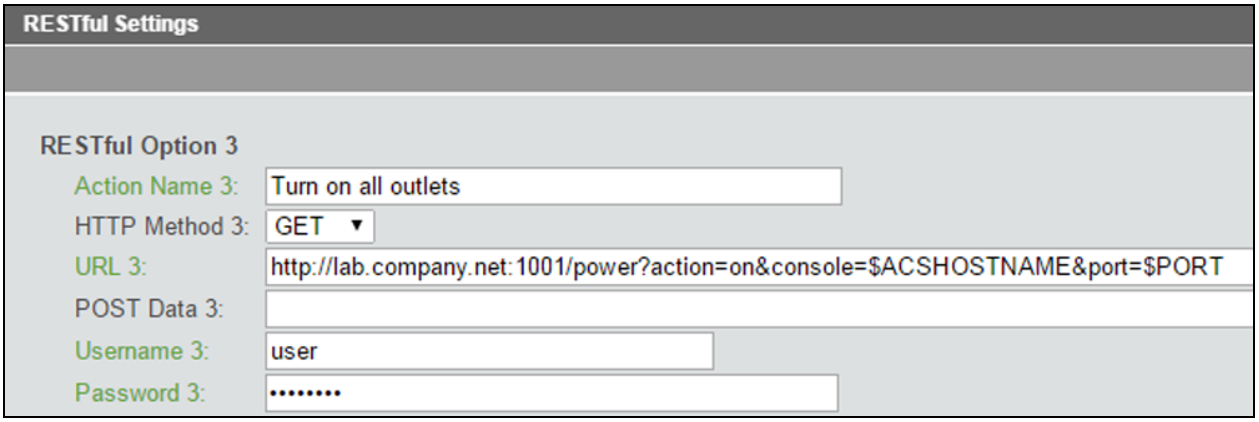
1. Haga clic en *Puertos - Perfil CAS - Ajustes RESTful*.
2. Introduzca el nombre de acción, la URL, los datos POST, el nombre de usuario y la contraseña en los campos correspondientes y use el menú desplegable para seleccionar GET o POST como método HTTP para cada opción RESTful. Haga clic en *Guardar* cuando haya acabado.

Cuando se configuren acciones se pueden utilizar las siguientes variables de contexto.

Tabla 3.16 Descripciones de las variables de contexto

Variable de contexto	Descripción
$PORT	Identifica el puerto serie (1-48) cuando se invoca el menú.
$PORTNAME	El nombre del puerto.
$IPPORTALIAS	El alias IPv4 del puerto.
$TCPPORTALIAS	El alias TCP (puerto Telnet) del puerto.
$ACSHOSTNAME	El nombre del host del sistema de consola.
$ACSIPADDR	La dirección IP del sistema de consola.

Figura 3.3 Ejemplo de configuración del ciente RESTful



NOTA: En algunos casos, los POST HTTP pueden usar el cuerpo de la solicitud HTTP para enviar la información adecuada a los servidores, normalmente codificada como XML o JSON.

Para activar el cliente RESTful:

1. Si el acceso a los puertos se aplica a todos los usuarios, en la barra de navegación lateral de la pestaña *Experto* , haga clic en *Sistema - Seguridad - Perfil de seguridad* y, a continuación, en Dispositivos serie, haga clic en la casilla de verificación Menú RESTful y haga clic en *Guardar*.

   -O bien-

   Si el acceso a los puertos se controla mediante la autorización asignada a los grupos de usuarios, en la barra de navegación lateral de la pestaña Experto, haga clic en *Usuarios - Autorización - Grupos*.

   a. Haga clic en el grupo para el que desee activar el cliente RESTful.
   b. En la barra de navegación lateral, haga clic en *Derechos de acceso - Serie*.
   c. Haga clic en el puerto para el que desee activar el menú RESTful. En Derechos de acceso del destino, haga clic en le casilla Menú RESTful.
2. En la barra de navegación lateral de la pestaña Experto, haga clic en *Puertos - Puertos serie*.
3. Haga clic en el puerto para el que desee activar el menú RESTful y, a continuación, haga clic en el encabezado CAS en la parte superior de la ventana.
4. En el campo Tecla de acceso rápido RESTful, introduzca la tecla de acceso rápido que desee utilizar para iniciar el cliente RESTful y haga clic en *Guardar*.

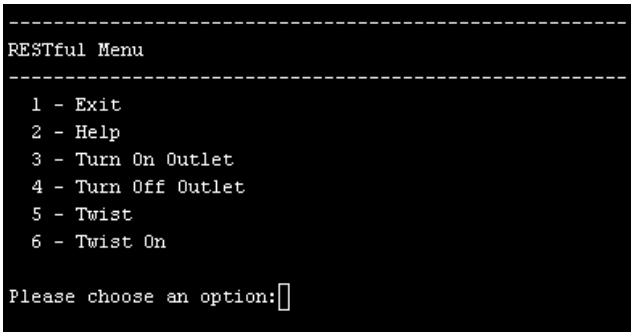
NOTA: La tecla de acceso rápido no está configurada de forma predeterminada.

Uso de la interfaz del cliente RESTful

Después de abrir una sesión serie, pulse la tecla de acceso rápido para abrir la interfaz del cliente RESTful para la sesión actual. Introduzca el número de la solicitud del cliente RESTful que desee realizar. De forma predeterminada, Salir y Ayuda son las dos primeras solicitudes en el menú. Puede configurar hasta ocho solicitudes adicionales desde la interfaz de usuario web del sistema de consola.

A continuación se muestra un ejemplo del menú RESTful de una sesión serie.

Figura 3.4 Ejemplo de cliente RESTful



Perfil de marcado de entrada

Un administrador puede configurar ajustes de marcado de entrada seguros como, por ejemplo, el inicio de sesión OTP, conexiones PPP, la autenticación PPP/PAP, el retorno de llamada y usuarios OTP para conexiones PPP.

NOTA: Si se utilizan dispositivos conectables para el marcado de salida, se debe desactivar el marcado de entrada.

Para configurar ajustes de marcado de entrada seguros para puertos con el perfil de marcado de entrada:

1. Seleccione *Puertos - Perfil de marcado de entrada - Ajustes*.
2. Para activar el inicio de sesión en el sistema de consola a través del módem y seleccionar una condición para la que se permita iniciar sesión, realice los pasos siguientes:
   a. Para permitir solo conexiones de retorno de llamada, seleccione *Retorno de llamada*.
   b. Para permitir cualquier conexión, seleccione *Activar*.
3. Para activar la autenticación OTP, seleccione *Activar* en el menú Autenticación de inicio de sesión OTP.
4. Para activar y seleccionar una condición para conexiones PPP, realice los pasos siguientes.
   a. Para permitir solo conexiones de retorno de llamada PPP, seleccione *Retorno de llamada*.
   b. Para permitir cualquier conexión, seleccione *Activar*.
5. Cuando el protocolo de autenticación PAP se configure para el puerto, seleccione el tipo de autenticación en el menú Autenticación PPP/PAP.
6. Use el menú desplegable para activar o desactivar el filtro de identificación de llamadas.
7. Haga clic en *Guardar*.

Para configurar usuarios de devolución de llamada y números de teléfono para puertos con el perfil de marcado de entrada:

1. Seleccione *Puertos - Perfil de marcado de entrada - Marcado de entrada seguro - Usuarios de devolución de llamada*.
2. Haga clic en *Añadir*.
3. Introduzca el nombre y el número de teléfono utilizados para realizar el retorno de llamada en los campos correspondientes y haga clic en *Guardar*.

Para configurar usuarios PPP OTP para puertos con el perfil de marcado de entrada:

1. Seleccione *Puertos - Perfil de marcado de entrada - Marcado de entrada seguro - Usuarios PPP OTP*.
2. Haga clic en *Añadir*.
3. Introduzca el nombre de usuario y la frase de contraseña en los campos correspondientes y haga clic en *Guardar*.

NOTA: Este usuario PPP OTP establecerá una conexión PPP una vez que se haya autenticado correctamente.

Para configurar EAP-TLS como autenticación PPP para puertos con el perfil de marcado de entrada:

1. Seleccione *Puertos - Puertos auxiliares*.
2. Marque la casilla situada al lado del puerto en el que el módem está conectado y haga clic en *Definir marcado de entrada*.
3. Configure los ajustes de dirección PPP. Por ejemplo, defina la Dirección PPP a Configuración local con 10.0.0.1 como dirección IPv4 local y 10.0.0.2 como dirección IPv4 remota.
4. Para la autenticación PPP, seleccione el botón que hay al lado de la opción Por equipo y, a continuación, seleccione el botón junto a EAP para el protocolo. Haga clic en Guardar.
5. Seleccione *Puertos - Perfil de marcado de entrada - Ajustes*.
6. Use el menú desplegable para activar la conexión PPP y haga clic en *Guardar*.
7. Copie los certificados y las claves al archivo /etc/ppp/cert. Se les debe asignar el nombre server.crt (el certificado del ACS800/8000), ca.crt (el certificado de la autoridad de certificados) y server.key (la clave asimétrica del ACS800/8000).

Identificación de llamadas

Puede filtrar las llamadas entrantes según la identificación de llamadas, activando el filtro de identificación de llamadas en los ajustes de Marcado de entrada seguro. Cuando está activado, el número de identificación de la llamada entrante debe figurar como llamada que se debe responder. De forma predeterminada, está desactivado.

Puede añadir los números directamente, por intervalo o por prefijo.

Para introducir un número directamente, introduzca el número sin símbolos. Por ejemplo: 8881234567.

Puede introducir un intervalo insertando un guion (-) entre dos números de identificación de llamada. Cualquier número que se encuentre entre esos dos números o que los contenga, será aceptado. Por ejemplo: 8881234560-8881234569.

NOTA: El intervalo debe ser inferior a los 100 números de teléfono.

Puede introducir un prefijo colocando un asterisco (*) a continuación de un número de teléfono parcial. La llamada entrante se responderá si el número de teléfono comienza por el número parcial especificado. Por ejemplo: 8881234*.

Si el filtro de identificación de llamadas está activado y no se ha especificado ningún número, se bloquearán todas las llamadas. Las llamadas bloqueadas no se responden y siguen sonando hasta que se agota el tiempo de espera. Si la función de identificación de llamadas está desactivada, se responden todas las llamadas.

Para introducir una lista de números de identificación de llamadas:

1. Seleccione *Puertos - Perfil de marcado de entrada - Marcado de entrada seguro - Identificación de llamadas*.
2. Haga clic en *Añadir* e introduzca el número de identificación de llamadas, intervalo o prefijo.
3. Haga clic en *Guardar*.

Para eliminar un número de identificación de llamadas de la lista:

1. Seleccione *Puertos - Perfil de marcado de entrada - Marcado de entrada seguro - Identificación de llamadas*.
2. Marque la casilla situada junto al número que se va a eliminar.
3. Haga clic en *Eliminar*.

Perfil de marcado de salida

Para configurar el perfil de marcado de salida para un puerto serie con un módem conectado:

1. Seleccione *Puertos – Puertos serie*.
2. Haga clic en la casilla de verificación de un puerto serie con un módem conectado.
3. Haga clic en el botón *Definir marcado de salida*.
4. Use el menú desplegable para activar/desactivar el puerto.
5. Configure el número de teléfono para marcar bajo demanda en el campo Número de teléfono.
6. Utilice el menú desplegable para configurar la velocidad del módem.
7. Configure el chat inicial con el módem en el campo Iniciar chat.
8. Configure los parámetros PPP (dirección, autenticación, etc.) y haga clic en *Guardar*.

NOTA: El perfil de marcado de salida solo funcionará para establecer un enlace PPP bajo demanda. El administrador debe configurar la ruta estática para que los paquetes se enruten hacia la interfaz PPP.

Tabla 3.17 Parámetros de marcado de salida

Parámetro	Descripción
Estado	Activa o desactiva el puerto. Predeterminado: Desactivado.
Número de teléfono	El número de teléfono que se debe marcar.
Velocidad	La velocidad que se usará para configurar el dispositivo serie y comunicarse con el módem conectado.
Iniciar chat	Chat para la inicialización del módem.
Dirección IPv4/IPv6 local	Configura la dirección IPv4/IPv6 local para esta conexión PPP. Si se deja en blanco, PPP aceptará la dirección del equipo remoto del mismo nivel.
Dirección IPv4/IPv6 remota	Configura la dirección IPv4/IPv6 remota para esta conexión PPP. Si se deja en blanco, PPP aceptará la dirección del equipo remoto del mismo nivel.
Protocolo de autenticación PPP	Configura qué extremo de la conexión controla esta autenticación PPP y selecciona el método que se usará.
Tiempo de espera de inactividad PPP	Número de segundos de inactividad antes de que se agote el tiempo de espera de PPP. Predeterminado: 0 (no hay tiempo de espera).
CHAP	Configura los ajustes específicos de autenticación PPP CHAP.

Perfil de cliente de socket

Para configurar el perfil de cliente de socket para un puerto serie con un dispositivo conectado:

1. Seleccione *Puertos - Puertos serie*.
2. Haga clic en la casilla de verificación de un puerto serie con un dispositivo conectado.
3. Haga clic en *Configurar cliente de socket* y utilice los menús desplegables para configurar los ajustes físicos.
4. Configure los ajustes de cliente de socket (dirección del servidor remoto, puerto TCP y desencadenador de eventos) y haga clic en *Guardar*.

Tabla 3.18 Parámetros de cliente de socket

Parámetro	Descripción
Contactos RJ-45	Define los contactos del puerto serie.
Estado	Define el estado del puerto serie como activado o desactivado. Predeterminado: Desactivado.
Velocidad	Define la velocidad como 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 o 230400. Predeterminado: 9600.
Paridad	Define la paridad como Par, Impar o Ninguno. Predeterminado: Ninguno.
Bits de datos	Define los bits de datos como 5, 6, 7 u 8. Predeterminado: 8.
Bits de parada	Define los bits de parada como 1 o 2. Predeterminado: 1.
Control de flujo	Define el control de flujo como ninguno, hardware, software, software RxON o software TxON. Predeterminado: Ninguno.
Servidor remoto	Dirección IPv4 o IPv6 del servidor remoto.
Puerto TCP remoto	Puerto TCP que se utilizará para establecer una conexión con un servidor remoto.
Establecer conexión	Configure el evento que desencadenará el establecimiento de la conexión: Saludo DCD o siempre.

3.3.8 Módem móvil

La interfaz de configuración del módem móvil del sistema de consola avanzada ACS800/8000 de Avocent® es similar a la interfaz de configuración del módem de 56k interno. El módem móvil se configura a través del puerto auxiliar del sistema de consola.

Para configurar o editar un puerto auxiliar con un módem móvil:

1. Seleccione *Puertos - Puertos auxiliares*.
2. Haga clic en el enlace *ttyM1* para abrir la página de configuración de marcado de salida del módem.

NOTA: El módem móvil solo se puede configurar para el modo de marcado de salida.

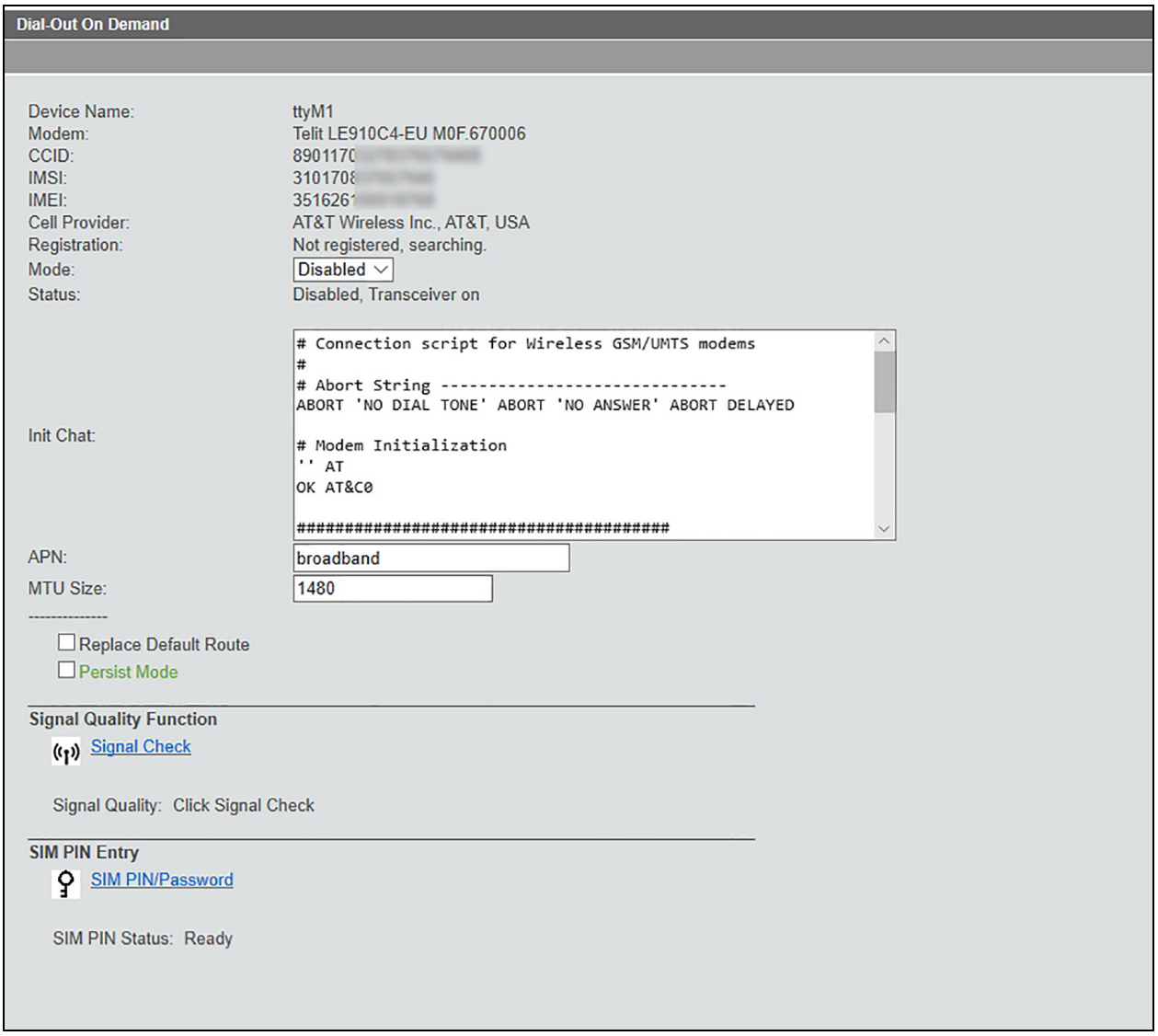
3. Utilice el menú desplegable para activar el modem. Cuando está activado, el módem se enciende tras cada reinicio.
4. El proveedor puede utilizar la secuencia de comandos de chat de forma predeterminada. Si lo desea, puede realizar cambios en la secuencia de comandos de chat desde la ventana Iniciar chat.
5. El campo APN es el nombre del punto de acceso predeterminado. Puede cambiar el APN aquí sin tener que editar la secuencia de comandos de chat.

NOTA: Si cambia el APN, cualquier edición de la secuencia de comandos de chat se perderá.

6. Active o desactive la opción de reemplazar la ruta predeterminada.
7. Active o desactive el modo persistente.

Para obtener más información sobre la configuración del módem móvil, consulte las secciones siguientes.

Figura 3.5 Página de configuración del marcado de salida del módem móvil



En la parte superior de la pantalla se muestran los números CCID e IMSI obtenidos de la tarjeta SIM. Si dichos números no están presentes, o si se muestra algún elemento no válido como número, significa que hubo un problema al leer la tarjeta SIM. Verifique que la tarjeta SIM esté correctamente instalada. El número de IMEI procede del conjunto de chips del módem móvil.

Modo

El selector de modo está desactivado de forma predeterminada. Si se ajusta como activado se inicia el daemon punto a punto (pppd) y se pone en funcionamiento el módem móvil. Cuando está activado, el módem móvil se enciende tras cada reinicio.

Si se encuentra en el modo de conmutación por error, el módem móvil se enciende aunque esté desactivado. Las condiciones de conmutación por error siguen activadas.

Estado

La línea de estado indica el estado actual:

- Desactivado o activado: Indica si el módem móvil está activado o desactivado. El módem se puede activar manualmente o mediante conmutación por error.
- Transceptor desactivado: Ajuste predeterminado. El transceptor está desactivado cuando el módem está desactivado.
- Transceptor activado: El transceptor estará activo cuando se haya activado el módem, ya sea de forma manual o mediante conmutación por error.
- Conmutación por error: No: Si se configura como un dispositivo con conmutación por error, indica si el módem móvil está en conmutación por error.
- Activo o inactivo: Indica si la interfaz de la red del módem está activa.

Iniciar chat

La secuencia de comandos de chat, en una ventana del editor. Puede realizar cambios personalizados en la secuencia de comandos de chat desde esta ventana. La secuencia de comandos de chat predeterminada procede del proveedor de servicio.

NOTA: La mayoría de usuarios deben usar la secuencia de comandos de chat predeterminada.

APN

El nombre del punto de acceso, que figura en la secuencia de comandos de chat. Desde este campo, puede modificar el APN sin tener que editar la secuencia de comandos de chat directamente. Si modifica el APN aquí, en la secuencia de comandos de chat se perderá cualquier otro cambio que haya realizado.

Reemplazar ruta predeterminada

Envía una opción de configuración al daemon ppp para que el módem móvil se convierta en la puerta de enlace predeterminada. La puerta de enlace se restaura cuando se apaga el módem móvil. Se trata de algo similar a introducir una ruta estática, pero resulta útil para que el módem móvil sea la puerta de enlace predeterminada para la conmutación por error.

Modo persistente

Cuando está activado el modo persistente, el sistema de consola intenta poner de nuevo en funcionamiento el módem móvil si el daemon ppp se apaga por cualquier motivo. Si está desactivado, el módem móvil seguirá sin funcionar si el daemon ppp se apaga (por ejemplo, si se interrumpe el servicio móvil).

Función de calidad de la señal

Permite obtener lecturas de nivel de señal sin procesar y de índice de error binario, para poder diagnosticar un problema de conexión con la red móvil o una conexión lenta. Haga clic en *Verificación de señal* para obtener una respuesta.

El nivel de señal puede oscilar entre -113 db o menos y -51 db o más. El índice de error binario oscila entre menos de un 1% y un 12,8% o más.

Puede obtener una comprobación de la calidad de la señal mientras el módem está en sesión. El transceptor del módem está encendido, pero no se está ejecutando la secuencia de comandos de chat. En sesión, la interfaz serie del módem móvil está bloqueada para el daemon ppp.

Introducción del PIN de la SIM

Haga clic en *PIN/contraseña de la SIM* para introducir su PIN y activar el servicio móvil con una tarjeta SIM.

Verificación de la conexión móvil

La línea de estado de la pantalla de marcado de salida indica si el módem móvil está activo. Puede obtener la dirección IP del módem móvil desde la página de Supervisión. Vaya a *Supervisión - Red - Dispositivos*.

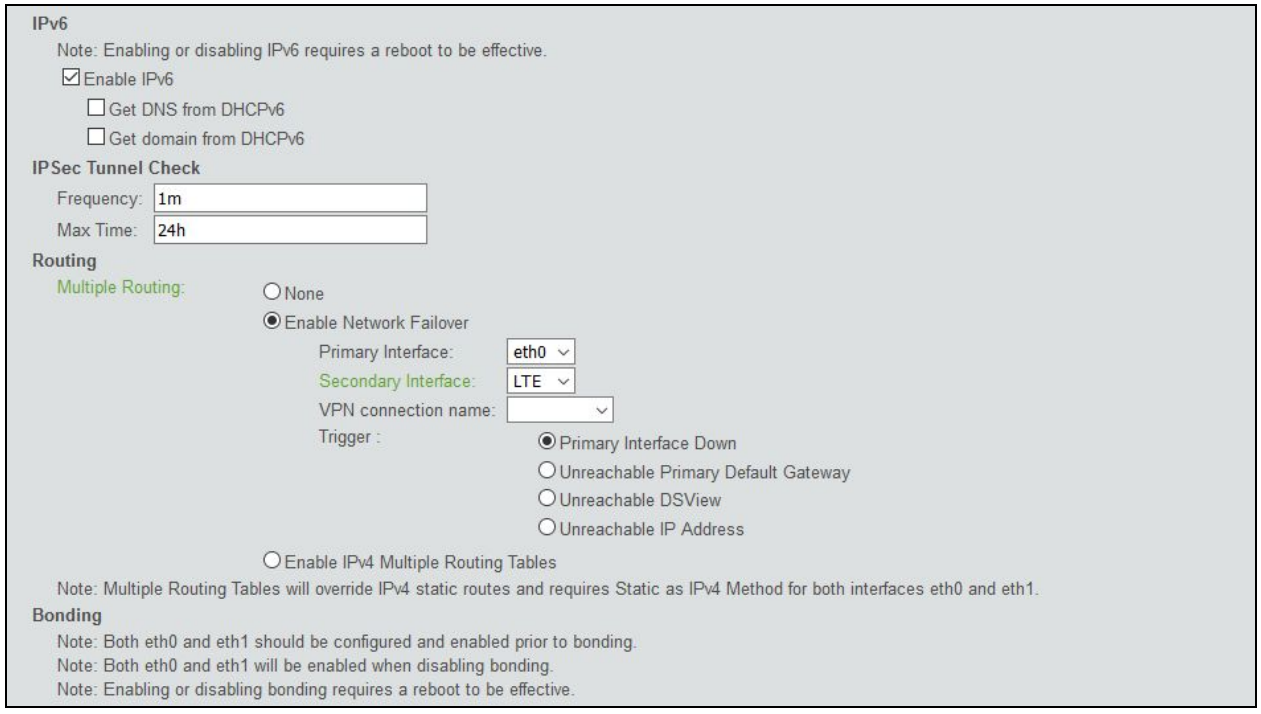
En la página Dispositivos, el dispositivo ppp0-LTE es el módem. Se muestra la dirección IPv4 y el estado del enlace está activo cuando el módem está activado. La dirección IP es para el servicio de red privada. La dirección IPv4 no es fija y cambia cada vez que se reinicia o se restablece la conexión de la red móvil.

NOTA: Los usuarios avanzados pueden ejecutar una secuencia de comandos para obtener más información sobre depuración.

Uso del módem móvil en la conmutación por error

Vaya a *Red - Ajustes* y seleccione *Enrutamiento - Activar conmutación por error de la red*. En la lista de la interfaz secundaria, seleccione el dispositivo ppp0 (o lte0). Puede realizar esto tanto si el módem está activado como si no.

Figura 3.6 Configuración del módem móvil como dispositivo de conmutación por error



La condición de conmutación por error, que en este caso es la interfaz primaria, no está activa. Con la conmutación por error activada, si eth0 se vuelve inactiva, el módem móvil se activará para entrar en funcionamiento. Con el proveedor de servicio, esto solo proporciona acceso a Internet. Un servidor de Internet no puede iniciar sesión directamente. Es posible que algún tipo distinto de servicio o proveedor le pueda proporcionar acceso.

La otra alternativa es usar un servicio VPN. Configure la VPN para conectarse a través de IPsec a una puerta de enlace segura con una dirección IP pública, y después podrá acceder al sistema de consola a través del túnel IPsec.

Para configurar IPsec:

1. Active el servicio IPsec. Vaya a la página *Sistema - Seguridad - Perfil de seguridad*, desplácese hacia abajo y seleccione la casilla para Activar IPsec.
2. Vaya a la página *Red - IPSec (VPN)* y agregue un nuevo perfil de VPN.
3. Introduzca los parámetros de la VPN. A continuación se muestra una imagen de ejemplo. Cuando haya terminado, haga clic en *Guardar*.
4. Vuelva a la pantalla de conmutación por error en *Red - Ajustes* y seleccione la VPN de conmutación por error.

Figura 3.7 Ejemplo de VPN IPsec

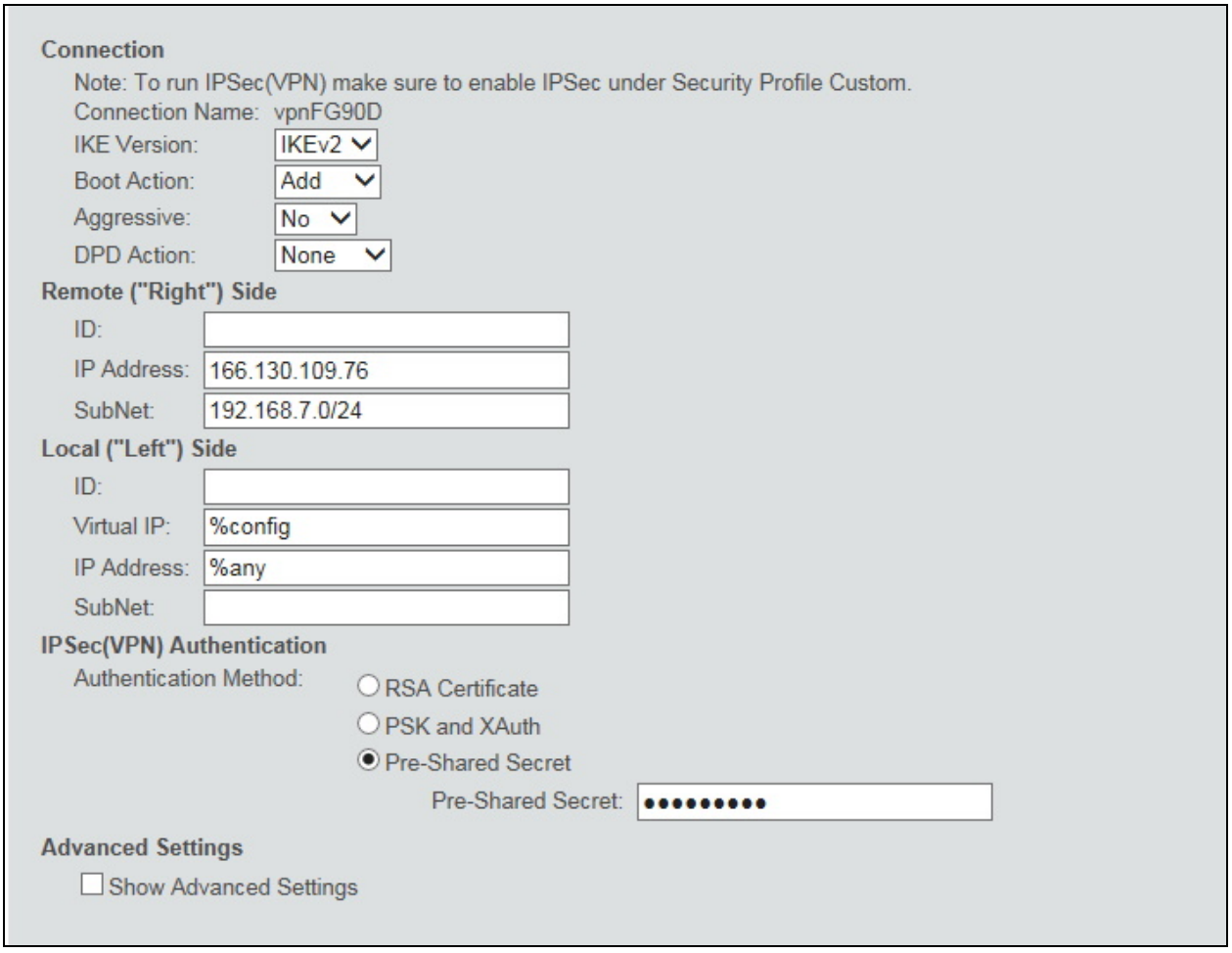
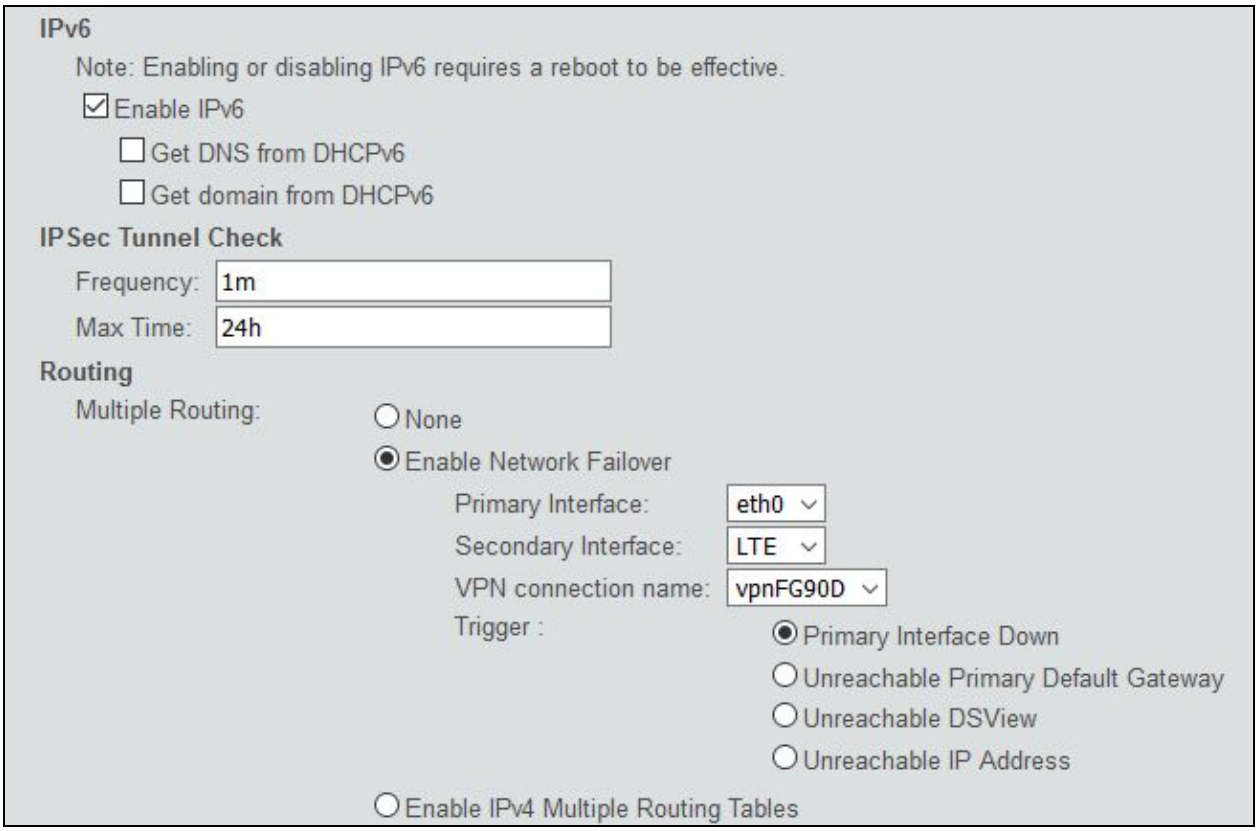


Tabla 3.19 Descripciones de IPsec

Elemento	Descripción
Versión de IKE	Normalmente será IKEv2, salvo que la puerta de enlace a la que se esté conectando sea antigua.
Acción de inicio	Ajústelo en Añadir para conmutación por error. Si lo ajusta en Iniciar, la VPN intentará activarse en cuanto se reinicie el sistema de consola.
Agresiva	Se debe ajustar en No.
Acción DPD	Ninguna. Se podría ajustar a "Reiniciar". Significa "Detección de pares muertos".
Identificador	Se deja en blanco porque desea identificar la puerta de enlace remota por la dirección IP.
Subred	La subred a la que estamos accediendo por detrás de la puerta de enlace segura remota. En este caso, se está usando una Fortigate, y se está utilizando la subred de su LAN.
Lado izquierdo local	
Identificador	Los identificadores se utilizan para identificar cada lado, pero si se deja en blanco simplemente se usa la dirección IP.
IP virtual	Asigna la dirección IP del túnel.Si se ajusta en **%config** significa que estamos adquiriendo una dirección de la puerta de enlace remota segura.
Dirección IP	La dirección IP del sistema de consola que participa en el túnel. Para Ethernet normal, se puede ajustar en una dirección IP fija. En cuanto al módem móvil, el proveedor asigna la dirección IP, y en el caso del servicio AT&T, cambia. Si se ajusta en **%any** significa que se usará cualquier interfaz o dirección IP que esté activa.
Autenticación IPsec(VPN)	Ajústelo en "secreto precompartido" para usar la clave de paso/contraseña única en el túnel. Cada extremo de este túnel IPsec debe usar la misma contraseña/palabra secreta. Por supuesto, también podría usar los certificados X509/RSA.
Ajustes avanzados	Se han dejado en los valores predeterminados para que IPsec negocie el conjunto de cifrado.

Figura 3.8 Ejemplo de VPN seleccionada para conmutación por error



Con la opción Reemplazar ruta predeterminada activada, un evento de conmutación por error (eth0 se ha vuelto inactivo) pone en funcionamiento el módem móvil y, a continuación, inicia la VPN. Los clientes LAN de la puerta de enlace remota pueden acceder al sistema de consola a través de la dirección IP del túnel virtual.

3.3.9 Dispositivos conectables

El sistema de consola admite varios dispositivos conectables conectados a sus puertos USB. Algunos modelos también admiten una sola tarjeta SD en la ranura para tarjetas SD.

NOTA: Cuando un dispositivo conectable no está en la lista actual de dispositivos conectables admitidos, el sistema de consola puede intentar configurar el dispositivo con la configuración estándar, para que pueda funcionar con normalidad. Asimismo, cuando un dispositivo conectable no aparezca en la base de datos interna, puede que en la columna Información del dispositivo no se muestre ningún texto o se muestre un texto diferente según el tipo de tarjeta. Un ejemplo es dispositivo desconocido f024 (rev 01).

Para instalar y detectar un dispositivo conectable:

1. En la barra de navegación lateral, seleccione *Dispositivos conectables*.
2. Haga clic en *Activar detección de dispositivos conectables* para detectar dispositivos conectables conectados, a menos que esta función ya se haya activado en la página Sistema - Seguridad.
3. Conecte un dispositivo a un puerto USB o introduzca una tarjeta SD en la ranura para tarjetas SD del sistema de consola.
4. En la tabla Dispositivos conectables se muestran todos los dispositivos conectables detectados.

NOTA: Para desactivar la detección de dispositivos conectables, haga clic en *Desactivar detección de dispositivos conectables*.

Para expulsar o eliminar un dispositivo conectable:

1. En la barra de navegación lateral, seleccione *Dispositivos conectables*.
2. Seleccione la casilla de verificación situada junto al dispositivo conectable que desee expulsar o eliminar.
3. Haga clic en *Expulsar* o *Eliminar* como desee. Haga clic en *Guardar*.

NOTA: Siempre expulse los dispositivos conectables de la IU web antes de quitar los dispositivos físicamente.

Configuración de los dispositivos

Los dispositivos de almacenamiento se montan y configuran automáticamente una vez detectados por el sistema de consola, a menos que se haya desactivado la compatibilidad con dispositivos de almacenamiento. Las tarjetas Ethernet, los módems y los dispositivos de consola USB deben configurarse.

NOTA: La configuración de los dispositivos inalámbricos solo surte efecto después de que el dispositivo se haya expulsado y vuelto a introducir.

Para configurar un dispositivo conectable:

1. En la barra de navegación lateral, seleccione *Dispositivos conectables*.
2. Para un dispositivo de red, haga clic en su nombre para configurar sus parámetros de red.

   -O bien-

   Para un módem (V.92), haga clic en la casilla situada junto a su nombre y, a continuación, haga clic en *Definir marcado de entrada* o *Definir marcado de salida* para configurar sus parámetros de marcado de entrada y marcado de salida.

   -O bien-

   Para un dispositivo de consola USB, haga clic en la casilla junto a su nombre y, a continuación, haga clic en *Definir consola* para añadirlo al sistema como otro puerto. Puede aceptar la asignación del puerto predeterminado o introducir un puerto no usado en el campo Puerto y hacer clic en *Asignar*. A continuación, vaya a la página *Puertos - Puertos serie* para configurar y activar el puerto añadido.

Asignación de consolas USB

Los dispositivos de consola USB se corresponderán de forma predeterminada con un puerto basado en el número de puertos serie del sistema de consola. En la siguiente tabla se muestran las asignaciones de puertos predeterminados.

Tabla 3.20 Asignación de la consola USB ACS80X

	Puertos USB			
MODELO	Superior izquierdo	Inferior izquierdo	Superior derecho	Inferior derecho
ACS802	3	4	5	6
ACS804	5	6	7	8
ACS808	9	10	11	12

Tabla 3.21 Asignación de la consola USB ACS80XX

	Puertos USB traseros						Puertos USB frontales	
Modelo	Superior izquierdo	Inferior izquierdo	Superior medio	Inferior medio	Superior derecho	Inferior derecho	Superior	Inferior
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

Si el puerto asignado de forma predeterminada ya está en uso o si el dispositivo USB no está conectado directamente al sistema de consola, se utilizará el siguiente puerto disponible después de los puertos reservados. Por ejemplo, en un sistema de consola ACS808, el siguiente puerto disponible es el puerto 13.

Conexión en caliente

Los dispositivos de consola serie pueden desconectarse y volverse a conectar en el mismo puerto USB sin interrumpir ninguna sesión en serie abierta. En la mayoría de casos, el dispositivo USB recibe el mismo nombre de dispositivo asignado por Linux. En algunos casos, se asigna un nombre distinto si el nombre original ya está siendo usado.

NOTA: El dispositivo debe volverse a conectar en el mismo puerto para activar la conexión en caliente.

3.3.10 Autenticación

La autenticación se puede realizar de forma local, con OTP o de forma remota en un servidor de autenticación LDAP, Radius, Kerberos o TACACS+. Si el sistema de consola está gestionado por un servidor de DSView, también se admite la autenticación de DSView. El sistema de consola también admite las autorizaciones de grupos remotos para los métodos de autenticación LDAP, Radius, Kerberos y TACACS+.

Hay disponibles los siguientes tipos de mecanismos de reserva:

La autenticación local se puede probar en primer lugar, seguido por la remota, si la autenticación local falla (local/método_remoto).

-O bien-

La autenticación remota se puede probar en primer lugar, seguida por la local (método_remoto/local).

-O bien-

La autenticación local solo se puede intentar si un servidor de autenticación remoto está inactivo (método_remoto_inactivo_local).

Un administrador puede configurar la autenticación mediante la utilidad CLI y la interfaz de usuario web. El método de autenticación predeterminado para el sistema de consola y los puertos serie es local. Cualquier método de autenticación que esté configurado para el sistema de consola o los puertos se utiliza para la autenticación de cualquier usuario que intente iniciar sesión mediante Telnet, SSH o la interfaz de usuario web.

Autenticación del equipo

El sistema de consola se autentica para el sistema de consola y los puertos, ya sea en grupos o individualmente.

NOTA: Cuando se utilice la autorización de grupos, se recomienda usar la misma autenticación tanto para el sistema de consola como para todos los puertos serie, o bien utilizar la autenticación de inicio de sesión único para facilitar la autorización de grupos.

Cuando la autenticación de inicio de sesión único está desactivada, el sistema de consola utiliza la configuración individual basada en el destino del acceso: el propio sistema de consola o cada puerto serie. Los usuarios deben usar su contraseña cada vez que acceden a un puerto individual. Si está activada, la autenticación de inicio de sesión único utilizará el servidor de autenticación que elija en el menú desplegable para todos los accesos y no será necesaria ninguna autenticación adicional.

NOTA: Si se selecciona *sin configurar* en el menú desplegable, se permitirá que los puertos sigan usando servidores de autenticación individuales y se necesitará la contraseña la primera vez que acceda a cualquier puerto. A partir de ese momento, el puerto no requerirá autenticación de contraseña si la autenticación de inicio de sesión único está activada.

Para configurar la autenticación para el sistema de consola:

1. Haga clic en *Autenticación - Autenticación del equipo*.
2. Seleccione el servidor de autenticación deseado en el menú desplegable Tipo de autenticación.
3. Seleccione *Activar reserva a tipo local para usuario raíz en el puerto de consola del equipo* cuando la autenticación remota falle y un administrador desee acceder al equipo a través del puerto de consola como usuario raíz.
4. Seleccione *Activar inicio de sesión único* para activar la autenticación de inicio de sesión único y seleccione el servidor de autenticación deseado en el menú desplegable Tipo de autenticación.
5. Haga clic en *Guardar*.

Servidores de autenticación

Cuando se use un servidor de autenticación, debe configurar su dirección IP y, en la mayoría de los casos, otros parámetros para poder utilizarlo. Es necesario configurar los siguientes servidores de autenticación: Servidores RADIUS, TACACS+, LDAP(S)|AD, Kerberos, y DSView.

Para configurar un servidor de autenticación RADIUS:

1. Seleccione *Autenticación - Servidores de autenticación - RADIUS*.
2. Introduzca las direcciones IP del primer servidor de autenticación y del primer servidor de cuentas.

3. Si se usan, introduzca las direcciones IP del segundo servidor de autenticación y del segundo servidor de cuentas.
4. Introduzca la palabra secreta o frase de contraseña en el campo Secreto (se aplica a los servidores de autenticación y contabilidad primero y segundo) y, a continuación, vuelva a introducir la palabra secreta o la frase de contraseña en el campo Confirmar secreto.
5. Introduzca el número de segundos deseado para el tiempo de espera del servidor en el campo Tiempo de espera.
6. Introduzca el número de reintentos deseado en el campo Reintentos.
7. Si selecciona la casilla de verificación *Activar el atributo de tipo de servicio para especificar el grupo de autorización*, introduzca el nombre del grupo de autorización para cada uno de los siguientes tipos de servicio: inicio de sesión, estructurado, inicio de sesión de retorno de llamada, retorno de llamada estructurado, saliente y administrativo.
8. Haga clic en *Guardar*.

Para configurar un servidor de autenticación TACACS+:

1. Seleccione *Autenticación - Servidores de autenticación - TACACS+*.
2. Introduzca las direcciones IP del primer servidor de autenticación y del primer servidor de cuentas.
3. Si se usan, introduzca las direcciones IP del segundo servidor de autenticación y del segundo servidor de cuentas.
4. Seleccione el servicio deseado (PPP o raccess) en el menú desplegable Servicio.
5. Introduzca su palabra secreta o frase de contraseña en el campo Secreto (se aplica a los servidores de autenticación y contabilidad primero y segundo) y, a continuación, vuelva a introducir la palabra secreta o la frase de contraseña en el campo Confirmar secreto.
6. Introduzca el número de segundos deseado para el tiempo de espera del servidor en el campo Tiempo de espera.
7. Introduzca el número de reintentos deseado en el campo Reintentos.
8. Si selecciona la casilla de verificación *Activar el atributo de tipo de servicio para especificar el grupo de autorización*, introduzca el nombre del grupo de autorización para un máximo de 15 niveles de usuario.
9. Haga clic en *Guardar*.

Para configurar un servidor de autenticación LDAP(S)|AD:

1. Seleccione *Autenticación - Servidores de autenticación - LDAP(S)|AD*.
2. Introduzca la dirección IP del servidor.
3. Introduzca la base.
4. En el menú desplegable Seguro, seleccione *Desactivado*, *Activado* o *Start_TLS*.
5. Introduzca el nombre de usuario de base de datos.
6. Introduzca la contraseña de base de datos y, a continuación, vuelva a escribir la contraseña de base de datos en el campo Confirmar contraseña.
7. Introduzca los atributos de inicio de sesión que desee.
8. Haga clic en *Guardar*.

Para configurar un servidor de autenticación Kerberos:

1. Seleccione *Autenticación - Servidores de autenticación - Kerberos*.

2. Introduzca la dirección IP (dominio) del servidor.
3. Introduzca el nombre de dominio del dominio (ejemplo: AVOCENT.com).
4. Introduzca el nombre de dominio (ejemplo: .avocent.com).
5. Haga clic en *Guardar*.

Para configurar un servidor de autenticación DSView:

1. Seleccione *Autenticación - Servidores de autenticación - DSView*.
2. Introduzca la dirección IP 1 - 4 para los servidores DSView en los campos pertinentes.
3. Haga clic en *Guardar*.

3.3.11 Cuentas de usuarios y grupos de usuarios

El acceso a puertos y otros privilegios se pueden gestionar en base a las autorizaciones que un administrador puede asignar a grupos de usuarios personalizados y a cuentas de usuario individuales.

Los grupos y los usuarios también pueden estar autorizados a gestionar la alimentación mientras están conectados a dispositivos. El sistema de consola cuenta con dos usuarios predeterminados (administrador y raíz) y con cuatro grupos de usuarios predefinidos: administrador, administrador de equipo, perfil de inicio de sesión en el shell y usuario.

Se debe definir una cuenta de usuario para cada usuario en el sistema de consola o en un servidor de autenticación. Los usuarios administrador y raíz tienen cuentas de forma predeterminada, y cualquiera de los administradores puede añadir y configurar otras cuentas de usuario. Cada cuenta de usuario local se asigna a uno o más de los grupos de usuarios.

NOTA: Cuando se elimina un usuario en todos los grupos, los privilegios de ese usuario volverán a ser los del grupo de usuarios predeterminados. Por esta razón, se recomienda usar grupos personalizados y no conceder privilegios adicionales al grupo de usuarios predeterminados.

De forma predeterminada, todos los usuarios tienen acceso a todos los puertos del sistema de consola. Para autorizar el acceso mediante grupos de usuarios, el administrador debe permitir que el acceso a los puertos sea controlado por autorizaciones asignadas a los grupos de usuarios.

Para permitir que el acceso a los puertos sea controlado por autorizaciones asignadas a los grupos de usuarios:

1. En la pestaña Experto de la barra de navegación lateral, haga clic en *Sistema - Seguridad - Perfil de seguridad*.
2. En el encabezado Dispositivos serie, haga clic en el botón Controlado por los derechos de acceso asignados a grupos de usuarios y a usuarios específicos y, a continuación, haga clic en *Guardar*.

Cuentas locales

El sistema de consola tiene dos cuentas de usuario local de forma predeterminada de fábrica:

- admin: Realiza la configuración de red inicial. El usuario administrador es miembro del grupo de administradores y puede configurar el sistema de consola y los puertos, así como las autorizaciones de usuarios y grupos.

- raíz: Tiene los mismos permisos administrativos que el usuario administrador, pero también tiene privilegios ilimitados desde el shell. El usuario raíz es miembro de los grupos de administración y de perfil de inicio de sesión en el shell. Cuando un usuario raíz inicia sesión a través del puerto de CONSOLA, SSH o Telnet, la sesión está predefinida por el perfil de inicio de sesión para ir directamente al shell. El perfil de inicio de sesión se puede personalizar para que no vaya directamente al shell.

Para ver los derechos de acceso del equipo del usuario:

1. Haga clic en *Usuarios - Cuentas locales - Nombres de usuario*. La lista de nombres de usuario aparece en la zona de contenido.
2. Haga clic en un nombre de usuario en el encabezado Nombre de usuario. En la zona de contenido se muestra la información del usuario para el usuario seleccionado.

NOTA: Cuando se selecciona cualquier nombre de usuario, tanto la zona de contenido como la barra de navegación lateral cambian. En la barra de navegación lateral se muestran opciones de menú específicas para miembros y derechos de acceso (entre los que se incluyen derechos serie, de alimentación y del equipo).

3. En la barra de navegación lateral, haga clic en *Derechos de acceso - Serie* o *Derechos de acceso - Alimentación* para acceder a las pantallas en las que se muestran los derechos de acceso y permisos fijos para el usuario seleccionado.

NOTA: Las pantallas Serie y Alimentación son de solo lectura y no se pueden cambiar.

4. En la barra de navegación lateral, haga clic en *Derechos de acceso - Equipo*. Aparecerá la pantalla Derechos de acceso del equipo, en la que se indican todos los derechos de acceso disponibles para el usuario. Los derechos de acceso del equipo disponibles son:
   - Ver información del equipo
   - Desconectar sesiones
   - Reiniciar equipo
   - Actualizar flash del equipo y reiniciar equipo
   - Configurar ajustes del equipo
   - Configurar cuentas de usuario
   - Realizar copia de seguridad/restaurar configuración
   - Acceso al shell
   - Transferir archivos
   - Acceso telefónico

Para añadir nuevos usuarios:

1. Haga clic en *Usuarios - Cuentas locales - Nombres de usuario*. Se muestra la pantalla Nombres de usuario con una lista de todos los usuarios.
2. Haga clic en *Añadir*. Se muestra la pantalla Información del usuario local.
3. Introduzca el nuevo nombre de usuario y una contraseña y, a continuación, confirme la contraseña.
4. Marque o desmarque la casilla de verificación *El usuario debe cambiar la contraseña en el siguiente inicio de sesión*.

5. Para añadir el usuario a un grupo de usuarios disponible, seleccione el nombre del grupo de usuarios en el cuadro de la izquierda y haga clic en *Añadir* (usuario es el grupo predeterminado). Puede eliminar un grupo de usuarios del cuadro de la derecha si lo selecciona y hace clic en *Eliminar*.
6. Introduzca los parámetros que desee para la opción Caducidad de la contraseña.
   - Mín. días: Introduzca el número mínimo de días permitidos entre los cambios de contraseña. Los cambios de contraseña que se intenten antes se rechazarán. Para desactivar la restricción en el número de días que se permiten entre los cambios de contraseña, deje este campo vacío.
   - Máx. días: Introduzca el número máximo de días de validez de una contraseña. Una vez transcurrido este período, se forzará un cambio de contraseña. Para desactivar la restricción para el número máximo de días de validez de una contraseña, deje este campo vacío.
   - Días de advertencia: Introduzca el número de días en el que se emite una advertencia al usuario antes de la caducidad. Si se introduce 0, la advertencia se emitirá el día de la caducidad. Para desactivar la advertencia, deje este campo vacío.
7. Introduzca la fecha de Caducidad de la cuenta que desee (AAAA-MM-DD).
8. Haga clic en *Guardar*.

Para configurar las reglas de contraseña:

1. Haga clic en *Usuarios - Cuentas locales - Reglas de contraseña*.
2. Si se desea una contraseña compleja (recomendado), asegúrese de que la opción *Comprobar complejidad de la contraseña* esté seleccionada.
3. Si la opción de complejidad de la contraseña está activada, introduzca los valores de complejidad de la contraseña que desee.
4. Introduzca los parámetros que desee para la opción Caducidad predeterminada.
5. Haga clic en *Guardar*.

Grupos de usuarios

Los grupos de usuarios reciben acceso y autorizaciones de forma predeterminada o según lo asignado por un administrador. Los administradores pueden alterar los permisos y los derechos de acceso de los usuarios pertenecientes a los grupos de administradores del equipo o de usuarios o crear grupos adicionales con permisos y derechos de acceso personalizados. Los administradores pueden añadir, eliminar o modificar permisos y derechos de acceso para usuarios de cualquier grupo en cualquier momento.

Si un administrador configura el sistema de consola para restringir el acceso de los usuarios a los puertos, el administrador puede asignar usuarios a los grupos que están autorizados para acceder a los puertos. El administrador también puede autorizar grupos para la gestión de alimentación y la gestión de búfer de datos.

Este documento y el software hacen referencia a usuarios cuyas cuentas están configuradas en servidores de autenticación remota como usuarios remotos. Los usuarios remotos no necesitan cuentas locales.

NOTA: Cuando se elimina un usuario en todos los grupos, los privilegios de ese usuario volverán a ser los del grupo de usuarios predeterminados. Por esta razón, se recomienda usar grupos personalizados y no conceder privilegios adicionales al grupo de usuarios predeterminados.

Los servicios de autenticación Radius, TACACS+ y LDAP permiten la configuración de grupos. Si un usuario remoto está configurado como miembro de un grupo remoto, el servidor de autenticación proporciona el nombre del sistema de consola cuando autentica al usuario. Un grupo local con el mismo nombre también se debe configurar en el sistema de consola. Si un servidor de autenticación autentica un usuario remoto pero no devuelve un grupo, el usuario remoto se asigna de forma predeterminada al grupo de usuarios.

Grupo de administradores

Los miembros del grupo de administradores tienen privilegios administrativos plenos que no se pueden modificar. Tienen las mismas autorizaciones de acceso y configuración que el usuario administrador predeterminado. Los administradores pueden configurar puertos, añadir usuarios y gestionar dispositivos de alimentación conectados al sistema de consola.

Para ver los derechos de acceso del equipo del administrador:

1. Haga clic en *Usuarios - Autorización - Grupos*. Aparece la pantalla Nombres de grupo, en la que se muestran los tres grupos de usuarios predeterminados junto con los grupos que se puedan haber creado.
2. Haga clic en *administrador* en el encabezado Nombre del grupo. En la zona de contenido se mostrará la pantalla Miembros, en la que aparecen todos los miembros pertenecientes al grupo de administradores (los miembros predeterminados son usuarios administradores y raíz).

NOTA: Cuando se selecciona cualquier nombre de grupo, tanto la zona de contenido como la barra de navegación lateral cambian. En la barra de navegación lateral se muestran opciones de menú específicas para miembros y derechos de acceso (entre los que se incluyen derechos serie, de alimentación y del equipo).

3. En la barra de navegación lateral, haga clic en *Derechos de acceso - Serie* o *Derechos de acceso - Alimentación* para acceder a las pantallas en las que se muestran los derechos de acceso y permisos fijos para los miembros del grupo de administradores pertenecientes a los puertos serie y a la gestión de alimentación.

NOTA: Las pantallas Serie y Alimentación son de solo lectura y no se pueden cambiar.

4. En la barra de navegación lateral, haga clic en *Derechos de acceso - Equipo*. Aparecerá la pantalla Derechos de acceso del equipo, en la que se indican todos los derechos de acceso disponibles para un miembro que pertenezca al grupo de administradores. Todos los derechos de acceso del equipo se muestran activados (marcados). Los derechos de acceso del equipo disponibles son:
    - Ver información del equipo
    - Desconectar sesiones
    - Reiniciar equipo
    - Actualizar flash del equipo y reiniciar equipo
    - Configurar ajustes del equipo
    - Configurar cuentas de usuario
    - Realizar copia de seguridad/restaurar configuración
    - Acceso al shell
    - Transferir archivos
    - Acceso telefónico

NOTA: La pantalla Derechos de acceso del equipo para los grupos de usuarios de administradores y de administradores del equipo es de solo lectura y no se puede cambiar. Si se desmarca cualquier casilla y se hace clic en *Guardar*, aparecerá un mensaje de error. El sistema de consola mantendrá todos los derechos seleccionados.

Grupo de administradores del equipo

Los miembros del grupo de usuarios de administradores del equipo tienen acceso a los puertos serie y a las opciones de gestión de alimentación, a no ser que el acceso esté restringido por el perfil de seguridad. Los miembros del grupo también comparten todos los derechos de acceso del equipo como administrador, excepto para configurar cuentas de usuario y el acceso al shell, que están permanentemente desactivados para este grupo.

Grupo de usuarios

Los miembros del grupo de usuarios tienen acceso a los dispositivos de destino, a no ser que el acceso esté restringido por un administrador. Cuando un perfil de seguridad restringe el acceso a los puertos de forma global, un administrador puede conceder acceso a los puertos a los miembros del grupo de usuarios. Los miembros del grupo de usuarios no tienen derechos de acceso para el sistema de consola.

Los administradores pueden añadir permisos y derechos de acceso del equipo. Los administradores también pueden añadir usuarios a grupos de usuarios personalizados para añadir permisos y derechos de acceso según sea necesario. De forma predeterminada, todas las opciones de la pantalla Derechos de acceso del equipo estarán desactivadas.

NOTA: Un administrador puede modificar la pantalla Derechos de acceso del equipo para el grupo de usuarios en cualquier momento. Esto cambiará los derechos de acceso para todos los miembros del grupo de usuarios del sistema de consola.

Perfil de inicio de sesión en el shell

Los miembros del grupo de perfil de inicio de sesión en el shell tienen acceso al shell después de iniciar sesión. De forma predeterminada, el usuario raíz pertenece a este grupo. Este no es un grupo protegido y se puede eliminar.

Gestión de grupos de usuarios

Los administradores y miembros del grupo de administradores pueden crear grupos de usuarios personalizados que contengan a cualquier usuario.

Para crear un grupo de usuarios personalizado:

1. .Haga clic en *Usuarios - Autorización - Grupos*. Aparece la pantalla Grupos y en ella se muestra una lista de los tres grupos de usuarios predeterminados y cualquier grupo de usuarios personalizado adicional que se haya creado.
2. Haga clic en *Añadir* en la zona de contenido.
3. Introduzca el nombre del nuevo grupo de usuarios que está creando.
4. Haga clic en *Guardar*.

Para añadir miembros a un grupo de usuarios:

1. Haga clic en *Usuarios - Autorización - Grupos*.
2. Haga clic en el nombre del grupo de usuarios.

3. Haga clic en *Añadir*. Aparece la pantalla de asignación de miembros, en la que se muestra una lista de usuarios disponibles en el cuadro de la izquierda y un cuadro vacío a la derecha.
4. Mueva usuarios del cuadro Usuarios disponibles de la izquierda al cuadro de la derecha; para ello, haga doble clic en el nombre de usuario o seleccione el nombre y haga clic en el botón *Añadir*. Para eliminar nombres del cuadro de la derecha, haga doble clic en el nombre de usuario o seleccione el nombre y haga clic en el botón *Eliminar* .
5. Si desea añadir usuarios remotos al nuevo grupo de usuarios (estos deben ser nombres válidos en el servidor de autenticación remota), añádalos en el campo Nuevos usuarios remotos.
6. Haga clic en *Guardar*.

Para eliminar miembros de un grupo de usuarios:

1. Haga clic en *Usuarios - Autorización - Grupos*.
2. Haga clic en el nombre del grupo de usuarios.
3. Marque la(s) casilla(s) del (de los) miembro(s) que desee eliminar. Haga clic en *Eliminar* para eliminar los miembros seleccionados.

Para configurar un tiempo de espera de inactividad de sesión y/o un perfil de inicio de sesión para un grupo:

1. Haga clic en *Usuarios - Autorización - Grupos*.
2. Haga clic en el nombre del grupo cuyo tiempo de espera de inactividad de sesión y/o perfil de inicio de sesión desee definir. En la barra de navegación lateral, haga clic en *Perfil de inicio de sesión*.
3. Seleccione el botón de opción para utilizar los ajustes globales de tiempo de espera de sesión o para usar ajustes personalizados para el grupo de usuarios. Si se usan ajustes personalizados, introduzca el tiempo de espera de sesión personalizado (en segundos) en el campo.
4. Marque la casilla *Activar perfil de inicio de sesión*.
5. Haga clic en *ts_menu* para usar la aplicación ts_menu cuando un miembro del grupo de usuarios seleccionado abra una sesión en el sistema de consola. Introduzca las opciones de ts_menu en el campo Opciones.

   -O bien-

   Haga clic en *CLI* para usar CLI al abrir una sesión. Introduzca el comando de CLI en el campo Cmd de CLI y marque la casilla si desea salir después de ejecutar el comando.
6. Haga clic en *Guardar*.

NOTA: Si el usuario pertenece a varios grupos, el perfil de inicio de sesión utilizado será el primer perfil de inicio de sesión activado basado en el orden alfabético del grupo.

Tabla 3.22 Opciones de ts_menu

Comando	Descripción
-p	Muestra el puerto TCP
-i	Muestra la IPv4 local asignada al puerto serie
-i6	Muestra la IPv6 local asignada al puerto serie
-u <nombre>	Nombre de usuario que se usará en la sesión de destino
-e <[^]char>	Carácter de escape utilizado para cerrar la sesión de destino. Valor predeterminado: **Ctrl-X**
-l	Ordenar puertos de la lista y salir
-ro	Modo de solo lectura
<nombre del puerto>	Conectar directamente a un puerto serie
-t	Tiempo de espera de inactividad en segundos para elegir el destino

Para añadir acceso a puertos serie para un grupo de usuarios:

1. Haga clic en *Usuarios - Autorización - Grupos*.
2. Haga clic en el nombre del nuevo grupo de usuarios.
3. En la barra de navegación lateral, haga clic en *Derechos de acceso*.
4. En la zona de contenido, haga clic en *Añadir*.
5. Mueva los dispositivos de destino serie del cuadro Destino disponible de la izquierda al cuadro de la derecha; para ello, haga doble clic en el nombre del destino serie

   -O bien-

   Seleccione el destino y haga clic en el botón *Añadir*. Para eliminar destinos del cuadro de la derecha, haga doble clic en el destino o seleccione el destino y haga clic en el botón *Eliminar*.
6. Seleccione los derechos de acceso que desee.
7. Haga clic en *Guardar*. Aparecerá la pantalla Serie y se mostrarán los dispositivos de destino serie que ha autorizado para su uso por parte del grupo de usuarios con permiso(s) configurado(s).
8. Para editar los derechos de acceso, seleccione la casilla de verificación situada al lado de uno o más de los nombres de destino de la lista, según sea necesario, y haga clic en *Editar*. Aparecerá la pantalla Derechos de acceso del destino con los derechos de acceso. Seleccione los derechos de acceso que desee y haga clic en *Guardar*.

Para asignar acceso a una PDU para un grupo de usuarios:

NOTA: La asignación de acceso a una PDU a un grupo de usuarios les concede un acceso completo a todas las funciones de gestión de alimentación para esa PDU. Si desea que el grupo de usuarios solo tenga acceso a las tomas, utilice el procedimiento *Para asignar acceso a las tomas a un nuevo grupo de usuarios personalizado* que se describe a continuación.

1. Haga clic en *Usuarios - Autorización- Grupos*.
2. Haga clic en el nombre del grupo de usuarios.
3. En la barra de navegación lateral, haga clic en *Derechos de acceso - Alimentación*.
4. En la zona de contenido, haga clic en *Añadir*. Aparecerá la pantalla de asignación de PDU con la lista de PDU disponibles en el cuadro de la izquierda.

5. Mueva dispositivos de PDU del cuadro PDU disponible de la izquierda al cuadro de la derecha; para ello, haga doble clic en el nombre de la PDU o seleccione la PDU y haga clic en el botón *Añadir*. Para eliminar la PDU del cuadro de la derecha, haga doble clic en el nombre de la PDU o seleccione la PDU y haga clic en el botón *Eliminar* .
6. Puede especificar un identificador de PDU personalizado en el campo que hay en la parte inferior y asignarle un identificador de PDU personalizado.

NOTA: El identificador de PDU personalizado sirve para asignar la autorización de grupos de usuarios para gestionar las PDU que todavía no se han conectado al sistema de consola.

7. Haga clic en *Guardar*.

Para asignar acceso a tomas para un nuevo grupo de usuarios personalizado:

NOTA: La asignación de acceso a tomas a grupos de usuarios permite a los miembros del grupo encender o apagar las tomas y activar las funciones de bloqueo y de ciclo apagado y encendido en PDU compatibles.

1. Haga clic en *Usuarios - Autorización - Grupos*.
2. Haga clic en el nombre del nuevo grupo de usuarios.
3. En la barra de navegación lateral, haga clic en *Derechos de acceso - Alimentación - Tomas*.
4. Haga clic en *Añadir*. Aparece la pantalla Añadir toma.
5. Para PDU conectadas, haga clic en el botón *Seleccionar PDU* para activar los campos PDU conectadas y Tomas.
6. Seleccione *PDU conectada* en el menú desplegable.
7. Introduzca las tomas asignadas al grupo de usuarios.

NOTA: Las tomas se pueden especificar de forma individual (por ejemplo 1,3,6,8), como intervalo (por ejemplo 1-4) o como una combinación de ambos (por ejemplo 1-4,6,8, que asigna acceso a las tomas 1, 2, 3, 4, 6 y 8).

8. Si se ha creado un identificador de PDU personalizado para su uso en el futuro y desea preasignar tomas, haga clic en el botón *Personalizado* para introducir el nombre del identificador de PDU personalizado y especificar las tomas.
9. Haga clic en *Guardar*.

Para asignar acceso a un UPS para un grupo de usuarios:

1. Haga clic en *Usuarios - Autorización - Grupos*.
2. Haga clic en el nombre del grupo de usuarios.
3. En la barra de navegación lateral, haga clic en *Derechos de acceso - Alimentación - UPS*.
4. En la zona de contenido, haga clic en *Añadir*. Aparecerá la pantalla de asignación de UPS con la lista de UPS disponibles en el cuadro de la izquierda.
5. Mueva dispositivos de UPS del cuadro UPS disponible de la izquierda al cuadro de la derecha; para ello, haga doble clic en el nombre del UPS o seleccione el UPS y haga clic en el botón *Añadir*. Para eliminar dispositivos de UPS del cuadro de la derecha, haga doble clic en el nombre del UPS o seleccione el UPS y haga clic en el botón *Eliminar*.
6. Puede especificar un identificador de UPS personalizado en el campo que hay en la parte inferior de la página y asignarle un identificador de UPS personalizado.

NOTA: El identificador de UPS personalizado sirve para asignar la autorización de grupos de usuarios con el fin de gestionar dispositivos de UPS que todavía no se han conectado al sistema de consola.

Para asignar derechos de acceso del equipo para grupos de usuarios personalizados:

1. Haga clic en *Usuarios - Autorización - Grupos*.
2. Haga clic en el nombre del nuevo grupo de usuarios.
3. En la barra de navegación lateral, haga clic en *Derechos de acceso - Equipo*.
4. Seleccione los derechos de acceso del equipo que desee y haga clic en *Guardar*.

Para configurar un grupo en un servidor de autenticación TACACS+:

1. En el servidor, añada el servicio raccess a la configuración del usuario.
2. Defina a qué grupo(s) pertenece el usuario en el servicio raccess con esta sintaxis:

nombre_grupo = <Grupo1>[,<Grupo2,...,GrupoN>];

Por ejemplo:

En el sistema de consola, configure un nuevo grupo de autorización TACACS_1 y configure los derechos de acceso para este grupo. En el servidor TACACS+, configure el usuario "regina" con el siguiente atributo: `raccess = group_name=TACACS_1;`

A continuación, configure el usuario "special" con el atributo siguiente: `raccess = group_name=admin;`

Durante la fase de autenticación, el sistema de consola recibirá el atributo raccess desde el servidor TACACS+. El usuario regina pertenece al grupo de autorización TACACS_1 y el usuario special pertenece al grupo de autorización admin.

Para configurar un grupo en un servidor de autenticación RADIUS:

Defina a qué grupo(s) pertenece el usuario en el atributo FRAMED_FILTER_ID con la sintaxis siguiente:

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

NOTA: Los nombres de los grupos deben estar separados por una coma y terminar con un punto y coma.

NOTA: El ACS 800/8000 acepta varios atributos FRAMED_FILTER_ID.

Por ejemplo:

En el sistema de consola, configure nuevos grupos de autorización RADIUS_1 y RADIUS_2, y configure los derechos de acceso para estos grupos. En el servidor Radius, configure el usuario regina con el siguiente atributo:

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

-O bien-

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

-O bien-

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

A continuación, configure el usuario special con el atributo siguiente:

```
FramedFilterID = nombre_grupo=admin;
```

Durante la fase de autenticación, el sistema de consola recibirá el atributo FramedFilterID desde el servidor RADIUS. El usuario regina pertenece al grupo de autorización RADIUS_1 y RADIUS_2 y el usuario special pertenece al grupo de autorización admin.

Para configurar un grupo en un servidor de autenticación LDAP:

En el servidor LDAP, edite el atributo info para el usuario y añada la sintaxis siguiente.

```
info: nombre_grupo=<Grupo1>[,<Grupo2>,...,<GrupoN>];
```

Derechos de acceso del software DSView

Los administradores pueden configurar cómo se asignarán los derechos de sesión del visor del software DSView a los derechos de acceso del sistema de consola cuando un usuario acceda a un destino a través del visor serie del software DSView.

Para configurar la asignación de los derechos de acceso del software DSView a los derechos de acceso del sistema de consola:

1. Haga clic en *Usuarios – Autorización – Derechos de acceso de DSView*.
2. Seleccione los derechos de acceso que desee y haga clic en *Guardar*.

3.3.12 Notificaciones de eventos

El sistema de consola generará notificaciones para diversos eventos. Puede configurar el sistema de consola para dirigir o almacenar notificaciones de eventos en varios destinos para un uso inmediato o para su análisis posterior.

Lista de eventos

En la pantalla Lista de eventos se muestran los eventos del sistema de consola, cada uno de los cuales se puede configurar para capturas de SNMP, Syslog, software DSView, correo electrónico y SMS.

Para configurar eventos:

1. Haga clic en *Eventos y registros - Eventos*.
2. Localice los eventos para los que desee que se envíe una notificación y seleccione la(s) casilla (s) de verificación junto al (a los) número(s) de evento.
3. Haga clic en *Editar*.
4. Si desea enviar una notificación de evento para cualquier tipo de destino de evento configurado, haga clic en su casilla de verificación *Enviar* asociada.

5. Haga clic en *Guardar*. La página Eventos aparece con una X en la columna debajo del tipo de destino si se ha marcado la casilla Enviar en la pantalla Ajustes de eventos.

Destinos de evento

Para configurar destinos de evento:

1. Haga clic en *Eventos y registros - Destinos de evento*.
2. En el encabezado Syslog, utilice el menú desplegable para seleccionar el recurso.

   Seleccione *Servidor remoto - IPv4* para permitir que los mensajes de Syslog se envíen a uno o más servidores de Syslog de IPv4 remotos e introduzca la dirección IPv4 o el nombre de host y el puerto UPD para cada servidor de Syslog remoto.

   -O bien-

   Seleccione *Servidor remoto - IPv6* para permitir que los mensajes de Syslog se envíen a uno o más servidores de Syslog de IPv6 remotos e introduzca la dirección IPv6 o el nombre de host y el puerto UPD para cada servidor de Syslog remoto.
3. Seleccione *Consola del equipo* para enviar mensajes a la consola del sistema de consola.
4. Seleccione *Sesión raíz* para enviar mensajes de syslog a todas las sesiones en las que haya iniciado sesión como usuario raíz.
5. En el encabezado Captura de SNMP, introduzca el nombre de la comunidad definida en uno o más de los servidores de captura de SNMP en el campo Comunidad y, a continuación, introduzca las direcciones IP de hasta cinco servidores en los campos de servidor.
6. En el encabezado SMS, introduzca la información sobre el servidor de SMS, el puerto y el número de localizador en los campos correspondientes.
7. En el encabezado Correo electrónico, introduzca la información sobre el servidor, el puerto y el correo electrónico del destinatario en los campos correspondientes.
8. En el encabezado DSView, introduzca la dirección IP del servidor de DSView a la que se enviarán notificaciones de eventos en el campo Servidor de DSView. Introduzca el número de puerto de servidor de Syslog para el servidor DSView, la información SSH y la información de advertencia del búfer en los campos correspondientes.
9. Haga clic en *Guardar*.

Reenvío de captura

El sistema de consola recibirá capturas de SNMP y las reenviará a un servidor de capturas de SNMP remoto.

Para añadir un servidor de capturas de SNMP para el reenvío de capturas:

1. Haga clic en *Eventos y registros – Reenvío de captura*.
2. Haga clic en *Añadir*.
3. Introduzca la dirección IP del servidor remoto y el puerto UDP.
4. Introduzca el OID para filtrar capturas para enviar a este servidor (opcional).

Para editar la configuración del servidor de capturas de SNMP:

1. Haga clic en *Eventos y registros – Reenvío de captura*.
2. Haga clic en el índice del servidor que se va a editar.

3. Actualice el puerto UDP y/o el OID y haga clic en *Guardar*.

Almacenamiento en búfer de datos

Cuando el almacenamiento en búfer de datos está activado en uno o más puertos serie, los ajustes de la página Eventos y registros - Almacenamiento en búfer de datos se aplican al tipo (destino) del almacenamiento en búfer. El tamaño del segmento, que se especifica en kilobytes, determina el tamaño de cada archivo de almacenamiento en búfer de datos guardado. El campo Segmentos de reserva determina cuántos archivos históricos de almacenamiento en búfer adicionales del tamaño del segmento se conservan y se nombran con los sufijos .1, .2, etc.

Para configurar el almacenamiento en búfer de datos:

1. Seleccione *Eventos y registros - Almacenamiento en búfer de datos*.
2. Introduzca el tamaño de segmento en kilobytes y los segmentos de reserva en la sección Ajustes de almacenamiento en búfer de datos locales.
3. En la sección Ajustes de almacenamiento en búfer de datos NFS, introduzca la información siguiente: Servidor NFS, ruta NFS, tamaño de segmento (Kbytes) y segmentos de reserva.

NOTA: El servicio RPC se debe activar en la pantalla Perfil de seguridad antes de realizar la configuración de los ajustes de almacenamiento en búfer de datos NFS.

4. Para segmentar los archivos de almacenamiento en búfer de datos cada día en función de la hora, introduzca la hora en el campo Cerrar los archivos de registro y abrir nuevos a la hora (HH:MM). Esto será válido para el almacenamiento en búfer de datos local y NFS.
5. Para configurar el almacenamiento en búfer de datos en un servidor de syslog en la sección Ajustes de almacenamiento en búfer de datos de syslog, seleccione un número de recurso en el menú desplegable: Registro local 0, registro local 1, registro local 2, registro local 3, registro local 4 o registro local 5.
6. Haga clic en *Guardar*.

Para activar el almacenamiento en búfer de datos:

1. Seleccione *Puertos - Puertos serie*.
2. Haga clic en el puerto en el que desee activar el almacenamiento en búfer de datos.
3. En la pestaña Almacenamiento en búfer de datos, utilice el menú desplegable que aparece junto a *Activar* el almacenamiento en búfer de datos.

Registro del equipo

Cuando está activado Registro del equipo, los comandos (entrada) y la salida de las sesiones SSH y Telnet hacia el equipo se registran con fines de auditoría.

Para configurar el registro del equipo:

1. Haga clic en *Activar registro de datos de sesión del equipo*.
2. Seleccione el destino de los registros de datos de las sesiones del equipo en el menú desplegable. Las opciones son *Local*, *NFS*, *Syslog* y *DSView*.
    a. Si utiliza local como destino, use el menú desplegable para seleccionar el destino local. El destino *mmcblk0* es el almacenamiento flash integrado. La tarjeta SD (si está presente y activada) es *mmcblk1*. Los dispositivos USB (si están presentes y activos) son *sda1*, *sda2* , etc.

NOTA: Cuando el destino local es mmcblk0, el directorio de registro en el equipo es/mnt/hdUser/db. Cuando el destino local es mmcblk1 o un dispositivo USB, el directorio de registro es el directorio superior (raíz) de ese dispositivo.

3. Active o desactive la inclusión de un marca de hora en los registros de datos de las sesiones del equipo.
4. Haga clic en *Activar alertas de registro de datos de sesión del equipo*.
5. Introduzca las cadenas de alerta deseadas (diez como máximo) en los campos proporcionados.
6. Haga clic en *Guardar*.

3.3.13 Gestión de alimentación

Los dispositivos de alimentación conectados se pueden utilizar para la gestión de alimentación remota. El sistema de consola permite que los usuarios con autorización para la gestión de alimentación enciendan, apaguen y restablezcan los dispositivos que estén acoplados a una PDU conectada. Los usuarios autorizados también pueden supervisar y controlar un dispositivo de sistema de alimentación ininterrumpida (UPS) GXT4 o GXT5 de Liebert conectado.

Los siguientes tipos de PDU se pueden conectar a cualquier puerto serie.

- Unidad de distribución de la alimentación de gestión de alimentación (PM PDU) de Avocent.
- Unidades de distribución de la alimentación (PDU) en rack MPH2 de Vertiv, así como PDU en rack MPX y MPH con tarjetas RPC2 instaladas.
- Unidades de distribución inteligente de la alimentación (IPDU) PM de Cyclades - Con las IPDU PM de Cyclades, se pueden interconectar y gestionar hasta 128 tomas desde un único puerto serie.
- Dispositivos de control de la alimentación SPC de Avocent.
- Gama de dispositivos de alimentación de unidades de distribución de alimentación conmutada en armario (CDU), unidades de distribución de alimentación inteligente en armario (CDU inteligentes) y módulo de expansión de CDU conmutadas (CW/CX) de Server Technology Sentry. Se puede interconectar un nivel adicional de dispositivos de alimentación con los módulos de expansión de ServerTech.
- Dispositivos de alimentación Server Technology Sentry Power Tower XL (PTXL) y Power Tower Expansion Module (PTXM).
- PDU ePDU G3 de Eaton. Hasta un máximo de ocho ePDU se pueden encadenar y gestionar desde un único puerto serie.
- PDU PX G2 de Raritan.
- PDU rPDU2 de APC.
- Son compatibles las PDU Geist GU2 y R-Series Rack que ejecutan el firmware 5.3 o posterior.

NOTA: El término PDU se refiere a cualquiera de estos tipos de dispositivos de alimentación.

El sistema de consola automáticamente reconoce y admite tarjetas RPC2 de Liebert, PDU PM de Avocent, PDU PM de Cyclades, PDU de Raritan, ePDU de Eaton, PDU de APC, PDU de Vertiv, PDU de Geist y dispositivos SPC de Avocent cuando el puerto serie correspondiente está configurado para la gestión de alimentación.

PDU

Para gestionar una PDU:

1. Seleccione *Gestión de alimentación - PDU*.
2. Seleccione la casilla de verificación situada junto a la PDU que desee gestionar.
3. Haga clic en *Encendido, Apagado, Apagar y encender, Reiniciar PDU, Restablecer protección contra sobrecorriente de hardware* o *Valores predeterminados de fábrica*, si lo desea. Aparece un mensaje de confirmación. Haga clic en *Aceptar*.

NOTA: Los controles de alimentación (Encendido, Apagado y Apagar y encender) se aplicarán a todas las tomas de la PDU.

4. Para cambiar el identificador de la PDU, haga clic en *Cambiar nombre* e introduzca el nombre en el campo Nuevo identificador de PDU.
5. Haga clic en *Guardar*.

Para actualizar el firmware:

1. Seleccione la casilla de verificación situada junto a la PDU que desee actualizar y haga clic en el botón *Actualizar firmware*.

NOTA: Puede actualizar el firmware de varias PDU al mismo tiempo, pero solo en el caso de las PDU PM de Avocent y Vertiv (MPH2, MPH y MPX con tarjetas RPC2 instaladas). Si está actualizando las PDU en una conexión en cadena, seleccione únicamente la primera PDU de la cadena y el resto de las PDU de la cadena se actualizarán de forma automática.

2. Seleccione *Sitio remoto* e introduzca la información del servidor remoto.

   -O bien-

   Seleccione *Mi PC* y vaya a la ubicación en la que guardó el archivo del firmware.

3. Haga clic en *Descargar* para descargar el firmware al sistema de consola.
4. Cuando la descarga haya finalizado, el sistema de consola mostrará las versiones del firmware actual y descargado. Si la información de la versión descargada es correcta, haga clic en *Actualizar* para iniciar la actualización del firmware de la PDU.
5. Una vez que haya comenzado la actualización, haga clic en *Finalizar*. Se mostrará un mensaje que indica que la actualización ha sido correcta. La página Información general de la PDU muestra el estado de la actualización. La PDU se reinicia cuando finaliza la actualización.

Para ver la información de una PDU y gestionar las tomas:

1. Seleccione *Gestión de alimentación - PDU*.
2. Haga clic en el nombre de la PDU que desee ver o gestionar.
3. Aparece la ventana Tabla de tomas con controles de alimentación y en la barra de navegación lateral se muestra una lista de opciones.
4. Para gestionar las tomas de una PDU:
   a. Marque la(s) casilla(s) del (de los) número(s) de toma que desee gestionar.
   b. Haga clic en *Encendido, Apagado, Apagar y encender*, *Bloquear* o *Desbloquear* para realizar esa función para la(s) toma(s) seleccionada(s).
5. Haga clic en *Información* en la barra de navegación lateral para ver la información de una PDU.

6. Haga clic en *Información general* en la barra de navegación lateral para ver la información de supervisión de datos.
7. Haga clic en *Corriente, Tensión, Consumo de potencia, Consumo energético* o *Entorno* en la barra de navegación lateral para ver una tabla con la información adecuada. Haga clic en *Restablecer valores* para borrar los valores Máx, Mín y Promedio.

Para configurar una PDU:

1. Haga clic en *Ajustes* para expandir la barra de navegación lateral.
2. Haga clic en *Tomas*.
3. Haga clic en el número de una toma para cambiar sus ajustes. Haga clic en *Guardar* y luego en *Cerrar*.

   -O bien-

   Marque dos o más casillas junto a las salidas para las que desee modificar los ajustes. Haga clic en *Editar* para cambiar los ajustes de las tomas seleccionadas. Haga clic en *Guardar*.
4. Haga clic en *PDU* para ver y configurar los ajustes de la PDU. Haga clic en *Guardar* cuando haya acabado.
5. Haga clic en *Fases* o *Bancos*.
   a. Haga clic en el nombre de una fase o un banco para cambiar sus ajustes o haga clic en una o más casillas junto a la(s) fase(s) o banco(s) que desee cambiar.
   b. Haga clic en *Guardar* para guardar los ajustes y en *Cerrar* para volver a la pantalla Fase.

NOTA: El modelo de PDU define los parámetros disponibles en la ventana Ajustes.

UPS

Para gestionar un UPS:

1. Seleccione *Gestión de alimentación - UPS*.
2. Seleccione la casilla de verificación situada junto al UPS que desee gestionar.
3. Haga clic en *Apagar salida*, *Encender salida* o *Apagar y volver a encender salida* si lo desea. Aparece una opción para introducir el tiempo de retraso deseado antes de realizar la operación. Haga clic en el botón para realizar la operación.
4. Para cambiar el identificador de UPS, haga clic en *Cambiar nombre* e introduzca el nombre en el campo Nuevo identificador del UPS.
5. Haga clic en *Guardar*.

Para ver la información de un dispositivo de UPS:

1. Seleccione *Gestión de alimentación - UPS*.
2. Haga clic en el nombre del UPS que desee ver o gestionar.
3. Haga clic en las opciones en la barra de navegación lateral para ver la información del UPS.

Para configurar un UPS:

1. Haga clic en *Ajustes* para expandir la barra de navegación lateral.
2. Haga clic en las opciones de la barra de navegación lateral para configurar el UPS.

Inicio de sesión

Los administradores pueden cambiar la contraseña de inicio de sesión de los tipos de PDU compatibles. El sistema de consola usa esta contraseña para comunicarse con la PDU (solo se admite una contraseña para todas las PDU del mismo tipo).

Para cambiar la contraseña de una PDU:

1. Seleccione *Gestión de alimentación - Inicio de sesión*.
2. Introduzca la nueva contraseña para cada tipo de PDU que desee cambiar.
3. Haga clic en *Guardar*.

Grupos de tomas

Si selecciona la pestaña *Grupos de tomas*, podrá ver el estado, la toma y el consumo de potencia de los grupos de tomas, así como configurarlos. También puede encender, apagar o apagar y encender grupos de tomas seleccionados.

Para gestionar grupos de tomas:

1. Seleccione *Gestión de alimentación - Grupos de tomas*.
2. Marque la casilla situada al lado del nombre del grupo de tomas que desee gestionar.
3. Haga clic en el botón de opción *Encendido*, *Apagado* o *Apagar y encender*, si lo desea.

   -O bien-

4. Haga clic en *Añadir* para añadir un grupo de tomas. Aparece la pantalla Añadir grupo. Introduzca el nombre en el campo Nombre del grupo.
5. Haga clic en *Guardar*.

Para ver y cambiar la información del grupo de tomas:

1. Seleccione *Gestión de alimentación - Grupos de tomas*.
2. Haga clic en el nombre del grupo de tomas que desee ver o gestionar.
3. Para añadir tomas, haga clic en *Añadir* para añadir una nueva toma al grupo. Rellene los campos y haga clic en *Guardar* para volver a la tabla Detalles del grupo de tomas.
4. Para eliminar tomas, marque una o más casillas junto a la(s) toma(s) que desee eliminar del grupo. Haga clic en *Eliminar* y en *Cerrar* cuando haya acabado.

PDU de red

Los dispositivos de alimentación conectados a la red con SNMP (lectura/escritura) activado se pueden usar para la gestión de alimentación remota. El sistema de consola permite que los usuarios autorizados enciendan y apaguen los dispositivos conectados a la PDU de red.

NOTA: Es necesario que SNMP esté activado y disponer de una comunidad con permiso de escritura activada en la PDU.

Al seleccionar el nodo *PDU de red*, los administradores pueden añadir nuevos dispositivos de PDU de red o editar la configuración de los actuales.

Las siguientes funcionalidades están disponibles para las PDU de red: Control de la alimentación (encender, apagar y apagar y encender/reiniciar), cambiar el nombre de la PDU y cambiar el nombre de las tomas

Para añadir una PDU de red:

1. Seleccione *Gestión de alimentación – PDU de red*.
2. Haga clic en *Añadir*.
3. Introduzca la dirección IP de la PDU.
4. Seleccione el tipo de PDU.
5. Introduzca el intervalo de sondeo de la PDU para obtener información sobre el estado de las tomas.
6. Introduzca el nombre de la comunidad que tiene permiso de escritura en la PDU.

UPS de red

Los dispositivos de UPS Liebert GXT4 y GXT5 con tarjetas Liebert Intellislot Unity instaladas que estén conectados a la red con SNMP (lectura/escritura) activado, pueden supervisarse y controlarse. El sistema de consola permite que los usuarios autorizados supervisen la información de la batería y la información de entrada y de salida del sistema, y controlar los receptáculos de salida.

NOTA: Es necesario que SNMP esté activado y disponer de una comunidad con permiso de escritura activada en el UPS.

Al seleccionar el nodo UPS de red, los administradores pueden añadir nuevos dispositivos de UPS de red o editar la configuración de los actuales.

3.3.14 Sensores

Interno

El sistema de consola cuenta con sensores que controlan la temperatura interna. Puede especificar un intervalo de funcionamiento para el sistema de consola que se ajuste a su entorno. Hay dos sensores de temperatura internos que pueden generar notificaciones de eventos: El sensor de temperatura de la CPU y el sensor de temperatura de la placa.

PRECAUCIÓN: No utilice valores que superen las temperaturas máxima y mínima. Apéndices en la página 91.

Para configurar los sensores de temperatura:

1. Haga clic en *Sensores - Equipo - Interno* para abrir la página Interno, en la que se muestran los sensores de temperatura de la CPU y de la placa.
2. En el campo Temperatura máxima del sensor de temperatura de la CPU o de la placa introduzca la temperatura en grados Celsius que, si se supera, generará una notificación de evento.
3. En el campo Temperatura máxima del sensor de temperatura de la CPU o de la placa introduzca el umbral de temperatura en grados Celsius por debajo de la temperatura máxima.

NOTA: El campo Umbral de temperatura máxima definirá una región alrededor de la temperatura máxima. Cuando la temperatura supere la temperatura máxima más el umbral, se generará una notificación de evento. Cuando la temperatura se sitúe por debajo de la temperatura máxima menos el umbral, se generará una notificación de evento de que el sistema de consola ha vuelto a la temperatura de funcionamiento normal. Esto también es cierto para ajustar el umbral de temperatura mínima.

4. En el campo Temperatura mínima, introduzca la temperatura en grados Celsius que, si la temperatura del sistema de consola se sitúa por debajo de este valor, generará una notificación de evento.
5. En el campo Umbral de temperatura mínima, introduzca el umbral de temperatura en grados Celsius por encima de la temperatura mínima.
6. Haga clic en *Guardar*.

Sensores externos de 1 cable

Se puede conectar un sensor externo de 1 cable al puerto SENSOR de la parte delantera del sistema de consola con un cable CAT 5. De forma predeterminada, la compatibilidad con el sensor de 1 cable está activada. Se puede desactivar en la página del Perfil de seguridad.

Para configurar un sensor de 1 cable:

En la barra de navegación lateral, haga clic en *Sensores - Equipo - 1 cable*. Los sensores detectados se muestran en una tabla con el tipo de sensor y la información de los valores actuales.

NOTA: Esta opción aparece en todos los modelos de sistema de consola, aunque algunos modelos no incorporan un puerto SENSOR. Si su modelo no incorpora un puerto SENSOR, deje esta opción desactivada.

NOTA: Si un sensor conectado no se muestra, haga clic en *Actualizar lista* para actualizar la página.

NOTA: Las opciones de configuración de los sensores dependen del tipo de sensor. Los sensores tienen ajustes de configuración comunes para su nombre y ubicación.

Sensores de contacto (SN-2D/SN-3C)

Este tipo de sensor puede generar una notificación de evento cuando una de sus entradas cambie de estado. Una entrada se puede encontrar en estado *Desactivado*, en *Alarma cuando esté abierto* o en *Alarma cuando esté cerrado*.

Temperatura externa

Este tipo de sensor puede generar una notificación de evento cuando la temperatura cruce un umbral definido por el usuario. La unidad de medida puede configurarse como *Celsius* o *Fahrenheit*. Los umbrales de Baja advertencia, Baja crítica, Alta advertencia o Alta crítica se deben configurar para permitir la generación de eventos. Además, el estado de la alarma debe definirse en *Activado* para generar una alerta.

Humedad externa

Este tipo de sensor puede generar una notificación de evento cuando la humedad cruce un umbral definido por el usuario. Los umbrales de Baja advertencia, Baja crítica, Alta advertencia o Alta crítica se deben configurar para permitir la generación de eventos. Además, el estado de la alarma debe definirse en *Activado* para generar una alerta.

Presión diferencial (SN-DP)

Este tipo de sensor puede generar una notificación de evento cuando la presión diferencial cruce un umbral definido por el usuario. Los umbrales de Baja advertencia, Baja crítica, Alta advertencia o Alta crítica se deben configurar para permitir la generación de eventos. Además, el estado de la alarma debe definirse en *Activado* para generar una alerta.

Sensor de fugas (SN-L)

Este tipo de sensor puede generar dos tipos de alarmas: Una alarma de fugas, que se produce cuando se detecta una fuga, y una alarma de fallo de cable, que se produce cuando se detecta un problema de conexión en el cableado. Un parámetro de configuración es el Tiempo de filtro (segundos). Este es el tiempo, en segundos, que la fuga debe persistir para que se genere un evento.

Sensores de entrada digital

Se puede conectar un sensor de entrada digital al puerto DIGITAL IN de la parte delantera del sistema de consola con un cable CAT 5.

Para configurar un sensor de entrada digital:

1. En la barra de navegación lateral, haga clic en *Sensores - Equipo - Entrada digital*. Las entradas digitales detectadas se muestran en una tabla.
2. Haga clic en el número asociado a la posición del sensor para abrir la página de ajustes.
3. Introduzca el nombre y la ubicación del sensor y utilice el menú desplegable para seleccionar el tipo de sensor.
4. Si se configura el parámetro Alarma, se puede configurar un sensor de entrada digital para generar un evento. Use el menú desplegable para seleccionar *Alarma cuando esté abierto*, *Alarma cuando esté cerrado* o para *desactivar* la alarma.

NOTA: Esta opción aparece en todos los modelos de sistema de consola, aunque algunos modelos no incorporan un puerto DIGITAL IN. Si su modelo no incorpora un puerto DIGITAL IN, deje esta opción desactivada.

Sensores de salida digital

El sistema de consola avanzada ACS800 admite dos salidas digitales. Las salidas digitales son puertos de relé controlados de forma remota que se pueden usar para abrir o cerrar un circuito eléctrico.

NOTA: El sistema de consola avanzada ACS8000 no admite salidas digitales.

Para configurar un sensor de salida digital:

1. En la barra de navegación lateral, haga clic en Salida digital.
2. Haga clic en el número asociado a la posición del sensor para abrir la página de ajustes.
3. Si lo desea, escriba un nombre para el sensor.
4. Use el menú desplegable para *activar* o *desactivar* un circuito eléctrico y, a continuación, haga clic en *Guardar*.

3.3.15 Sesiones activas

El sistema de consola permite que varios usuarios inicien sesión y ejecuten sesiones simultáneamente. La función Sesiones activas le permite ver todas las sesiones activas y terminar las sesiones no deseadas. Haga clic en Sesiones activas para ver todas las sesiones abiertas en el sistema de consola.

NOTA: Si inicia otra sesión en el sistema de consola mientras visualiza esta pantalla, no será visible hasta que haga clic en *Actualizar* en la parte superior de la ventana de la IU web.

Para terminar una sesión activa:

1. Haga clic en *Sesiones activas*. Aparece la pantalla Sesiones activas y en ella se muestran todas las sesiones abiertas al sistema de consola por la IP de la estación de trabajo del usuario.
2. Seleccione la casilla de verificación situada junto a la sesión que desee terminar y, a continuación, haga clic en el botón *Terminar*. Al cabo de unos segundos, en la pantalla Sesiones activas se volverán a mostrar las sesiones abiertas, menos la que ha terminado.

3.3.16 Supervisión

Cuando hace clic en *Supervisión*, se pueden visualizar diversos datos sobre la red y el puerto de consola. Las pantallas solamente permiten la visualización de información y no ofrecen interactividad con el usuario. En la siguiente tabla se muestran los tipos de información disponibles.

Tabla 3.23 Pantallas de supervisión

Nombre de la pantalla	Definición
Red - Dispositivos	Muestra los puertos Ethernet y el adaptador de red USB, el estado (activado/desactivado), la dirección IPv4, la máscara IPv4 y la dirección IPv6.
Red - Tabla de enrutamiento IPv4	Muestra información sobre destino, puerta de enlace, máscara de dirección de ruta, indicadores, métrica, ref., uso e interfaz.
Red - Tabla de enrutamiento IPv6	Muestra información sobre destino, próximo salto, indicadores, métrica, ref., uso e interfaz.
Puertos serie	Muestra información sobre el nombre del dispositivo, perfil, ajustes, señales, bytes TX, bytes RX, error de trama, error de paridad, interrupción y saturación. El botón Restablecer contadores permite que los administradores restablezcan los contadores de estadísticas para los puertos seleccionados.
Modo FIPS	Muestra el nombre del servicio y la indicación de modo.
Registro sin necesidad de intervención	Muestra el archivo de registro de aprovisionamiento sin necesidad de intervención y permite que un administrador lo borre.
Registro de identificación de llamadas	Muestra las últimas 20 llamadas.
Estado del túnel IPSec	Muestra los detalles de la conexión IPSec, incluido el estado del túnel, dirección IP remota, duración del IKE, tiempo establecido, algoritmos de fase y nombre del certificado.

3.3.17 Cambiar contraseña

Los administradores o usuarios pueden cambiar su propia contraseña en esta pantalla.

Para cambiar su propia contraseña:

1. Seleccione *Cambiar contraseña*.
2. Introduzca la contraseña antigua y la contraseña nueva en los campos correspondientes.
3. Confirme la contraseña nueva y haga clic en *Guardar*.

3.4 Información general sobre la interfaz de usuario web para usuarios normales

Tabla 3.24 Opciones de la interfaz de usuario web para usuarios normales

Opción de menú	Descripción
Acceso	Muestra todos los dispositivos a los que el usuario puede acceder. Haga clic en *Visor serie* en la columna Acción de un dispositivo para iniciar una sesión de terminal con ese dispositivo.
Grupos de tomas de gestión de alimentación PDU	Haga clic en *PDU* para encender, apagar, encender, apagar y encender, restablecer la protección de sobrecorriente de hardware, volver a los valores predeterminados de fábrica o cambiar el nombre de las PDU conectadas al sistema de consola. Haga clic en *Grupos de tomas* para gestionar grupos de tomas en PDU conectadas. Haga clic en UPS para supervisar y controlar dispositivos UPS conectados.
Cambiar contraseña	Cambie su propia contraseña.

Apéndices

Apéndice A: Especificaciones técnicas

Tabla A.1 Especificaciones técnicas de hardware del sistema de consola avanzada ACS8000

Categoría	Valor
Información general	
CPU	ARM Cortex-A9 de doble núcleo a 766 MHz
Memoria	1 GB DDR3L/16 GB eMMC FLASH
Interfaces	• Dos puertos de fibra 1000Base-TX de cobre/1 Gbps SFP de doble medio • 48 puertos serie con detección automática y funciones de conmutación para contactos de Cyclades y Cisco Dos de los puertos serie son compatibles con RS232/422/485 multiprotocolo con detección automática y funciones de conmutación para contactos de Cyclades y Cisco en modo RS232 • Un puerto de consola serie • Ocho puertos de host USB 2.0 (puertos frontales no disponibles en algunos modelos) Una ranura para tarjeta SD (no disponible en algunos modelos) Puerto de módem analógico opcional V.92/56K • Interfaz de 1 cable para sensores externos (no disponible en algunos modelos) • Un conector RJ45 con cuatro puertos de entrada digital para sensores de cierre de contactos externos (no disponible en algunos modelos)
Información de alimentación	
Fuente de alimentación	Interna de 100-240 V de CA, fuentes de alimentación redundantes de entrada doble opcionales de 50/60 Hz Opción de -48 V de CC disponible
Consumo de potencia	Tensión nominal 120 V de CA: Habitual 0,17 A, 20 W, máximo 0,25 A, 30 W Tensión nominal 230 V de CA: Habitual 0,1 A, 23 W, máximo 0,15 A, 35 W Tensión nominal -48 V de CC (20% tolerancia) habitual 0,5 A
Especificaciones de las condiciones atmosféricas ambientales	
Temperatura de funcionamiento	De 0 °C a 50 °C (unidades con alimentación de CC) De -10 ° C a 70 °C (unidades con alimentación de CA)
Temperatura de almacenamiento	De -20 °C a 70 °C
Humedad	Del 20% al 80% de humedad relativa (sin condensación) en todo el intervalo de temperatura de funcionamiento
Dimensiones	
Altura x Anchura x Profundidad	4,318 x 43,434 x 24,13 cm
Peso	2,722- 3,175 kg en función del modelo

Tabla A.2 Especificaciones técnicas de hardware del sistema de consola avanzada ACS800

Categoría	Valor
Información general	
CPU	ARM Cortex-A9 de doble núcleo a 766 MHz
Memoria	1 GB DDR3L/16 GB eMMC FLASH
Interfaces	• Dos puertos de cobre 1000Base-TX de doble medio • Ocho puertos serie con detección automática y funciones de conmutación para contactos de Cyclades y Cisco Los ocho puertos son compatibles con RS232/422/485 multiprotocolo con detección automática y funciones de conmutación para contactos de Cyclades y Cisco en modo RS232 • Un puerto de consola serie • Cuatro puertos de host USB 2.0 • Puerto de módem analógico V.92/56K • Interfaz de 1 cable para sensores externos Un conector RJ45 con cuatro entradas digitales para sensores de cierre de contactos • Conectores digitales de salida que proporcionan cuatro señales de salida.
Información de alimentación	
Fuente de alimentación	Interna de 100-240 V de CA, 50/60 Hz
Consumo de potencia	Tensión nominal 120 V de CA: Habitual 80,5 mA/3,5 W, máximo 306 mA/17 W Tensión nominal 240 V de CA: Habitual 60 mA/3,75 W, máximo 191 mA/17 W
Especificaciones de las condiciones atmosféricas ambientales	
Temperatura de funcionamiento	De -20 °C a 70 °C
Temperatura de almacenamiento	De -20 °C a 70 °C
Humedad	Del 20% al 80% de humedad relativa (sin condensación) en todo el intervalo de temperatura de funcionamiento
Dimensiones	
Altura x Anchura x Profundidad	3,302 x 21,2852 x 18,1864 cm
Peso	1,72365 kg

Apéndice B: Aprovisionamiento sin necesidad de intervención

La función de aprovisionamiento sin necesidad de intervención es una extensión de la recuperación de la configuración de Bootp del sistema de consola y es un método para implementar numerosos sistemas de consola en un entorno. Para poder usar la función de aprovisionamiento sin necesidad de intervención, necesitará un servidor DHCP y un servidor TFTP válidos. Puede configurar sus servidores DHCP para que instruyan a los sistemas de consola recién introducidos que descarguen una configuración de plantilla y actualicen/degraden el firmware.

La preparación de los archivos de configuración/DHCP/TFTP solo debería llevar unos minutos y podría suponer un ahorro de varias horas de tiempo de configuración para los sistemas de consola que se añadan a su red posteriormente. Una vez que se haya completado el paso de aprovisionamiento, se puede acceder a los sistemas de consola de forma individual para realizar cualquier tarea de configuración posterior al aprovisionamiento que se desee (como, por ejemplo, asignar una IP estática y un nombre de host).

Gracias a la función de aprovisionamiento sin necesidad de intervención, los sistemas de consola se pueden configurar y actualizar automáticamente después de que hayan arrancado y se hayan inicializado. Esto ayuda a facilitar la introducción e instalación del sistema de consola en la red existente.

Los administradores pueden ver un registro de las configuraciones sin necesidad de intervención si hacen clic en *Monitoring-Zero-touch Log* (Registro sin necesidad de intervención) en la barra lateral de la pestaña Experto.

B.1 Archivo de configuración de aprovisionamiento sin necesidad de intervención

Para poder utilizar la función de aprovisionamiento sin necesidad de intervención, en primer lugar los administradores deben guardar el archivo de configuración de un sistema de consola en un servidor remoto. El archivo de instalación que se creará para el aprovisionamiento sin necesidad de intervención utilizará el archivo de configuración como referencia. Para obtener información sobre cómo crear y guardar un archivo de configuración, consulte Archivos de configuración en la página 20.

NOTA: Los parámetros presentes en el archivo de configuración se aplicarán a todos los sistemas de consola que reciban el archivo. Si no desea que un parámetro se aplique a todos los sistemas de consola, por ejemplo un nombre de host, asegúrese de incluir un comentario para evitarlo y para ello introduzca un signo (#) delante del parámetro.

B.2 Archivo de configuración

Una vez que el archivo de configuración se haya guardado en un servidor remoto y el servidor DHCP se haya configurado, un administrador debe crear un archivo de configuración. El sistema de consola utiliza el archivo de configuración para identificar parámetros de configuración e información de aprovisionamiento importante como, por ejemplo, el nombre de archivo de la imagen de firmware, el nombre del archivo de configuración y la dirección IP del servidor remoto en el que se ha guardado el archivo de configuración. Una vez que el archivo de configuración se ha creado, debe almacenarse en un servidor TFTP, FTP o SFTP. La dirección IP del servidor TFTP, FTP o SFTP se enviará en el mensaje de oferta de DHCP.

NOTA: Si almacena el archivo en un servidor TFTP, se recomienda que lo almacene en la carpeta raíz de dicho servidor.

A continuación se muestra un ejemplo del archivo de configuración.

```
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
```

Tabla B.1 Descripciones del archivo de configuración

Parámetro	Descripción
ONE_TIME_CONFIG	Cuando el parámetro se establece en Sí, el sistema de consola recupera el archivo de configuración en el arranque inicial y no se envía en arranques subsiguientes. Cuando se establece en No, el sistema de consola recupera el archivo de configuración cada vez que se inicia.
FIRMWARE_VERSION	La versión del firmware que se enviará al equipo.
FIRMWARE_FILENAME	La ruta y el nombre de archivo del firmware.
FIRMWARE_SERVER_IP	La dirección IP o el nombre de host del servidor en el que se aloja el firmware.
FIRMWARE_SERVER_USERNAME	Si el firmware está alojado en un servidor seguro, las credenciales para acceder al servidor.
FIRMWARE_SERVER_PASSWORD	
FIRMWARE_SERVER_PROTOCOL	El protocolo del servidor utilizado para alojar el firmware. Los protocolos compatibles son tftp, ftp, stfp, scp y wget.
CONFIG_FILENAME	La ruta y el nombre de archivo del archivo de configuración.
CONFIG_SERVER_IP	La dirección IP o el nombre de host del servidor en el que se aloja el archivo de configuración.
CONFIG_SERVER_USERNAME	Si el archivo de configuración se aloja en un servidor seguro, las credenciales para acceder al servidor. En la mayoría de casos, las credenciales serán necesarias. El nombre de usuario es texto sin formato, pero la contraseña debe estar cifrada.
CONFIG_SERVER_PASSWORD	
CONFIG_SERVER_PROTOCOL	El protocolo del servidor utilizado para alojar el archivo de configuración. Los protocolos compatibles son ftp, stfp, scp y wget.

Cifrado de contraseñas

Se debe crear un hash cifrado de una contraseña para los parámetros FIRMWARE_SERVER_PASSWORD o CONFIG_SERVER_PASSWORD. El hash debe generarse desde un entorno Linux en el que se ejecute openSSL. Introduzca los siguientes comandos en un símbolo del sistema de Linux o en un shell del sistema de consola, como se muestra. A continuación, introduzca el hash de la contraseña resultante en el archivo de configuración para el tipo de servidor definido.

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

NOTA: En el ejemplo anterior, sustituya <MyPassword> por una contraseña válida.

B.3 Copia del archivo de configuración en un servidor

Una vez que el archivo de configuración se ha creado, debe copiarse en un servidor TFTP. En el ejemplo siguiente se muestra qué se debe introducir en el sistema para copiar los archivos en su servidor y, a continuación, verificar que el sistema de consola puede descargar el archivo.

Copia del archivo de configuración en un servidor TFTP:

```
Ejemplo: tftpd-hpa
Directorio raíz TFTP predeterminado /var/lib/tftpboot
~$ sudo cp zerotouch.setup /var/lib/tftpboot
```

B.4 Obtención del archivo de configuración

Después de obtener las direcciones IP tanto para el sistema de consola como para el servidor TFTP o en el que haya cargado el archivo de configuración, el proceso de aprovisionamiento sin necesidad de intervención intentará descargar el archivo de configuración. Una vez que el sistema de consola descargue el archivo de configuración, usará la información contenida en el archivo para obtener la imagen y/o procesar la configuración del sistema de consola.

B.5 Configuración del servidor DHCP

Durante el proceso de arranque, si es necesario puede que el sistema de consola emita una solicitud de asignación de direcciones IP. Durante este proceso, el servidor DHCP consultará el servidor DNS para obtener la ubicación del servidor TFTP o HTTP en el que reside el archivo de configuración. Un administrador puede, si así lo desea, crear una entrada en el servidor DHCP que identifique de forma exclusiva a un sistema de consola específico o a un intervalo de sistema de consola. Esta entrada filtra qué sistema de consola se aprovisionan.

Un administrador debe configurar dos opciones. La opción 66 define el nombre de host o la dirección IP del servidor TFTP en el que reside el archivo de configuración. La opción 67 define el nombre del archivo de configuración (por ejemplo, acszero.cfg).

Para configurar las opciones 66 y 67:

1. Use Windows Server Manager o el complemento de herramientas DHCP Microsoft Management Console (MMC) para abrir la consola de su servidor DHCP.
2. En el panel izquierdo de la ventana del servidor DHCP, haga clic en *IPv4*.
3. Haga clic con el botón derecho en *Server Options* (Opciones de servidor) y haga clic en *Configure Options* (Configurar opciones) para configurar un ámbito global.

   -O bien-

   Haga clic con el botón derecho en *Scope Options* (Opciones de ámbito) y haga clic en *Configure Options* (Configurar opciones) para configurar un ámbito único.
4. Haga clic en Opción *066* para introducir la ubicación del servidor en el que se alojará el archivo de configuración.
5. Introduzca el nombre de host del servidor TFTP.
6. Haga clic en Opción *067* para introducir el nombre del archivo de configuración.

Un administrador puede usar dos opciones de DHCP adicionales para filtrar el aprovisionamiento sin intervención para determinados sistemas de consola. La opción 60 define la clase de proveedor, Avocent_ ACSsistema de consola<número de serie del 800/8000>. La opción 61 define la dirección MAC del sistema de consola.

Para crear las opciones 60 y 61 (opcional):

1. Use Windows Server Manager o el complemento de herramientas DHCP MMC para abrir la consola de su servidor DHCP.
2. En el panel izquierdo de la ventana DHCP, haga clic en *IPv4*.
3. En la barra de pestañas, haga clic en *Action* (Acción) y, a continuación, en *Set Predefined Options* (Definir opciones predefinidas) en el menú desplegable.
4. En la clase Options (Opciones), seleccione *DHCP Standard Options* (Opciones estándar de DHCP) y haga clic en *Add* (Añadir).
5. Introduzca un nombre para la opción en el campo Name (Nombre), seleccione *String* (Cadena) en el menú desplegable Data (Datos), introduzca 060 en el campo Code (Código) e introduzca una descripción para la opción. Haga clic en *OK* (Aceptar).
6. Repita el paso 5 e introduzca 061 en el campo Code (Código).

Servidor DNS

Si la opción de ámbito DNS todavía no se ha definido en su servidor DHCP y si la entrada de la opción 66 es un nombre de host en lugar de una dirección IP, puede configurar el servidor DNS.

Para configurar el servidor DNS:

1. Use Windows Server Manager o el complemento de herramientas DHCP MMC para abrir la consola de su servidor DHCP.
2. En el panel izquierdo de la ventana DHCP, haga clic en *IPv4*.
3. Haga clic con el botón derecho en *Server Options* (Opciones de servidor) y haga clic en *Configure Options* (Configurar opciones).
4. Haga clic en Opción *006* para definir los servidores DNS.
5. Introduzca la dirección IP en el campo adecuado y haga clic en *Add* (Añadir).

NOTA: Si introduce el nombre del servidor, el servidor DNS lo resolverá.

Reservas

Puede reservar direcciones IP para cada sistema de consola que deba actualizarse. Una reserva es una dirección IP que siempre se emitirá a un sistema de consola especificado cuando este renueve su concesión DHCP.

Para reservar una dirección IP:

1. Use Windows Server Manager o el complemento de herramientas DHCP Microsoft Management Console (MMC) para abrir la consola de su servidor DHCP.
2. En el panel izquierdo de la ventana DHCP, haga clic en *IPv4*.
3. Haga clic con el botón derecho del ratón en *Reservations* (Reservas) y, a continuación, en *New Reservation* (Nueva reserva).

4. Introduzca un nombre para la reserva, la dirección IP que se asignará al sistema de consola, la dirección MAC del sistema de consola y una descripción en los campos correspondientes.

NOTA: La dirección MAC del sistema de consola se encuentra en la parte inferior del sistema de consola.

5. En Supported types (Tipos admitidos), use el botón de opción para seleccionar Both (Ambos) o DHCP only (Solo DHCP).
6. Haga clic en *Add* (Añadir). La dirección IP reservada se mostrará en la tabla Reserve (Reservas).

A continuación se muestra un ejemplo de configuración de un servidor DHCP Linux.

```
Ejemplo: Servidor DHCP ISC para Linux
Edite /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 Activación del aprovisionamiento sin necesidad de intervención

Los administradores pueden activar el aprovisionamiento sin necesidad de intervención desde la interfaz de usuario web o desde la CLI. Una vez que el aprovisionamiento sin necesidad de intervención se haya activado, deberá borrar el registro de aprovisionamiento sin necesidad de intervención.

Para activar el aprovisionamiento sin necesidad de intervención desde la interfaz de usuario web:

1. En la barra lateral de la interfaz de usuario web, haga clic en *Sistema - Seguridad - Perfil de seguridad*.
2. En el encabezado Recuperación de la configuración de Bootp, marque las casillas para activar Bootp y la recuperación de la configuración en vivo.
3. Utilice el menú desplegable para seleccionar *eth0* como interfaz de Bootp.
4. Haga clic en *Guardar*.
5. En la barra lateral de la interfaz de usuario web, haga clic en *Supervisión - Registro sin necesidad de intervención* y, a continuación, en *Borrar registro*.

Para activar el aprovisionamiento sin necesidad de intervención desde la CLI:

1. Inicie sesión en el sistema de consola como usuario **raíz** .
2. Escriba **cd system/security/security_profile/** para acceder al nivel de perfil de seguridad.
3. Escriba set **bootp_enabled=yes** y pulse **Entrar**.
4. Escriba set **bootp_interface=eth0** y pulse **Entrar**.
5. Escriba set **enable_live_configuration_retrieval_(any_time_dhcp_renews)=yes** y pulse **Entrar**.
6. Escriba **commit** para guardar la configuración.
7. Escriba **cd /monitoring/zero-touch_log/** para acceder al nivel de registro sin necesidad de intervención.
8. Escriba **clear_log**. Escriba **Yes** cuando se le solicite si desea borrar el registro de aprovisionamiento sin necesidad de intervención.

Apéndice C: Recuperación de la configuración de Bootp

Puede configurar el sistema de consola para que se reconfigure durante el arranque o al renovar la IP.

Para generar la configuración que se va a recuperar:

1. Haga clic en *Herramientas del sistema - Guardar configuración* y guarde la configuración en un sitio FTP o de forma local.

   -O bien-

   Use el comando list_configuration para obtener las secuencias de comandos de plantilla de CLI, edite la configuración del sistema de consola y guárdela como un archivo de texto.

   -O bien-

   Edite un archivo con comandos CLI y guárdelo.

2. Transfiera el archivo guardado a un servidor DHCP.
3. Configure el servidor DHCP para transferir el archivo de configuración al sistema de consola.

Para reconfigurar un sistema de consola con Bootp:

1. Haga clic en *Sistema - Seguridad - Perfil de seguridad*. En el encabezado Recuperación de la configuración de Bootp, compruebe que la casilla *Activado* esté marcada.
2. Desmarque la casilla *Activar configuración en vivo*. La configuración guardada se recupera y se aplica tras el siguiente reinicio.

   -O bien-

   Compruebe que la casilla *Activar configuración en vivo* esté marcada. La configuración guardada se recupera y se aplica en la próxima renovación de IP.

NOTA: Debe configurar el servidor DHCP para transferir el archivo de configuración al sistema de consola.

Apéndice D: Recuperación de una contraseña del sistema de consola

Para recuperar la contraseña raíz del sistema de consola:

1. Conéctese directamente al puerto CONSOLE del sistema de consola.
2. Apague el sistema de consola y vuelva a encenderlo.
3. Pulse la barra espaciadora para acceder a la pantalla uboot.
4. Escriba hw_boot single y pulse Entrar.
5. El sistema de consola se iniciará en modo de usuario único. Escriba passwd y pulse Entrar.
6. Introduzca la contraseña nueva y confírmela.
7. Escriba reboot y permita que el sistema de consola se inicie normalmente.

Apéndice E: Configuración SSH que permite la autenticación de pares de claves RSA en lugar de un nombre de usuario/contraseña

Para configurar un sistema cliente Linux para acceder al sistema de consola avanzada ACS800/8000:

1. En el sistema de consola, cree un nuevo usuario administrador. Por ejemplo: acsadmin.
2. Agregue el nuevo usuario a los grupos de administración y de perfil de inicio de sesión en el shell.
3. En su sistema de cliente Linux, genere un par de claves para usarlo en el acceso ssh a su sistema de consola.

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

4. Pulse Entrar dos veces para no instalar una frase de contraseña para este par de claves en su servidor,

   -O bien-

   Introduzca una frase de contraseña

NOTA: Nota: Estos dos archivos los crea el ssh-keygen anterior:

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

5. En su sistema de cliente Linux, agregue líneas similares a las siguientes, en el archivo $HOME/.ssh/config:

```
Host:acsadmin132
HostName <dirección IP del sistema de consola>, por ejemplo, 10.207.24.132
Usuario acsadmin
IdentityFile ~/.ssh/acsadmin-id_rsa
```

6. Inicie sesión en el sistema de consola a través de SSH con el usuario acsadmin (el usuario nuevo).
7. Utilice los cuatro comandos siguientes para instalar la clave pública para la cuenta de acsadmin en el sistema de consola.

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

Por ejemplo, para el comando ssh

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

8. Desde el enlace *Sistema - Seguridad - Perfil de seguridad* de la interfaz de usuario web, desmarque la casilla para desactivar *Autenticación SSH mediante nombre de usuario/contraseña*. El siguiente inicio de sesión SSH desde su sistema de cliente Linux en el sistema de consola será correcto si utiliza el par de claves y no se le solicitará una conraseña.

NOTA: Si desactiva esta función evitará que cualquier usuario que no tenga un par de claves establecido tanto en el cliente como en el sistema de consola inicie sesión en el sistema de consola a través de SSH. Usted tampoco podrá abrir sesiones en serie desde la interfaz de usuario web, ya que dichas sesiones requieren autenticación con nombre de usuario/contraseña.

Un ejemplo de comando de inicio de sesión ssh utilizando la entrada del host given.ssh/config es: ssh acsadmin@acsadmin132.

Apéndice F: Información sobre puertos para la comunicación con el software DSView

Los siguientes puertos de un sistema de consola avanzada ACS800/8000 de Avocent® pueden aceptar conexiones procedentes del software de gestión DSView:

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

Los siguientes puertos de software DSView pueden aceptar conexiones procedentes del sistema de consola:

- Puerto TCP 4122 (predeterminado: servidor SSH)
- Puerto TCP 4514 (predeterminado: registro de datos o servidor de Syslog)

Apéndice G: Acceso a un sistema de consola con una instalación del software DSView mediante acceso telefónico

Cuando un usuario del software DSView establece una sesión serie, se producen los siguientes eventos:

- El usuario selecciona un puerto serie al que acceder.
- Se descarga un visor desde el servidor de DSView a la estación de trabajo del usuario.
- El software DSView transmite información al visor como, por ejemplo, una clave de autorización, la dirección IP y el puerto serie del sistema de consola.
- A continuación, el visor accede al puerto serie del sistema de consola a través de una sesión SSH, mediante la transmisión de la clave de autorización obtenida del servidor de DSView.
- Comienza la sesión serie.

Para asegurar una conectividad constante, un servidor de DSView puede configurarse fuera de banda (OOB) para permitirle que llame a un sistema de consola a través de un módem en caso de que se produzca un fallo de la red o de Internet.

G.1 Instalación del software DSView fuera de banda

El servidor de DSView debe estar ejecutándose en hardware que tenga un módem conectado y el sistema de consola debe tener un módem integrado o acceso a un módem a través de USB o puerto serie.

Para esta instalación, el servidor de DSView debe ser el punto central de recepción de los paquetes que salen del visor descargado y del sistema de consola. Para asegurarse de que esto sea así, el modo Proxy debe estar configurado en el software DSView. El visor señalará al servidor de DSView (no al sistema de consola) para establecer la conexión SSH. El servidor de DSView entonces enrutaría los paquetes mediante el cambio de las direcciones IP de origen y de destino y actuaría como un punto medio de comunicación.

En condiciones normales de funcionamiento, los paquetes recibidos desde el visor serie se enrutarían a través del servidor de DSView a través de Ethernet. En un estado de error, el servidor de DSView detectaría que la ruta normal al sistema de consola se ha interrumpido y marcaría hacia el sistema de consola, superaría la autenticación y establecería una conexión PPP. Los paquetes que normalmente pasarían a través de Ethernet se encaminarían a través de PPP.

Debido a las diferencias de velocidad entre Ethernet y el acceso telefónico, el rendimiento sería notablemente más lento. Las conexiones multiusuario degradarían aún más el rendimiento y no se recomiendan. Por esta razón, el acceso telefónico de reserva solo se recomienda como una función de reserva en casos de emergencia.

G.2 Configuración del acceso telefónico para un sistema de consola

Para configurar el acceso telefónico para acceder a un sistema de consola en el software DSView:

1. En una ventana de la vista Unidades que contenga equipos, seleccione el ACS 800/8000 que desee configurar.Para el marcado de entrada con retorno de llamada, primero debe seleccionar *Servidor de DSView - Propiedades - Sesiones de módem de DSView* en la pestaña Sistema e introducir el número de teléfono asignado al servidor de DSView en el campo Número de teléfono analógico.
2. Seleccione *Ajustes de DSView - Acceso telefónico* y haga clic en *Activar acceso telefónico*.

3. Seleccione *Tipo de módem - Analógico*.
4. Introduzca el número de teléfono del sistema de consola que desee utilizar.
5. Introduzca el usuario PPP y seleccione el protocolo de autorización PPP en los campos adecuados.
6. Para el marcado de entrada con retorno de llamada, active la casilla de verificación de retorno de llamada.
7. Seleccione *Ajustes de DSView - Acceso telefónico - Contraseña PPP* e introduzca y confirme la contraseña necesaria para acceder al sistema de consola ACS 800/8000.
8. Seleccione *Ajustes de DSView - Acceso telefónico - Direcciones IP*.
9. Haga clic en *Generar automáticamente* para definir la dirección IP de forma automática o introduzca la dirección IP local PPP y la dirección IP del equipo de forma manual.
10. Seleccione Ajustes de DSView - Acceso telefónico y haga clic en Guardar.
11. Para configurar un sistema de consola para recibir la conexión de acceso telefónico en el software DSView.
12. En una ventana de la vista Unidades que contenga equipos, seleccione el ACS 800/8000 que desee configurar.
13. Para el módem interno, seleccione *Puertos - Puertos auxiliares* y seleccione el módem.
14. Seleccione Ajustes de DSView - Acceso telefónico y haga clic en *Insertar configuración*.

NOTA: El paso siguiente solo es necesario si se ha seleccionado *CHAP* en el campo Protocolo de autorización PPP en la ventana de configuración de acceso telefónico del software DSView.

15. Inicie sesión en la CLI del sistema de consola y acceda al shell de Linux. Edite /etc/ppp/chap-secrets y añada una línea en el formato, en la que la primera columna debe tener el usuario PPP y la tercera columna debe tener la contraseña PPP, como se muestra en el ejemplo siguiente:

    pppuser * "ppppassword" *

Apéndice H: Módem interno

Algunos modelos del sistema de consola están equipados con un módem interno. Este módem se utiliza para originar y responder a llamadas telefónicas y establecer comunicación con otros módems para transmitir datos.

Las funciones del módem se controlan mediante los comandos "AT". Estos comandos se usan para indicar al módem que realice funciones como, por ejemplo, marcar o responder a llamadas y normalmente los emite automáticamente un software de comunicación. Sin embargo, para algunas aplicaciones, puede que sea necesario crear software personalizado debido a la ausencia de un sistema operativo normal.

El módem aceptará y procesará los comandos AT automáticamente con la mayoría de configuraciones de paridad y velocidad de DTE (equipos de terminal de datos) estándar. Para cada comando emitido, el módem responderá con un código de resultado para informarle del estado del módem. El formato de un comando AT básico y el código de resultado es el siguiente:

AT<Comando><CR>

OK

AT = Atención.

<Comando> = Cualquier comando válido

<CR> = Retorno de carro o tecla Entrar

OK = Código de resultado

Tabla H.1 Cadena de comando de ejemplo

Comando	Descripción
ATDT7678900<CR>	Indica al módem que marque el número 7678900 y que intente conectarse al dispositivo remoto.
ATS0=2<CR>	Activar la opción de respuesta automática. Cuando el módem detecte un timbre, intentará responder al cabo de dos timbres.

Tabla H.2 Commandos AT básicos

Comando	Descripción
ATA/	Repetir el comando anterior.
ATA	Responder.
ATB0	Funcionamiento de CCITT a 300 o 1200 bps.
ATB1	Funcionamiento de Bell a 300 o 1200 bps (predeterminado).
ATD	Marcar.
ATD0-9	Marque los dígitos DTMF de 0 a 9.
ATDA-D	Marque los dígitos A, B, C y D.
ATDP	Seleccione la marcación por pulsos; afecta la marcación actual y subsiguiente.
ATDT	Seleccione la marcación por tonos; afecta la marcación actual y subsiguiente.
ATD!	Flash: Se cuelga en función del tiempo definido por S29.
ATDW	Espere a que se detecte el tono de marcado antes de marcar un número. Si no se detecta ningún tono de marcación dentro del tiempo especificado por S7, el módem interrumpe el resto de la secuencia, se cuelga y genera un mensaje de error.
ATD@	Espere cinco segundos de silencio antes de continuar con la siguiente cadena de marcación y, a continuación, complete la secuencia de protocolo de enlace.
ATD,	Pausar. El módem se pausa durante un tiempo especificado por S8 antes de marcar el número. Se utiliza normalmente cuando se marca una línea externa a través de una PBX.
ATD;	Vuelva al modo de comandos después de procesar el comando.
ATE0	Desactiva el eco de comando.
ATE1	Activa el eco de comando (predeterminado).
ATH0	Colgar.
ATH1	Fuerza el descuelgue del módem.
ATI0	Indica el código del producto.
ATI2	Notifica OK (para compatibilidad de software).
ATI3	Indica la versión de firmware del módem. Ejemplo: CX810801-V90.
ATL0	Desactiva el volumen del altavoz.
ATL1	Establece el volumen del altavoz en bajo (predeterminado).
ATL2	Establece el volumen del altavoz en medio.
ATL3	Establece el volumen del altavoz en alto.
ATM0	El altavoz siempre está desactivado.
ATM1	El altavoz está activado durante el establecimiento de la llamada pero se desactiva cuando se detecta el operador (predeterminado).
ATM2	El altavoz siempre está activado.
ATM3	El altavoz está desactivado durante la marcación y al recibir el operador pero está activado durante la respuesta.
ATQ0	Activa los códigos de resultado al DTE (predeterminado).
ATQ1	Desactiva los códigos de resultado al DTE.
ATSr	Establece el registro S "r" como registro predeterminado.
ATSr=n	Establece el registro S "r" en el valor "n".
ATSr?	Notifica el valor del registro S "r".

Tabla H.2 Commandos AT básicos (continuación)

Comando	Descripción
ATV0	Activa los códigos de resultado abreviados.
ATV1	Activa los códigos de resultado extendidos.
ATW0	Tras la conexión, el módem solo notifica la velocidad de DTE (por ejemplo, CONEXIÓN 9600). Se desactivan las respuestas sucesivas (predeterminado).
ATW1	Tras la conexión, el módem notifica el tipo de modulación, la velocidad de la línea, el protocolo de corrección de errores y la velocidad de DTE. Se desactivan las respuestas sucesivas.
ATW2	Tras la conexión, el módem notifica la velocidad de DCE (por ejemplo, CONEXIÓN 2400). Se desactivan las respuestas sucesivas.
ATX0	Hace caso omiso del tono de marcado y ocupado. Envía el mensaje CONEXIÓN cuando se establece una conexión mediante marcación ciega.
ATX1	Desactiva la supervisión de los tonos de ocupado. Solo envía los mensajes OK, CONEXIÓN, TIMBRE, NO HAY OPERADOR y ERROR. Si se exige la detección de tono de ocupado y se detecta un tono de ocupado, se notificará el mensaje NO HAY OPERADOR en lugar de OCUPADO. Si se exige o selecciona la detección de tono de marcado y no se detecta el tono de marcado, se notificará el mensaje NO HAY OPERADOR en lugar de NO HAY TONO DE MARCADO.
ATX2	Desactiva la supervisión de los tonos de ocupado. Envía solo los mensajes OK, CONEXIÓN, TIMBRE, NO HAY OPERADOR, ERROR, NO HAY TONO DE MARCADO y CONEXIÓN XXXX. Si se exige la detección de tono de ocupado y se detecta un tono de ocupado, se notificará el mensaje NO HAY OPERADOR en lugar de OCUPADO. Si se exige o selecciona la detección de tono de marcado y no se detecta el tono de marcado, se notificará el mensaje NO HAY OPERADOR en lugar de NO HAY TONO DE MARCADO.
ATX3	Activa la supervisión de los tonos de ocupado. Envía solo los mensajes OK, CONEXIÓN, TIMBRE, NO HAY OPERADOR, ERROR, NO HAY TONO DE MARCADO y CONEXIÓN o OPERADOR XXXX. Si se exige la detección de tono de marcado y no se detecta el tono de marcado, se notificará el mensaje NO HAY OPERADOR.
ATX4	Activa la supervisión de los tonos de ocupado. Envía todos los mensajes (predeterminado).
ATZ0	Restablecimiento parcial.
AT&C0	DCD permanece activado en todo momento.
AT&C1	DCD sigue el estado del operador (predeterminado).
AT&D0	Omite DTR.
AT&D1	Entra en el modo de escape cuando se detecta una transición de activado a desactivado en DTR.
AT&D2	Cuelga, asume el estado de comando y desactiva la respuesta automática tras detectar una transición de activado a desactivado en DTR (predeterminado).
AT&D3	La transición de activado a desactivado hace que el módem realice un restablecimiento parcial. Es igual que si se emite un comando ATZ.
AT&F	Restaura la configuración de fábrica.
AT&G0	Desactiva el tono de protección (predeterminado).
AT&G1	Activa el tono de protección de 550 Hz.
AT&G2	Activa el tono de protección de 1800 Hz.
AT&K0	Desactiva el control de flujo.
AT&K3	Activa el control de flujo RTS/CTS (predeterminado para modos de datos).
AT&K4	Activa el control de flujo XON/XOFF.
AT&K5	Admite el control de flujo XON/XOFF transparente.
AT&P0	Relación de conexión/desconexión de 39/61 a 10 pulsos por segundo (predeterminado).
AT&P1	Relación de conexión/desconexión de 33/67 a 10 pulsos por segundo.
AT&P2	Relación de conexión/desconexión de 39/61 a 20 pulsos por segundo.

Tabla H.2 Commandos AT básicos (continuación)

Comando	Descripción
AT&P3	Relación de conexión/desconexión de 33/67 a 20 pulsos por segundo.
AT&Q0	Selecciona el funcionamiento asíncrono directo.
AT&Q5	El módem intentará un enlace con corrección de error.
AT&Q6	Selecciona el funcionamiento asíncrono en modo normal (permite el almacenando en búfer de velocidad y el control de flujo, pero no la corrección de errores).
AT&V	Muestra la configuración actual del módem. Cuando se introduce este comando, el módem mostrará su configuración actual de comandos y registros.
AT%C0	Desactiva la compresión de datos.
AT%C1	Activa la compresión de datos MNP 5.
AT%C2	Activa la compresión de datos V.42 bis (establece S46 bit 1).
AT%C3	Activa la compresión de datos V.42 bis y MNP 5 (predeterminado).
AT%E0	Desactiva el monitor de calidad de la línea y el reciclaje automático.
AT%E1	Activa el monitor de calidad de la línea y el reciclaje automático.
AT%E2	Activa el monitor de calidad de la línea y la reserva/el aumento de la velocidad de transmisión (predeterminado).
AT%L	Nivel de la señal de línea. Devuelve un valor que indica el nivel de la señal recibida. Ejemplo: 009 = -9dBM.
AT%Q	Calidad de la señal de línea. Notifica la calidad de la señal de línea (dependiente de DAA). Devuelve un byte de orden superior del valor EQM. En función del valor de EQM, se puede iniciar el reciclaje o la reserva/el aumento de la velocidad de transmisión si se activa con comandos AT%E1 o AT%E2.
AT+MS	Seleccionar/forzar la modulación.

H.1 Selección de modulación AT+MS

Este parámetro compuesto de formato extendido controla el modo de funcionamiento de las funciones de modulación del módem. Acepta seis subparámetros:

+MS=<operador>, <modo automático>, <tasa de transferencia mín.>, <tasa de transferencia máx.>, <tasa de recepción mín.), <tasa de recepción máx.><CR>.

Para leer la configuración actual, introduzca AT+MS?<CR>

Tabla H.3 Tasas admitidas del comando +MS

Modulación	Operador	Descripción
Bell 103	B103	300
Bell 212	B212	1200
V.21	V21	300
V.22	V22	1200
V.22 bis	V22	2400 o 1200
V.23	V23C	1200rx/75tx o 75rx/1200tx
V.32	V32	9600 o 4800
V.32 bis	V32B	14400, 12000, 9600, 7200 o 4800
V.34	V34	33600, 31200, 28800, 26400, 19200, 16800, 14400, 12000, 9600, 7200, 4800 o 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 descendente	V92	56000, 54667, 53333, 52000, 50667, 49333, 48000, 46667, 45333, 42667, 41333,, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000
V92 ascendente	V92	48000, 46667, 45333, 42667, 41333,, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000, 26667, 25333, 24000

H.2 Opción de extensión telefónica definida

Este comando activa/desactiva las opciones "línea en uso" y "recogida de extensión".

Tabla H.4 Opciones de extensión telefónica definidas

Valor -STE=n	Recogida de extensión	Línea en uso
0 (predeterminado)	Desactivado	Desactivado
1	Desactivado	Activado
2	Activado	Desactivado
3	Activado	Activado

Si la línea está en uso y el módem recibe un comando ATDT para marcar, el módem no se descolgará y mostrará el código de resultado "LÍNEA EN USO". Si el módem está descolgado y se recoge la extensión, el módem interrumpirá la conexión y mostrará el código de resultado "INTRUSIÓN DE DESCOLGADO".

H.3 Registros AT S

Los registros S usan el formato siguiente: ATSr=n<CR> donde la "r" es el número de registro S y la "n" es el parámetro al que se debe ajustar. Para leer los contenidos actuales de un registro S, emita un comando ATSr?<CR> en el que la "r" sea el registro en cuestión. A continuación, el módem mostrará el valor del registro S.

Tabla H.5 Registros AT S

Registro	Intervalo	Unidades	Predeterminado	Descripción
S0	0-255	Timbres	0	Número de timbres de respuesta. ATS0=1<CR> significa responder a la llamada tras detectarse el primer timbre.
S1	0-255	Timbres	0	Número de timbres contados.
S2	0-127	ASCII	43	Carácter de código de escape.
S3	0-127	ASCII	13	Terminador del comando <CR>.
S4	0-127	ASCII	10	Carácter de avance de línea.
S5	0-127	ASCII	8	Carácter de retroceso.
S6	2-255	Segundos	2	Tiempo de espera de detección del tono de llamada.
S7	1-255	Segundos	50	Tiempo de espera del operador.
S8	0-255	Segundos	2	Tiempo de pausa para la coma en la cadena de marcación.
S10	1-255	0,1 seg.	14	Pérdida de operador para el retraso de colgado.
S11	50-255	0,01 seg.	85	Duración del tono DTMF.
S12	0-127	1/50 seg.	50	Tiempo de protección del código de escape.
S24	0-255	1 seg.	0	Temporizador de inactividad del modo de suspensión.
S29	0-255	10 mS	70	Tiempo del modificador de marcación flash de enlace.
S30	0-255	10 seg.	0	Temporizador de desconexión por inactividad.
S95			0	Control de código de resultado.

H.4 Códigos de resultado básicos del módem

Hay códigos básicos que el módem emitirá en respuesta al procesamiento de un comando AT. Los códigos de resultado pueden mostrarse en formato textual (V1) o numérico (V0) mediante el comando Vn. El comando Qn controla si los códigos de resultado se emiten (Q0) o no se emiten (Q1). Los comandos Xn y Wn y el registro S95 determinan qué formato de código de resultado se mostrará en el módem para indicar el tipo de conexión establecida. Hay más de 300 códigos. Los más utilizados se enumeran en la tabla siguiente.

Tabla H.6 Lista de códigos de resultado básicos

Numérico	Detallado	Descripción
0	OK	El módem ha recibido y confirmado el comando.
1	CONEXIÓN	Conexión realizada a 300 bps o los códigos de resultado extendidos están desactivados (X0).
2	TIMBRE	Se ha detectado una señal de llamada entrante.
3	NO HAY OPERADOR	Este código de resultado refleja una desconexión intencionada o un fallo a la hora de completar una conexión.
4	ERROR	Se ha emitido un comando no válido al módem.
5	CONEXIÓN 1200	Indica una línea de 1200 bps o una conexión DTE.
6	NO HAY TONO DE LLAMADA	
7	OCUPADO	El módem ha detectado un tono de ocupado.
8	NO HAY RESPUESTA	Una vez que ha transcurrido el tiempo S7, no se ha recibido ninguna respuesta por parte del servidor.
10	CONEXIÓN 2400	Velocidad de la línea o conexión DTE a 2400 bps.
12	CONEXIÓN 9600	Velocidad de la línea o conexión DTE a 9600 bps.
15	CONEXIÓN 14400	Velocidad de la línea o conexión DTE a 14400 bps.
16	CONEXIÓN 19200	Velocidad de la línea o conexión DTE a 19200 bps.
17	CONEXIÓN 38400	Velocidad de la línea o conexión DTE a 38400 bps.
18	CONEXIÓN 57600	Velocidad de la línea o conexión DTE a 57600 bps.

H.5 Protector de entrada digital

El módem cuenta con un circuito de protección de la línea digital opcional que detecta automáticamente una situación de sobrecarga en las clavijas de punta y timbre. Cuando el módem se descuelgue, comprobará inmediatamente la corriente en las clavijas de punta y timbre. Si la corriente es superior a 150 mA, el módem mostrará el código de resultado "LÍNEA DIGITAL DETECTADA" y luego volverá a colgarse. El módem continuará mostrando este código de resultado hasta que se detecte una corriente normal en las clavijas de punta y timbre durante una situación de descolgado. La función DLG protegerá el módem en caso de que se conecte accidentalmente a una línea telefónica digital.

H.6 Funcionamiento en modo de suspensión

El módem se puede configurar para que entre en el modo de suspensión de bajo consumo mediante el ajuste de ATS24=n. En este caso, "n" es el tiempo, en segundos, que el módem funcionará en modo normal sin línea telefónica detectada o sin actividad de línea DTE antes de entrar en el modo de suspensión de bajo consumo. El temporizador se restablece al detectar cualquier actividad de DTE o en la línea telefónica. Si S24 se ajusta a cero, el módem no entrará nunca en el modo de suspensión de bajo consumo.

H.7 Desconexión de una llamada

Hay varias formas de desconectar una llamada. A continuación se muestran las opciones disponibles.

Si se restablece la alimentación del módem o se activa/desactiva la línea de restablecimiento (clavija nº 12), el módem se desconectará y el módem se volverá a colocar en el estado de línea desactivada.

Una transición de activado a desactivado de la señal DTR (clavija nº 4) también desconectará el módem. Si utiliza este método, compruebe que el comando DTR está establecido en &D2 o &D3 y no forzado (&D0).

El dispositivo remoto también puede causar que el módem se desconecte. Si el módem remoto se desconecta, su módem detectará automáticamente la pérdida de la señal portadora y volverá al estado de línea desactivada.

Los comandos ATH o ATZ también se pueden utilizar para desconectar una llamada. Para poder emitir un comando al módem cuando está en línea, el módem debe colocarse en el estado de comando en línea. Esto se logra mediante la emisión de una secuencia de escape especial. El valor predeterminado de esta secuencia de escape de tres dígitos es el carácter "+" (consulte S2 para cambiarlo). El "+++" está protegido por un retraso de un segundo antes y después de ser enviado (consulte S12 para cambiar el tiempo). Cuando el módem detecta la secuencia de escape, se mostrará el código de resultado OK y el módem se situará en el estado de comando en línea. Ahora se puede emitir el comando ATH o ATZ para desconectar la llamada.

H.8 Selección de códigos de país

La configuración del código de país del módem se realiza mediante el comando + GCI. Para cambiar a uno de los 30 códigos de país disponibles, emita el comando AT+GCI=n, en el que "n" es uno de los códigos de país de dos dígitos. Este comando se debe emitir cada vez que se enciende el módem. No almacenará ni guardará automáticamente esta configuración. Debe formar parte de la cadena de inicialización.

Ejemplo: AT+GCI=00<CR> Significado: Cambiar el código de país a Japón.

OK Significado: El módem ha aceptado el comando y está

ahora configurado para funcionar en Japón

AT+GCI?<CR> Significado: Mostrar el código de país actual

+GCI:00 Significado: (Japón es el país seleccionado actualmente).

OK

Para ver qué países están disponibles en el firmware del módem, introduzca AT+GCI=?<CR>.

El módem mostrará todos los códigos de país de dos dígitos posibles y disponibles.

Tabla H.7 Lista de códigos de país

País	Código	País	Código	País	Código
Australia	09	Hong Kong	50	Polonia	8A
Austria	0A	India	53	Portugal	8B
Bélgica	0F	Irlanda	57	Sudáfrica	9F
Brasil	16	Italia	59	Singapur	9C
China	26	Japón	00	España	A0
Dinamarca	31	Corea	61	Suecia	A5
Finlandia	3C	México	73	Suiza	A6
Francia	3D	Holanda	7B	Taiwán	Fe
Alemania	42	Noruega	82	TBR21	FD
Estados Unidos	B5	Reino Unido	B4		

H.9 Uso de la identificación de llamadas

El módem puede utilizarse para mostrar determinada información sobre las llamadas telefónicas entrantes. El módem puede informarle sobre la fecha, la hora, el número de teléfono y el nombre asociado a las llamadas entrantes. Cuando la opción de identificación de llamadas esté activada, la información se mostrará entre el primer y el segundo "TIMBRE" entrante. Para que esta opción funcione correctamente, la línea telefónica conectada al módem debe suscribirse al servicio de identificación de llamadas ofrecido por la compañía telefónica local. A continuación se muestra un ejemplo de la información proporcionada:

TIMBRE

FECHA = 0513

HORA = 1346

NMBR = 408 767 8900

NOMBRE = RADICOM RESEARCH

TIMBRE

La información de identificación de llamadas se puede presentar con el formato que se ha mostrado anteriormente o sin formato. Los comandos +VCID y +VRID controlan la opción de identificación de llamadas del módem.

Tabla H.8 Información sobre la identificación de llamadas

Comando	Parámetro	Descripción
+VCID?	NA	Mostrar el ajuste +VCID actual (0-2)
+VCID=	0	Desactivar las notificaciones de identificación de llamadas (predeterminado).
+VCID=	1	Activar la identificación de llamadas con presentación con formato al DTE.
+VCID+	2	Activar la identificación de llamadas con presentación sin formato al DTE.
+VRID=	0	Muestra la información de identificación de llamadas con formato correspondiente a la última llamada recibida.
+VRID+	1	Muestra la información de identificación de llamadas sin formato correspondiente a la última llamada recibida.

Apéndice I: Información normativa relativa al módem analógico instalado en este producto

I.1 Advertencias de seguridad sobre telecomunicaciones analógicas

Antes de realizar tareas de mantenimiento, desconecte este producto de su fuente de alimentación y de la red telefónica. También:

- No instale nunca cableado telefónico durante una tormenta eléctrica.
- No instale nunca un conector telefónico en lugares húmedos a menos que el conector esté diseñado específicamente para lugares húmedos.
- No toque nunca cables ni terminales telefónicos no aislados a menos que la línea telefónica se haya desconectado en la interfaz de red.
- Tenga cuidado al instalar o modificar líneas telefónicas.

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 Restricciones internacionales para módems

Algunos valores predeterminados y restricciones de marcado y respuesta pueden variar para los módems internacionales. Un cambio en la configuración puede provocar que un módem no cumpla los requisitos normativos nacionales en determinados países. También tenga en cuenta que algunos paquetes de software pueden tener características o carecer de restricciones que pueden hacer que el módem no cumpla los requisitos.

EE. UU., 47 CFR parte 68 telecomunicaciones

1. Este equipo cumple los requisitos de la parte 68 de las normas y requisitos 47 CFR adoptados por el ACTA (Administrative Council for Terminal Attachments). Este equipo cuenta con una etiqueta que contiene, entre otra información, el número de registro y el número de equivalencia de timbre (REN) para este equipo o un identificador de producto con el formato:

   Para productos actuales: US:AAAEQ##Txxxx.

   Para productos anteriores: AU7USA-xxxxx-xx-x.

   Si se solicita, este número se debe proporcionar a la compañía telefónica.

2. El enchufe y la toma que se usan para conectar este equipo al cableado y a la red telefónica del edificio deben cumplir las normas y los requisitos aplicables de 47 CFR parte 68 adoptados por el ACTA. El equipo se ha diseñado para conectarse a una toma modular compatible que también cumple dichos requisitos.
3. El número de equivalencia de timbre (REN) se utiliza para determinar el número de dispositivos que se pueden conectar a una línea telefónica. Un número excesivo de REN en una línea telefónica puede provocar que los dispositivos no suenen en respuesta a una llamada entrante. En la mayoría de zonas, aunque no en todas, la suma de REN no debe ser superior a cinco (5,0). Para estar seguro del número de dispositivos que se pueden conectar a una línea, según lo determinado por el número total de REN, póngase en contacto con la compañía telefónica local. Para los productos con fecha de aprobación posterior al 23 de julio de 2001, el REN para este producto forma parte del identificador del producto que tiene el formato US:AAAEQ##Txxxx. Los dígitos representados por ## son los REN sin punto decimal (p. ej.: 03 es un REN de 0,3). En productos anteriores, el REN se muestra en la etiqueta por separado.
4. Si este equipo tiene un efecto perjudicial sobre la red telefónica, la compañía telefónica le notificará por adelantado que puede ser necesaria la interrupción temporal del servicio. Sin embargo, si una notificación por adelantado no resulta práctica, la compañía telefónica notificará al cliente lo antes posible. También se le informará de su derecho a presentar una queja ante la FCC, si cree que es necesario.
5. La compañía telefónica puede realizar cambios en las instalaciones, equipos, operaciones o procedimientos de la compañía que pudieran afectar el funcionamiento del equipo. Si esto sucede, la compañía telefónica le avisará con antelación para que haga las modificaciones necesarias para mantener un servicio ininterrumpido.
6. Si se experimenta algún problema con este equipo, póngase en contacto con Vertiv en la dirección que se muestra a continuación para obtener información sobre los pasos que deben seguirse para que se realicen las reparaciones. Si el equipo está teniendo un efecto perjudicial sobre la red telefónica, la compañía telefónica puede solicitar que desconecte el equipo hasta que se resuelva el problema.
7. Información de fabricación en el dispositivo de telecomunicaciones (módem):

   Fabricante: Multi-Tech Systems, Inc.

   Nombre comercial: Socket Módem Socket Módem Socket Módem

   Número de modelo: MT5692SMI

   Número de registro: US:AU7MM01BMT5692SMI

   Equivalencia de timbre: 0,1 B

   Toma modular (USOC): RJ11C, RJ11W o RJ45 (una sola línea)

   Vertiv

   4991 Corporate Drive

   Huntsville, AL 35805 EE. UU.

   1-888-793-8763

I.4 Aprobación de Tailandia para MT5692SMI

Este dispositivo de telecomunicaciones cumple con los requisitos de NTC1.

NTC1 es la Comisión Nacional de Telecomunicaciones, el organismo regulador de las telecomunicaciones de Tailandia.

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

I.5 Advertencia del operador Telecom de Nueva Zelanda

1. La concesión de un permiso de telecomunicaciones (Telepermit) para cualquier artículo de equipo de terminal solamente indica que Telecom ha aceptado que dicho artículo cumple las condiciones mínimas para la conexión a su red. No indica ninguna aprobación del producto por parte de Telecom, ni proporciona ningún tipo de garantía. Por encima de todo, no garantiza que ningún artículo funcione correctamente en todos los aspectos con otro artículo de equipo con permiso de telecomunicaciones de una marca o un modelo distinto, ni implica que cualquier producto sea compatible con todos los servicios de red de Telecom.

   En todas las condiciones de funcionamiento adecuado, este equipo no puede funcionar de forma correcta a una velocidad superior a la que se le ha designado. Es probable que las conexiones de 33,6 kbps y 56 kbps sean restringidas a tasas de bits inferiores cuando se conecten a algunas implementaciones PSTN. Telecom no asumirá ninguna responsabilidad en caso de que surjan dificultades en dichas circunstancias.

2. Si este equipo sufre daños físicos, desconéctelo inmediatamente y organice su eliminación o reparación.
3. Este módem no se utilizará de ninguna manera que pueda constituir una molestia para otros clientes de Telecom.
4. Este dispositivo está equipado con marcación por pulsos, mientras que el estándar de Telecom es la marcación por tonos DTMF. No hay ninguna garantía de que las líneas de Telecom siempre seguirán permitiendo la marcación por pulsos.

   El uso de la marcación por pulsos, cuando este equipo esté conectado a la misma línea que otros equipos, puede provocar un "tintineo" o producir ruido y también puede causar una situación de respuesta falsa. En caso de que se produzcan estos problemas, el usuario NO debe ponerse en contacto con el servicio de asistencia para fallos de Telecom.

   El método de marcación preferido es el uso de tonos DTMF, ya que es más rápido que la marcación por pulsos (decádica) y este método está disponible en la práctica totalidad de las centrales telefónicas de Nueva Zelanda.

5. Advertencia: No se pueden realizar llamadas al número de emergencia "111" ni otro tipo de llamadas desde este dispositivo durante una interrupción del suministro eléctrico.
6. Puede que este equipo no proporcione una transferencia efectiva de una llamada a otro dispositivo conectado a la misma línea.
7. Algunos parámetros necesarios para el cumplimiento de los requisitos del permiso de telecomunicaciones de Telecom dependen del equipo (PC) asociado a este dispositivo. Para poder cumplir con las especificaciones de Telecom, el equipo asociado deberá estar configurado para funcionar dentro de los siguientes límites:

Para repetir llamadas al mismo número:

- No habrá más de 10 intentos de llamada al mismo número durante un período de 30 minutos para cualquier iniciación de llamada manual única, y
- El equipo debe colgarse durante un período mínimo de 30 segundos entre el final de un intento y el inicio del siguiente intento.
- Para llamadas automáticas a números diferentes:

- El equipo se configurará para asegurar que las llamadas automáticas a números diferentes estén espaciadas de modo que no haya menos de 5 segundos entre el final de un intento de llamada y el inicio de otro.

8. Para un funcionamiento correcto, el total de RN de todos los dispositivos conectados a una sola línea en cualquier momento no debe ser superior a 5.

I.6 Requisitos para Japón

El módem cumple los requisitos estipulados por el Instituto de Aprobación de Equipos de Telecomunicaciones de Japón (JATE):

MT5692SMI – Aprobación de JATE 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 | Sede central de Vertiv, 1050 Dearborn Drive, Columbus, OH, 43085, EE. UU.

590-1536-520H