Conmutador de transferencia de rack Geist™

Guía de uso e instalación

(Unidades con firmware 6.x.x)

La información contenida en este documento está sujeta a cambios sin previo aviso y es posible que no se adapte a todas las aplicaciones. Aunque se han tomado todas las precauciones para garantizar la precisión y la integridad de esta documentación, Vertiv no asume ningún tipo de responsabilidad y rechaza toda responsabilidad legal por daños que surjan del uso de esta información y por cualquier error u omisión.

Consulte los reglamentos locales y los códigos de construcción relativos a la aplicación, la instalación y el funcionamiento de este producto. El ingeniero consultor, el instalador o el usuario final son responsables del cumplimiento de todas las leyes y reglamentos aplicables en relación con la aplicación, la instalación y el funcionamiento de este producto.

Vertiv fabrica o vende los productos que están cubiertos en este manual de instrucciones. Este documento es propiedad de Vertiv y contiene información confidencial y exclusiva que pertenece a Vertiv. La reproducción, utilización o divulgación sin autorización por escrito por parte de Vertiv quedan estrictamente prohibidas.

Los nombres de compañías y productos son marcas comerciales o marcas comerciales registradas de las respectivas compañías. Cualquier duda relativa al uso de los nombres de marcas registradas se debe dirigir al fabricante original.

Sitio de asistencia técnica

Si tiene algún problema de instalación o funcionamiento con el producto, consulte la sección pertinente de este manual para tratar de resolver el problema mediante los procedimientos descritos.

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

ÍNDICE

Esta página se ha dejado en blanco intencionadamente

1 Instrucciones importantes sobre seguridad

Cumplimiento normativo

Los productos de Vertiv están regulados en cuanto a seguridad, emisiones e impacto medioambiental conforme a los siguientes organismos y políticas.

Underwriters Laboratories (UL)

Las normas UL se utilizan para evaluar productos, probar componentes, materiales, sistemas y rendimiento, y evaluar productos con sostenibilidad medioambiental, energías renovables, productos alimentarios y de agua, sistemas de reciclaje y otras tecnologías innovadoras.

Las normas UL específicas de este equipo son las que se indican en la placa de identificación del dispositivo.

CE

Si un producto incluye la marca CE, significa que cumple con los requisitos europeos (UE) aplicables en cuanto a salud, seguridad y protección ambiental, incluidas la legislación y las directivas sobre productos de la UE. La marca CE es obligatoria para los productos que se ponen a la venta en el Espacio Económico Europeo (EEE).

Los reglamentos, directivas y normas específicas aplicables a cada producto se especifican en la declaración de conformidad.

Comisión Federal de Comunicaciones (CFC)

La Comisión Federal de Comunicaciones (CFC) regula las comunicaciones interestatales e internacionales por radio, televisión, alámbricas, satélite y cable en los 50 estados, el Distrito de Columbia y los territorios de los Estados Unidos. La CFC, agencia gubernamental independiente supervisada por el Congreso, es la principal autoridad de Estados Unidos en materia de legislación, reglamento e innovación tecnológica de las comunicaciones.

Las normas de la CFC específicas para este equipo son:

- Este dispositivo de Clase A cumple con la sección 15 de las normas de la CFC. Su funcionamiento está sujeto a las dos condiciones siguientes:
  - Este dispositivo no debe causar interferencias perjudiciales.
  - Este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan provocar un funcionamiento no deseado.
- Este aparato digital de Clase A cumple con la normativa canadiense ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

¡ADVERTENCIA! Los cambios o modificaciones en esta unidad que no estén expresamente aprobados por la parte responsable del cumplimiento pueden anular la autorización del usuario para usar este equipo.

NOTA: Visite http://www.Vertiv.com/ComplianceRegulatoryInfo antes de la instalación para consultar la información importante sobre seguridad.

Todas las declaraciones de seguridad en VM1227 que hacen referencia al equipo de rack Vertiv se aplican al RTS Geist™.

Algunas cargas pueden generar una corriente de irrupción alta al conmutar las fuentes de energía. No sobrecargue el RTS para evitar fallas en el relé y la activación de la protección del circuito derivado.

Si el RTS se instala en un gabinete, la temperatura ambiente del rack no debe ser superior a 60 °C.

El RTS Geist™ depende de la instalación del edificio para la protección contra condiciones de sobrecorriente. Se requiere un dispositivo de protección contra sobrecorriente certificado en la instalación del edificio. El dispositivo de protección contra sobrecorriente debe dimensionarse de acuerdo con las clasificaciones de la placa de identificación del RTS y los códigos eléctricos locales/nacionales.

El RTS admite la distribución de energía de CA monofásica desde fuentes conectadas a la red de CA de sistemas de distribución de energía TN-S que proporcionen circuitos de tierra y neutro de protección separados, si procede, con una conexión eléctrica directa del equipo al punto conectado a tierra del sistema de distribución de energía según IEC 60364-3.

2 Información general

El conmutador de transferencia de rack (RTS) Vertiv™ Geist™ se utiliza en el centro de datos para facilitar la conmutación o transferencia de la infraestructura de distribución de alimentación del espacio de rack entre dos fuentes de alimentación independientes, de modo que se mantenga el funcionamiento ininterrumpido de los equipos informáticos conectados. La transferencia puede producirse automáticamente cuando se detectan condiciones de calidad de alimentación subóptimas en la fuente activa o mediante intervención manual cuando se requiere el mantenimiento de una fuente.

Consulte en la Tabla 2.1 abajo las condiciones de funcionamiento que provocan una transferencia automática.

Tabla 2.1 Condiciones de desconexión de la fuente de alimentación

Parámetro	Descripción
Voltage Shape	Una distorsión o perturbación de la sinusoidal, una pérdida completa de fase o una desconexión.
Voltage Peak	Una caída repentina de 1/2 ciclo de línea por debajo del pico del 85% de la sinusoidal en estado estacionario.
Voltage RMS	Un cambio gradual superior a ±10% RMS del valor nominal.
Frequency	Frecuencia de línea superior a ±3,75 Hz del valor nominal.

A continuación se enumeran las principales características del RTS:

- Variantes de producto 1U y 2U con tomacorrientes combinados C13/C19 o tomacorrientes NEMA.
- Precisión de clase 1.0 de medición de entrada, circuitos y salidas, incluyendo voltaje y corriente (rms), potencia real (W), potencia aparente (VA), energía (kW-h), factor de potencia y factor de cresta.
- Topología de conmutación híbrida con un tiempo de transferencia total típico de 4 a 8 ms.
- Acción de rotura antes de la fabricación con interruptores redundantes y termistor con fusible a prueba de fallas para mitigar el aumento de corriente durante la transferencia.
- Arranque suave que es la rampa de voltaje de salida, en el arranque en frío para mitigar la corriente de irrupción.
- Controlador de espera en caliente para reducir a cero el tiempo de inactividad durante la actualización del firmware y el reinicio del procesador.
- Fuentes de potencia internas redundantes para resistir un único punto de falla.
- El modo de diagnóstico interno determina, en tiempo real, el estado de los circuitos de interruptor inactivos.
- HMI local con teclas táctiles y gráficos de una línea para cambiar el modo de retransferencia, cambiar la fuente preferida, iniciar la transferencia manual y notificar el estado del sistema.
- El IMD admite la configuración avanzada, el control remoto y la presentación de datos de medición y registro, así como del estado del sistema.

2.1 Requisitos ambientales

Los límites ambientales operativos relativos a la temperatura, la humedad y la elevación son los definidos en la Tabla 2.2 abajo, Tabla 2.3 abajo y la Tabla 2.4 abajo.

Tabla 2.2 Límites de temperatura

Descripción	Mínimo	Máximo
Funcionamiento	10 °C (50 °F)	60 °C (140 °F)
Almacenamiento	-40 °C (-40 °F)	70 °C (158 °F)

Tabla 2.3 Límites de humedad

Descripción	Mínimo	Máximo
Funcionamiento	5%	95% (sin condensación)
Almacenamiento	5%	95% (sin condensación)

Tabla 2.4 Límites de elevación

Descripción	Mínimo	Máximo
Funcionamiento	0 m (0 ft)	3050 m (10.000 ft)
Almacenamiento	0 m (0 ft)	15.240 m (50.000 ft)

2.2 Características de electricidad

Las características y el rendimiento de electricidad se describen en la Tabla 2.5 abajo. Consulte la placa de identificación del producto para ver los límites de clasificación adicionales.

Tabla 2.5 Clasificaciones del receptáculo

Tipo	Clasificaciones
Combinación C13/C19	250 VCA, 16 A (UL y CSA 16 A, 250 VCA) con cable C20 250 VCA, 10 A (UL y CSA 12 A, 250 VCA) con cable C14
German Schuko	250 VCA, 16 A
IEC-60320 C13	250 VCA, 10 A (UL y CSA 12 A, 250 VCA)
IEC-60320 C19	250 VCA, 16 A (UL y CSA 16 A, 250 VCA)
IEC309 PS6	230 VCA, 16 A
IEC309 PS56	230/400 VCA, 32 A
NEMA 5-15R o L5-15R	125 VCA, 12 A
NEMA 6-15R o L6-15R	250 VCA, 12 A
NEMA 5-20R o L5-20R	125 VCA, 16 A
NEMA 6-20R o L6-20R	250 VCA, 16 A
NEMA L5-30R	125 VCA, 24 A
NEMA L6-30R	250 VCA, 24 A

Tabla 2.5 Clasificaciones del receptáculo

Tipo	Clasificaciones
NEMA L7-15R	277 VCA, 12 A
NEMA L7-20R	277 VCA, 16 A
Saf-D-Grid	277 VCA, 16 A
Bloqueo U-Lock IEC-60320 C13	250 VCA, 10 A (UL y CSA 12 A, 250 VCA)
Bloqueo U-Lock IEC-60320 C19	250 VCA, 16 A (UL y CSA 16 A, 250 VCA)
United Kingdom BS1363	250 VCA, 13 A

2.3 Red

Los requisitos de comunicación del producto se definen en las siguientes secciones.

2.3.1 Ethernet

La velocidad de enlace Ethernet para este producto es de 10/100/1000 MB; dúplex completo.

2.3.2 Protocolos

Entre los protocolos de comunicaciones que admite este producto se incluyen: ARP, IPv4, IPv6, ICMP, ICMPv6, TCP, UDP, RSTP, STP, DNS, HTTP, HTTPS (TLSv1.2 y TLSv1.3), SMTP, SMTPS, Modbus TCP/IP, DHCP, SNMP (V1/V2c/V3), LDAP, TACACS+, RADIUS, NTP, SSH, RS232 y Syslog.

2.3.3 Interfaces de usuario

Este producto es compatible con las siguientes interfaces de usuario: SNMP, JSON-based Web GUI, JSON API e interfaz de línea de comandos que utilice SSH y serie (RS232).

Esta página se ha dejado en blanco intencionadamente

3 Instalación

Utilizando la información de Montaje abajo, instale su RTS Vertiv™ Geist™.

Para instalar la unidad:

1. Utilizando el hardware adecuado, monte el RTS en el rack (consulte la sección Montaje abajo para obtener instrucciones adicionales).
2. Enchufe el RTS en receptáculos de circuito derivado sin corriente.
3. Conecte los dispositivos a los receptáculos de salida del RTS. Se recomienda apagar los dispositivos hasta que todos estén conectados al RTS.
4. Encienda el circuito derivado para la fuente A para energizar el RTS.
   - La unidad emitirá un pitido en el arranque.
5. Encienda el circuito derivado para la fuente B.
   - La unidad emitirá dos pitidos durante el arranque después de que se bloquee en la primera frecuencia de línea fuente disponible.
6. Encienda los dispositivos.

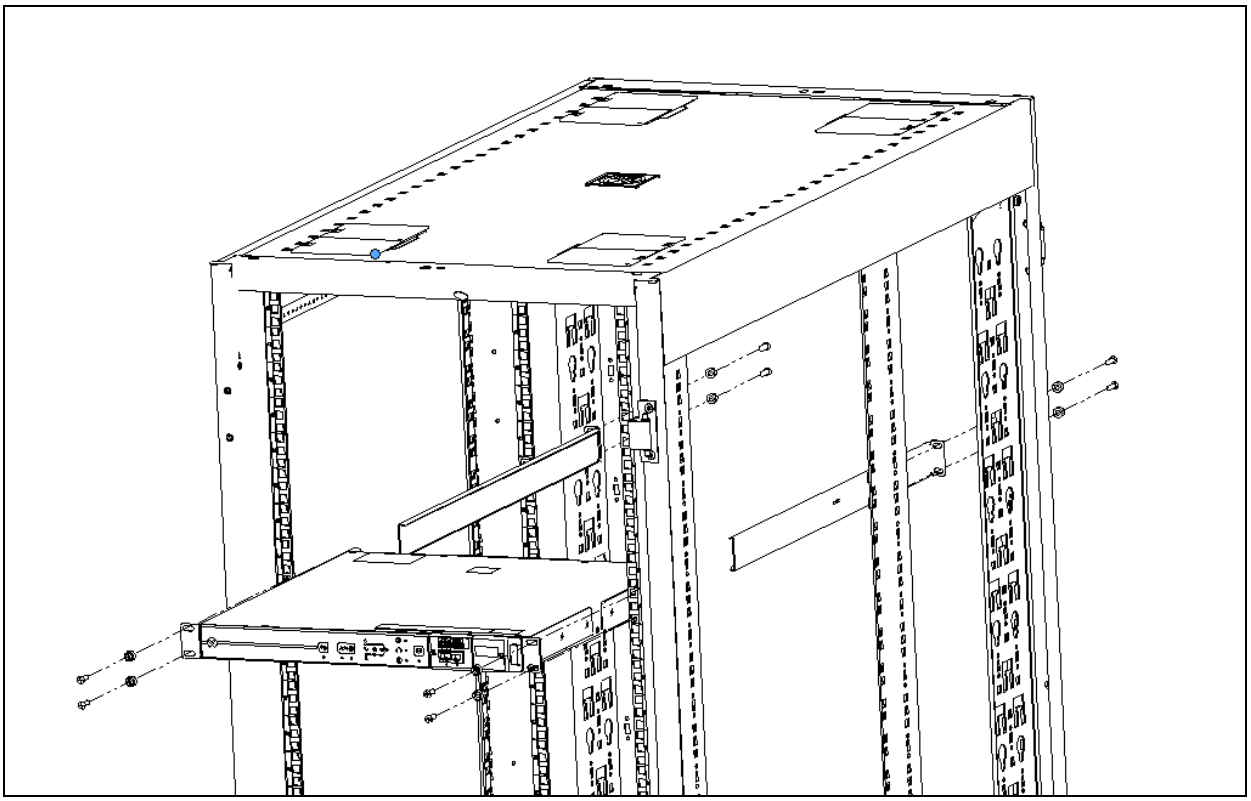
NOTA: De forma predeterminada, la fuente A está designada como fuente preferida y la retransferencia está habilitada. En el arranque en frío, si la fuente B se conecta y califica primero, la alimentación se habilita a través de la fuente B. Una vez que la fuente A se haya conectado y calificado, transferirá la alimentación a la fuente A.

3.1 Montaje

3.1.1 Montaje en rack de 4 postes

1. Instale los soportes de montaje en la unidad RTS.
2. Instale los soportes deslizantes en el rack.
3. Inserte la unidad de RTS con soportes en los soportes deslizantes. La Figura 3.1 en la página siguiente ilustra la instalación de la unidad de RTS.

Figura 3.1 Soportes deslizantes del RTS



3.1.2 Montaje en rack de 2 postes

NOTA: Cada soporte de montaje puede utilizarse en el lado izquierdo o derecho de la unidad de RTS. La unidad de RTS puede montarse orientada hacia dentro o hacia fuera del rack de 2 postes.

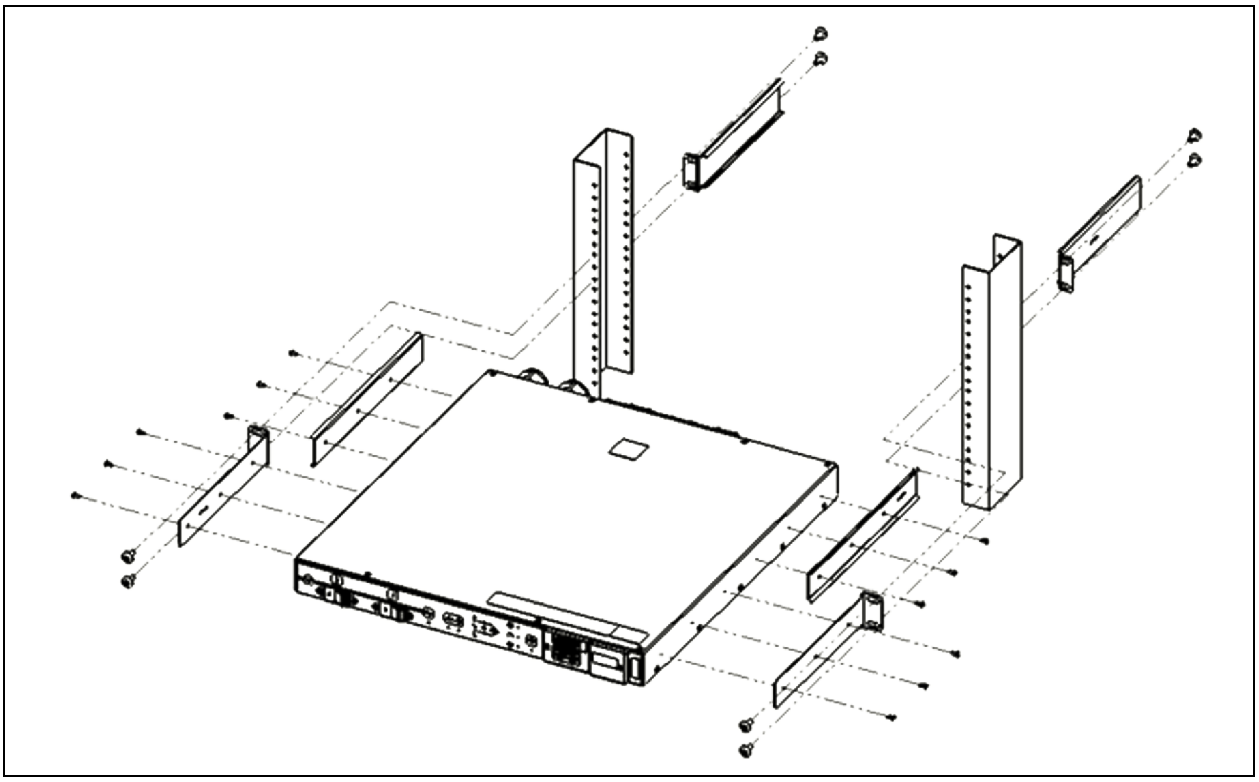
Para fijar los soportes en el RTS:

- Alinee el soporte en U (sin aleta de montaje de 2 orificios) con la parte posterior del RTS y fije el soporte al RTS con dos tornillos. Repita el paso en el otro lado del RTS.
- Alinee el soporte de montaje con la aleta de montaje de 2 orificios con la parte frontal del RTS y fije el soporte al RTS con dos tornillos. Consulte la orientación tal y como se muestra en la Figura 3.2 en la página opuesta. Repita el paso en el otro lado del RTS.
- Alinee el soporte deslizante con la aleta de montaje de 2 orificios del juego de montaje con el lado opuesto del rack de 2 postes y fije el soporte al rack con dos tornillos (proporcionados por el cliente). Repita el paso en el otro lado del rack.

Para fijar el RTS al rack de 2 postes:

1. Inserte el RTS con soportes en los soportes deslizantes. La Figura 3.2 en la página opuesta ilustra la instalación de la unidad de RTS.
2. Fije cada soporte lateral al rack con dos tornillos (proporcionados por el cliente).

Figura 3.2 Soportes deslizantes del RTS



3.2 Conexión de alimentación

Enchufe los cables de potencia de entrada doble del RTS Vertiv™ Geist™ en los receptáculos del circuito derivado debidamente clasificados y protegidos. Asegúrese de que el cable de alimentación no supere el radio de curvatura del fabricante (10X).

3.2.1 Funcionamiento de U-Lock

Enchufe los dispositivos que van a recibir alimentación del RTS Vertiv™ Geist™.

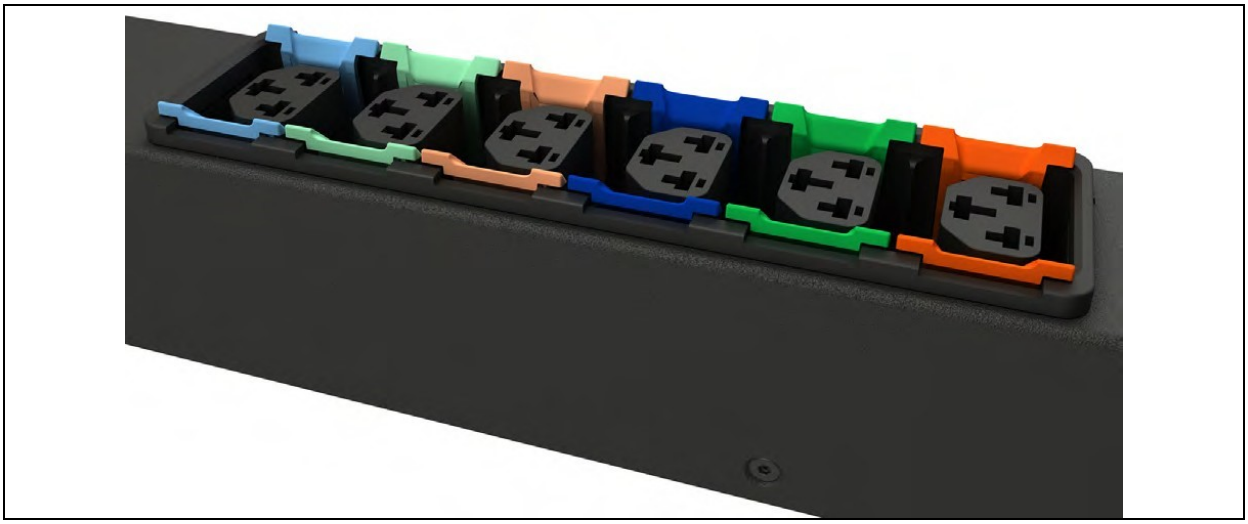
- Retención de cables de alimentación U-Lock patentado por Vertiv
- Utiliza cables de alimentación estándares
- Al insertar el cable, se activa el sistema de bloqueo
- Fácil desbloqueo del bisel con solo mantenerlo presionado

Figura 3.3 Funcionamiento de la retención de cables U-Lock

3.2.2 Funcionamiento de P-Lock

- Enchufe los dispositivos que van a recibir alimentación del RTS Vertiv™ Geist™.
- Tomacorrientes C13/C19 Vertiv combinados con retención de cable de alimentación P-Lock.
- Compatible con cables de alimentación P-Lock.
- Utilice las lengüetas de tipo "presionar y mantener" del cable P-Lock para liberarlo del tomacorriente.

Figura 3.4 Funcionamiento de la retención del cable P-Lock



4 Mejores prácticas de seguridad

La configuración predeterminada en el soporte del IMD está predeterminada para una configuración segura en la instalación. Una seguridad adecuada de los equipos de infraestructura crítica requiere la configuración correcta de TODOS los servicios de comunicación. En esta sección se resumen los ajustes.

En todo el ciclo de vida de nuestro producto Vertiv SECURE, Vertiv está comprometido a minimizar el riesgo de ciberseguridad en sus productos. Para lograrlo, implementa las mejores prácticas de ciberseguridad en todo el diseño de ingeniería de productos y soluciones, y así los hace más seguros, confiables y competitivos para nuestros clientes.

A continuación se ofrecen algunas recomendaciones de ciberseguridad para el ciclo de vida. Las recomendaciones en materia de ciberseguridad no pretenden ser una guía exhaustiva al respecto, sino complementar los programas de ciberseguridad ya existentes de los clientes. Para obtener más información sobre las mejores prácticas y directrices generales en materia de ciberseguridad, consulte los siguientes sitios:

https://www.cisa.gov/topics/cybersecurity-best-practices

https://www.vertiv.com/en-us/support/security-support-center/

La Tabla 4.1 abajo siguiente incluye una lista de los elementos que se deben revisar. Cada uno de ellos se debe revisar y configurar en función de las necesidades operativas de gestión de los equipos; asimismo, se debe verificar que los ajustes admiten la funcionalidad operativa deseada sin agregar accesos innecesarios o no autorizados a los equipos de infraestructura crítica. Se proporciona una referencia a la sección correspondiente de este documento para configurar cada elemento.

Tabla 4.1 Ajustes que se deben revisar y verificar para reducir el riesgo de acceso no autorizado

Elemento	Descripción	Referencia
Cuentas y contraseñas	Cambie inmediatamente los nombres y contraseñas de las cuentas de administrador y usuario para eliminar el acceso a las credenciales por defecto.	Consulte Página Users en la página 57.
Acceso a la red IP	Habilite/deshabilite el acceso de red IPV4 e IPV6 a la tarjeta; deshabilite el acceso de red no utilizado.	Consulte Pestaña Network en la página 61.
Acceso SSHv2	Habilite/deshabilite el acceso SSHv2 para soporte de diagnóstico y configuración; deshabilítelo cuando no esté en uso.	Consulte SSH en la página 80.
Protocolo de servicio web	Seleccione HTTPS para utilizar el cifrado SSL al acceder a los datos a través de la interfaz de usuario web.	Consulte Pestaña Web Server en la página 71.
Certificados TLS	Cuando utilice HTTPS, instale sus propios certificados TLS de una autoridad de certificación de confianza o genere certificados alternativos autofirmados.	Consulte SSL Certificate: le permite cargar su propio archivo de certificado SSL firmado para remplazar el predeterminado. El certificado puede estar autofirmado o firmado por una

Tabla 4.1 Ajustes que se deben revisar y verificar para reducir el riesgo de acceso no autorizado

Elemento	Descripción	Referencia
		autoridad de certificación. El certificado SSL debe tener formato PEM o PFX (PKCS12). en la página 72.
Acceso de escritura remoto por web	Para controlar/escribir a través de la interfaz web, debe iniciar sesión de forma remota y disponer de una cuenta de usuario de nivel de administrador o de control. Para prohibir el acceso remoto, deshabilite tanto HTTP como HTTPS. **¡ADVERTENCIA! Al deshabilitar tanto HTTP como HTTPS se terminará inmediatamente esta conexión y el acceso remoto solo estará disponible utilizando SSH.**	Consulte Pestaña Web Server en la página 71.
Protocolos de comunicación	Habilite/deshabilite SNMP; deshabilite protocolos no utilizados.	Consulte Modbus en la página 85.
Configuración de la versión SNMP	Habilite/deshabilite las versiones SNMP deseadas, considere el uso de SNMPv3 con autenticación de usuario y cifrado.	Consulte SNMP en la página 83.
Ajustes de la tabla de acceso SNMP	Para cada entrada de la tabla de acceso SNMPv1/v2c, configure el tipo de acceso SNMP como *Read-Only* para evitar cambios en el dispositivo desde los hosts identificados en la entrada de la tabla.	Consulte SNMP en la página 83.
Cadenas de comunidad SNMP	Utilice valores suficientemente fuertes para la comunicación SNMP, de acuerdo con la política de contraseñas de su organización.	Consulte SNMP en la página 83.
Ajustes SNMPv3	Utilice algoritmos hash y de cifrado adecuados para los ajustes de autenticación y privacidad de SNMPv3 para que las comunicaciones SNMPv3 sean más seguras.	Consulte SNMP en la página 83.
Cuenta de usuario invitado	A menos que sea necesario, esta cuenta debe permanecer deshabilitada, dado que proporciona acceso de solo lectura al dispositivo y, si está habilitada, puede dar contexto adicional a la configuración del dispositivo.	Consulte Página Users en la página 57.

Para mayor seguridad, el *firewall* y el *gateway* de la red local se pueden restringir para permitir solo el tráfico necesario en los puertos de red requeridos. Los puertos utilizados por la tarjeta IMD-5M se enumeran en la Tabla 4.2 abajo. Algunos ajustes de puertos pueden ser modificados por el administrador.

Tabla 4.2 Puertos utilizados por la tarjeta IMD-5M (v6.1 o superior)

Servicio de red	Puerto utilizado	Predeterminado	Se requiere modificación
HTTP	TCP80	N	S
HTTPS	TCP443	S	S
DNS	TCP&UDP 53	S	N
NTP	TCP&UDP 123	S	N
SMTP	TCP25	S	S
SSH	TCP UDP 22	S	N

Tabla 4.2 Puertos utilizados por la tarjeta IMD-5M (v6.1 o superior)

Servicio de red	Puerto utilizado	Predeterminado	Se requiere modificación
SNMP	UDP 161, 162	N	Solo se puede cambiar el puerto de trampa 162.
Modbus	TCP 502	N	S
VID/VIP	GDP/HTTP	N	N
DHCP Client	UDP 68	S	N
GDP (Geist Discovery Protocol)	UDP 6687	S	N
LDAP	TCP 389	N	S
RADIUS	UDP1812/1813/1645/1646	N	N
TACACS	TCP 49	N	N
Remote Syslog	TCP 514	N	S

Los detalles para la configuración de todas las opciones se proporcionan más adelante en esta guía.

4.1 Evaluación de riesgos

Vertiv recomienda realizar una evaluación de riesgos para identificar y evaluar los riesgos internos y externos razonablemente previsibles para la seguridad, disponibilidad e integridad del sistema y su entorno. Este ejercicio se debe llevar a cabo de conformidad con los marcos técnicos y reglamentarios aplicables, como IEC 62443 y NERC-CIP. La evaluación de riesgos se debe repetir periódicamente.

4.2 Seguridad física

El IMD5 está diseñado y pensado para ser instalado y utilizado en un lugar físicamente seguro. Vertiv recomienda revisar la seguridad física y el entorno operativo de la unidad. Dado que las amenazas de atacantes externos o internos pueden causar graves trastornos, a continuación se indican algunas de las mejores prácticas recomendadas:

- Restringir el acceso a áreas, racks y unidades con tarjetas RFID/etiquetas encriptadas, autenticación de código de acceso multifactor único, trampas para personas y escáneres biométricos para el acceso físico al equipo.
- Guardias de seguridad de confianza y con antecedentes comprobados con presencia física las 24 horas del día, los 7 días de la semana, los 365 días del año y registros escritos para documentar y anotar el acceso físico a un centro de datos, edificios y racks.
- Acceso físico restringido a los equipos de telecomunicaciones y al cableado de red. El acceso físico a las líneas de telecomunicaciones y al cableado de red debe estar restringido para proteger contra los intentos de interceptar o sabotear las comunicaciones. Las mejores prácticas incluyen el uso de conductos metálicos para el cableado de red que se extiende entre los gabinetes de los equipos.
- Todos los puertos USB, RJ45 o cualquier otro puerto físico deben estar restringidos en las unidades.

- No conectar medios extraíbles (como dispositivos USB y tarjetas SD) para ninguna operación (como actualización de firmware, cambio de configuración o cambio de aplicación de arranque) a menos que el origen del medio sea conocido y de confianza. Antes de conectar cualquier dispositivo portátil a través de un puerto USB o una ranura para tarjetas SD, analícelo en busca de malware y virus.

4.3 Acceso a la cuenta

Los privilegios de acceso a la cuenta del IMD5 se deben administrar para proporcionar el menor número de funciones de cuenta que aún permita al usuario final realizar sus funciones de trabajo. El acceso al IMD5 debe estar restringido a usuarios legítimos. Los procedimientos escritos para el acceso a la red y a los equipos de las organizaciones deberían adoptar algunas de las siguientes mejores prácticas:

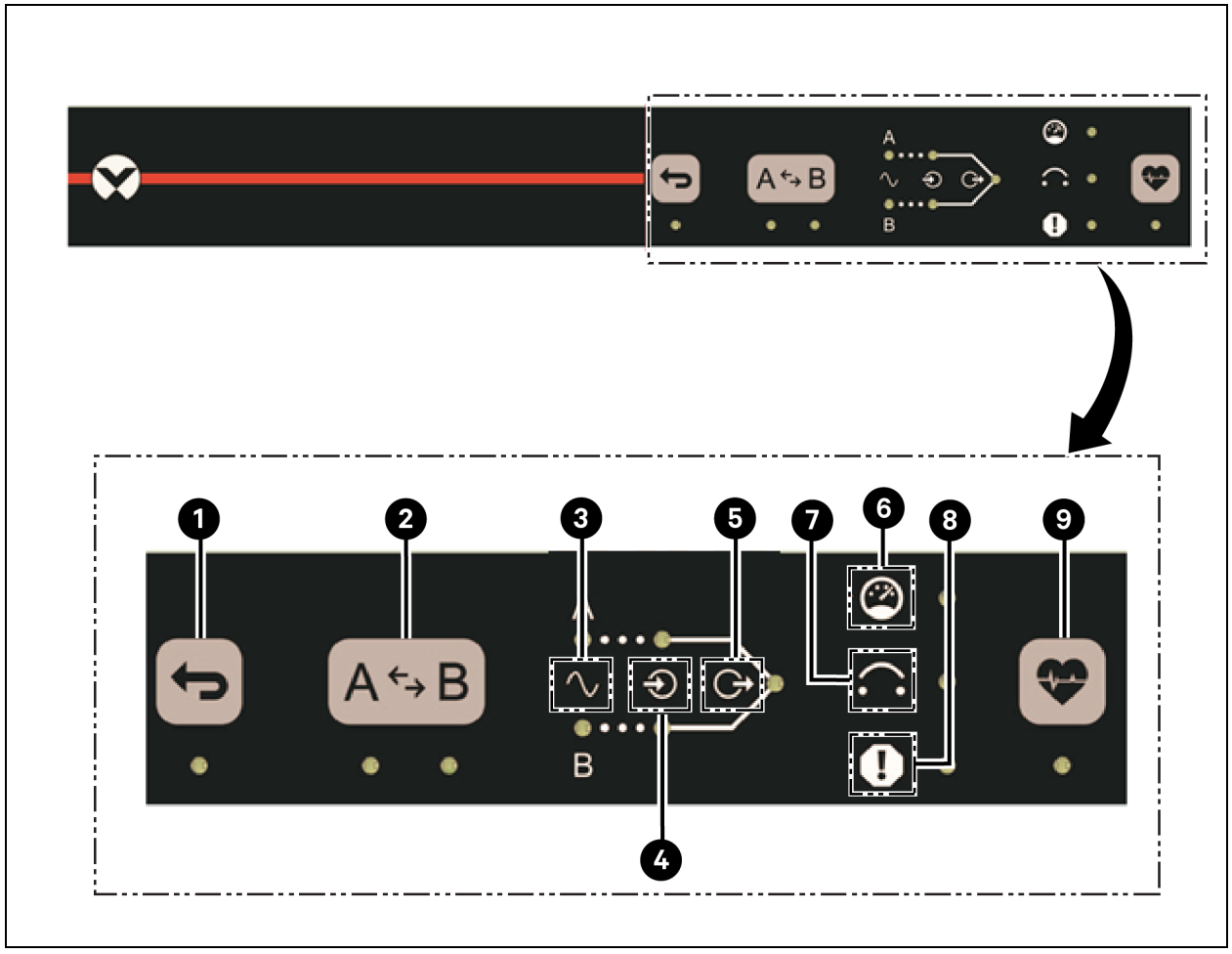
- El primer acceso al IMD5 requiere la creación de credenciales.
- No se comparten cuentas ni inicios de sesión. Cada usuario debe tener su propia cuenta y contraseña específicas. Las funciones de anotación de registros del IMD5 requieren que cada cuenta sea de un único usuario no compartido.
- Los administradores deben restringir el acceso y los privilegios únicamente a las funciones requeridas por el puesto de trabajo del usuario.
- Restringir todos los privilegios de nivel de administrador (como actualizaciones de firmware, activación/desactivación de protocolos, etc.) únicamente a los administradores autorizados.
- Asegurarse de que los requisitos de seguridad, complejidad y longitud de las contraseñas se aplican al más alto nivel según la política de TI de la empresa.
- Asegurarse de que los empleados desvinculados no tengan acceso a la unidad. Algunos ejemplos incluyen el usuario de un proceso de autenticación de usuario AAA, TACACS+.
- Establecer el tiempo de espera de la sesión tras un período de inactividad.
- Utilizar la función *remote syslog* para recibir alertas sobre eventos del sistema y de la red, amenazas a la seguridad y visibilidad del dispositivo para solucionar problemas (esto también puede ser necesario en su entorno para el cumplimiento de PCI-DSS/SOX/HIPAA).

5 Configuración

5.1 HMI local

La interfaz hombre-máquina (HMI) local utiliza una etiqueta de teclas táctiles como medio de control local y transmite el estado operativo mediante sus indicadores visuales. La Figura 5.1 abajo ilustra la disposición de la HMI.

Figura 5.1 Visión general de la HMI



Elemento	Descripción
1	Retransferencia habilitada
2	Fuente preferida
3	Fuente calificada
4	Fuente activa
5	Salida activa

Elemento	Descripción
6	Estado de capacidad
7	Estado del dispositivo de protección contra sobrecorriente (OCPD)
8	Estado de falla interna
9	Autodiagnóstico de estado

La funcionalidad de los siguientes elementos se describe en el contexto de la Figura 5.1 en la página anterior.

Retransferencia habilitada

Esta tecla habilita o deshabilita la retransferencia de la fuente alternativa a la fuente preferida. Esta tecla se inhibe si el IMD configura una condición de bloqueo o si está pendiente un autodiagnóstico de estado. La luz LED indica el estado habilitado o deshabilitado del modo de retransferencia. La luz LED se enciende de forma continua cuando está habilitado y se apaga cuando está deshabilitado. La luz LED parpadea rápidamente tres (3) veces y la unidad emitirá con rapidez tres (3) pitidos si la tecla está inhibida.

Si se habilita la retransferencia antes de una transferencia automática de la fuente preferida a la alternativa, se producirá una transferencia automática de vuelta a la fuente preferida después de que haya transcurrido el tiempo de retardo de la retransferencia y se haya calificado la fuente preferida.

Si se deshabilita la retransferencia antes de una transferencia automática de la fuente preferida a la alternativa, la retransferencia a la fuente preferida se aplazará hasta que se haya calificado la fuente preferida y se habilite la retransferencia o hasta que se alterne una vez la selección de la fuente preferida.

NOTA: El tiempo de retardo de la retransferencia empieza a contar desde el momento de la transferencia.

Fuente preferida

Esta tecla alterna la selección de la fuente preferida.

Si las condiciones de funcionamiento lo permiten:

- La unidad RTS funcionará normalmente a partir de la fuente preferida siempre que ambas fuentes estén calificadas.
- Con esta tecla se forzará una transferencia a la nueva fuente preferida seleccionada.

NOTA: Si una o ambas fuentes no están calificadas, el cambio de la fuente preferida está permitido pero no da lugar a una transferencia. Esta tecla puede estar inhibida si está pendiente una condición de bloqueo como un autodiagnóstico de estado.

La luz LED indicará que se prefiere la fuente A o B. La luz LED se enciende de forma continua para la fuente preferida y se apaga para la fuente alternativa. La luz LED parpadea rápidamente tres (3) veces y la unidad emitirá con rapidez tres (3) pitidos si la tecla está inhibida.

Fuente calificada

La luz LED indica que la fuente de alimentación está disponible y calificada. Significa que lous parámetros eléctricos están dentro de los límites aceptables para alimentar los ITE según la sección 6.2. La luz LED se apagará mientras la fuente no esté disponible o no se detecte. La luz LED parpadea mientras la fuente está disponible y su determinación de calidad de energía está pendiente.

La luz LED se enciende de forma continua mientras la fuente se considera estable y adecuada para alimentar los dispositivos informáticos.

Fuente activa

Estas luces LED indicarán la fuente activa que suministra alimentación a la carga. La luz LED se enciende de forma continua para la fuente activa y se apaga para la fuente inactiva.

Salida activa

La luz LED indica el estado activo/inactivo de la salida. La luz LED se enciende de forma continua mientras el circuito de conmutación y los disyuntores (si hay) están cerrados. La luz LED se apagará si todos los disyuntores están abiertos.

Estado de capacidad

La luz LED indica una condición de advertencia/aviso de sobrecorriente. La luz LED parpadea lentamente mientras el consumo de corriente supera un valor umbral del 80% de la clasificación de corriente y se apaga mientras el consumo de corriente es inferior a este umbral.

Estado del dispositivo de protección contra sobrecorriente (OCPD)

La luz LED indica una condición de OCPD abierto, causada por una condición de sobrecorriente que excede los valores nominales de OCPD o el actuador se abre manualmente. La luz LED parpadea lentamente mientras se dispara el OCPD y se apaga después de que se haya corregido la condición de sobrecorriente y se haya cerrado manualmente el actuador del OCPD.

Estado de falla interna

La luz LED indica un estado de funcionamiento defectuoso del producto. La luz LED parpadea cuando se diagnostica una falla interna y se apaga cuando el estado de funcionamiento es normal.

Autodiagnóstico de estado

Esta tecla ejecuta el modo autodiagnóstico de estado. Cuando se presiona la tecla táctil de modo de estado habilitado, se emitirán cuatro (4) pitidos. Todas las luces LED de la HMI parpadearán continuamente mientras esté activo el modo autodiagnóstico de estado. El modo activo persistirá durante unos segundos. La luz LED se enciende de forma continua cuando está pendiente de realizar el programa de autodiagnóstico de estado. Se emiten tres (3) pitidos rápidos si la llave está inhibida.

NOTA: Esta tecla se inhibirá si existe una condición de falla persistente. Si el modo de estado no puede ejecutarse en el momento de presionar la tecla táctil, se emitirán cuatro (4) pitidos y todas las luces LED se mantendrán encendidas momentáneamente, pero no se producirá ninguna acción de conmutación.

5.2 Dispositivo de monitoreo intercambiable

El dispositivo de monitoreo intercambiable (IMD) es la base de la línea de productos eléctricos actualizables del conmutador de transferencia de rack Vertiv™ Geist™. El IMD se puede remplazar y actualizar para permitir que los centros de datos puedan probar sus ubicaciones en el futuro. La instalación de un IMD incorrecto para su remplazo en un RTS puede provocar daños en el IMD.

5.2.1 Básico

El RTS Geist™ actualizable básico es el punto de referencia para la línea de productos GU. Lleva integrado el módulo IMD-01X y proporciona una distribución de energía de bajo costo con la opción de actualizarse para agregar características de medición local o monitoreo remoto, entre otras, en el futuro.

5.2.2 Medición

El RTS Geist™ actualizable con medición es una opción con medición local para la línea de productos GU. Lleva integrado el módulo IMD-01D y proporciona una pantalla local para ver el consumo de corriente (amperios) con la opción de actualizarse para agregar monitoreo y otras características en el futuro.

Figura 5.2 Módulo IMD-01D

Tabla 5.1 Descripciones del módulo IMD-01D

Elemento	Nombre	Descripción
1	Pantalla local	La pantalla local muestra los valores de fase, línea y corriente del circuito (en amperios).
2	Botones de la pantalla	Hay tres botones cerca de la pantalla del IMD: un botón para retroceder, otro para avanzar y otro para centrar. Las funciones de estos botones se describen en la **Tabla 5.2** en la página opuesta.

Tabla 5.2 Funciones de los botones de la pantalla

Botón	Símbolo	Descripción
Botón de retroceso		Desciende al canal anterior.
Botón de avance		Avanza al canal siguiente.
Botón central		Alterna entre los modos de pantalla de desplazamiento y estático. Si se mantiene presionado este botón durante 10 segundos, se realizará un restablecimiento de red, lo cual restaurará la dirección IP predeterminada y restablecerá las cuentas de usuario.
Botón central x3		Al pulsar este botón tres veces en dos segundos, se habilita el modo VLC. Al pulsar el botón mientras el modo VLC está activo, la unidad vuelve a la pantalla actual estándar.
Botones de avance y retroceso		Cuando se presionan ambos botones al mismo tiempo, la pantalla se voltea 180 grados.

NOTA: Las funciones de los botones de la pantalla pueden variar según la configuración de la unidad.

5.2.3 Conmutación y monitoreo

Las versiones anteriores de las unidades de RTS Vertiv™ Geist™ de monitoreo a nivel de unidad, monitoreo a nivel de tomacorrientes, monitoreo a nivel de unidades conmutadas y monitoreo a nivel de tomacorrientes conmutados se enviaron con el módulo IMD-3E-G.

Figura 5.3 Módulo IMD-3E-G

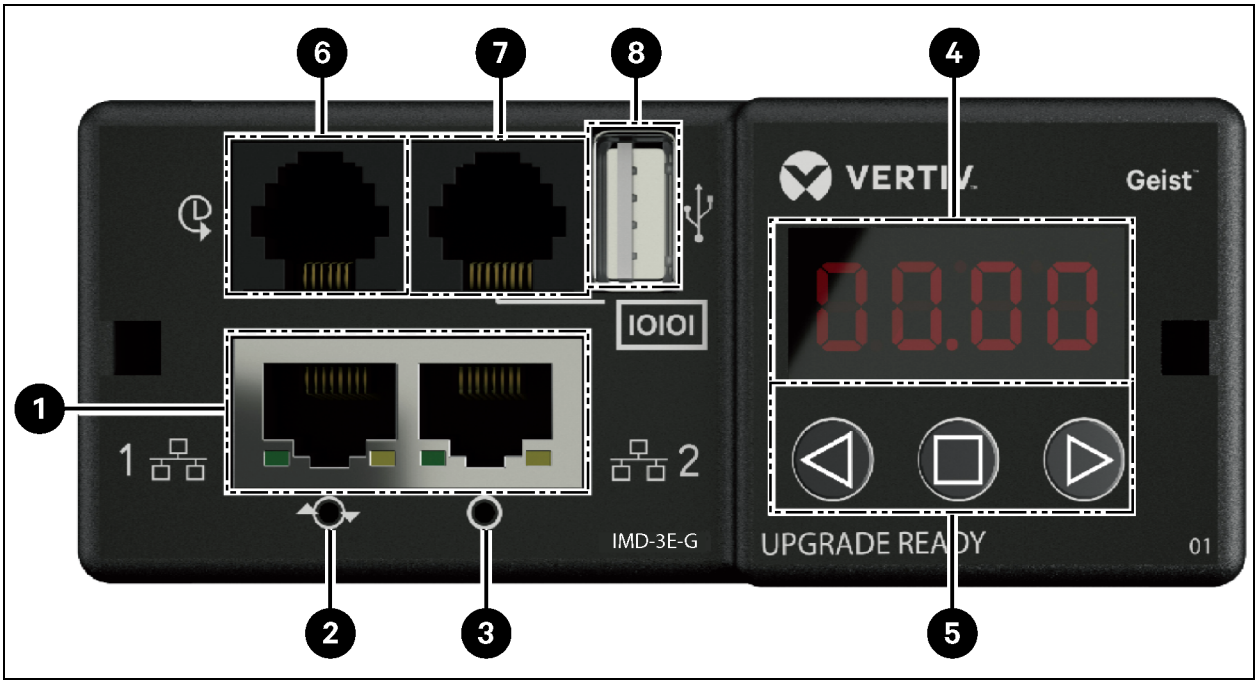


Tabla 5.3 Descripciones del módulo IMD-3E-G

Número	Nombre	Descripción
1	Puertos Ethernet dobles	Los puertos Ethernet dobles actúan como un conmutador Ethernet de dos puertos, lo que permite conectar varios dispositivos en cadena margarita. Los puertos Ethernet dobles se pueden configurar independientemente como interfaces de red Ethernet dobles, lo que permite que el RTS se pueda conectar a dos redes diferentes.
2	Botón de reinicio por hardware	Cuando se presiona el botón de reinicio por hardware, se reinicia el IMD. Actúa como un ciclo de desconexión y conexión de la energía, y no cambia ni elimina información del usuario.
3	Botón de restablecimiento de red	Si se mantiene presionado el botón de restablecimiento de red 5 segundos durante el funcionamiento normal, se restaurará la dirección IP predeterminada y se restablecerán las cuentas de usuario.
4	Pantalla local	La pantalla local muestra los valores de fase, línea y corriente del circuito (en amperios).
5	Botones de la pantalla	Hay tres botones cerca de la pantalla del IMD: un botón para retroceder, otro para avanzar y otro para centrar. Las funciones de estos botones se describen en Funciones de los botones de la pantalla en la página opuesta.
6	Puerto del sensor remoto	Puerto RJ-12 para conectar sensores digitales remotos *plug-and-play* de Vertiv (se venden por separado). Cada sensor digital tiene un número de serie único y se detecta automáticamente. Las PDU GU2 admiten hasta 16 sensores. Se puede agregar el convertidor Vertiv™ A2D opcional para admitir la detección analógica. El SN-ADAPTER opcional puede agregarse para admitir sensores integrados y modulares Liebert. Para obtener más información, consulte Sensores disponibles en la página 116.
7	Puerto serie	RS-232 a través del puerto RJ-45.
8	Puerto USB	Puerto USB que se utiliza para cargar el firmware, hacer una copia de seguridad/restaurar la configuración del dispositivo, ampliar la capacidad de registro a través de un dispositivo de almacenamiento USB o admitir adaptadores USB inalámbricos TP-Link. El puerto USB debe estar habilitado, consulte USB en la página 80. Proporciona hasta 5 vatios de capacidad de alimentación para dispositivos conectados por USB.

NOTA: Se admiten dispositivos USB MSC, como unidades USB o discos duros externos. Los dispositivos de almacenamiento USB deben tener formato FAT32.

NOTA: La conexión en serie no permite el control de flujo.

Botones de la pantalla

Hay tres botones cerca de la pantalla del IMD: un botón de retroceso, otro de avance y otro central. Las funciones de estos botones se describen en la Tabla 5.4 en la página opuesta.

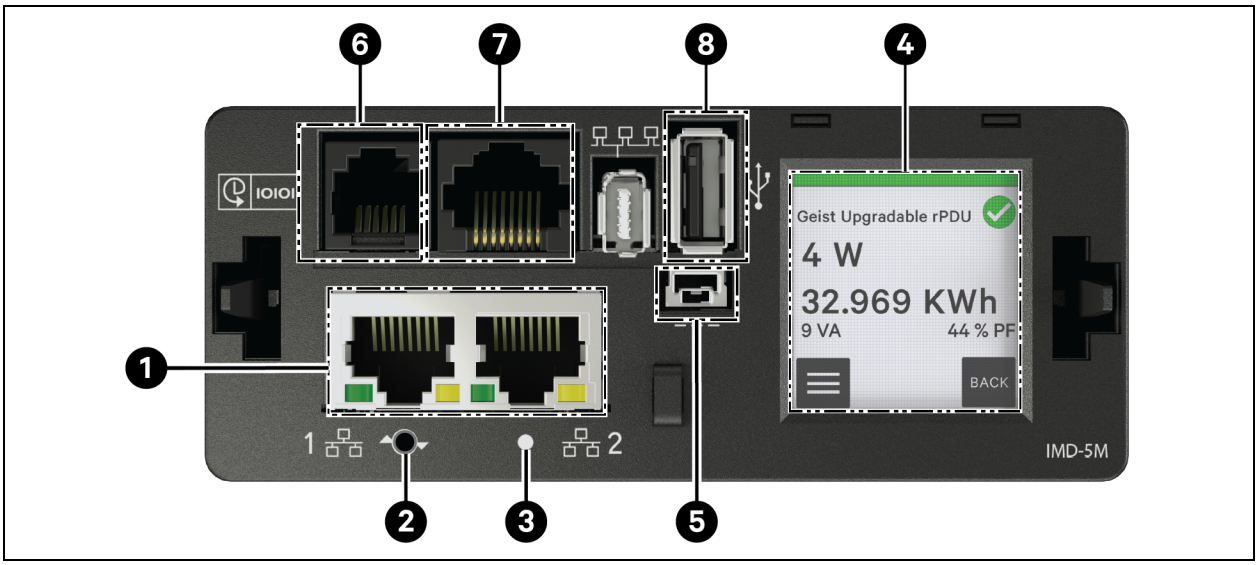
Tabla 5.4 Funciones de los botones de la pantalla

Botón	Símbolo	Descripción
Botón de retroceso		Presione para volver al canal anterior. Si se mantiene presionado este botón durante 3 segundos, se inicia una copia de seguridad de la configuración. Mientras se genera la copia de seguridad, aparece en pantalla el mensaje **bcup**, y luego vuelve al estado normal. Las copias de seguridad se almacenan en dispositivos de almacenamiento USB disponibles, y no se pondrá en funcionamiento si dichas unidades no están disponibles.
Botón de avance		Presione para avanzar al canal siguiente. Si se mantiene presionado este botón durante 3 segundos, se inicia la restauración de la configuración. Aparece en pantalla el mensaje **load**, seguido de un mensaje **conf** y una cuenta atrás de 3 segundos. Una vez que termina la cuenta atrás, aparece el mensaje **8888** y se aplica la copia de seguridad. La copia de seguridad se leerá desde dispositivos de almacenamiento USB. Si se suelta el botón en cualquier momento de esta secuencia, la restauración se anula. Una vez aplicada la copia de seguridad, o si no hay imágenes de copia de seguridad o no hay un dispositivo de almacenamiento USB conectado, la pantalla vuelve al estado normal.
Botón central		Alterna entre los modos de pantalla de desplazamiento y estático. Si se mantiene presionado este botón durante 3 segundos, se inicia una secuencia de restablecimiento de parámetros. Durante la secuencia, se muestra un mensaje **rest**, seguido de un mensaje **dflt** y una cuenta atrás de 3 segundos. Una vez que termina la cuenta atrás, se muestra un mensaje **8888** y la información de red, http, cuentas de usuario y LDAP/RADIUS se restablecen a los valores predeterminados. Si se suelta el botón en cualquier momento de esta secuencia, el restablecimiento se anula.
Botón central x3		Al pulsar este botón tres veces en 2 segundos, se habilita el modo VLC. Al pulsar el botón mientras el modo VLC está activo, la unidad vuelve a la pantalla actual estándar.
Botones de avance y retroceso		Cuando se presionan ambos botones al mismo tiempo, la pantalla se voltea 180 grados.
Botones de retroceso y central		Al pulsar ambos botones al mismo tiempo, se muestra la dirección IPv4 primaria de la unidad.

5.2.4 Unidades monitoreadas y conmutadas (IMD-5M)

Con el módulo IMD-5M se envían todas las unidades de RTS Vertiv™ Geist™ monitoreadas y conmutadas.

Figura 5.4 Módulo IMD-5M



Elemento	Nombre	Descripción
1	Puertos Ethernet dobles	Los puertos Ethernet dobles actúan como un conmutador Ethernet de dos puertos, lo que permite conectar varios dispositivos en cadena margarita. Los puertos Ethernet dobles se pueden configurar independientemente como interfaces de red Ethernet dobles, lo que permite que el RTS se pueda conectar a dos redes diferentes.
2	Botón de reinicio/restablecimiento	Mantenga presionado el botón durante 10 segundos (hasta que el indicador LED parpadee) para reiniciar el IMD. Actúa como una desconexión y conexión de la potencia para el IMD y no cambia ni elimina información del usuario. Si se mantiene presionado el botón durante 25 segundos (hasta que el indicador LED parpadee rápidamente) durante el funcionamiento normal, se restaurará la dirección IP predeterminada y se restablecerán las cuentas de usuario.
3	LED de estado RGB	LED verde: la unidad está en funcionamiento. LED amarillo: la unidad está arrancando.
4	Menú de la pantalla táctil	Utilice el menú de la pantalla táctil para buscar los valores de corriente de fase, línea y circuito (en amperios).
5	Entrada de alimentación redundante	Si el cable de conexión opcional está enchufado a la segunda unidad, el IMD permanecerá alimentado cuando el RTS pierda alimentación.

Elemento	Nombre	Descripción
6	Puerto del sensor remoto	Puerto RJ-12 para conectar sensores digitales remotos *plug-and-play* de Vertiv™ (se venden por separado). Cada sensor digital tiene un número de serie único y se detecta automáticamente. Las PDU del RTS admiten hasta 16 sensores. Se puede agregar el convertidor Vertiv™ A2D opcional para admitir la detección analógica. El SN-ADAPTER opcional puede agregarse para admitir sensores Liebert® integrados y modulares. Para obtener más información, consulte Sensores disponibles en la página 116.
7	Puerto serie	RS-232 a través del puerto RJ-45.
8	Puerto USB	Puerto USB que se utiliza para cargar el firmware, ampliar la capacidad de registro a través de un dispositivo de almacenamiento USB o admitir ciertos adaptadores USB inalámbricos TP-Link. El puerto USB debe estar habilitado, consulte USB en la página 80. Proporciona hasta 5 vatios.

NOTA: La conexión en serie no permite el control de flujo.

Flujo de trabajo del menú de la pantalla táctil

Cada sección se compone de uno o más grupos de páginas, y cada grupo de páginas contiene una o más páginas. La mayoría de las páginas incluyen los botones *Home*, *Enter* y *Next*. Las únicas excepciones son la pantalla de arranque, la página de inicio, las páginas mostradas durante la actualización del firmware y las páginas mostradas momentáneamente para confirmar los resultados de una operación. El botón *Home* permite navegar a la página de inicio. El botón *Enter* permite navegar a la página siguiente del grupo de páginas. Si está en la última página del grupo de páginas, la navegación es a la primera página del grupo de páginas. El botón *Next* permite navegar a la primera página del grupo de páginas. Si está en el último grupo de páginas, la navegación es al primer grupo de páginas.

La línea superior de cada página incluye la etiqueta del sistema sobre un fondo verde, amarillo o rojo que indica la alarma no reconocida de mayor prioridad, junto con un ícono para la indicación adicional del estado de la alarma. Además, la medida de alarma se muestra en amarillo o rojo.

Página de inicio

La página de inicio consta de vínculos a las tres secciones siguientes:

- *System*
- *Devices*
- *Alarms* (se muestra en Funciones del menú de la pantalla táctil en el firmware 6.3.0 en la página 27)

La página de inicio es la única sin botones de navegación *Home*, *Next* y *Enter*.

NOTA: En la Figura 5.5 en la página siguiente, Figura 5.6 en la página siguiente, Figura 5.7 en la página 25 y Figura 5.8 en la página 25, los cuadros con texto negro reflejan el funcionamiento actual del menú de la pantalla táctil en el firmware 6.2.0 y los cuadros con texto rojo reflejan las funciones adicionales en el firmware 6.3.0.

Figura 5.5 Flujo de trabajo del menú de la pantalla táctil

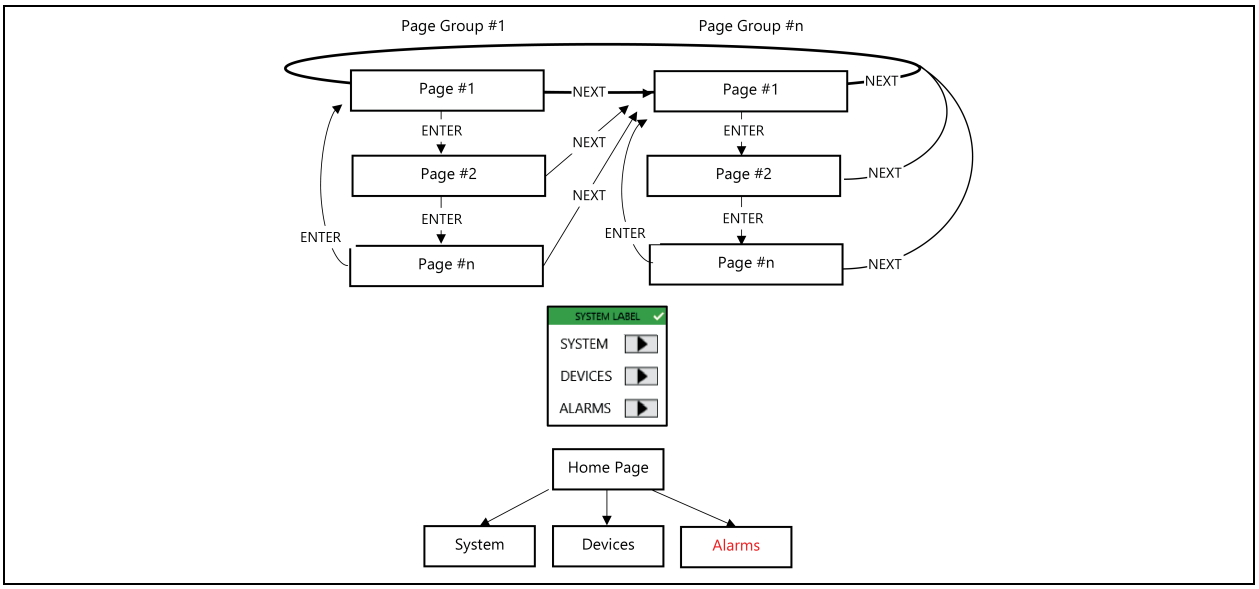


Figura 5.6 Sección de System

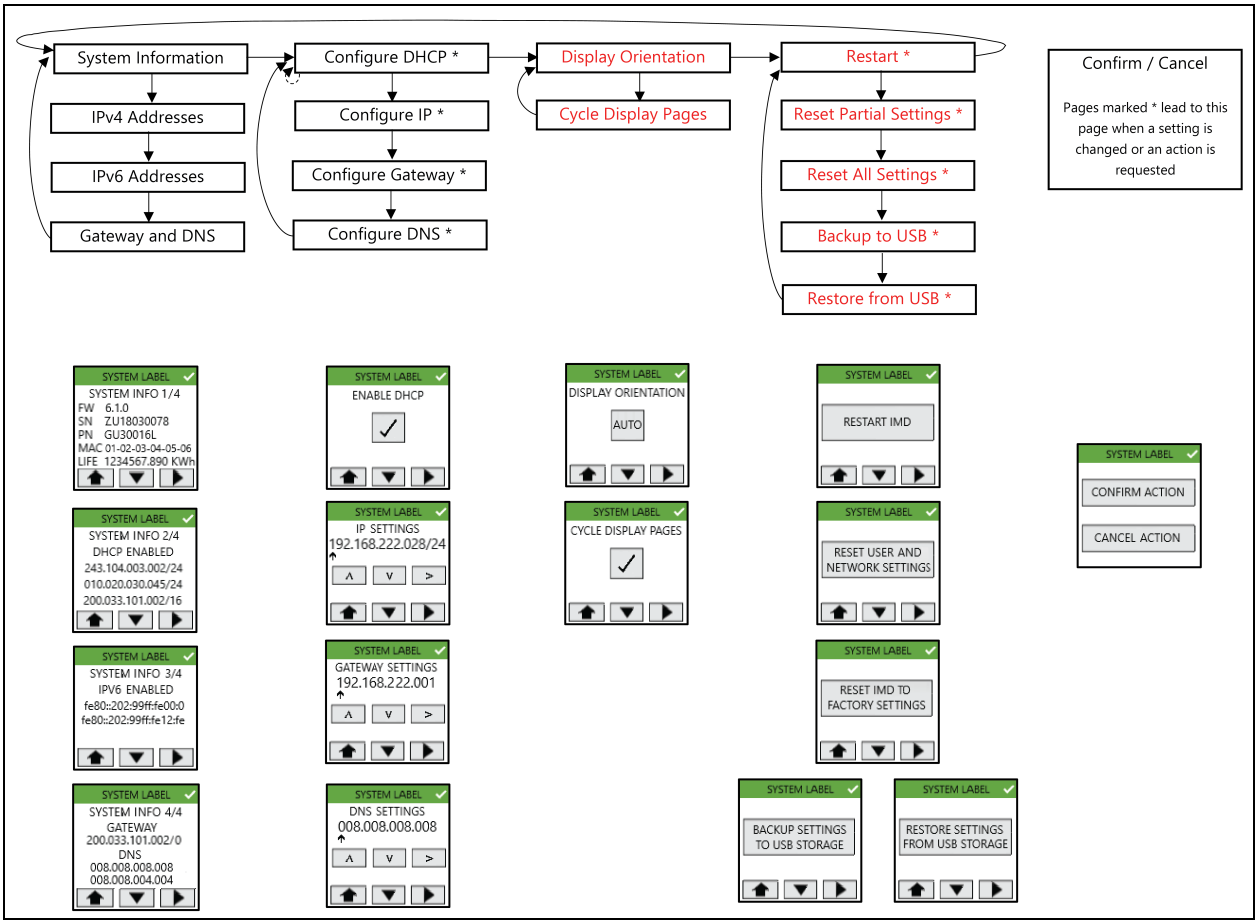


Figura 5.7 Sección de Device

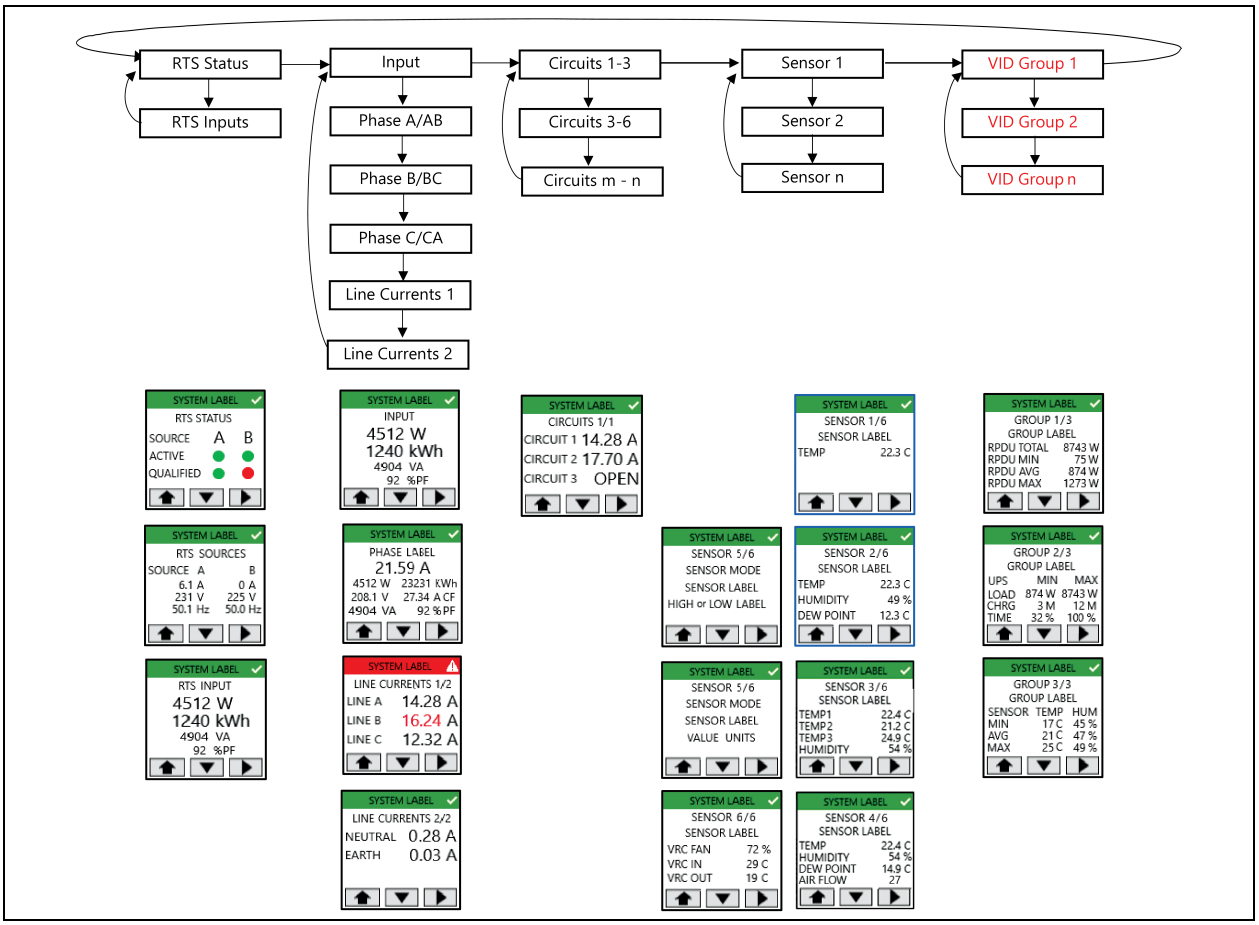
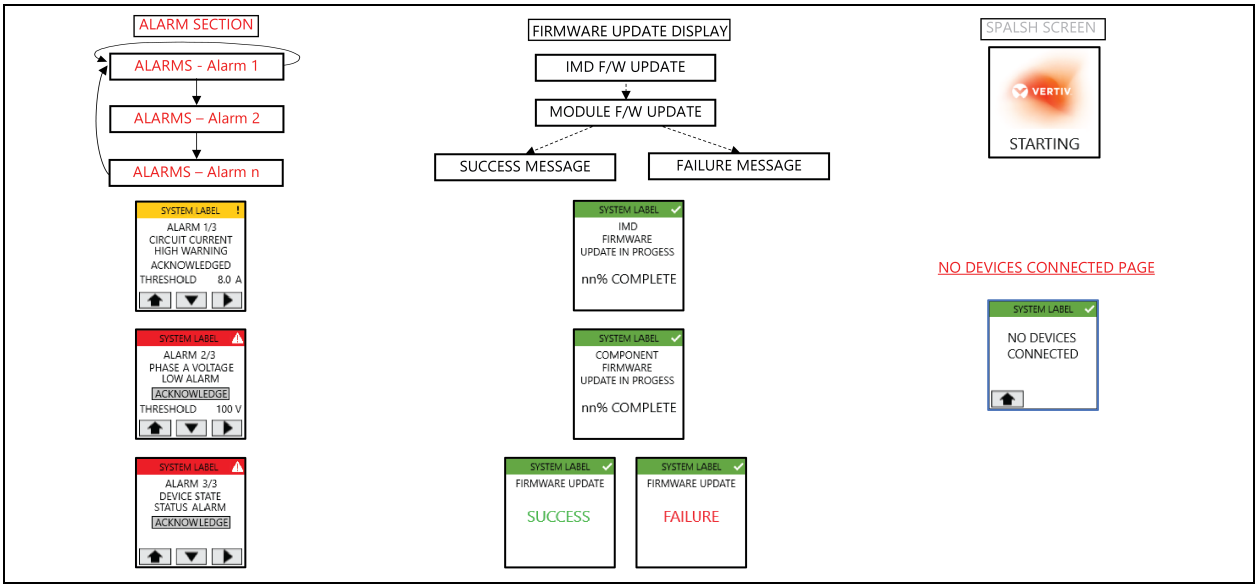


Figura 5.8 Sección de Alarm y Firmware Update Display



Funciones del menú de la pantalla táctil en el firmware 6.2.0

- La página *Splash Screen* se muestra durante la inicialización del IMD.
- La página predeterminada que se muestra tras el encendido o tras un tiempo de inactividad de 60 segundos en el menú de la pantalla táctil, y está determinada por el tipo de dispositivo:
  - RTS: página de estado del RTS
  - Rack PDU: página de entrada
  - RDU202: página del sensor 1
- La retroiluminación de la pantalla reducirá su intensidad tras 75 segundos de inactividad en el menú táctil.
- En la mayoría de los casos, se muestran los nombres. La etiqueta del sistema se desplaza para mostrar la etiqueta completa. Otras etiquetas pueden aparecer truncadas cuando superan los 10 caracteres.
- Cada línea de encabezado de página tendrá un color de fondo verde, ámbar o rojo para indicar el estado de alarma no reconocida de mayor prioridad, y un ícono para indicar los estados de advertencia y alarma.
- El punto de color de la página de salida indica el estado del tomacorriente (verde = encendido, rojo = apagado) con PDU para rack conmutadas de tomacorriente. No se muestra ningún punto cuando la rPDU no es capaz de conmutar tomacorrientes.
- Las páginas de configuración IP solo harán referencia a la configuración IPv4 y la configuración de la dirección IP solo configura la primera dirección IP y la dirección DNS.
- Cuando DHCP está habilitado, las páginas de configuración de dirección IP, puerta de enlace y dirección DNS no se muestran.
- La marca de verificación del botón de la página DHCP aparece/desaparece al presionar el botón para indicar la opción seleccionada.
- La pantalla de actualización de firmware se muestra cuando comienza una actualización de firmware, independientemente de la fuente (interfaz de usuario web, CLI, API, SCP, USB). El porcentaje de progreso de actualización del firmware del componente se calculará como: (placas actualizadas hasta el momento)/(total de placas pendientes de actualización) * 100
- Una vez completadas todas las actualizaciones de firmware, se muestra la página *Firmware Update Success* o *Firmware Update Failure* durante 15 segundos. A continuación, aparecerá la página predeterminada.
- Durante la actualización del firmware, la retroiluminación de la pantalla se ajustará al 100% de intensidad. Una vez completada, la retroiluminación de la pantalla reducirá su intensidad tras 75 segundos de inactividad en el menú de la pantalla táctil.
- Solo se muestran las tres primeras direcciones IPv4 y/o IPv6 en el grupo de páginas de *System Information*.
- Una acción pendiente, como esperar la confirmación de una acción o la confirmación de la dirección IP ingresada, será cancelada por un evento asíncrono, como el tiempo de espera de la pantalla (consulte el punto 2) o la actualización del firmware.
- Al presionar cualquier botón de navegación después de realizar cambios en la configuración de DHCP, dirección IP, puerta de enlace o DNS, se mostrará una página de acción de confirmación/cancelación. Al seleccionar la confirmación se ejecuta el cambio y se vuelve a la página anterior, en la que se muestran los ajustes modificados. Al seleccionar la cancelación se revoca el cambio y se vuelve a la página anterior, en la que se muestran los ajustes sin modificar.

Funciones del menú de la pantalla táctil en el firmware 6.3.0

- Cuando se selecciona la opción *Cycle Display Pages*, la pantalla predeterminada recorrerá las páginas del grupo de páginas del dispositivo y se mostrará cada página durante 5 segundos. Por ejemplo, si se activa *Cycle Display Pages* para una PDU para rack, la pantalla recorrerá las páginas de entrada, fase y corriente de línea.
- Cuando un grupo VID incluye más de un tipo de dispositivo (por ejemplo, PDU para rack y UPS), se mostrará una página de grupo VID para cada tipo de dispositivo dentro del grupo.
- El vínculo *Alarms* de la página de inicio solo se mostrará cuando se haya disparado una alarma.
- Las alarmas pueden confirmarse mediante el botón *Acknowledge*, que cambia al texto Acknowledged cuando se activa.
- La página *Display Orientation* alterna entre Auto, 0 grados, 90 grados, 180 grados y 270 grados al presionar los botones (con el ajuste de 270 grados regresando a Auto). La acción es instantánea al presionar el botón.
- Cuando se selecciona una acción *Restart*, *Reset User/Network*, *Factory Reset*, *Backup* o *Restore*, aparece una página de confirmación/cancelación. Si se confirma, la acción continúa; si se cancela, la pantalla vuelve a la página anterior. Una vez finalizada una acción de *Reset User/Network*, *Factory Reset*, *Backup* o *Restore*, se muestra la página *Action Completed* durante 5 segundos antes de que el menú de la pantalla táctil vuelva a la página predeterminada.
- La página *No Devices Connected* debería sustituir a la página del menú de pantalla táctil de forma predeterminada (o a las páginas del menú de pantalla táctil predeterminada de forma cíclica) cuando no se detecten ramas api/dev en estado normal.
- Al seleccionar una acción de grupo de páginas de utilidades (como *Restart*), se mostrará una página de confirmación/cancelación de la acción. Al seleccionar la confirmación se ejecuta la solicitud, tras lo cual la pantalla vuelve a la página de inicio. Al seleccionar la cancelación se revoca la solicitud y se vuelve a la página anterior.

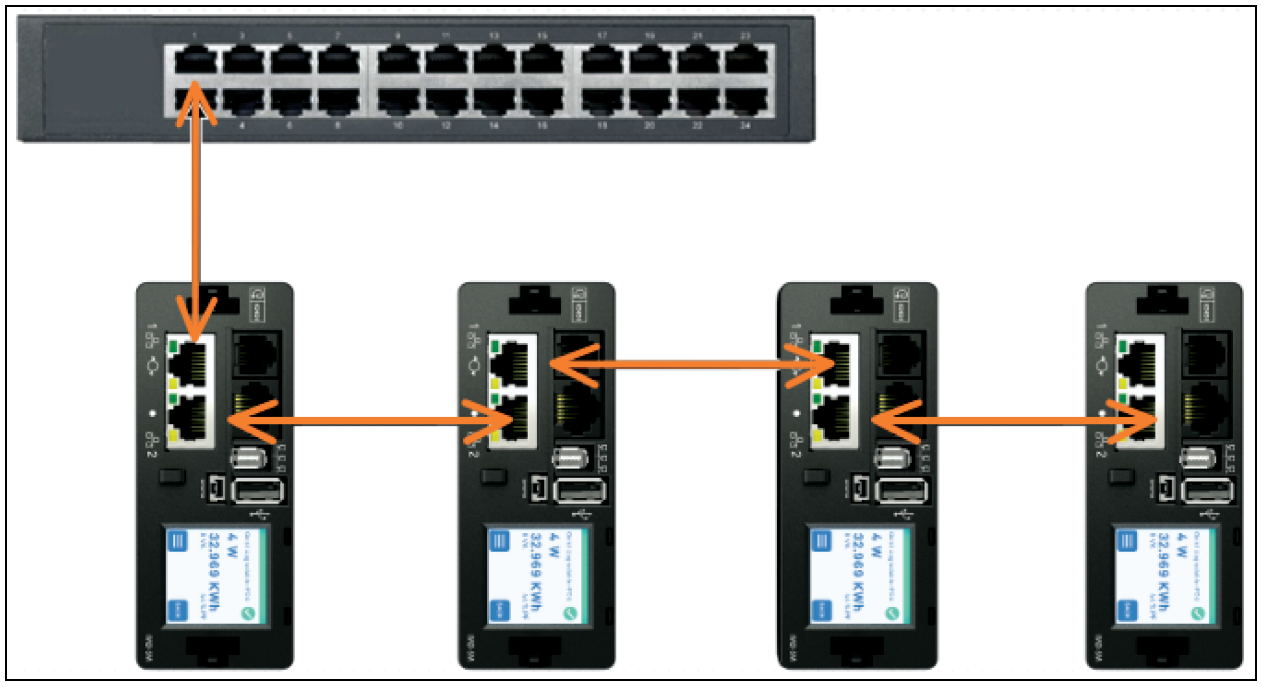
5.2.5 *Rapid Spanning Tree Protocol* (RSTP)

Los dispositivos monitoreados actualizables, que llevan integrados el IMD3 e IMD5, incluyen dos puertos Ethernet que funcionan juntos como un puente Ethernet interno. Uno de estos puertos se puede utilizar para conectar el IMD a una red existente, o ambos puertos se pueden utilizar al mismo tiempo para conectar un IMD a otro en una configuración de conexión en cadena margarita.

Conexión en cadena margarita

- Utilice la conexión en cadena margarita para reducir el número de puertos de conmutación de red.
- Las PDU para rack se conectan mediante una cadena margarita Ethernet.
- La cabeza de la PDU para rack en cadena se conecta a un puerto de conmutación de red.
- Cada PDU para rack tiene su propia dirección IP única.

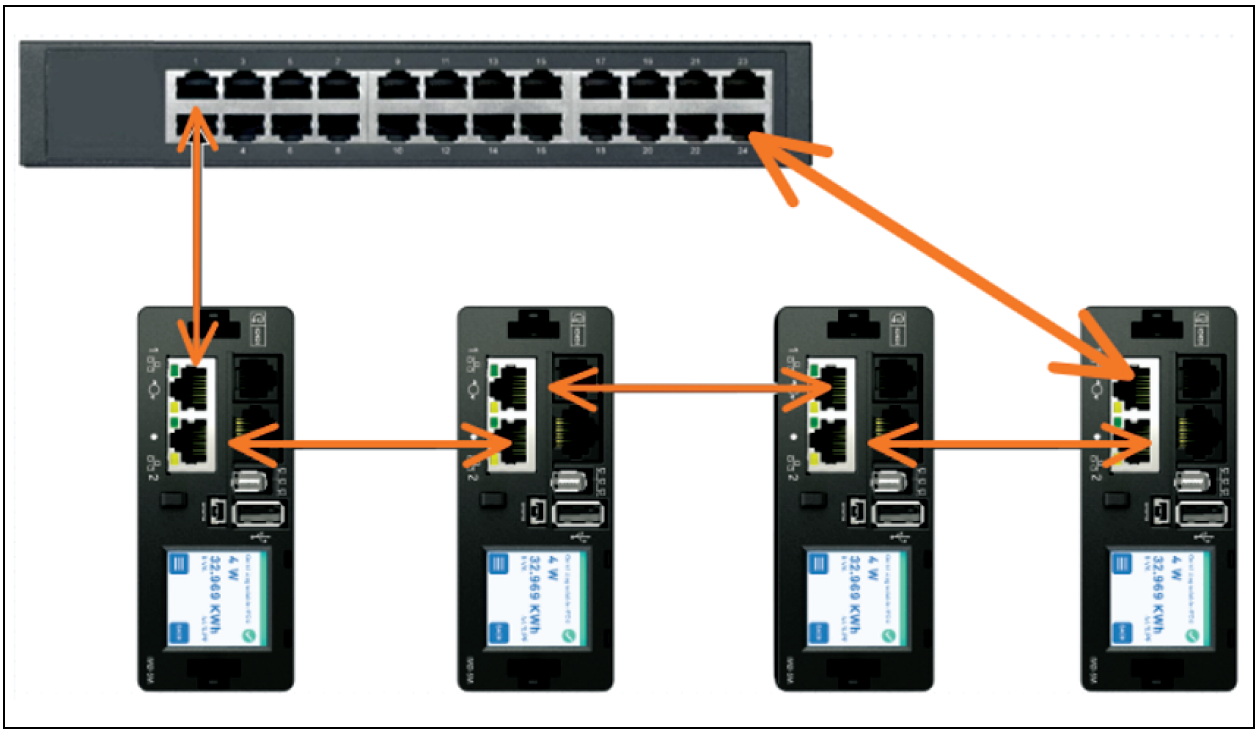
Figura 5.9 Conexión en cadena margarita



Cadena margarita tolerante a errores

- Utilice la conexión de cadena margarita tolerante a errores para proporcionar una conectividad de red resistente.
- Las PDU para rack se conectan mediante una cadena margarita Ethernet.
- Tanto la cabeza como la cola de la PDU para rack en cadena se conectan a puertos de conmutación de red.
- Cada PDU para rack tiene su propia dirección IP única.
- El protocolo Rapid Spanning Tree (RSTP) se debe configurar para gestionar la tolerancia a errores y mantener la conectividad en caso de error de los cables o pérdida de potencia de la PDU para rack.

Figura 5.10 Cadena margarita tolerante a errores



Cuando ambas interfaces de red están conectadas, el IMD implementa un protocolo de puente de red llamado protocolo de árbol de expansión rápido (RSTP). El RSTP es un estándar de IEEE que se aplica en todos los puentes gestionados. Si se utiliza el RSTP, los puentes de la red intercambian información para encontrar rutas o bucles redundantes. Se debe desactivar IPv6 cuando se utiliza conectividad de red redundante.

Cuando se detecta un bucle, los puentes de la red trabajan simultáneamente para deshabilitar de forma temporal las rutas redundantes. Esto permite a la red evitar las tormentas de difusión provocadas por los bucles. Además, el RSTP comprueba periódicamente los cambios en la topología de la red. Cuando se pierde una conexión, el RSTP permite que los puentes cambien rápidamente a una ruta redundante.

NOTA: El protocolo RSTP impone un límite de 40 enlaces entre puentes, incluidos los IMD.

NOTA: Vertiv Intelligence Director no se puede utilizar junto con RSTP y conectividad de red redundante.

5.3 Configuración de red

El IMD actualizable tiene una dirección IP predeterminada para la configuración inicial y el acceso.

Para restaurar la dirección IP predeterminada y restablecer toda la información de la cuenta de usuario:

Para IMD-03X/IMD-3X:

1. Si la dirección o las contraseñas asignadas por el usuario se pierden o se olvidan, mantenga presionado el botón de restablecimiento de la red, situado debajo del puerto Ethernet, durante 15 segundos.

2. Si se mantiene presionado el botón central de la pantalla LED durante 10 segundos, también se restablece la información de la red y de la cuenta del usuario.

Para IMD-5M:

1. Mantenga presionado el botón de reinicio/restablecimiento durante 10 segundos (hasta que el indicador LED parpadee) para reiniciar el IMD. Actúa como una desconexión y conexión de la potencia para el IMD y no cambia ni elimina información del usuario.
2. Si se mantiene presionado el botón durante 25 segundos (hasta que el indicador LED parpadee rápidamente) durante el funcionamiento normal, se restaurará la dirección IP predeterminada y se restablecerán las cuentas de usuario.

La página *Network*, ubicada en la ficha *System*, permite asignar las propiedades de la red manualmente o utilizar DHCP para conectarse a la red. Para acceder a la unidad, es necesario conocer la dirección IP. Se recomienda el uso de una IP estática o un DHCP reservado. La dirección predeterminada se muestra en la parte delantera de la unidad.

- Dirección IP: *192.168.123.123*
- Máscara de subred: *255.255.255.0*
- *Gateway: 192.168.123.1*

Para acceder a la unidad por primera vez, debe cambiar temporalmente la configuración de la red de la computadora para que coincida con la subred 192.168.123. xxx. Para configurar la unidad, conéctela al puerto Ethernet de la computadora y siga las instrucciones adecuadas para el sistema operativo de la computadora.

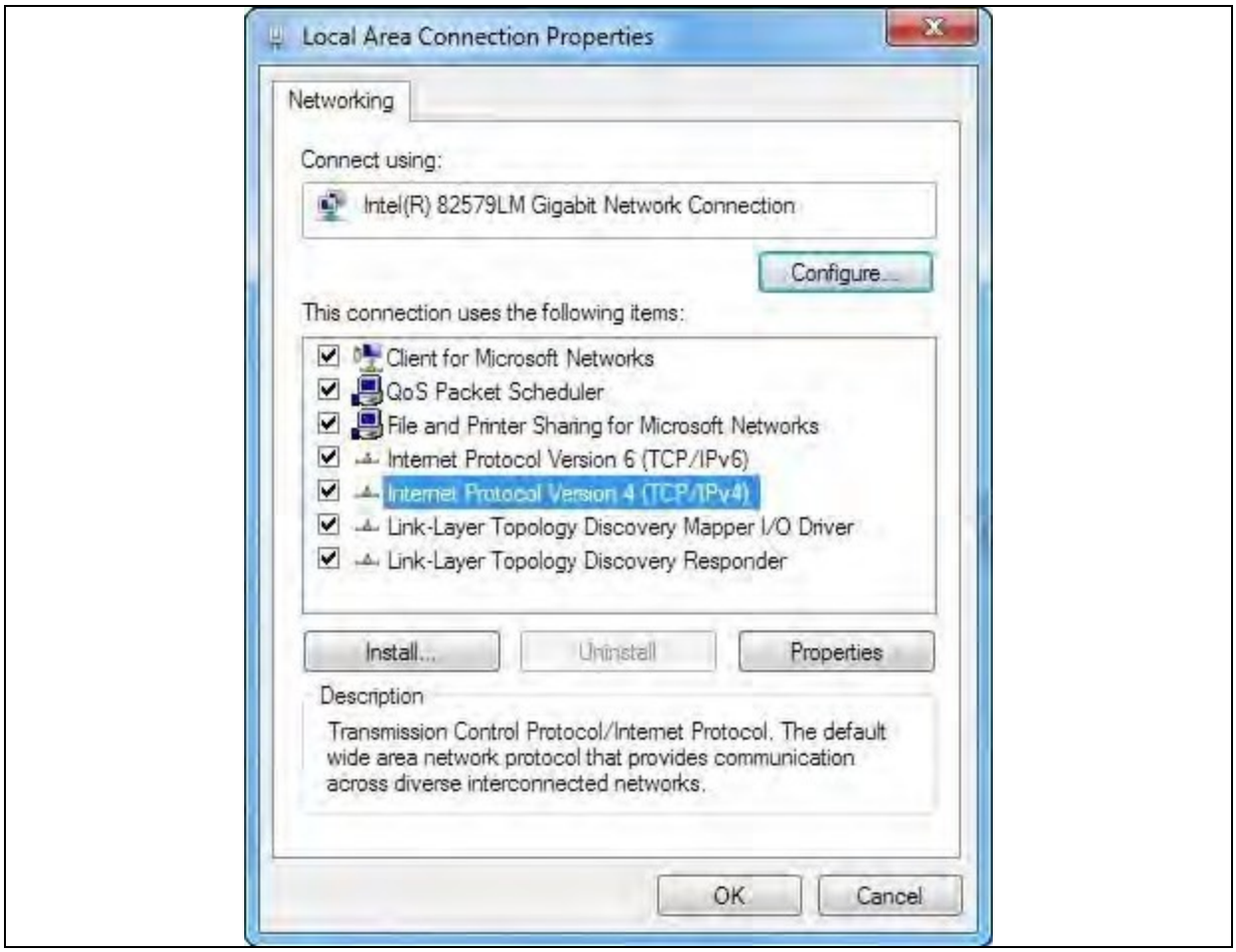
Para configurar la red para un sistema operativo Windows:

1. Acceda a la configuración de red de su sistema operativo.
   - Windows Server 2022 y 2019.
   - En Microsoft Windows 10, haga clic en *Start>Network* y en *Internet>Change Adapter Settings*.
   - En Microsoft Windows 11, haga clic en *Start>Network* y en *Internet>Change Adapter Settings*.
2. Localice la entrada bajo la LAN, Internet de alta velocidad o conexión de área local que corresponda a la tarjeta de red (NIC). Haga doble clic en la entrada del adaptador de red en la lista Conexiones de red.

NOTA: La mayoría de las computadoras tendrán una sola NIC Ethernet instalada, pero también aparecen como NIC en esta lista los adaptadores wifi o de datos móviles. Asegúrese de elegir la entrada correcta.

3. Haga clic en *Properties* para abrir la ventana Local Properties.

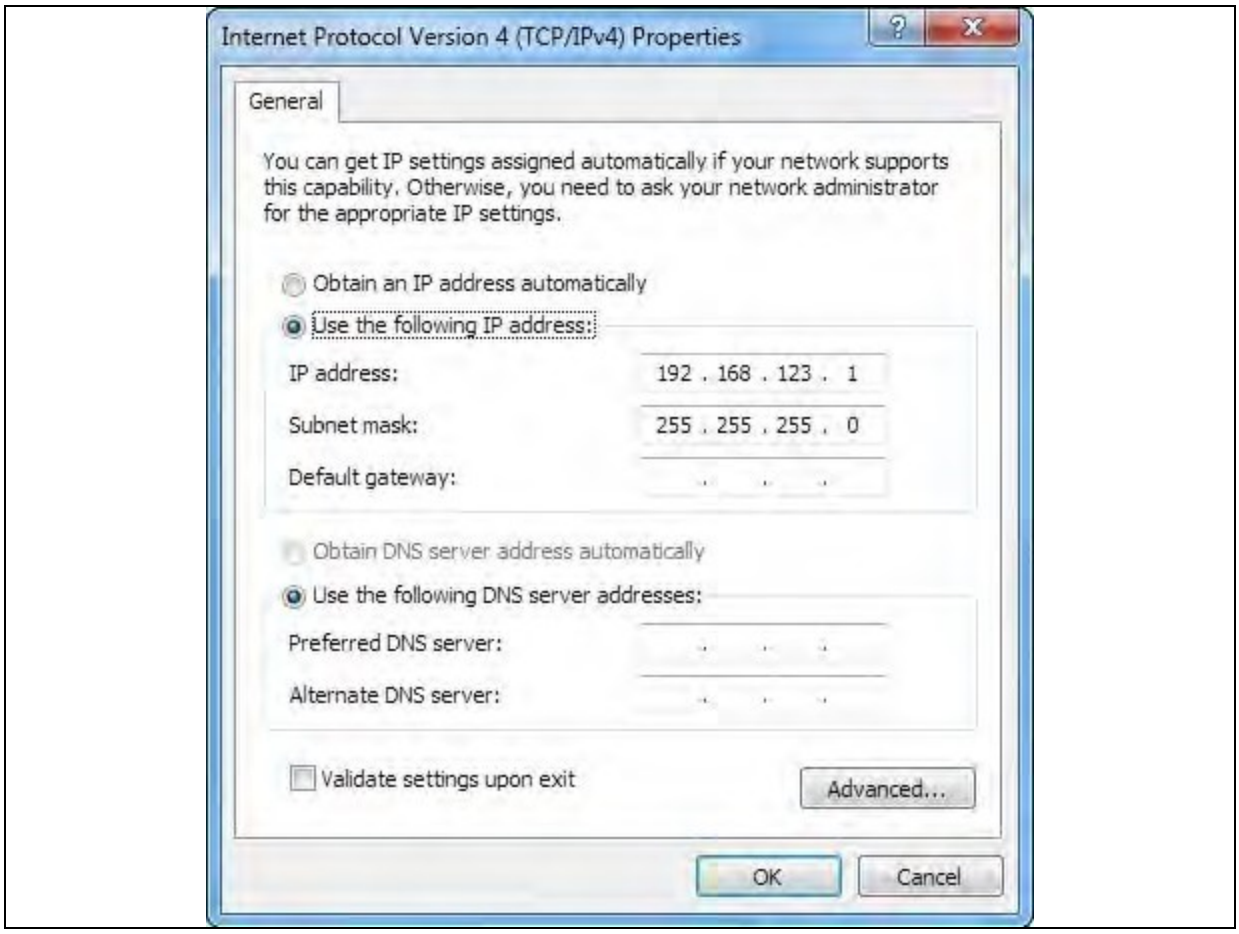
Figura 5.11 Propiedades de conexión de área local



4. En la lista, seleccione *Internet Protocol Version 4 (TCP/IPv4)*, luego haga clic en *Properties*.

NOTA: Si ve más de una entrada TCP/IP, como en el ejemplo anterior, la computadora puede estar configurada para compatibilidad con IPv6, así como con IPv4; asegúrese de seleccionar la entrada para el protocolo IPv4. Anote la configuración actual de la tarjeta NIC para que pueda restaurarla a la normalidad después de haber terminado el procedimiento de configuración.

Figura 5.12 Internet Protocol Version 4



5. Seleccione *Use the following IP address*, establezca **192.168.123.1** en IP address y **255.255.255.0** en Subnet Mask. Para la configuración inicial, las entradas *Default Gateway* y *DNS Server* pueden dejarse en blanco. Seleccione *OK* -*OK* para cerrar las ventanas *Internet Protocol Properties* y *Local Properties*.
6. En un navegador web, ingrese **http://192.168.123.123** para acceder a la unidad. Si es la primera vez que configura la unidad, debe crear una cuenta de tipo *Admin* y una contraseña antes de poder continuar.
7. Una vez creada la cuenta *Admin*, inicie sesión en la unidad.
8. De forma predeterminada, se muestra la página de sensores predeterminados. Desplácese a la pestaña *System* y luego a la página *Network* para configurar las propiedades de la red del dispositivo. La dirección IP de la unidad, la máscara de subred, la puerta de enlace y la configuración del DNS se pueden asignar manualmente o adquirirse a través de DHCP.
9. Haga clic en *Save*.

NOTA: Una vez guardados los cambios, el navegador ya no podrá recargar la página web desde la dirección 192.168.123.123 y muestra el mensaje *Page not Found* o *Host Unavailable*, esto es normal. Cuando termine de configurar la dirección IP de la unidad, repita los pasos anteriores cambiando la configuración de la tarjeta NIC Ethernet de la computadora a la que anotó antes de cambiarla.

Para configurar la red para una Mac:

1. Haga clic en el ícono *Preferencias del sistema* en el *Dock* y elija *Network*.

Figura 5.13 *Preferencias del sistema* de MAC

2. Asegúrese de que esté resaltado Ethernet en el lado izquierdo de la ventana NIC. En la mayoría de los casos, habrá una entrada Ethernet en una Mac. Anote la configuración actual para que pueda restaurarla a la normalidad después de haber terminado el procedimiento de configuración.
3. Seleccione *Manually* en la lista desplegable *Configure Ipv4* y establezca **192.168.123.1** en *IP address* y **255.255.255.0** en *Subnet Mask*, y haga clic en *Apply*.

NOTA: Los ajustes del router y del servidor DNS se pueden dejar en blanco para esta configuración inicial. En un navegador web, ingrese http://192.168.123.123 para acceder a la unidad. Si es la primera vez que configura la unidad, debe crear una cuenta de tipo *Admin* y una contraseña antes de poder continuar.

4. Una vez creada la cuenta *Admin*, inicie sesión en la unidad.
5. De forma predeterminada, se muestra la página de sensores predeterminados. Desplácese a la pestaña *System* y luego a la página *Network* para configurar las propiedades de la red del dispositivo. La dirección IP de la unidad, la máscara de subred, la puerta de enlace y la configuración del DNS se pueden asignar manualmente o adquirirse a través de DHCP.
6. Haga clic en *Save*.

NOTA: Una vez guardados los cambios, el navegador ya no podrá recargar la página web desde la dirección 192.168.123.123 y muestra el mensaje *Page not Found* o *Host Unavailable*, esto es normal. Cuando termine de configurar la dirección IP de la unidad, repita los pasos anteriores cambiando la configuración de la tarjeta NIC Ethernet de la computadora a la que anotó antes de cambiarla.

5.4 Interfaz del usuario web

Se puede acceder a la unidad a través de una conexión HTTP estándar no cifrada, así como mediante una conexión HTTPS (TLS) cifrada. Las unidades se redirigirán de forma predeterminada de HTTP a HTTPS, a menos que el administrador habilite HTTP explícitamente.

NOTA: Cuando se accede al dispositivo por primera vez, se debe crear una cuenta de administrador (nombre de usuario y contraseña).

NOTA: Si aparece el mensaje Clock not set en la parte superior de la página, siga el procedimiento indicado en Time en la página 79.

5.4.1 Menú principal

El menú principal está situado verticalmente en el extremo izquierdo. Vea la Figura 5.14 en la página opuesta para ver el menú principal.

¡ADVERTENCIA! No conecte radiadores eléctricos, aparatos de calefacción eléctricos o cualquier otro aparato eléctrico que puedan provocar incendios, descargas eléctricas o lesiones cuando funcionan sin monitoreo.

Figura 5.14 Menú principal

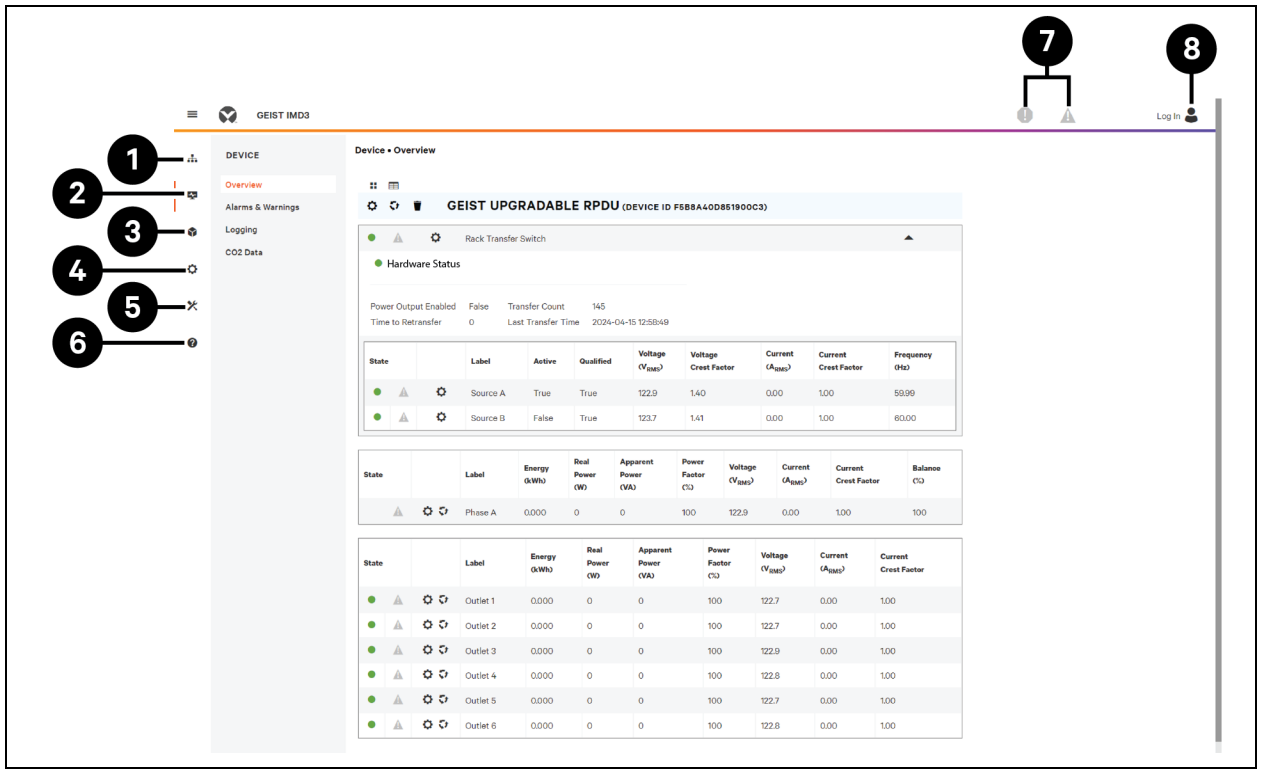


Tabla 5.5 Descripciones del menú principal

Elemento	Descripción
1	*Aggregation*
2	*Device*
3	*Provisioner*
4	*System*
5	*Utilities*
6	*Help*
7	*Alarms & Warnings*
8	*Log In/Log Out*

5.5 Submenú *Device*

Haga clic en el submenú *Device* para acceder a los menús *Overview, Alarms & Warnings, Logging* y *CO2 Data*.

5.5.1 Página *Overview*

Debe iniciar sesión antes de realizar cualquier cambio. Solo los usuarios con autorizaciones de nivel de control o superiores tienen acceso a esta configuración.

Figura 5.15 Descripciones del submenú *Device Overview*

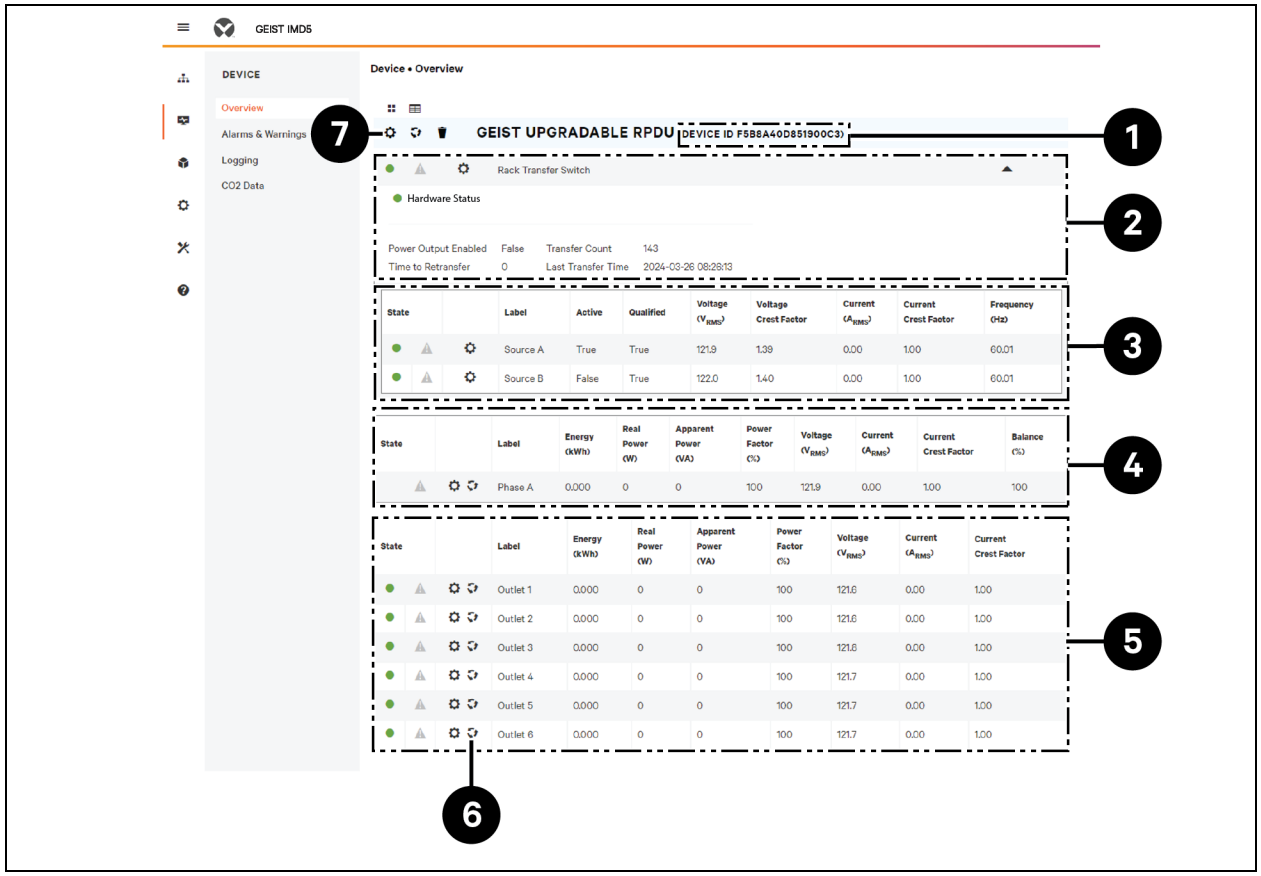


Tabla 5.6 Descripciones del submenú *Device Overview*

Número	Nombre	Descripción
1	*Device ID*	La identificación del producto es única y no se puede modificar. Puede ser necesario para recibir asistencia técnica.
2	*Hardware Status*	Muestra información sobre la potencia de salida habilitada, el recuento de transferencias, el tiempo para la retransferencia y la hora de la última transferencia.
3	*Rack Transfer Switch* *Power sources A and B*	Muestra el estado de ambas fuentes de alimentación, incluida la fuente activa (TRUE INDICA ACTIVA) y las estadísticas de cada fuente: *Qualified* (TRUE indica que la fuente está calificada), *Voltage*, *Voltage Crest Factor*, *Current Crest Factor* y *Frequency*.
4	*Total and Individual Phase Monitor*	Muestra las estadísticas de corriente alterna, voltaje y potencia de cada fase individual y del total de todas las fases combinadas. También se indican el factor de cresta de corriente y el equilibrio de fase (%).
5	*Outlet Monitor*	Se aplica SOLO a las unidades de RTS de monitoreo de tomacorrientes/tomacorrientes

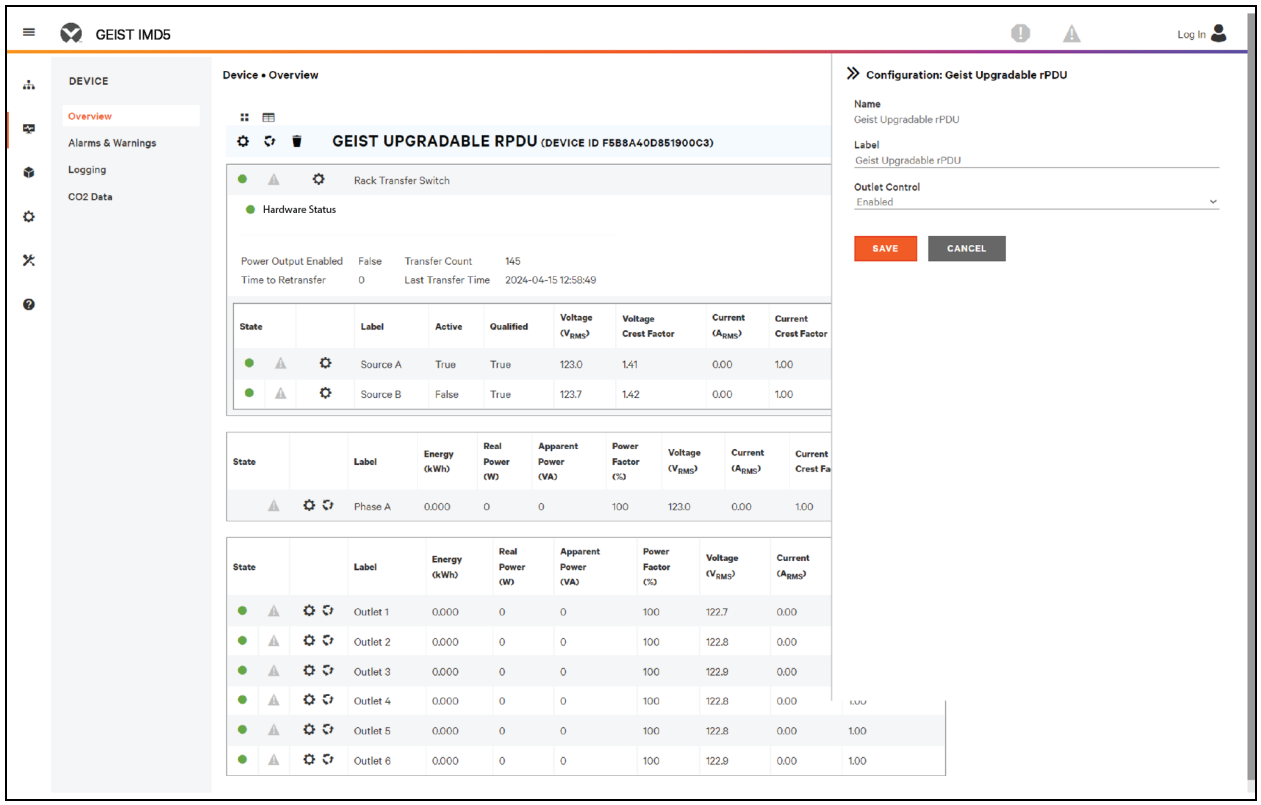
Tabla 5.6 Descripciones del submenú *Device Overview*

Número	Nombre	Descripción
		conmutados. Muestra las estadísticas de corriente alterna, voltaje y potencia de cada circuito y tomacorriente. También se indica el factor de cresta de corriente. (Solo monitoreo de potencia a nivel de tomacorrientes y monitoreo a nivel de tomacorrientes conmutados). Muestra el estado del tomacorriente (solo monitoreo de potencia a nivel de tomacorrientes y monitoreo a nivel de tomacorrientes conmutados).
6	Ícono *Operation*	Se aplica SOLO a las unidades de RTS de monitoreo de tomacorrientes/tomacorrientes conmutados: modificación de ajustes.
7	Ícono *Configuration*	Se aplica SOLO a las unidades de RTS de monitoreo de tomacorrientes/tomacorrientes conmutados: modificación del nombre de la etiqueta.

Para cambiar la etiqueta de un dispositivo:

1. Haga clic en el ícono *Configuration* para cambiar la etiqueta del RTS Vertiv™ Geist™, y cambie la etiqueta. El valor bajo *Name* es el nombre de fábrica o modelo de la unidad del RTS y no se puede cambiar.
2. Haga clic en *SAVE*.

Figura 5.16 Cambio de la etiqueta de un dispositivo



Para cambiar la operación del dispositivo:

1. Haga clic en el ícono *Operation*  .
2. Seleccione la operación que desea realizar:
   - On/Off: activa o desactiva todos los tomacorrientes.
   - Reboot: para los tomacorrientes que están activados, esta opción inicia un clico de desactivación/activación después del retardo de espera de reinicio. Los tomacorrientes que estén desactivados se activan tras el reinicio.
   - Cancel: cancela la operación en curso, si no se ha completado.
   - Reset Energy: restablece la energía total medida en kWh.
   - Restore Defaults: restablece la configuración del dispositivo a sus valores predeterminados de fábrica. Esto incluye las etiquetas, los retardos y las acciones de encendido del dispositivo.

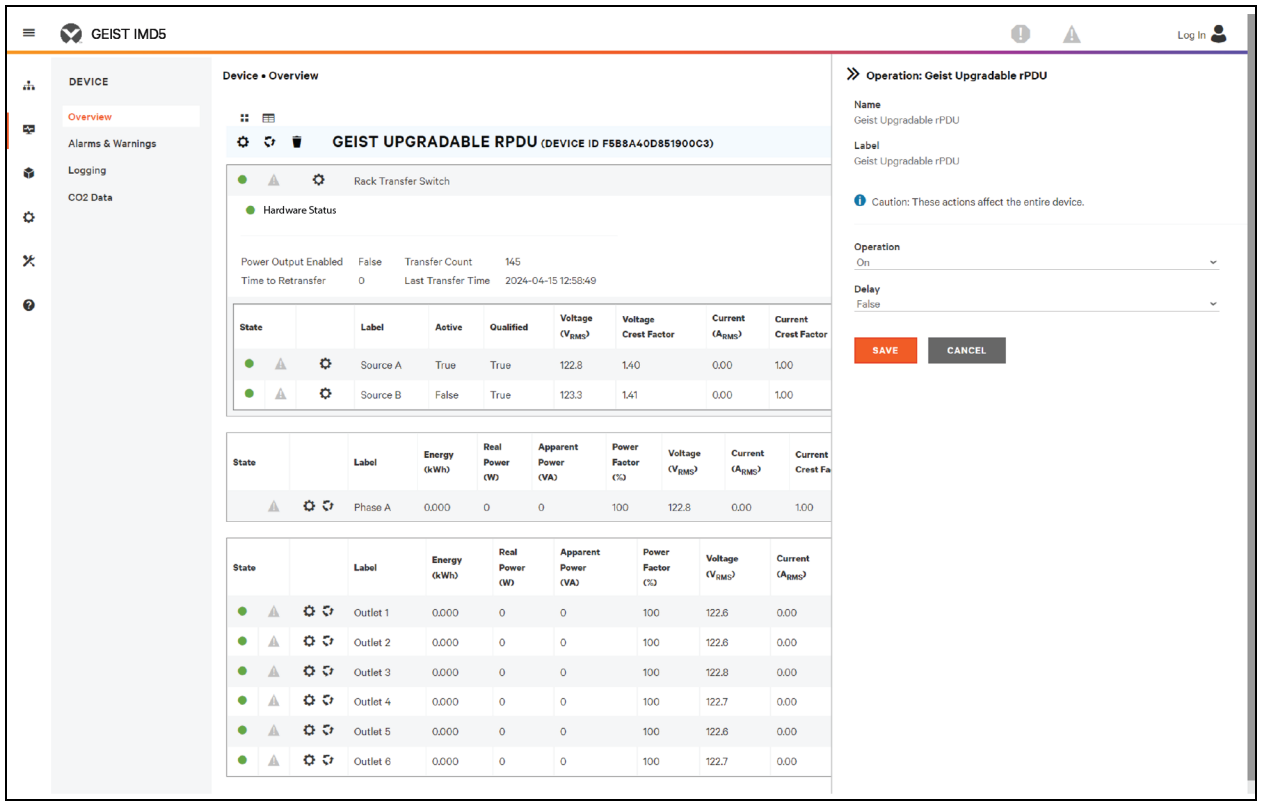
NOTA: Estas acciones afectan al dispositivo en su totalidad.

NOTA: Las operaciones de activación/desactivación y reinicio solo se aplican a la unidad de RTS Geist™ de tomacorrientes conmutados.

3. Para las operaciones relacionadas con el estado de los tomacorrientes, cuando se configura *Delay* como *True*, al realizar la operación seleccionada, se utiliza la configuración de retardo actual para cada tomacorriente.
4. Haga clic en *SAVE* para iniciar la acción.

NOTA: Los retardos en la acción de encendido están relacionados con el tiempo transcurrido desde que se enchufó la unidad, no con el tiempo transcurrido desde que se completó el arranque. Se pueden ejecutar antes de que la unidad se arranque por completo.

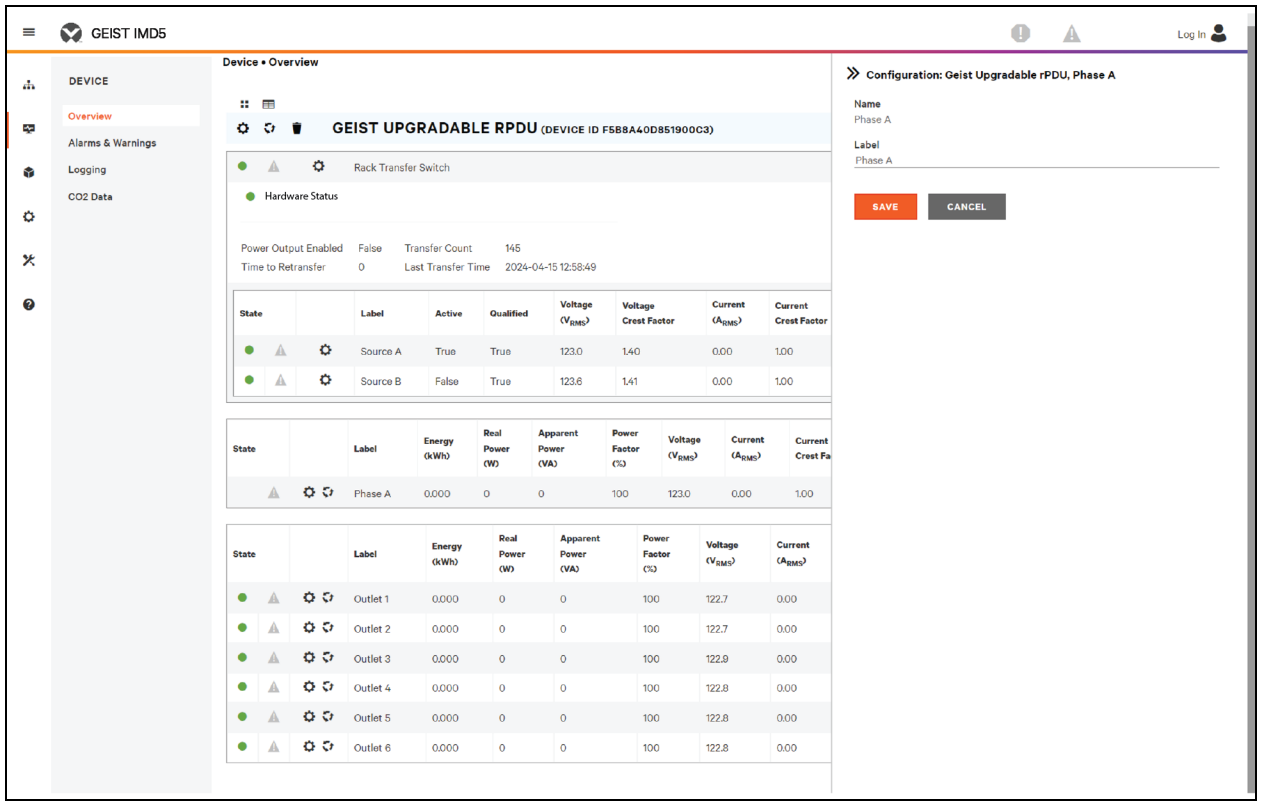
Figura 5.17 Operación de cambio de dispositivo



Para cambiar una etiqueta de fase o circuito:

1. Haga clic en el ícono *Configuration* de la fase o el circuito, y cambie la etiqueta. El valor bajo *Name* es la fase física o el nombre del circuito y no se puede cambiar.
2. Haga clic en *SAVE*.

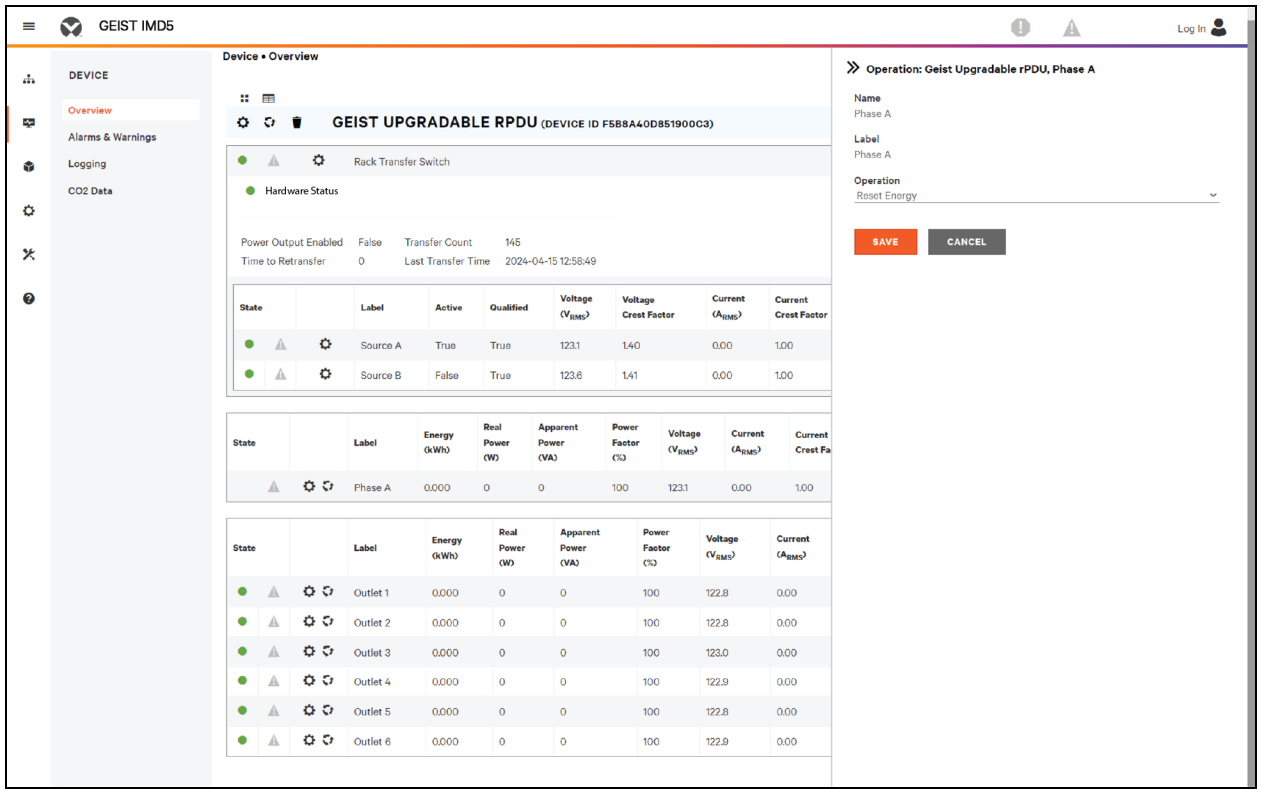
Figura 5.18 Cambio de etiqueta de fase o circuito



Para cambiar la operación de la fase:

1. Haga clic en el ícono *Operation* .
2. Seleccione *Reset Energy*, para restablecer la energía total medida en kWh para la fase seleccionada.
3. Haga clic en *SAVE* para iniciar la acción.

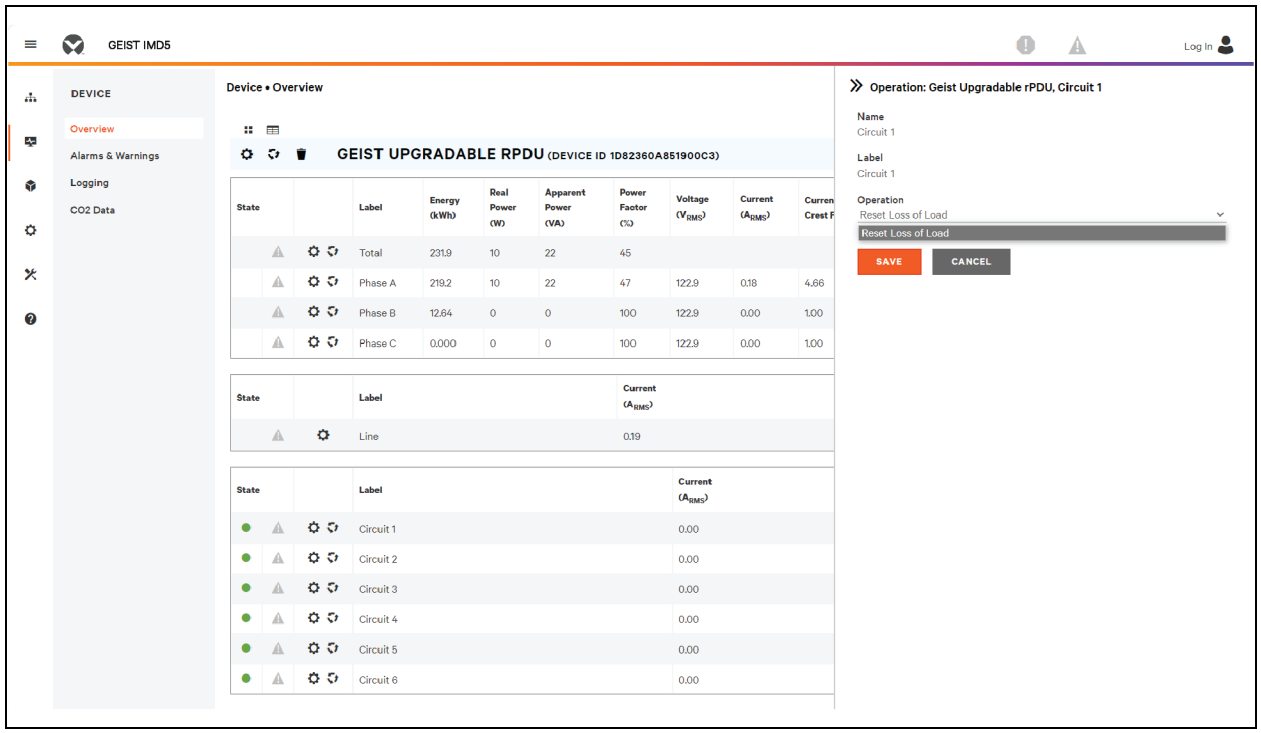
Figura 5.19 Cambio de la operación de la fase



Para cambiar la operación del circuito:

1. Haga clic en el ícono *Operation* .
2. Seleccione *Reset Loss of Load* para restablecer la alarma de pérdida de carga.
3. Haga clic en *SAVE* para iniciar la acción.

Figura 5.20 Cambio de la operación del circuito



NOTA: Este paso se requiere cuando *State* muestra una alarma de pérdida de carga y el problema se resolvió. La alarma de pérdida de carga se activa por una caída repentina de la corriente detectada por el transductor de medición de corriente del disyuntor cuando funciona cerca del límite de carga del circuito. Para las unidades horizontales actualizables conmutadas, la alarma de pérdida de carga se activa además por la pérdida de voltaje del disyuntor (independientemente de la carga del circuito).

Para configurar un tomacorriente:

NOTA: Se aplica únicamente a las unidades de RTS Vertiv™ Geist™ de monitoreo de tomacorrientes/tomacorrientes conmutados.

1. Haga clic en el ícono *Outlet Configuration* .
2. Cambie la configuración, según sea necesario.
   a. Etiqueta del tomacorriente.

NOTA: Los pasos 2b a 2k se aplican solo a tomacorrientes conmutados.

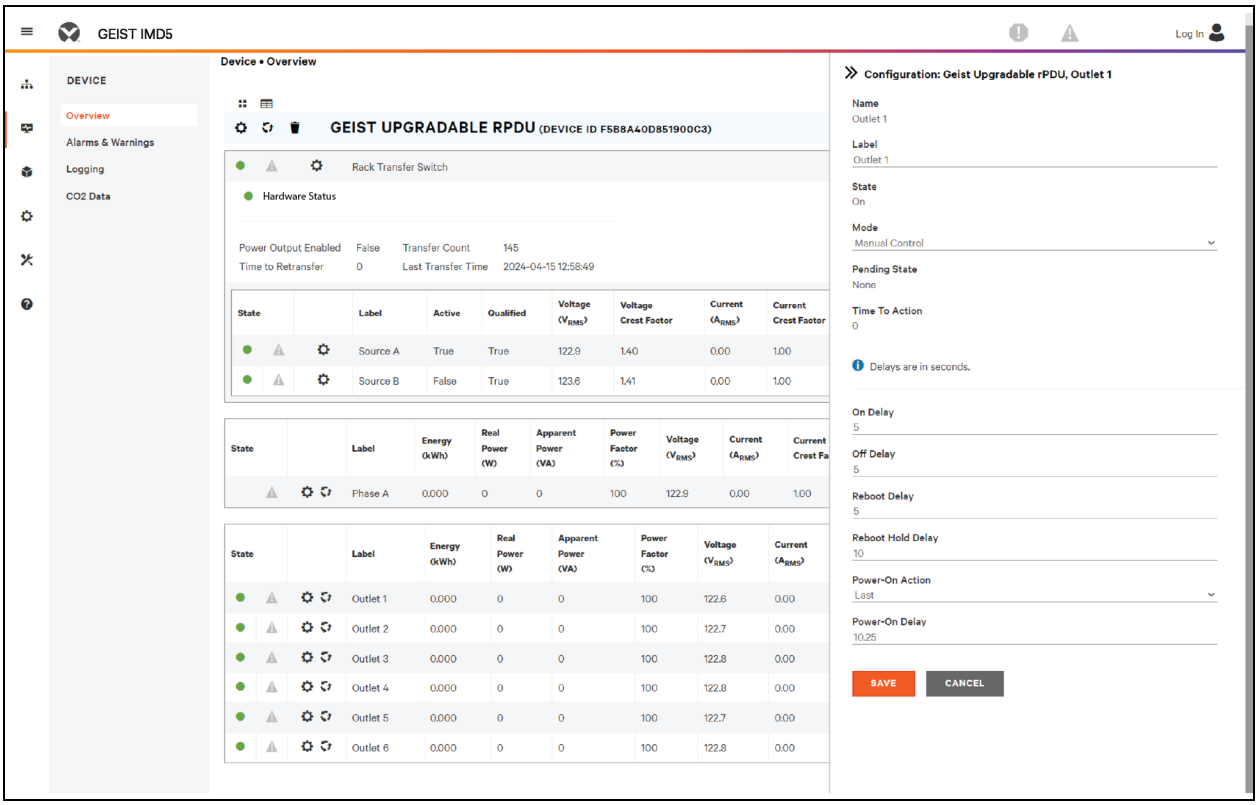
   b. **State:** el estado actual del tomacorriente (*On/Off*).
   c. **Mode:** modo en que se controlará el tomacorriente:
      - **Manual Control:** el estado del tomacorriente se controla mediante la interfaz del usuario de web, SNMP o la API.
      - **Alarm Control (normalmente en *Off*, se activa cuando se dispara una alarma relacionada):** el estado del tomacorriente está normalmente en *Off*, y se activa cuando se dispara cualquier evento de alarma del tomacorriente.

- **Alarm Control (normalmente en *On*, se desactiva cuando se dispara una alarma relacionada):** el estado del tomacorriente está normalmente en *On*, y se desactiva cuando se dispara cualquier evento de alarma del tomacorriente.
- **Alarm Control (normalmente en *Off*, se activa cuando se disparan todas las alarmas relacionadas):** el estado del tomacorriente está normalmente en *Off*, y se activa cuando se disparan todos los eventos de alarma del tomacorriente.
- **Alarm Control (normalmente *On*, se desactiva cuando se disparan todas las alarmas relacionadas):** el estado del tomacorriente está normalmente en *On*, y se desactiva cuando se disparan todos los eventos de alarma del tomacorriente.

d. **Pending State:** estado al que el tomacorriente está pasando.
e. **Time To Action:** el tiempo que falta para que se produzca la acción pendiente. Esto se ajusta con las funciones de *Delay*.
f. **On Delay:** el tiempo, en segundos, que la unidad espera antes de activar un tomacorriente.
g. **Off Delay:** el tiempo, en segundos, que la unidad espera antes de desactivar una tomacorriente.
h. **Reboot Delay:** el tiempo, en segundos, que la unidad espera antes de reiniciar una tomacorriente.
i. **Reboot Hold Delay:** el tiempo, en segundos, que la unidad espera después de apagar el tomacorriente antes de volver a encenderlo durante un reinicio.
j. **Power-On Action:** describe el estado en que se iniciará el tomacorriente cuando se encienda (*On*, *Off* o *Last*).
k. **Power-On Delay:** el tiempo, en segundos, que la unidad espera después del encendido antes de activar un tomacorriente.

3. Haga clic en *SAVE*.

Figura 5.21 Configuración de tomacorrientes

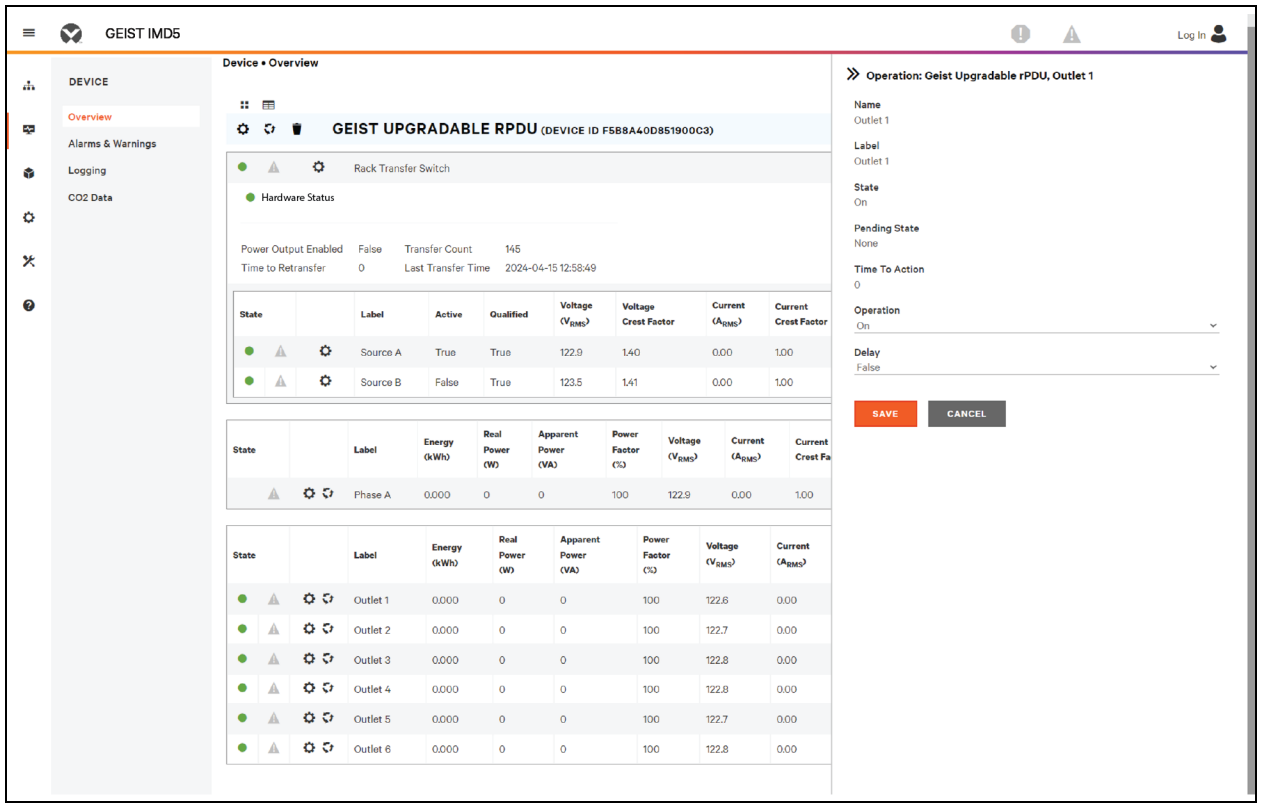


Para cambiar la operación del tomacorriente:

NOTA: Se aplica únicamente a las unidades de RTS Vertiv™ Geist™ de monitoreo de tomacorrientes/tomacorrientes conmutados.

1. Haga clic en el ícono *Outlet Operation* .
2. Seleccione la operación que desea realizar:
   - On/Off: activa o desactiva el tomacorriente seleccionado.
   - Reboot: para los tomacorrientes que están activados, esta opción los desactiva y luego los vuelve a activar después del retardo de espera de reinicio. Los tomacorrientes que estén desactivados se activan tras el reinicio.
   - Cancel: cancela la operación en curso, si no se ha completado.
   - Reset Energy: restablece la energía total medida en kWh para el tomacorriente seleccionado.
3. Para las operaciones relacionadas con el estado de los tomacorrientes, cuando se configura *Delay* como *True*, al realizar la operación seleccionada, se utiliza la configuración de retardo actual para cada tomacorriente.
4. Seleccione *SAVE* para iniciar la acción.

Figura 5.22 Cambio de la operación del tomacorriente



5.5.2 Página *Alarms & Warnings*

La página *Alarms & Warnings* permite establecer condiciones de alarma o de advertencia (eventos) para cada lectura de potencia y de circuito. Los eventos se disparan cuando una medición supera un umbral definido por el usuario, ya sea porque asciende por encima del umbral (activación por valor alto) o cae por debajo de él (activación por valor bajo). Los eventos se muestran en diferentes secciones, según el dispositivo o la medición a la que se asocia. Cada evento, frente a su ocurrencia, puede implicar llevar a cabo una o más acciones.

Figura 5.23 Página *Alarms & Warnings*

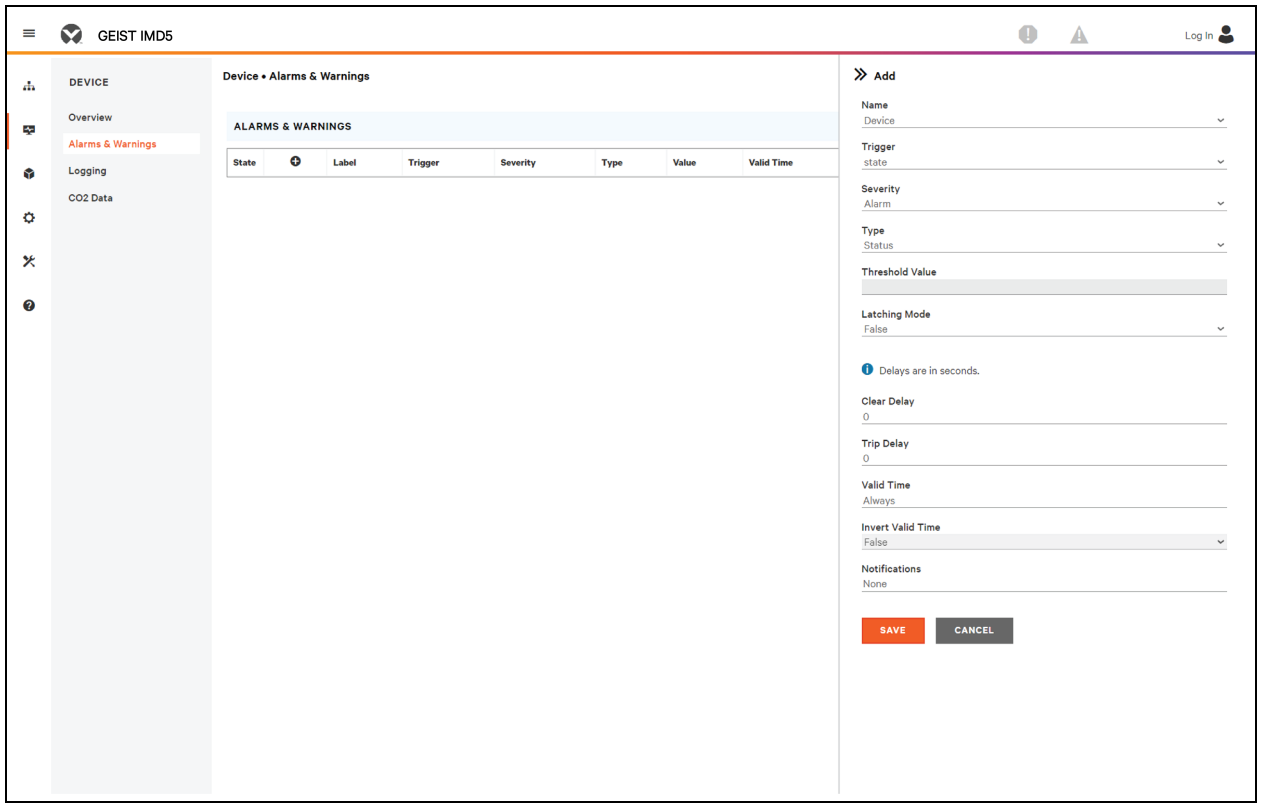


Tabla 5.7 Descripciones de *Alarms & Warnings*

Número	Descripción	Símbolo	Descripción
1	Estado de cada evento.		Símbolo de advertencia. El evento se muestra en naranja.
			Símbolo de alarma. La alarma se muestra en rojo.
			Símbolo de evento confirmado. El símbolo permanece hasta que la condición medida vuelve a la normalidad.
2	Agregar/eliminar/modificar alarmas y advertencias.		Agregar nuevas alarmas y advertencias.
			Modificar alarmas y advertencias existentes.
			Eliminar alarmas y advertencias existentes.

Tabla 5.7 Descripciones de *Alarms & Warnings*

Número	Descripción	Símbolo	Descripción
3	Notificar al usuario de los Eventos disparados y solicita reconocimiento.	N/A	Vacío, si no hay una condición de alerta.
		✔	Cuando se produce un evento de advertencia o alarma, puede hacer clic en este símbolo para confirmar el evento e impedir que la unidad envíe más notificaciones. **NOTA: Al hacer clic en este símbolo, no se borra el evento de advertencia o alarma; solo se evita que se repitan las notificaciones.**
4	Muestra las condiciones de la configuración de alarmas y advertencias.		

Para agregar un nuevo evento de alarma o advertencia:

1. Haga clic en el botón *Add/Modify Alarms* y *Warnings*.
2. Establezca las condiciones para este evento de la siguiente manera:
   a. En las listas desplegables, seleccione el nombre de la fase o circuito, la medición de activación, la gravedad y el tipo.

NOTA: Se dispara por valor alto si la medición supera el umbral y se dispara por valor bajo si la medición desciende por debajo del umbral.

   b. Introduzca el valor de umbral deseado en *Threshold Value* (cualquier número entre -999,0 y 999,0).
   c. En *Clear Delay*, introduzca el tiempo de retardo de borrado deseado en segundos. Cualquier valor distinto de *0* significa que una vez que este evento se active, la medición debe volver a la normalidad durante este número de segundos antes de que el evento se borre y se restablezca. El valor ingresado en *Clear Delay* puede ser de hasta 14.400 segundos (4 horas).
   d. Introduzca en *Trip Delay* el tiempo deseado para el retardo de activación en segundos. Cualquier valor distinto de *0* significa que la medición debe superar el umbral durante este número de segundos antes de que el evento se active. El valor ingresado en *Trip Delay* puede ser de hasta 14.400 segundos (4 horas).
   e. *Latching Mode*: si está habilitado, este evento y sus acciones asociadas permanecen activos hasta que se reconozca el evento, incluso si la medición vuelve posteriormente a la normalidad.
   f. Para especificar dónde se envían las notificaciones de alerta cuando se produce este evento de alarma o advertencia, haga clic en el ícono *Add* para crear una nueva acción.
   g. Seleccione una de las opciones que desee en el menú desplegable:
      - *Target* es la dirección de correo electrónico o el administrador de SNMP donde se envían las notificaciones cuando se dispara el evento. Para obtener más información sobre cómo configurar una dirección de correo electrónico de destino, consulte Email en la página 81.

- O bien, cuando se selecciona un número de tomacorriente como *Target*, el estado del tomacorriente cambia cuando se activa un evento y permanece en ese estado hasta que el evento se restablece o se reconoce. En el caso de esta opción, en *Alarm Control* se debe haber configurado el modo *Outlet*, consulte Página Alarms & Warnings en la página 45.

NOTA: Los valores de los retardos y repeticiones objetivo se comparten en todas las alarmas. Si se necesitan varios valores de retardo o repetición para objetivos específicos, cada uno de ellos se debe agregar a la lista de objetivos y luego se debe marcar la casilla correspondiente *Enabled* en cada alarma.

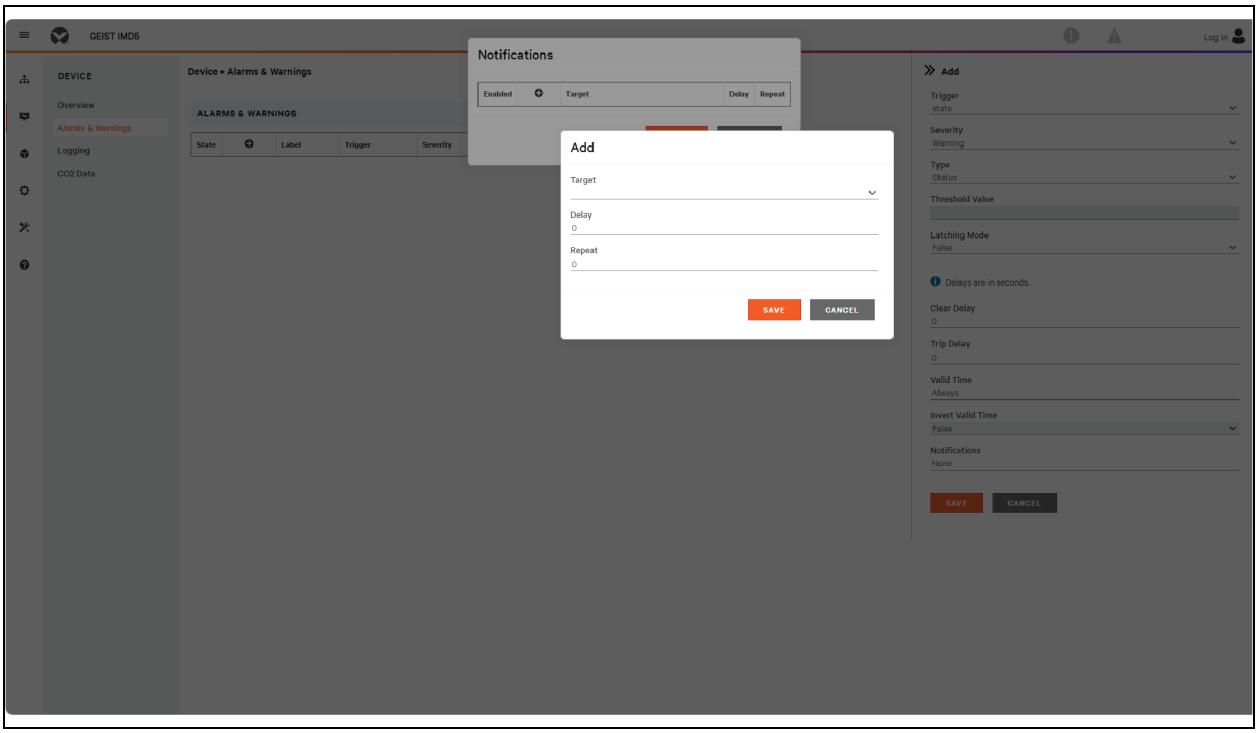
NOTA: Se aplica únicamente a las unidades de RTS Vertiv™ Geist™ de monitoreo de tomacorrientes/tomacorrientes conmutados.

- *Delay* determina el tiempo durante el que este evento debe permanecer activado antes de que se envíe la primera notificación de esta acción. Este valor es distinto del valor de *Trip Delay* anterior. *Trip Delay* determina el tiempo durante el que se debe superar el valor umbral antes de que se active el evento en sí. Este retardo determina el tiempo durante el que el evento debe permanecer activado antes de que tenga lugar esta acción. Este valor puede ser de hasta 14.400 segundos (4 horas). Un valor de *0* enviará la notificación inmediatamente.
- *Repeat* determina si se enviarán varias notificaciones para esta acción. Las notificaciones repetidas se envían en los intervalos especificados hasta que el evento se confirme o se borre y se restablezca. Este valor puede ser de hasta 14.400 segundos (4 horas). Un valor de *0* deshabilita esta característica y solo se envía una notificación.

3. Haga clic en *SAVE* para guardar esta acción de notificación.

NOTA: Se puede configurar más de una acción para una alarma o advertencia. Para agregar varias acciones, solo hay que hacer clic de nuevo en el ícono *Add* y establecer cada una como se desee. Cada alerta puede tener hasta 32 acciones asociadas.

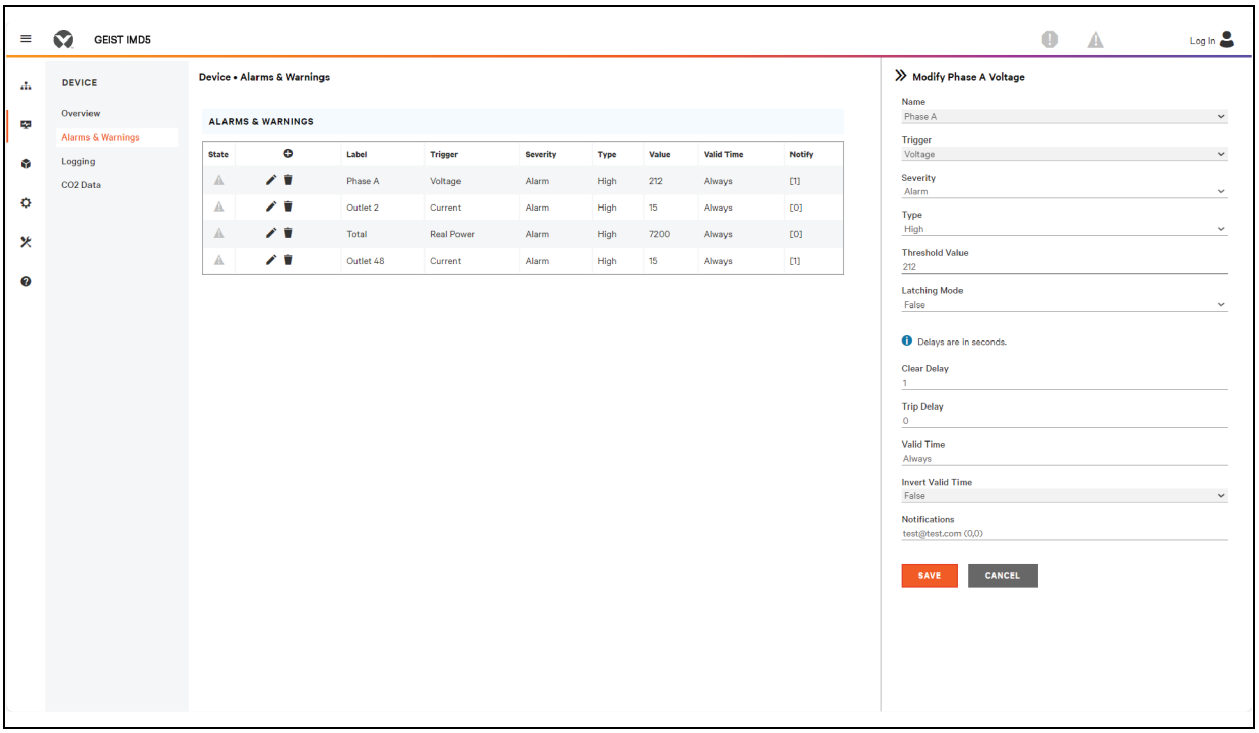
Figura 5.24 Ventana para agregar alarmas y advertencias



Para cambiar un evento de alarma o advertencia existente:

1. Haga clic en el ícono *Modify* situado junto al evento de alarma o advertencia que desee cambiar.
2. Modifique la configuración según sea necesario y haga clic en *SAVE*.
3. Después de agregar una acción, esta tiene una casilla de verificación en la columna de habilitado en el extremo izquierdo. De forma predeterminada, cuando se agrega una acción, esta casilla está sin marcar (deshabilitada). Haga clic en la casilla de verificación para habilitarla. Esto permite activar y desactivar selectivamente distintas acciones para probarlas.

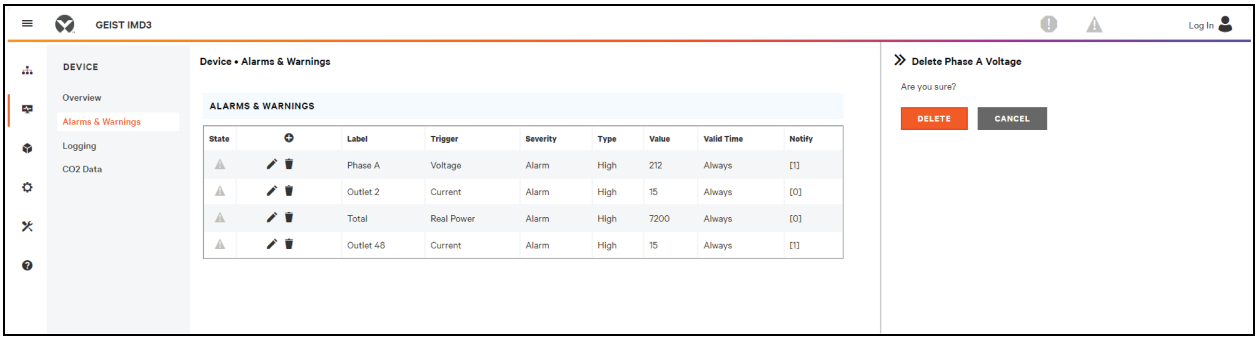
Figura 5.25 Ventana para cambiar alarmas y advertencias



Para eliminar un evento de alarma o advertencia existente:

1. Haga clic en el ícono *Delete* situado junto al evento de alarma o advertencia que desee quitar.
2. Haga clic en *DELETE* y en *SAVE* para confirmar.

Figura 5.26 Eliminación de eventos de alarma y advertencia



5.5.3 Página *Logging*

La página *Logging* permite acceder a los datos históricos registrados por el RTS Vertiv™ Geist™; para ello, es necesario seleccionar los sensores y el intervalo de tiempo que se registrarán. La página *Logging* permite seleccionar todos o no seleccionar ninguno.

Para seleccionar o anular la selección del valor de medición:

1. Haga clic en el ícono *Device* y luego en el submenú *Logging*.
2. En la página *Logging*, haga clic en *Select All* para seleccionar el valor de medición y haga clic en *Select None* para anular la selección del valor de medición.

Figura 5.27 Página *Logging*

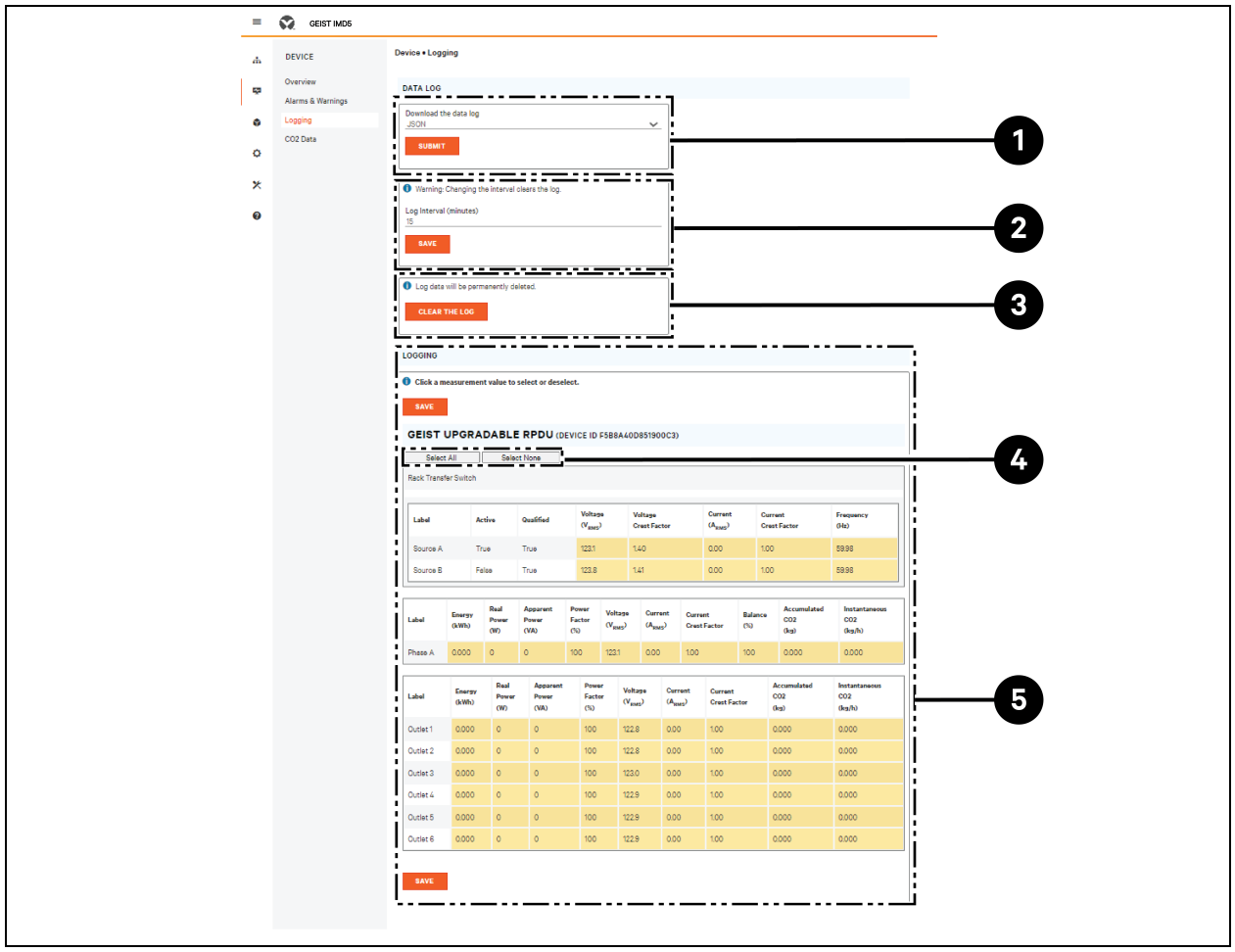


Tabla 5.8 Descripciones de la página *Logging*

Elemento	Nombre	Descripción
1	*Download the data log*	Haga clic en el menú desplegable y seleccione una de las opciones: *JSON* para el formato *JSON*. CSV para el formato **.csv** en software de hojas de cálculo. Haga clic en *SUBMIT* para descargar el registro de datos.
2	*Log interval*	Frecuencia con la que se escriben los datos en el archivo de registro. Puede ser de 1 a 600 minutos; el ajuste predeterminado es de 15 minutos. **¡ADVERTENCIA! Los datos del registro se borrarán permanentemente.**
3	*Clear the log*	Elimina el archivo de registro. **¡ADVERTENCIA! Los datos del registro se borrarán permanentemente.**
4	*Select All/Select None*	Haga clic en *Select All* para seleccionar el valor de medición y haga clic en *Select None* para anular la selección del valor de medición.
5	*Logging*	Haga clic en el valor de medición para seleccionar o anular la selección de los parámetros de registro deseados. De forma predeterminada, se seleccionan todas las mediciones. Haga clic en *SAVE* para guardar los cambios.

NOTA: El tiempo de registro máximo está determinado por el número de mediciones que se registran y el intervalo en el que se escriben los datos en el archivo de registro.

5.5.4 Pestaña *CO2 Data*

Figura 5.28 Página de inicio de *CO2*

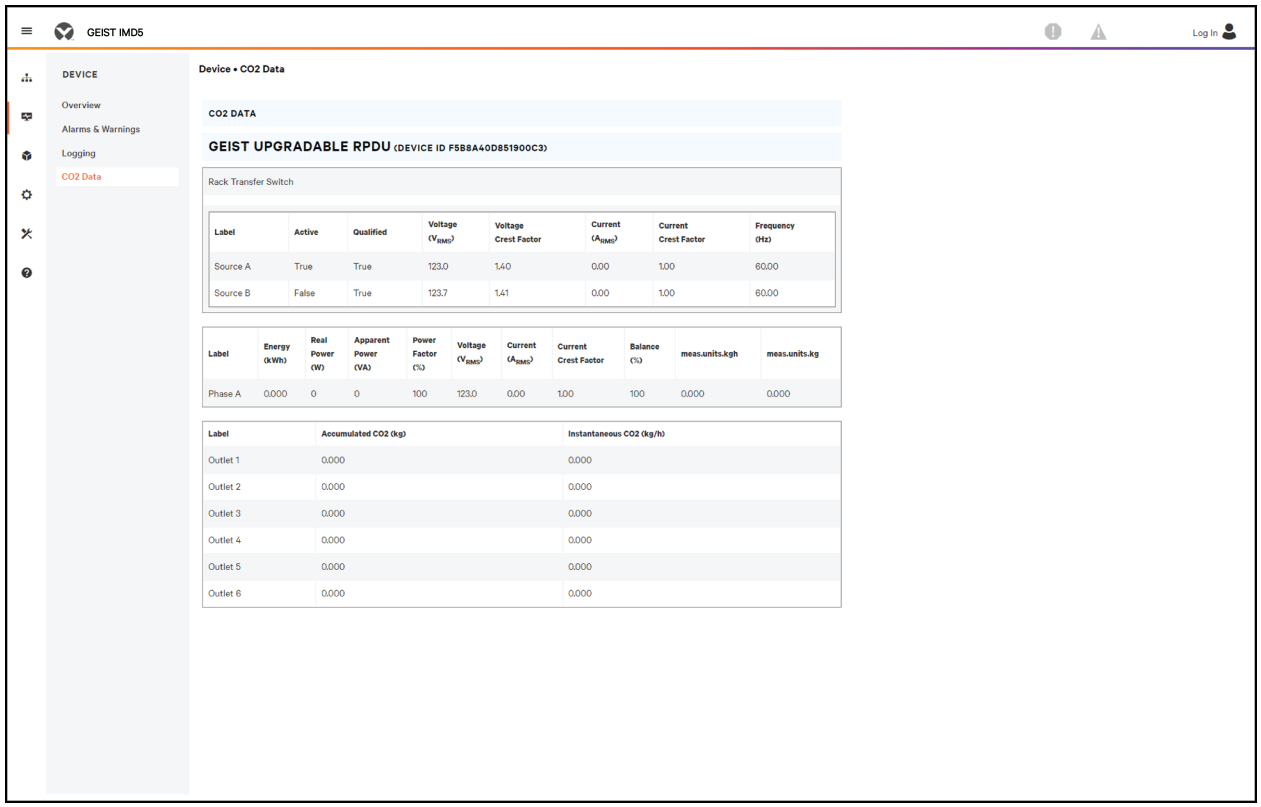
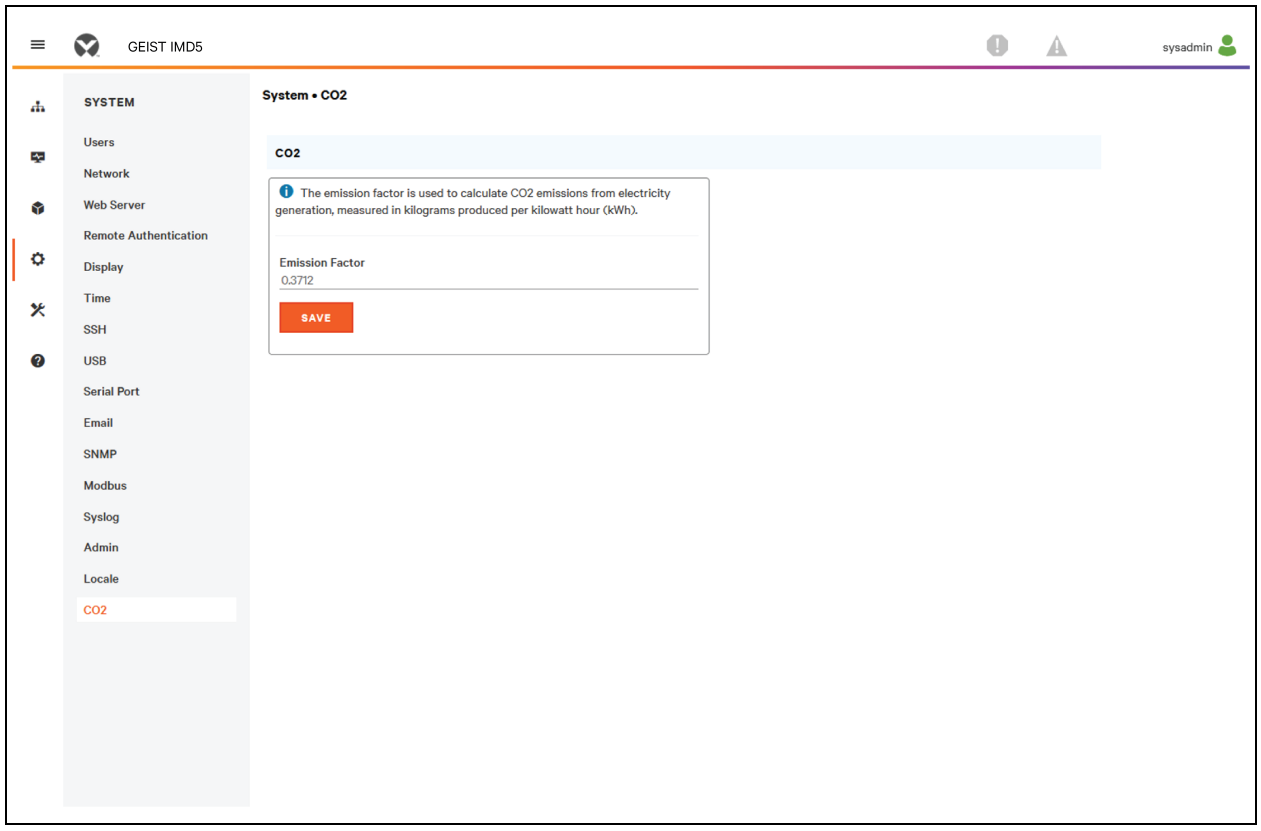


Figura 5.29 Pestaña de *CO2* bajo *System*



NOTA: Hay tres páginas asociadas a la página *CO2*. La primera página es *CO2 data*, en *Device* (Figura 5.28 en la página anterior), que muestra los cálculos acumulados e instantáneos para las fases y los tomacorrientes. La segunda página *CO2*, en *System*, donde se establece el factor de emisión para calcular el CO2 por kWH. El factor de emisión de CO2 predeterminado será de 0,3172. La tercera página se encuentra en la página de información de ayuda; el valor de *Lifetime CO2* se basa en el valor de *Lifetime Energy*. Si un usuario reinicia el consumo de energía de una PDU o de un tomacorriente específico, el valor volverá a 0. Sin embargo, el valor de *Lifetime Energy* de ese componente no se puede restablecer.

5.6 Submenú *Provisioner*

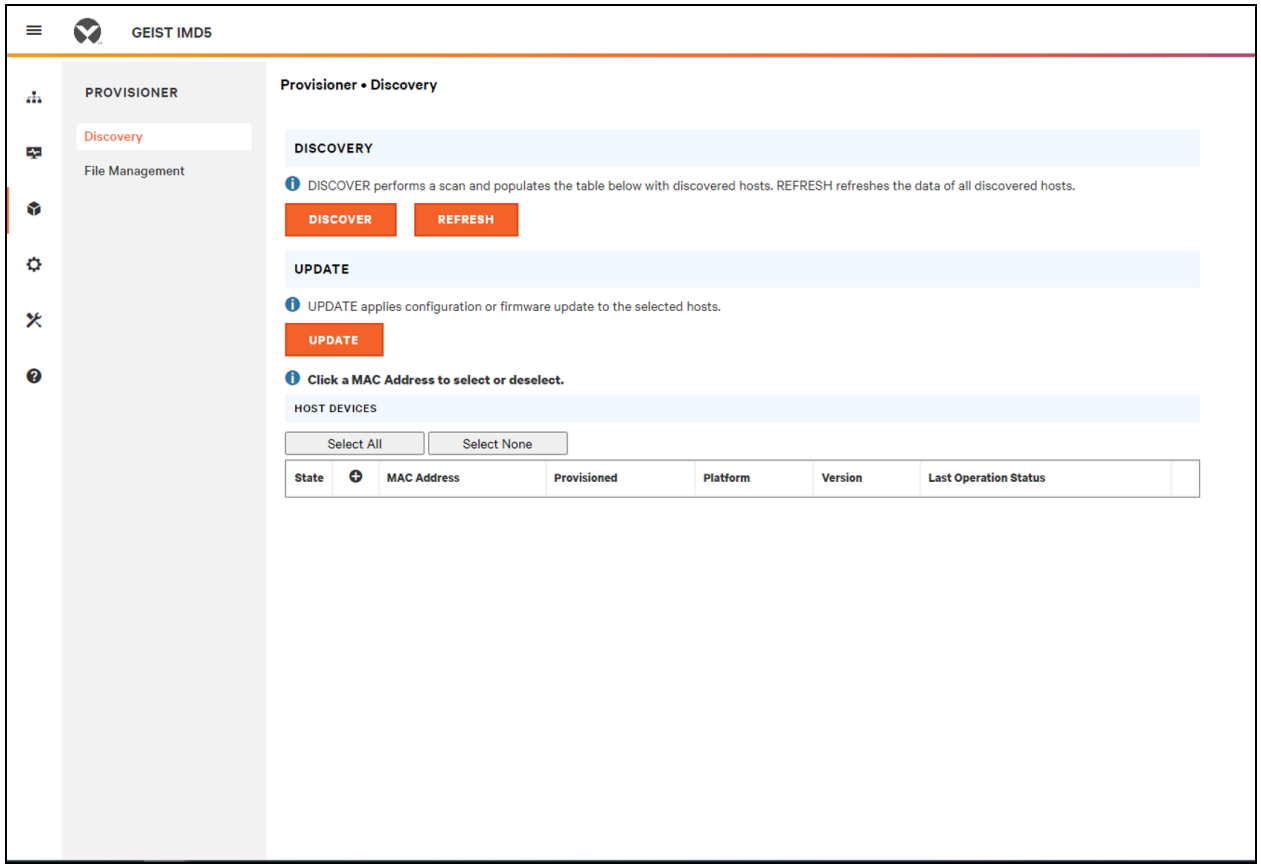
Provisioner permite al usuario descubrir dispositivos de rack Vertiv™ Geist™ conectados a nivel local. El usuario puede cargar un archivo de configuración para actualizar su firmware y configurarlo.

Provisioner ofrece la posibilidad de configurar los ajustes del dispositivo (por ejemplo, las alarmas) y los ajustes del sistema. Esta funcionalidad puede aprovisionar:

- Dispositivos de rack Geist™ que ejecuten el firmware 5.x.x (modelos IMD 3E, 03E, 3E-S y 03E-S)
- Dispositivos de rack Geist™ nuevos de fábrica o configurados anteriormente con 6.1.0.
- PDU para rack y unidades de RTS conectadas directamente a la red local o conectadas como parte de una red de Vertiv Intelligence Director (agregación)
- Todos los dispositivos de rack Geist™ descubiertos o los seleccionados

NOTA: Debe haber iniciado sesión como usuario de nivel de administrador para poder usar el menú *Provisioner*. IPV6 debe estar activado en el conmutador de transferencia de rack Geist™ que se está descubriendo. Es posible configurar la mayoría de los elementos en el menú de la interfaz del usuario *System*. Otros ajustes, como la configuración de los sensores y las alarmas, no se pueden configurar con esta versión de la herramienta de aprovisionamiento.

Figura 5.30 Página del submenú *Provisioner*

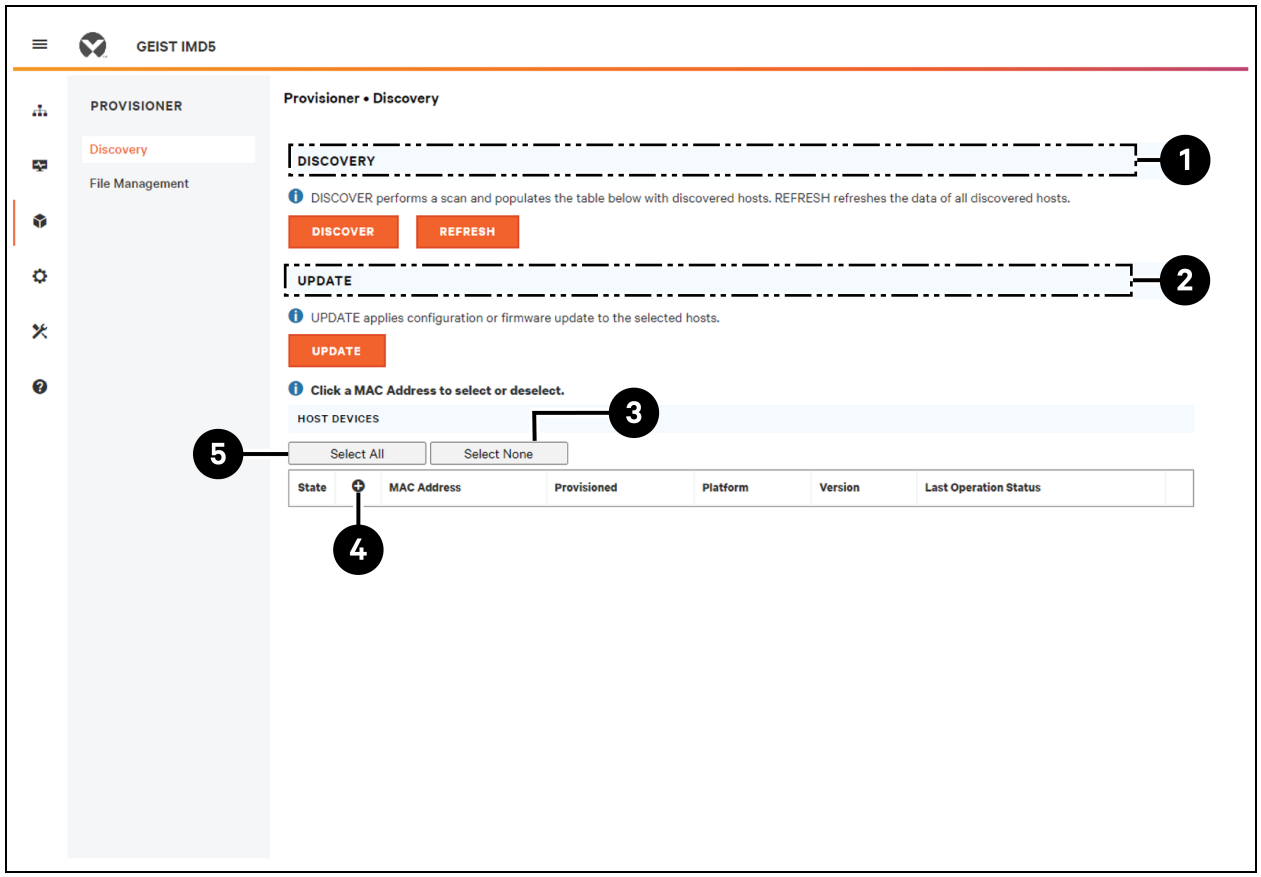


5.6.1 Discovery

1. Haga clic en *DISCOVER* para identificar los dispositivos de rack Vertiv™ Geist™ conectados a nivel local.
2. Haga clic en todos los conmutadores de transferencia de rack Geist™ del listado que desee actualizar el firmware y/o la configuración. Las unidades seleccionadas aparecerán resaltadas con color verde. También puede hacer clic en la opción *Select All* para actualizar todos los dispositivos de rack Geist™ que aparecen en la lista.
3. Haga clic en *UPDATE* para actualizar todos los conmutadores de transferencia de rack Geist™ seleccionados con el archivo de firmware y/o el archivo de configuración.

NOTA: Antes de realizar este paso, debe cargar los archivos de firmware y de configuración en la pestaña *File Management*.

Figura 5.31 ***Discovery***



Elemento	Nombre	Descripción
1	*Discover*	Identifica las PDU y los RTS para rack locales y con conexión a la red
2	*Update*	Actualiza el firmware o la configuración de los dispositivos de rack seleccionados
3	*Select All*	Selecciona todos los dispositivos de rack conectados
4	*Add MAC address*	Permite ingresar manualmente dispositivos de rack por dirección MAC
5	*Select All*	Selecciona todas las unidades RTS conectadas

5.6.2 *File management*

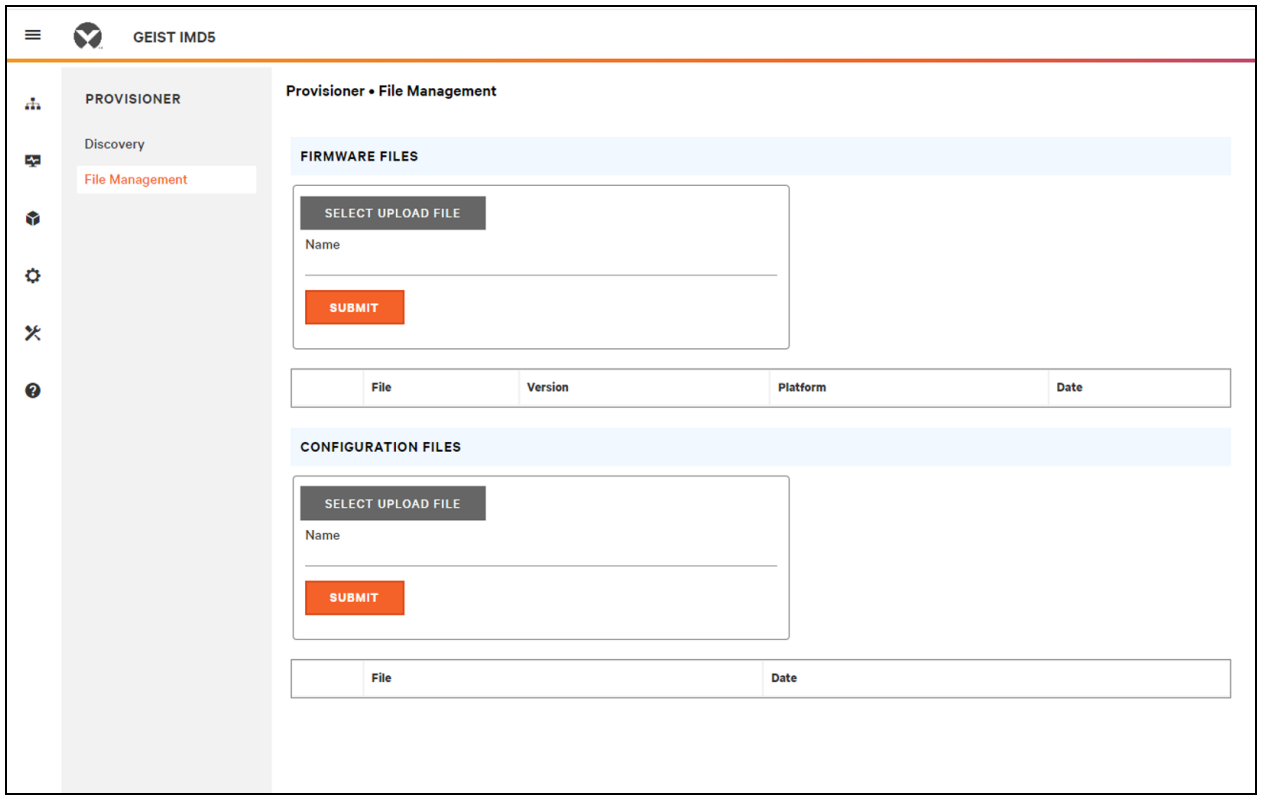
Firmware Files:

1. Haga clic en *SELECT UPLOAD FILE* y seleccione el ***archivo .firmware*** en la ventana *Open*.
2. Haga clic en *SUBMIT*. El archivo de firmware aparecerá en la lista.

Configuration Files:

1. Haga clic en *SELECT UPLOAD FILE* y seleccione el ***archivo .config*** en la ventana *Open*.
2. Haga clic en *SUBMIT*. El archivo de configuración aparecerá en la lista.

Figura 5.32 Página *File management*



Consulte la sección Aprovisionador: formato del archivo de ajustes de configuración en la página 120 para ver ejemplos de archivos de ajustes de configuración usados por *Provisioner* y el formato necesario para el archivo.

5.7 Submenú *System*

NOTA: Para modificar la configuración de la pestaña *System*, debe haber iniciado sesión como administrador.

5.7.1 Página *Users*

La página *Users* del menú *System* permite gestionar o restringir el acceso a las funciones de la unidad mediante la creación de cuentas para diferentes usuarios.

NOTA: Política de bloqueo de cuenta Web/SSH/CLI: una cuenta se bloquea durante 30 minutos cuando se realizan 10 intentos de inicio de sesión consecutivos sin éxito en un plazo de 60 minutos. Esto se puede editar con la última versión del *firmware*.

El alcance permite que una cuenta de nivel de administrador restrinja los usuarios a la visibilidad de la información de tomacorrientes especificada.

Figura 5.33 Página *Users*

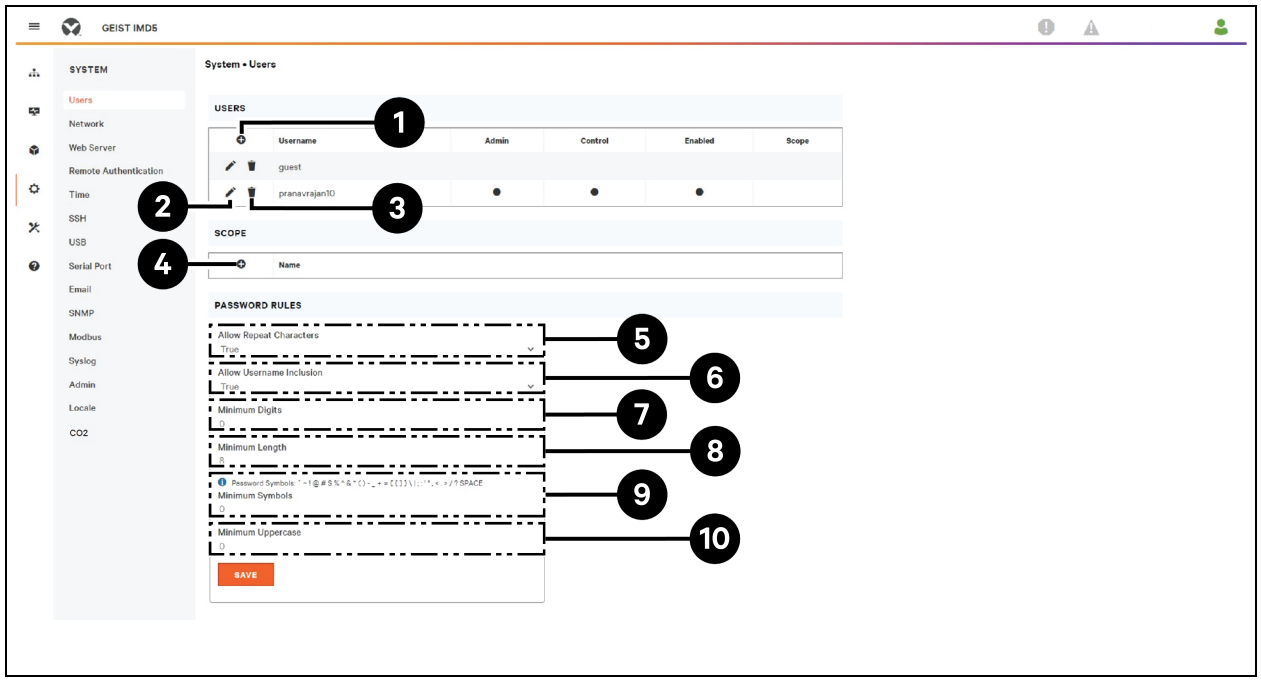


Tabla 5.9 Descripciones de la página *Users*

Número	Descripción
1	Para agregar una nueva cuenta de usuario
2	Para modificar una cuenta de usuario
3	Para eliminar una cuenta de usuario
4	*Add user scope* solo es visible cuando se inicia sesión como administrador*
5	*Allow Repeat Characters*: permite restringir el uso de más de 2 caracteres repetidos (el valor predeterminado es *false*)*
6	*Allow Username Inclusion*: permite restringir la inclusión del nombre de usuario en la contraseña (el valor predeterminado es *false*)*
7	*Minimum Digits*: permite ingresar la cantidad mínima de dígitos numéricos (el valor predeterminado es 0)*
8	*Minimum Length*: permite ingresar la cantidad mínima de caracteres de la contraseña (el valor predeterminado es 8, mínimo 6)*
9	*Minimum Symbols*: permite ingresar la cantidad mínima de símbolos (el valor predeterminado es 0)*
10	*Minimum Uppercase*: permite ingresar la cantidad mínima de caracteres en mayúsculas (el valor predeterminado es 0)*
NOTA: *Solo es visible cuando se inicia sesión como administrador.	

NOTA: Solo las cuentas de nivel *Administrator* permiten agregar, modificar o eliminar usuarios y alcances. Las cuentas de nivel *Control* y *View-Only* permiten el cambio de la contraseña propia mediante el ícono *Modify User*, pero no permiten agregar, eliminar ni modificar otras cuentas. La cuenta *Guest* no permite agregar, eliminar o modificar ninguna cuenta, ni siquiera la propia.

Para agregar o modificar una cuenta de usuario:

1. Haga clic en el ícono *Add* o *Modify User*.
2. Cree o modifique la información de la cuenta según sea necesario.
   a. Username: el nombre de la cuenta. Los nombres de usuario pueden tener un máximo de 24 caracteres, distinguen entre mayúsculas y minúsculas, y no pueden contener espacios ni ninguno de estos caracteres prohibidos: $& `:<>[ ] { }"+%@/ ; =?\^|~',

NOTA: No se puede cambiar un nombre de usuario después de crear la cuenta.

   b. Administrator: si se selecciona *True*, la cuenta tiene acceso de nivel de administrador a la unidad y permite cambiar cualquier ajuste.
   c. Control: si se selecciona *True*, la cuenta tiene acceso de nivel de control. Si para Administrator se seleccionó *True*, *Control* también aparecerá automáticamente como *True*. Si se selecciona *False*, la cuenta es una cuenta habilitada, que es de solo visualización.
   d. Scope: si se ha creado un alcance de usuario, seleccione el alcance aplicable a la cuenta. Consulte el paso Para agregar o modificar un alcance de usuario: en la página siguiente.
   e. New Password: los nombres de usuario pueden tener un máximo de 24 caracteres, distinguen entre mayúsculas y minúsculas, y no pueden contener espacios.
   f. Account Status: permite establecer la cuenta en *Enabled* o *Disabled*. Al deshabilitar una cuenta, se impide que se utilice para iniciar sesión, pero no se elimina de la lista de cuentas.
3. Haga clic en *SAVE*.

Tipos de cuentas de usuario

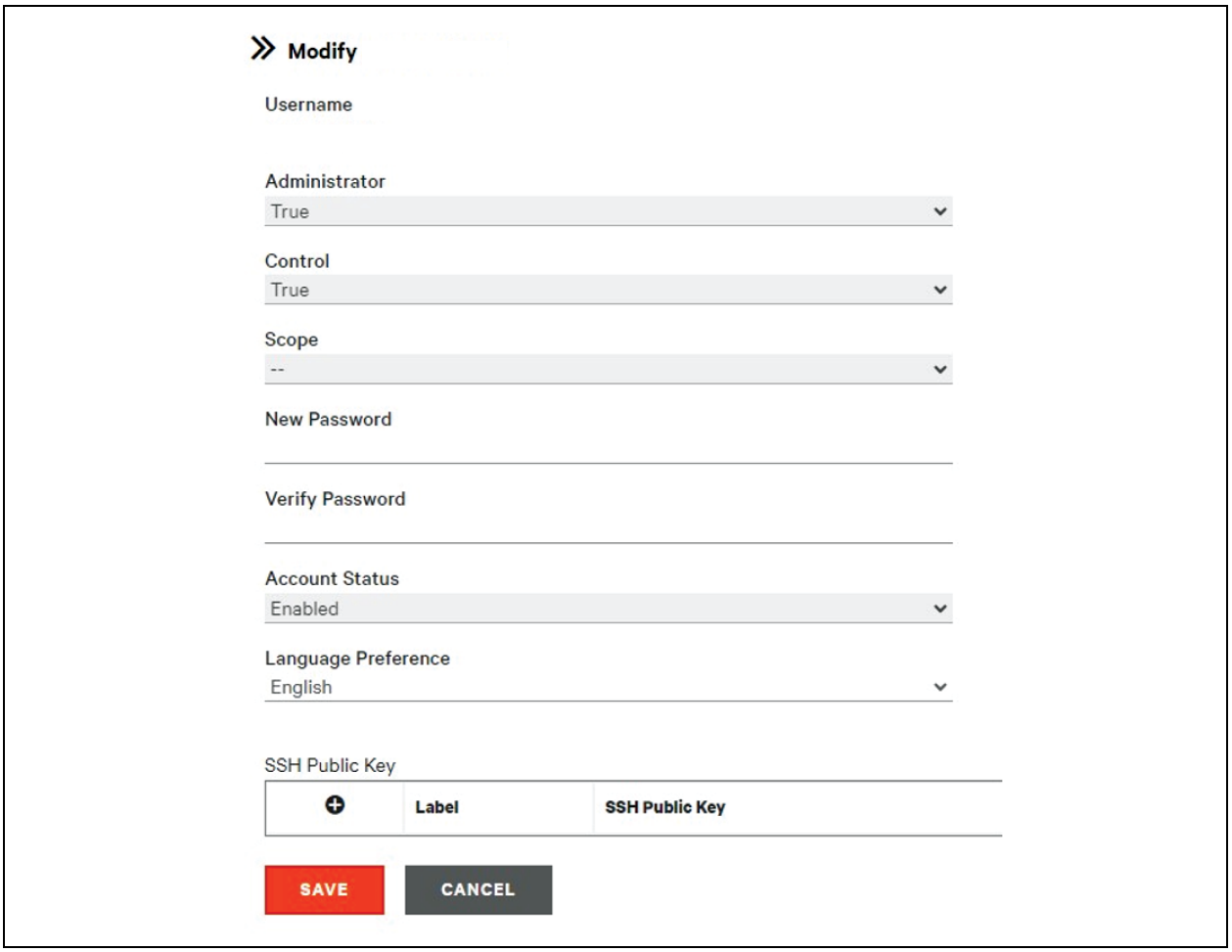
- Administrator: los usuarios de este tipo de cuentas (en las cuales tanto *Administrator* como *Control* están establecidos en *True*, como se indicó anteriormente) tienen un control total sobre todas las funciones y configuración disponibles en el dispositivo, incluida la capacidad de modificar la configuración del sistema y de agregar, modificar o eliminar las cuentas de otros usuarios.
- Control: los usuarios de este tipo de cuentas (cuentas solo con *Control* establecido en *True*) tienen el control de todos los ajustes pertenecientes a los sensores del dispositivo. Pueden agregar, modificar o borrar eventos de alarma y advertencia, y acciones de notificación; así como cambiar los nombres o etiquetas del dispositivo y sus sensores. Las cuentas de tipo *Control* no permiten modificar la configuración del sistema ni hacer cambios en las cuentas de otros usuarios.
- View-Only: si tanto las opciones *Administrator* como *Control* están establecidas en *False*, la cuenta de tipo *View-Only*. Los únicos cambios que pueden realizar los usuarios de este tipo de cuentas son el cambio de la contraseña de su propia cuenta y el cambio del idioma de preferencia para su propia cuenta. Los usuarios de cuentas *View-Only* no pueden cambiar la configuración de ningún dispositivo o sistema.

- **Guest:** cualquier usuario que vea la página web de la unidad sin iniciar sesión, la verá automáticamente como invitado. De forma predeterminada, la cuenta de invitado es una cuenta de solo lectura y no puede realizar cambios en ninguna configuración. Esta cuenta no permite cambios en los nombres, etiquetas, eventos de alarma y notificaciones. La cuenta de invitado no se puede eliminar, pero se puede deshabilitar, lo que obligaría al usuario a iniciar sesión para ver el estado del sistema.

Para cambiar una contraseña de usuario:

1. Inicie sesión en su cuenta.
2. Haga clic en el ícono *Modify User*.
3. Haga clic en *Username*, en la esquina superior derecha de la página.
4. Ingrese una nueva contraseña y verifíquela volviendo a ingresarla en el campo *Verify password*.
5. Haga clic en *SAVE*.

Figura 5.34 Página *Change User Password*



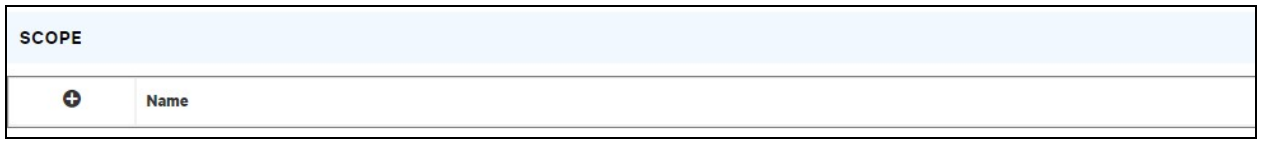
Para agregar o modificar un alcance de usuario:

1. Haga clic en el ícono *Add or Modify Scope*. Consulte la Figura 5.35 en la página opuesta.
2. Cree o modifique la información del alcance según sea necesario.

a. Label: ingrese el nombre deseado para el alcance seleccionado.
b. Remote Authentication Attribute: se utiliza para todos los tipos de autenticación remota.
c. Haga clic en los tomacorrientes aplicables a un usuario especificado (resaltado en verde)

3. Haga clic en *OK* para guardar los cambios.

Figura 5.35 Cómo agregar un alcance



Reglas de contraseña y configuración de políticas de cuentas

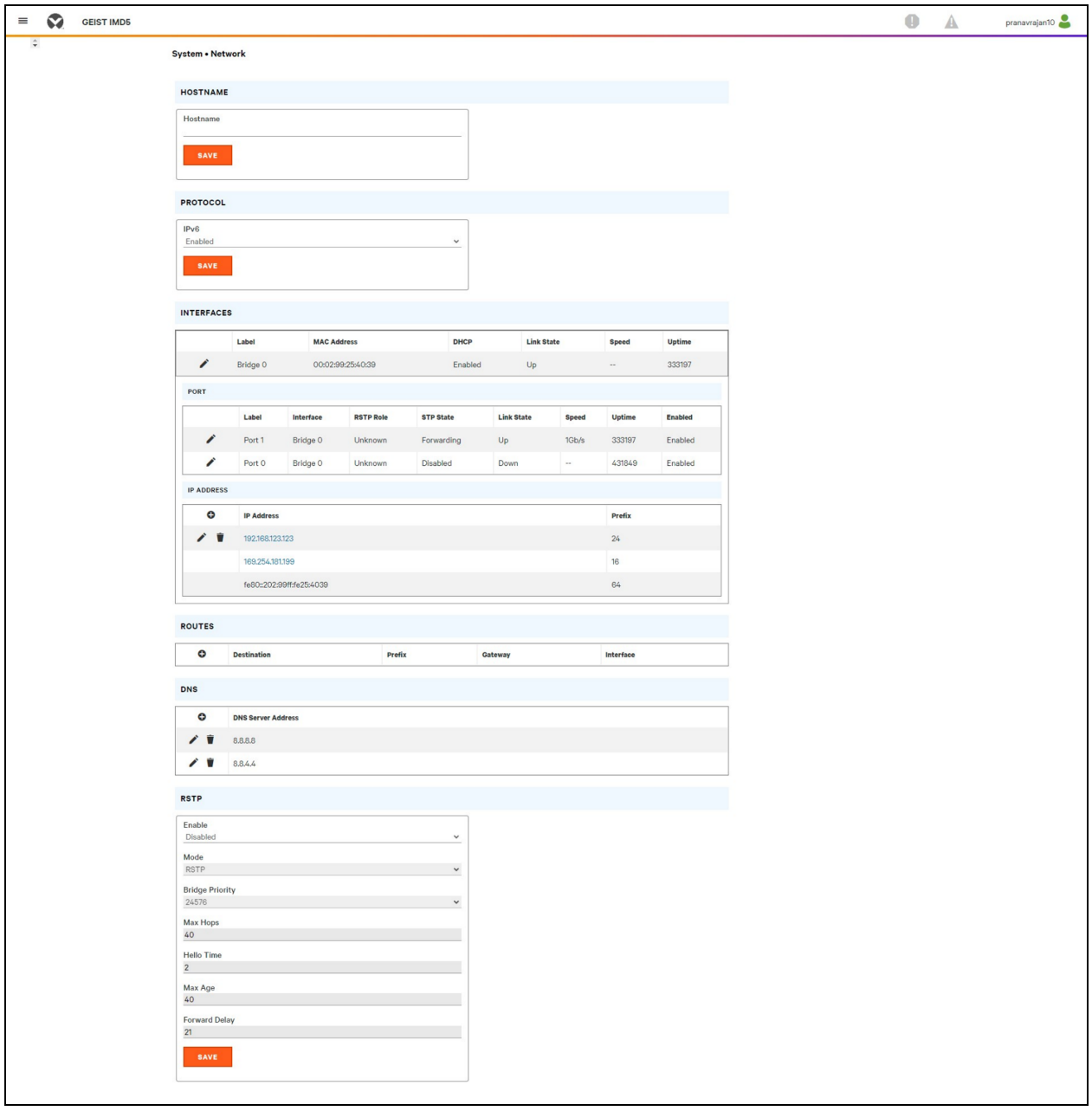
NOTA: Los usuarios se desconectarán automáticamente después de 10 minutos de inactividad.

5.7.2 Pestaña *Network*

La configuración de red de la unidad se establece en la *pestaña Network* del menú *System*. La configuración correspondiente a la conexión de red de la unidad es:

- Hostname: el nombre del host se puede utilizar como método de identificación del dispositivo en la red.
- Protocol: haga clic en el menú desplegable de IPv6, seleccione *Enabled* o *Disabled* y haga clic en *Save*.
- Interfaces: se utiliza para configurar la dirección IP del RTS Vertiv™ Geist™, habilitar/deshabilitar el DHCP y ver el estado del enlace, la velocidad y el tiempo de funcionamiento. El dispositivo admite hasta ocho entradas de direcciones IP configuradas por el usuario.
- Ports: se utiliza para ver o modificar la configuración del puerto Ethernet y el estado RSTP, interfaz, estado STP, estado del vínculo, velocidad, tiempo de funcionamiento, estado habilitado de cada puerto en el RTS Geist™.
- IP Address: se utiliza para agregar o modificar las direcciones IP.
- Routes: muestra las rutas configuradas y es donde configurará la dirección de su *Gateway* para el RTS Geist™. Las rutas predeterminadas se distinguen por un *destino* 0.0.0.0 o ::, con un prefijo 0 y una interfaz all. Solo puede haber una ruta predeterminada para IPv4 y otra para IPv6.
- DNS: permite a la unidad resolver nombres de host para los servidores de correo electrónico, NTP y SNMP.
- RSTP: se utiliza para ver y modificar el estado del RSTP, el modo, la prioridad de puente, el número máximo de saltos, el tiempo de respuesta, la antigüedad máxima (*Max*) y el retardo de reenvío.

Figura 5.36 Página *Network Configuration*



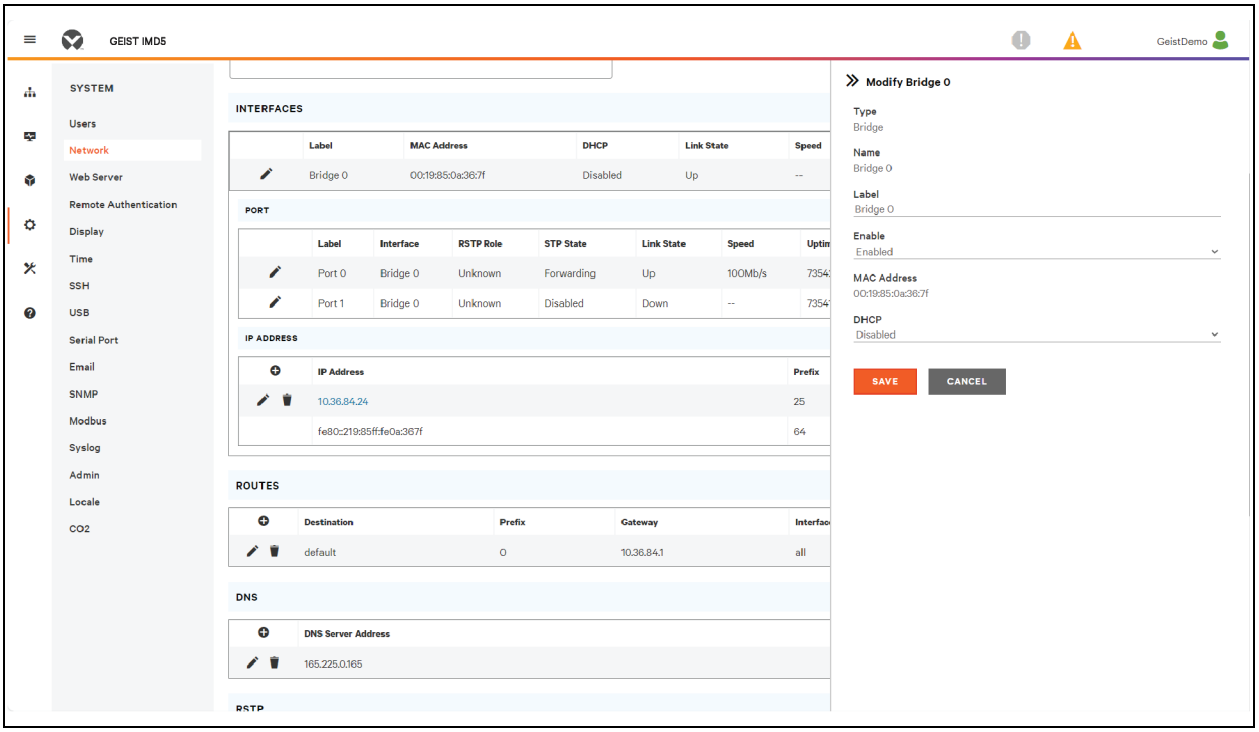
Para editar los parámetros de la interfaz:

1. Haga clic en el ícono *Modify*.
2. Modifique los campos deseados.
   a. **Label:** cambie el nombre deseado de la interfaz seleccionada.
   b. **Enable:** se utiliza para habilitar/deshabilitar la interfaz seleccionada. Si solo hay una interfaz disponible, al deshabilitarla se limita el acceso al dispositivo que requiere el restablecimiento de la red.
   c. **DHCP:** se utiliza para habilitar/deshabilitar DHCP en la interfaz seleccionada.

3. Haga clic en *SAVE*.

NOTA: Los cambios realizados en la configuración de la interfaz de red se aplican una vez que se hace clic en el botón *SAVE*. Si ha cambiado la dirección IP, aparecerá como si la unidad ya no respondiera porque el navegador no podrá recargar la página web. Cierre la ventana del navegador, escriba la nueva dirección IP en la barra de direcciones del navegador y se podrá acceder a la unidad.

Figura 5.37 Parámetros de las interfaces



Para agregar una interfaz para un adaptador USB inalámbrico:

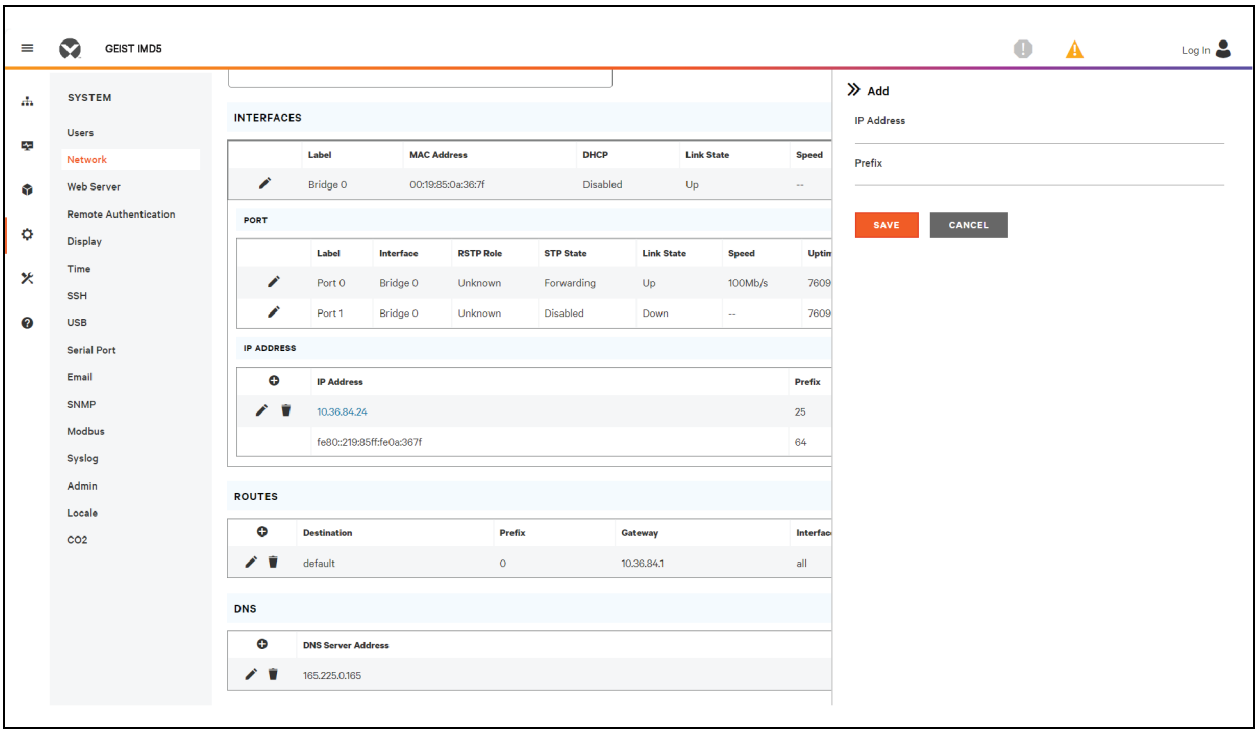
1. Introduzca el adaptador USB inalámbrico en el puerto USB (el RTS estará inaccesible durante unos segundos mientras la pila de red se reconfigura automáticamente).
2. Después de detectar automáticamente el adaptador, aparecerá una interfaz de wifi.
3. Haga clic en el ícono *Modify*. Seleccione el SSID aplicable del menú desplegable *Detected SSIDs*.

NOTA: Consulte la sección Adaptadores USB inalámbricos TP-Link en la página 117 para ver una lista de los adaptadores inalámbricos TP-Link.

Para agregar una nueva dirección IP:

1. Haga clic en el ícono *Add*.
2. Introduzca la dirección IPv4 o IPv6 y el prefijo/máscara de subred en los campos correspondientes. Se pueden asignar estadísticamente hasta ocho direcciones IP.
3. Haga clic en *SAVE*.

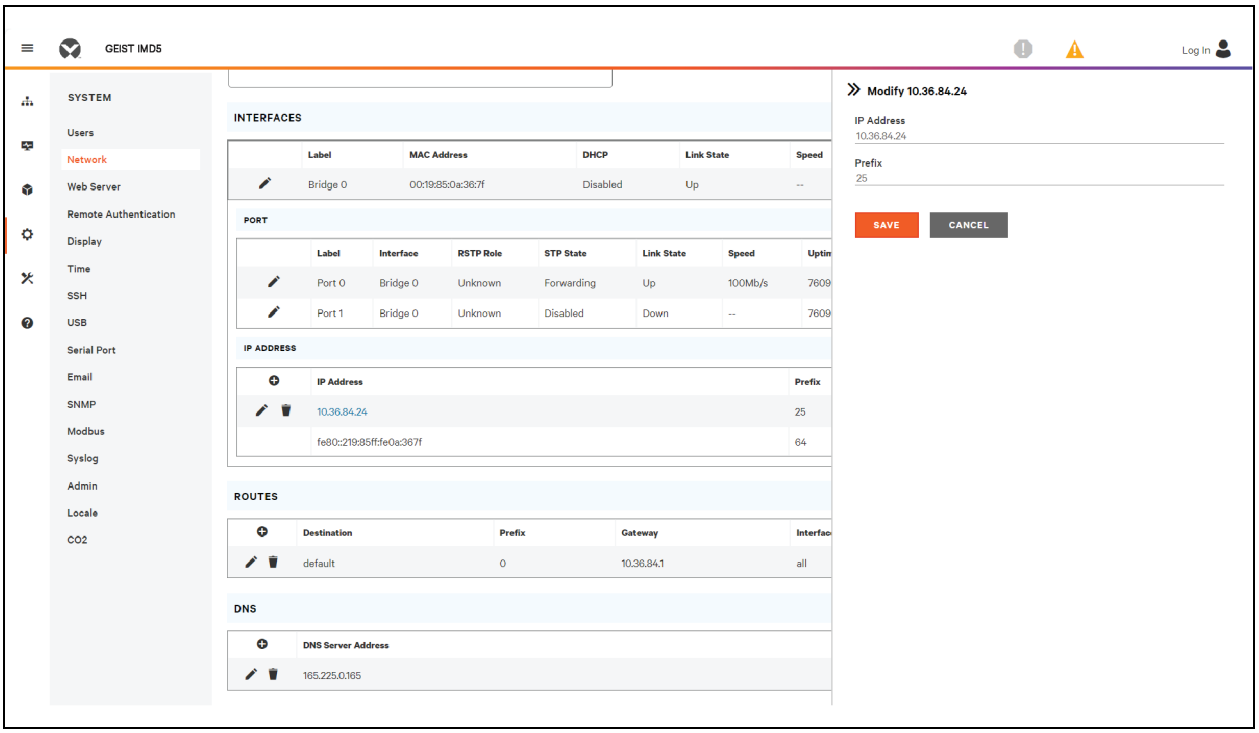
Figura 5.38 Agregar una nueva dirección IP



Para modificar una dirección IP existente:

1. Haga clic en el ícono *Modify*.
2. Edite la dirección IP y el prefijo/máscara de subred si es necesario.
3. Haga clic en *SAVE*.

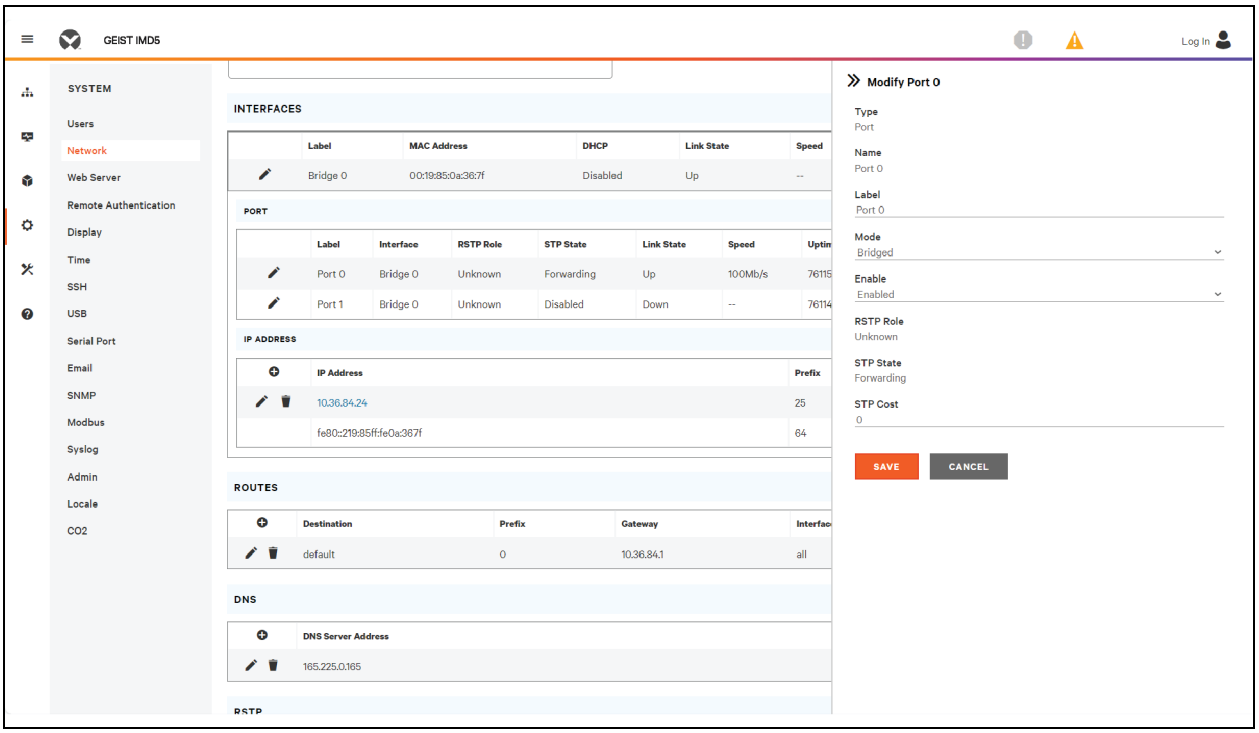
Figura 5.39 Modificar una dirección IP



Para modificar la configuración del puerto:

1. Haga clic en el ícono *Modify*.
2. Introduzca la información correspondiente.
   a. Cambie la etiqueta del puerto si lo desea.
   b. Seleccione el modo *Bridged* o *Independent*.
   c. Seleccione *Enable/Disable* para habilitar o deshabilitar el puerto.
   d. Asigne el estado de STP. De este modo se designa la contribución de esta interfaz al costo de la ruta raíz cuando sirve como puerto raíz.
3. Haga clic en *SAVE*.

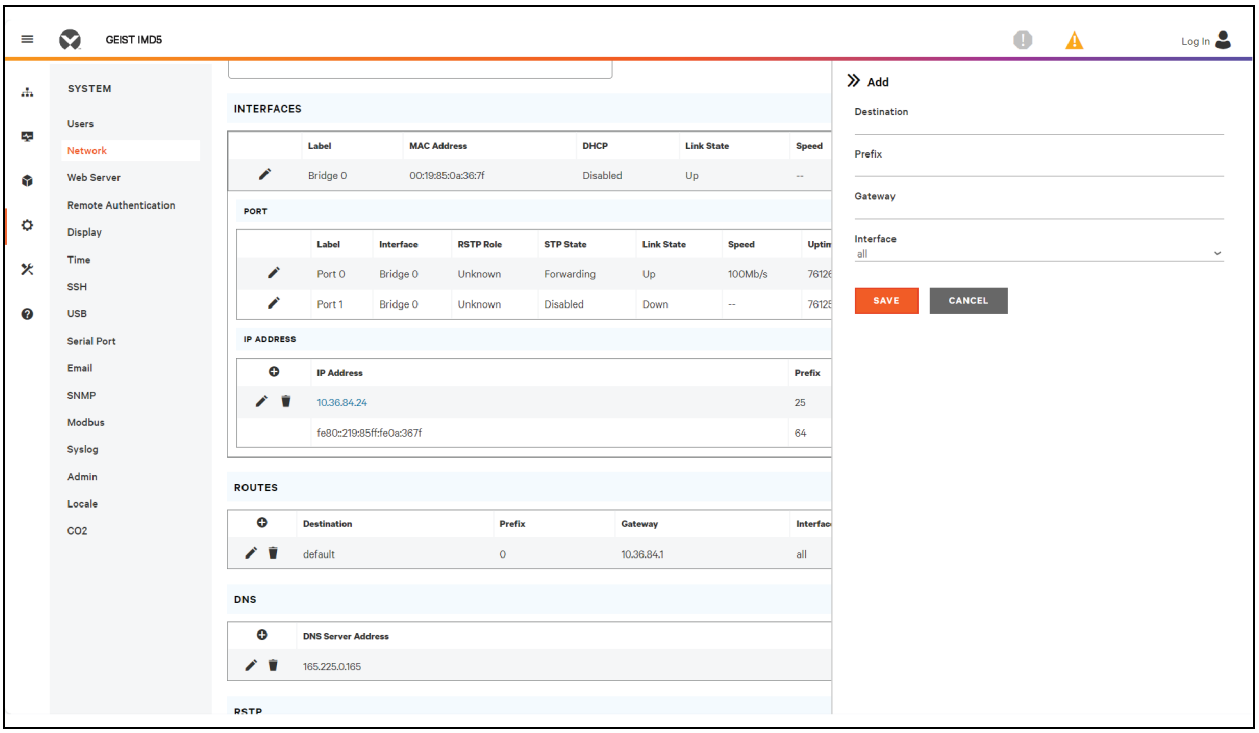
Figura 5.40 Modificación de los ajustes del puerto



Para agregar una ruta nueva:

1. Haga clic en el ícono *Add*.
2. Introduzca la información correspondiente.
   a. Dirección IP de destino para la ruta deseada.
   b. Ingrese el prefijo para la ruta deseada.
   c. Introduzca la dirección IP de la puerta de enlace.
   d. Seleccione la interfaz que se aplique a la ruta.
3. Haga clic en *SAVE*.

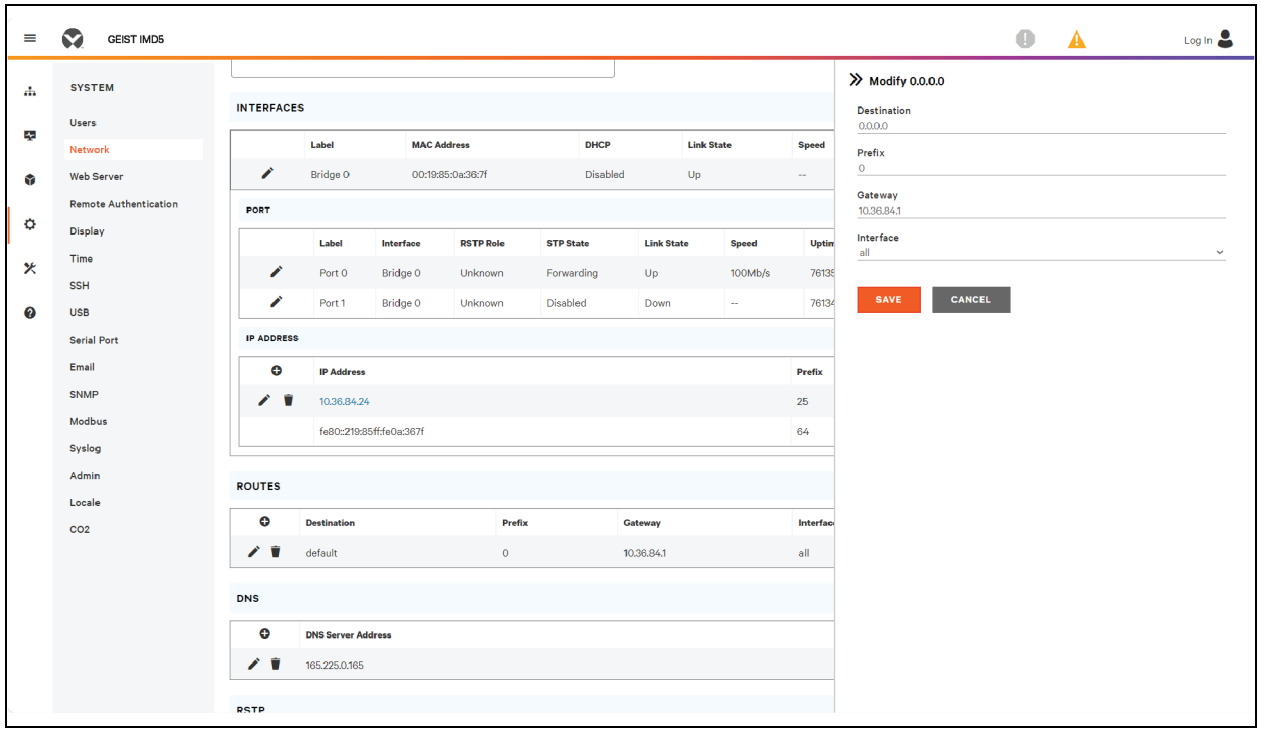
Figura 5.41 Agregar rutas



Para modificar una ruta existente:

1. Haga clic en el ícono *Modify*.
2. Edite los campos deseados.
3. Haga clic en *SAVE*.

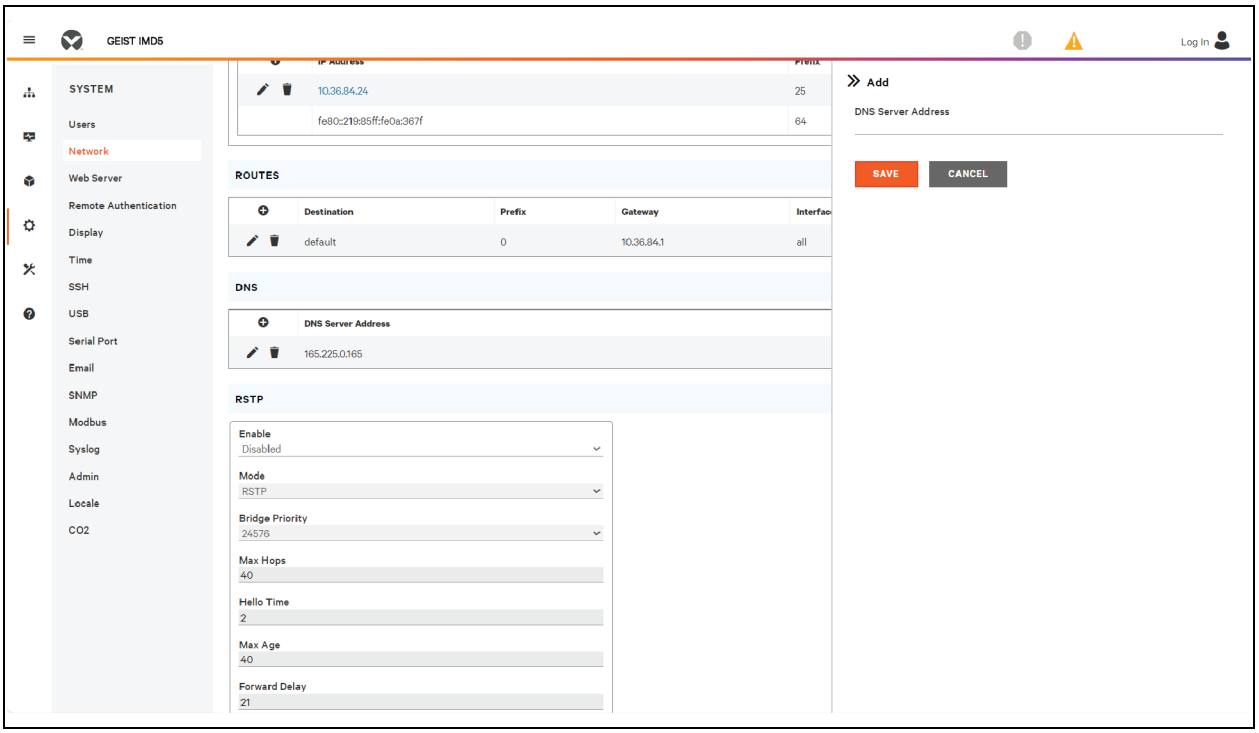
Figura 5.42 Modificación de rutas



Para agregar una nueva dirección de servidor DNS:

1. Haga clic en el ícono *Add*.
2. Introduzca la IP del servidor DNS que desee. Se pueden agregar hasta dos servidores DNS.
3. Haga clic en *SAVE*.

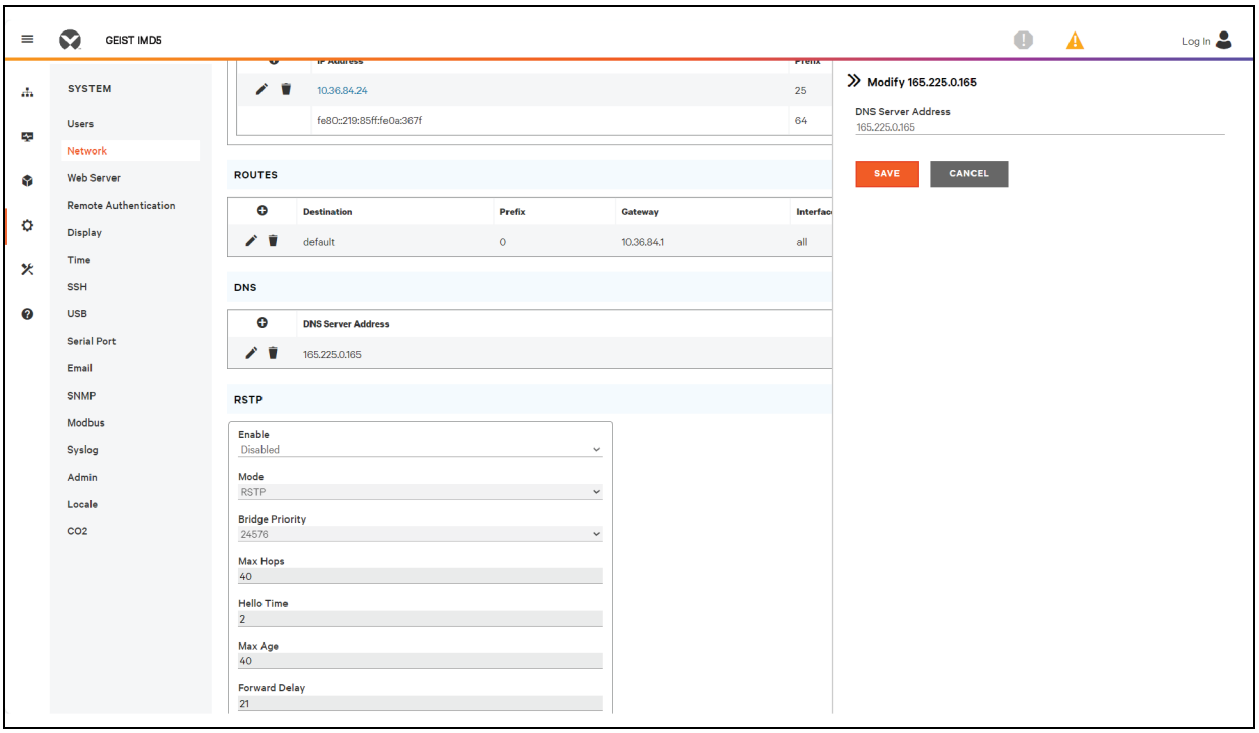
Figura 5.43 Agregar dirección de servidor DNS



Para modificar una dirección de servidor DNS existente:

1. Haga clic en el ícono *Modify*.
2. Edite el campo *DNS Server Address* según sea necesario.
3. Haga clic en *SAVE*.

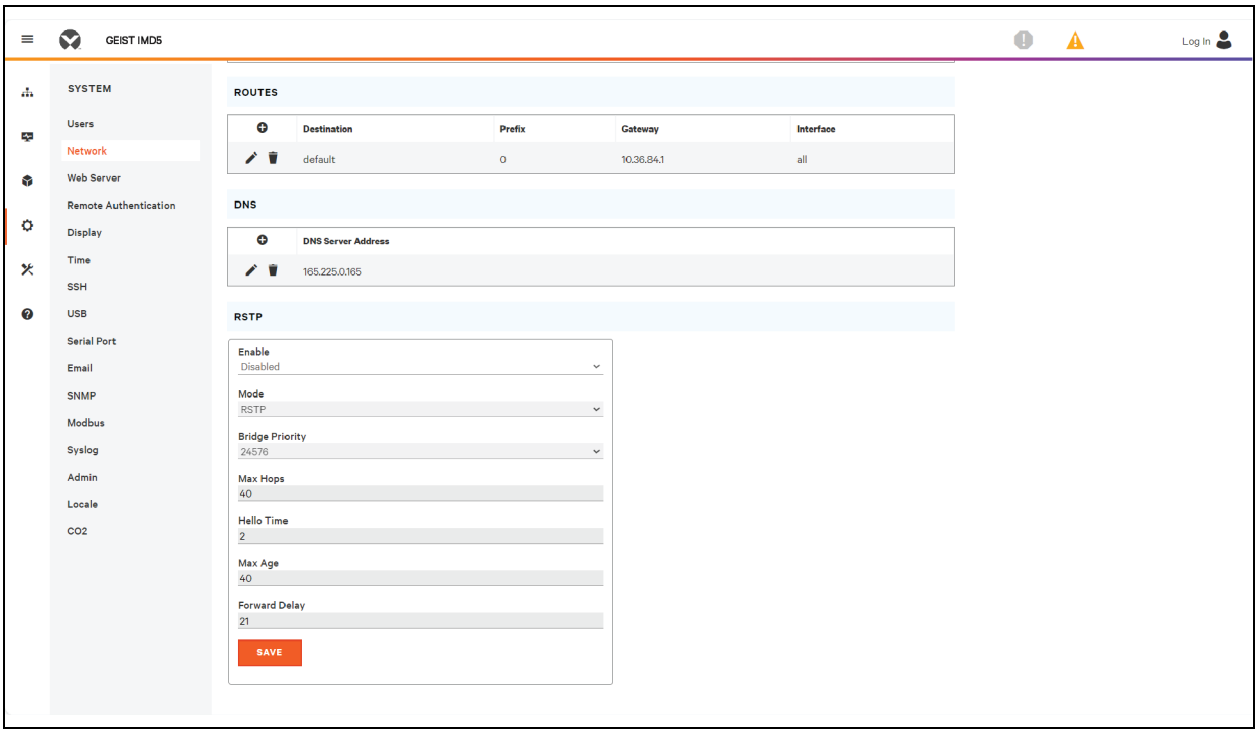
Figura 5.44 Modificar una dirección de servidor DNS



Para cambiar la configuración de RSTP:

1. Cambie la configuración como desee.
   a. **Enable:** habilite o deshabilite el protocolo RSTP.
   b. **Mode:** el modo RSTP permite volver a STP cuando sea necesario.
   c. **Bridge Priority:** haga clic en el menú desplegable, seleccione el valor adecuado y haga clic en *Save*.
   d. **Max Hops:** se usa cuando el modo está habilitado para RSTP.
   e. **Hello Time:** intervalo, en segundos, entre las transmisiones periódicas de los mensajes de configuración por los puertos designados.
   f. **Max Age:** antigüedad máxima, en segundos, de la información transmitida por esta interfaz, cuando sirve como puente de raíz. Establecido en 2 segundos.
   g. **Forward Delay:** retardo, en segundos, que utilizan los puentes para hacer la transición del puente raíz y los puertos designados al modo de reenvío. Establecido en 21 segundos.
2. Haga clic en *SAVE*.

Figura 5.45 Cambio de la configuración de RSTP



5.7.3 Pestaña *Web Server*

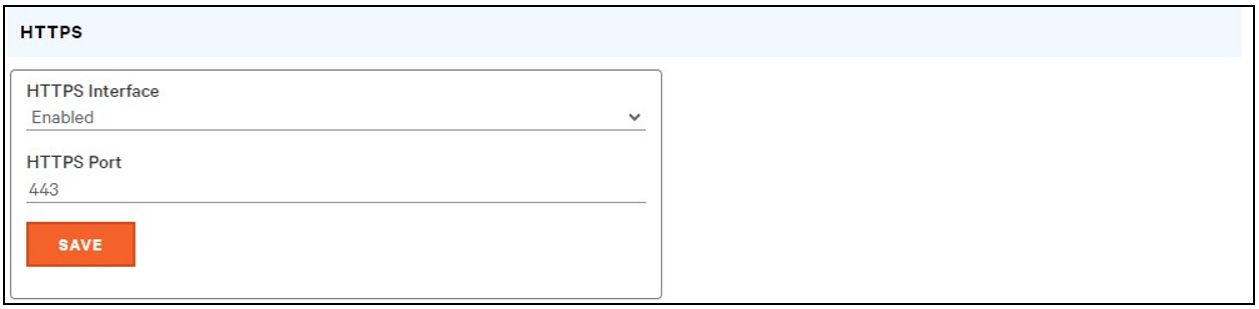
La configuración de *Web Server* de la unidad se puede actualizar en la pestaña *Web Server* del menú *System*.

- HTTP Interface: se puede habilitar o redirigir a HTTPS, mientras que la interfaz HTTPS se puede habilitar o deshabilitar. Cuando la interfaz HTTP se redirige a la interfaz HTTPS, pero esta se encuentra deshabilitada, la interfaz HTTP también se deshabilitará de forma efectiva.

NOTA: Tenga en cuenta que no es posible deshabilitar los protocolos HTTP, HTTPS y SSH al mismo tiempo.

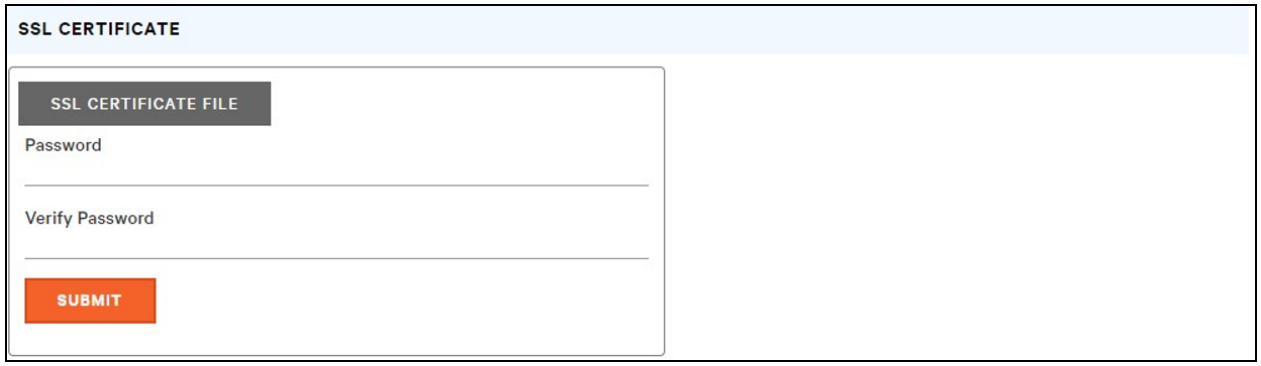
- HTTP/HTTPS Server Port: permite cambiar los puertos TCP a los que escuchan los servicios HTTP y HTTPS para las conexiones entrantes. Los valores predeterminados son el puerto 80 para HTTP y el puerto 443 para HTTPS.

Figura 5.46 Página *HTTPS Configuration*



- SSL Certificate: le permite cargar su propio archivo de certificado SSL firmado para remplazar el predeterminado. El certificado puede estar autofirmado o firmado por una autoridad de certificación. El certificado SSL debe tener formato *PEM* o *PFX* (PKCS12).

Figura 5.47 SSL Certificate



- Formato *PEM*:
  - El certificado público y la clave privada deben residir en el mismo archivo.
  - El certificado debe seguir el estándar x.509.
  - La clave privada debe generarse con el algoritmo RSA o con el algoritmo ECDSA. Debe estar en formato *PEM*.
    - No se admiten RSA de 2048 bits o inferiores.
    - P-384 es el tamaño de clave admitido para ECDSA.
  - La clave privada *PEM RSA* puede estar protegida por una contraseña.
- Formato *PFX*: también se dispone de compatibilidad con el estándar PKCS12 (*.pfx*), que es una combinación binaria cifrada de un certificado público *PEM* y de su clave privada *PEM*. Cuando se genera un certificado *PFX*, se le pide una contraseña opcional.

5.7.4 Página *Remote authentication*

La página *Remote Authentication* permite designar uno de los tres protocolos de autenticación para el acceso remoto al dispositivo. De forma predeterminada, el dispositivo utiliza la base de datos local para autenticar a los usuarios. La autenticación remota permite que el dispositivo autentique usuarios con servidores remotos. Si la autenticación remota falla, se volverá a la autenticación local.

Para cambiar la configuración de autenticación remota:

1. Seleccione el modo necesario en el menú desplegable.
   - Mode: Local Authentication (Disabled/LDAP/TACACS+/RADIUS).
   - LDAP: *Lightweight Directory Access Protocol*.
   - TACACS+: *Terminal Access Controller Access Control System Plus*.
   - RADIUS: *Remote Authentication Dial-In User Service*.
2. Haga clic en *SAVE*.

LDAP

El protocolo LDAP se puede configurar a través de este menú.

NOTA: Para configurar el dispositivo de RTS Vertiv™ Geist™ para este protocolo de autenticación remota, es necesario conocer la configuración del servidor LDAP. Si no está familiarizado con esta configuración, consulte al administrador del servidor LDAP.

Configuración para la autenticación remota mediante LDAP.

- LDAP Server Address: especifique la dirección de host para LDAP. El *HOST* puede ser una dirección IPv4, una dirección IPv6 entre corchetes (p. ej., *[2001:0DB8:AC10:FE01::]*) o un nombre de host.
- LDAP Server Port: se utiliza para establecer el número de puerto LDAP. El puerto predeterminado para LDAP es *389*; se utiliza para tipo de seguridad *None* o *StartTLS*. Use *636* para tipo de seguridad *SSL*.
- LDAP Mode: en el menú desplegable, seleccione *Active Directory* u OpenLDAP. Consulte Un ejemplo de configuración de LDAP para credenciales de Active Directory en la página 143.
- Security Type: en el menú desplegable, seleccione *None*, *SSL* o *StartTLS*.
- Bind DN: nombre distintivo utilizado como enlace al servidor de directorios. La cadena en blanco para el DN de enlace y la contraseña implican un enlace anónimo.
- Bind Password: contraseña utilizada como enlace al servidor de directorios.
- Base DN: DN para usar para la base de búsqueda.

Los campos restantes proceden del esquema NIS, definido en RFC2307. Se utilizan para autenticar usuarios en LDAP. Si se dejan en blanco, se utilizará el valor predeterminado.

- User Filter: filtro LDAP para seleccionar usuarios.
- "uid" Mapping: nombre del atributo de servidor que corresponde al atributo *uid* en el esquema.
- "uidNumber" Mapping: nombre del atributo de servidor que corresponde al atributo *uidNumber* en el esquema.
- Group Filter: filtro LDAP para seleccionar grupos.
- "gid" Mapping: nombre del atributo de servidor que corresponde al atributo *gid* en el esquema.
- "memberUid" Mapping: nombre del atributo de servidor que corresponde al atributo *memberUid* en el esquema.

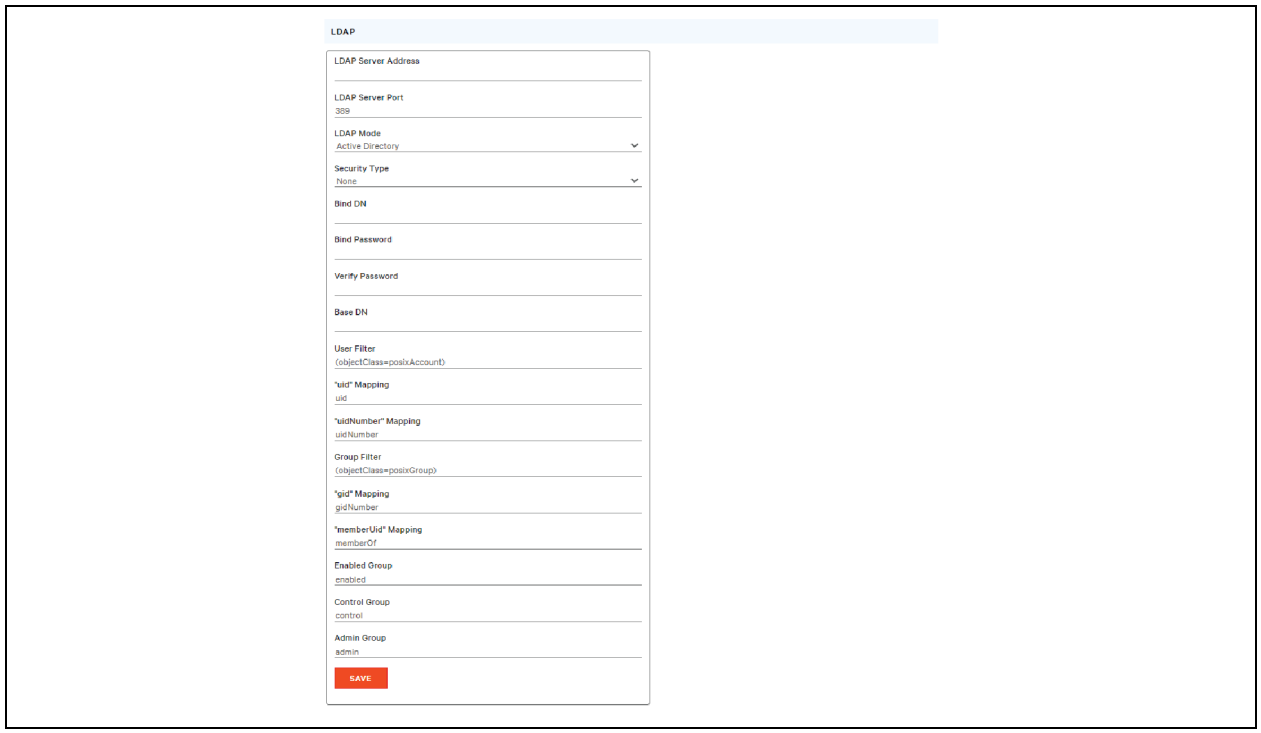
NOTA: Los usuarios *deben* completar el campo uidNumber. Si el valor es nulo o falta, fallará el inicio de sesión válido. El uidNumber del usuario *debe* ser 1000 o superior. Si el valor es inferior a 1000, fallará el inicio de sesión válido.

- Enabled Group: los usuarios de este grupo tienen privilegios de solo visualización, como se describe en la sección "Página *Users*" de este manual.
- Control Group: los usuarios de este grupo tienen privilegios de control, como se describe en la sección "Página *Users*" de este manual.
- Admin Group: los usuarios de este grupo tienen privilegios de administrador, como se describe en la sección "Página *Users*" de este manual. Los usuarios de LDAP no cuentan para calcular el número mínimo de usuarios administradores requeridos.

Haga clic en *SAVE*.

Los campos *Enabled Group*, *Control Group* y *Admin Group* indican cómo asignar grupos a los permisos de usuario. Un usuario debe pertenecer a uno de estos grupos para acceder al dispositivo. Si un usuario pertenece a más de un grupo, se utiliza el grupo con los permisos más elevados.

Figura 5.48 Menú *LDAP*



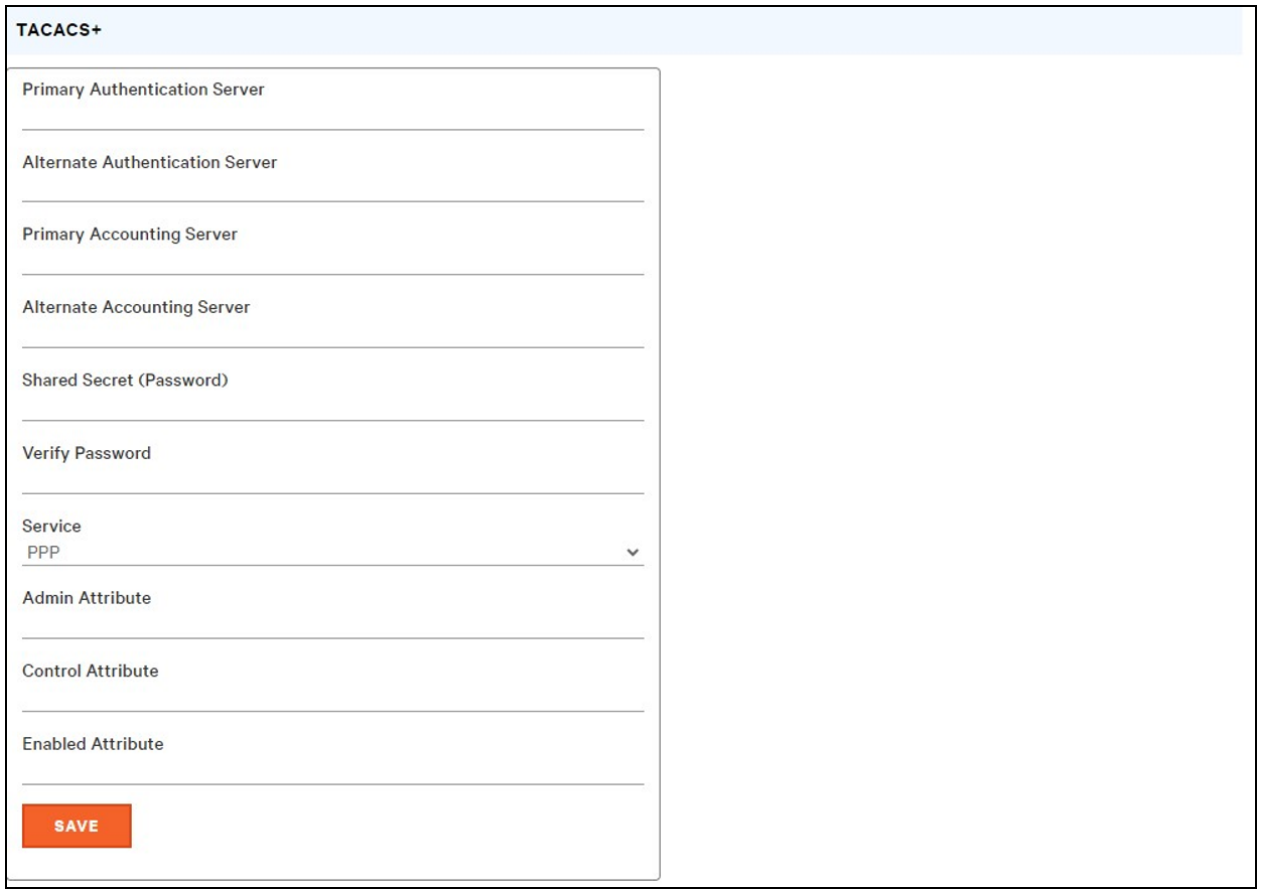
TACACS+

A través de este menú, se puede configurar el sistema de control de acceso del controlador de acceso a terminales plus (TACACS+).

NOTA: Para configurar el dispositivo de RTS Vertiv™ Geist™ para este protocolo de autenticación remota, es necesario conocer la configuración del servidor TACACS+. Si no está familiarizado con esta configuración, consulte al administrador del servidor TACACS+.

Configuración para la autenticación remota mediante TACACS+.

Figura 5.49 Menú TACACS+



- Primary Authentication Server: el servidor de autenticación/autorización primario, que puede ser una dirección IPv4, una dirección IPv6 entre corchetes (por ejemplo, *[2001:0DB8:AC10:FE01::]*) o un nombre de host. Se utiliza tanto para la autenticación como para la autorización. El ingreso de este nombre/dirección de host del servidor AA es obligatorio.
- Alternate Authentication Server: el servidor de autenticación/autorización alternativo, que puede ser una dirección IPv4, una dirección IPv6 entre corchetes o un nombre de host. Se utiliza tanto para la autenticación como para la autorización.
- Primary Accounting Server: el servidor de cuentas primario, que puede ser una dirección IPv4, una dirección IPv6 entre corchetes o un nombre de host. Este valor es opcional. Si se configura, se notifica al servidor cuando se autoriza a un usuario.
- Alternate Accounting Server: el servidor de cuentas alternativo, que puede ser una dirección IPv4, una dirección IPv6 entre corchetes o un nombre de host. Este valor es opcional. Si se configura, se notifica al servidor cuando se autoriza a un usuario.
- Shared Secret (Password): ingrese una palabra o frase de contraseña en el campo Shared Secret (se aplica tanto a los servidores de autenticación y cuentas primarios como a los secundarios).
- Service: el valor que se debe utilizar para el campo de servicio en las solicitudes TACACS+. Las opciones válidas son *PPP* y *raccess*.
- Admin Attribute: los usuarios con este atributo tendrán privilegios *admin*, como se describe en la sección "Página *Users*" de este manual. Los usuarios de TACACS+ no cuentan para calcular el número mínimo de usuarios de administración requeridos.

- Control Attribute: los usuarios con este atributo tendrán privilegios de control, como se describe en la sección "Página *Users*" de este manual.
- Enabled Attribute: los usuarios con este atributo tendrán privilegios de solo visualización, como se describe en la sección "Página *Users*" de este manual.

Haga clic en *SAVE*.

NOTA: Los pares atributo-valor (AVP) que devuelve el servidor durante la autenticación/autorización determinan los permisos del usuario. El campo Group Attribute indica al sistema qué AVP contiene el grupo de acceso del usuario. Si el valor de AVP coincide con el campo Admin Group, el usuario tiene acceso *Admin* (completo). Si el valor de AVP coincide con el campo Control Group, el usuario tiene acceso *Control*. Si el valor de AVP coincide con el campo Enabled Group, el usuario tiene acceso *View-Only*. Si no se encuentran coincidencias, el usuario no tendrá acceso a la unidad. El campo *Group* sin ningún valor no coincidirá con ningún AVP.

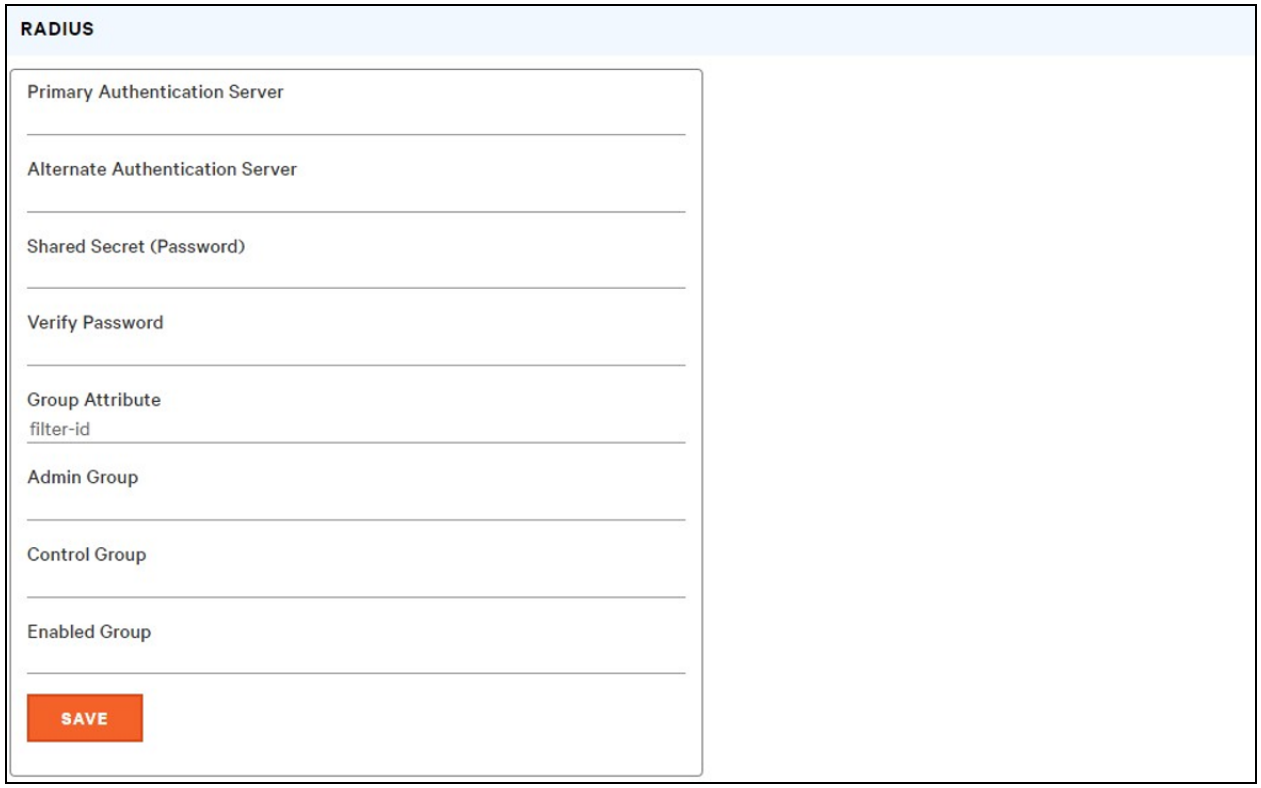
RADIUS

El protocolo de servicio de autenticación remota telefónica de usuarios (RADIUS) se puede configurar a través de este menú.

NOTA: Para configurar el dispositivo de RTS Vertiv™ Geist™ para este protocolo de autenticación remota, es necesario conocer la configuración del servidor RADIUS. Si no está familiarizado con esta configuración, consulte al administrador del servidor RADIUS.

Configuración para la autenticación remota mediante RADIUS.

Figura 5.50 Menú RADIUS



- Primary Authentication Server: introduzca la dirección IP del servidor primario de autenticación/autorización/cuentas. El servidor de autenticación primario puede ser una dirección IPv4, una dirección IPv6 entre corchetes (p. ej., *[2001:0DB8:AC10:FE01::]*) o un nombre de host. El servidor de autenticación primario se utiliza para autenticación, autorización y cuentas. Este servidor AA es obligatorio.
- Alternate Authentication Server: si corresponde, ingrese la dirección IP del servidor alternativo de autenticación/autorización/contabilidad. El servidor de autenticación alternativo puede ser una dirección IPv4, una dirección IPv6 entre corchetes o un nombre de host. El servidor de autenticación secundario se utiliza para autenticación, autorización y cuentas.
- Shared Secret (Password): ingrese una palabra o frase de contraseña en el campo Shared Secret (se aplica tanto a los servidores de autenticación y cuentas primarios como a los secundarios).
- Group Attribute: identifica el par de atributo-valor (AVP) que indica a qué grupo de acceso pertenece el usuario. Los valores válidos son *filter-id* y *management-privilege-level*.
- Admin Group: un usuario perteneciente a este grupo tiene privilegios de administrador, como se describe en la sección "Página *Users*" de este manual.
- Control Group: los usuarios pertenecientes a este grupo tienen privilegios de control, como se describe en la sección "Página *Users*" de este manual.
- Enabled Group: los usuarios pertenecientes a este grupo tienen privilegios de solo visualización Enabled, como se describe en la sección "Página *Users*"de este manual.

Haga clic en *SAVE*.

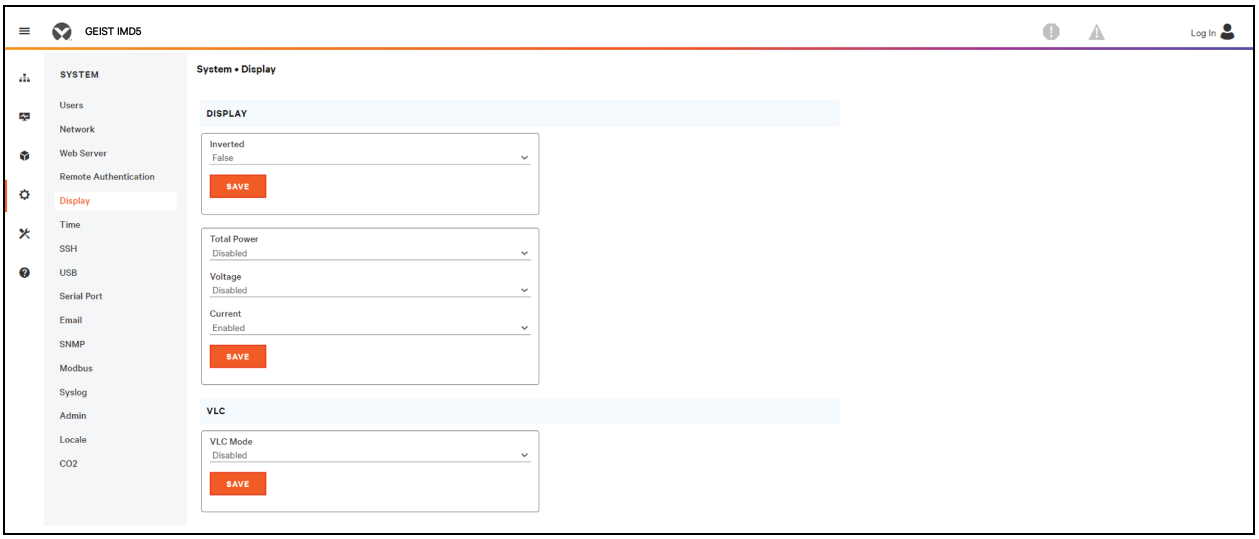
NOTA: Los pares atributo-valor (AVP) que devuelve el servidor durante la autenticación/autorización determinan los permisos del usuario. El campo Group Attribute indica al sistema qué AVP contiene el grupo de acceso del usuario. Si el valor de AVP coincide con el campo Admin Group, el usuario tiene acceso *Admin* (completo). Si el valor de AVP coincide con el campo Control Group, el usuario tiene acceso *Control*. Si el valor de AVP coincide con el campo Enabled Group, el usuario tiene acceso *View-Only*. Si no se encuentran coincidencias, el usuario no tendrá acceso a la unidad. El campo *Group* sin ningún valor no coincidirá con ningún AVP.

5.7.5 Pantalla

La configuración de la pantalla de la unidad puede modificarse a través de la ficha *Display* del menú *System*. Los ajustes relativos a la pantalla de la unidad son:

- *Inverted*: cuando es verdadero, la pantalla local se invierte 180 grados
- *Total Power*: aparece en la pantalla local cuando está habilitado (se muestra como kW).
- *Voltage*: aparece en la pantalla local cuando está habilitado.
- *Current*: aparece en la pantalla local cuando está habilitado.
- *VLC*: permite al usuario habilitar o deshabilitar el modo VLC desde la GUI (de forma predeterminada está deshabilitado).

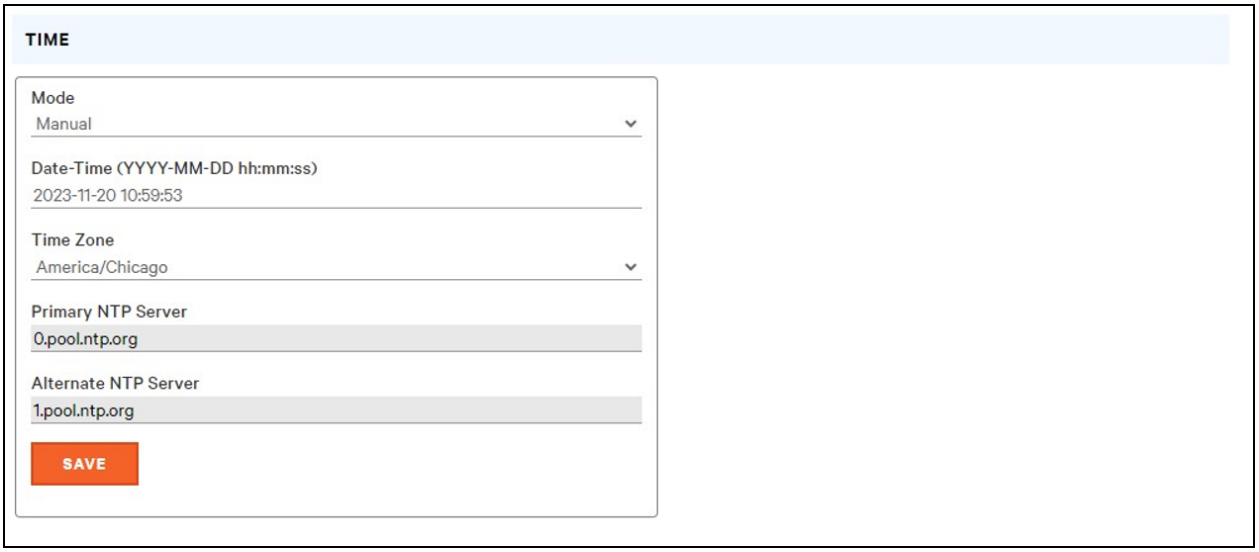
Figura 5.51 Página de configuración del modo de pantalla/VLC



5.7.6 Time

En esta página se establecen la fecha y hora de la unidad.

Figura 5.52 Página de configuración de fecha y hora



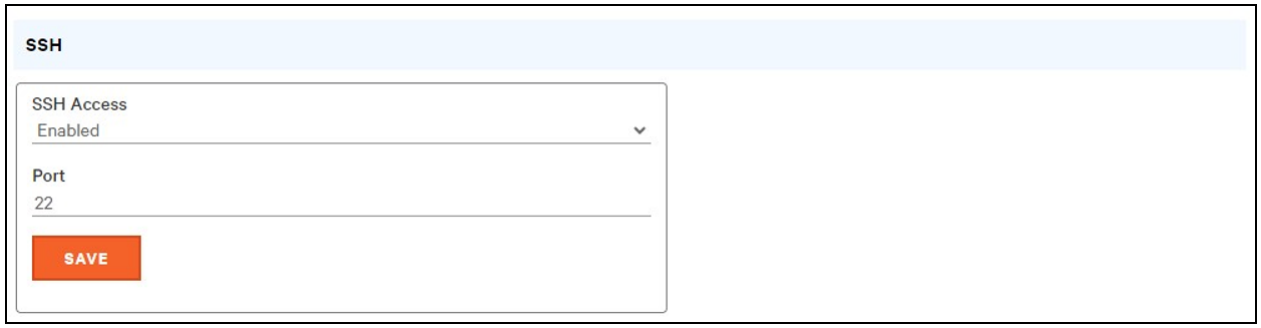
Hay dos modos disponibles:

- Network Time Protocol (NTP): sincroniza la hora y la fecha de la unidad con la zona horaria especificada utilizando los servidores NTP de la lista. Los servidores NTP se pueden reconfigurar.
- Manual: en este modo, la fecha y la hora se deben escribir como se indica a la izquierda del campo.

5.7.7 SSH

El menú SSH permite configurar los parámetros para el acceso SSH al dispositivo.

Figura 5.53 Página *SSH Configuration*



- SSH Access: habilita o deshabilita el acceso a través de SSH.
- SSH Port: permite cambiar el puerto al que el servicio SSH escucha para las conexiones entrantes. El puerto predeterminado es el 22.

NOTA: Las sesiones de los usuarios SSH se cerrarán automáticamente tras 10 minutos de inactividad.

5.7.8 USB

Para habilitar o deshabilitar el puerto USB:

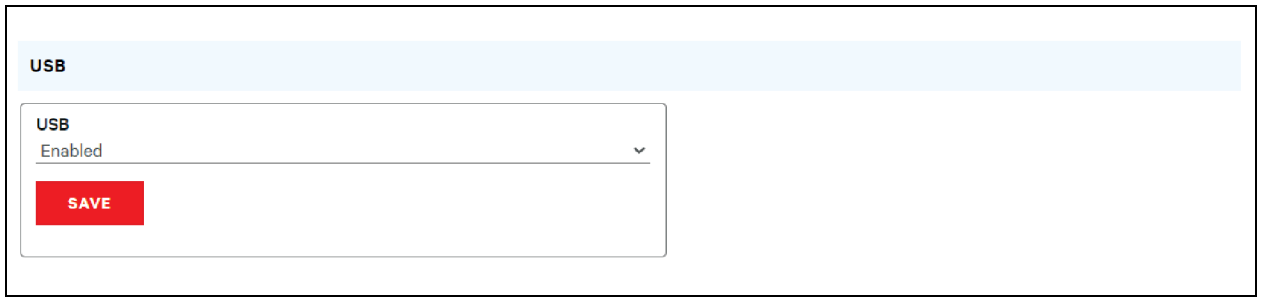
1. Seleccione *Enable* o *Disable* en el menú desplegable.
2. Haga clic en el botón *SAVE*.

Cuando el puerto USB está habilitado, los dispositivos USB conectados se muestran en la interfaz web.

NOTA: El dispositivo USB debe tener formato FAT32.

Si se detecta un dispositivo de almacenamiento USB válido y se están registrando datos históricos, estos datos también se almacenan en un archivo en la unidad de almacenamiento USB. Si aún no existe, se crea un archivo llamado log-1.csv bajo un directorio log en el nivel superior del sistema de archivos. Si ya existen archivos de registro, se utiliza como punto de partida el que tiene el identificador numérico más alto en el título. Cada periodo de registro, se agregan nuevos datos a este archivo en el mismo formato que la recuperación CSV. Si se crean o eliminan puntos de datos en relación con los enumerados en el encabezado CSV, se crea un nuevo archivo cuyo nombre incluirá el siguiente número secuencial. Si el sistema de archivos se llena, este proceso de registro se interrumpirá.

Figura 5.54 USB



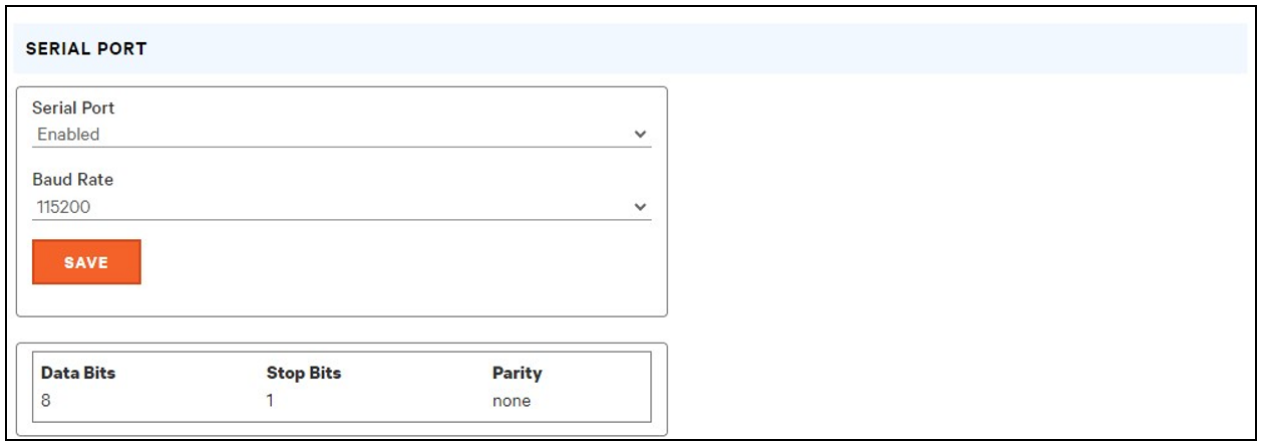
5.7.9 Puerto serie

NOTA: La conexión en serie no permite el control de flujo.

El menú *Serial Port* permite configurar los ajustes del puerto serie, habilitar o deshabilitar el puerto, y establecer la velocidad en baudios.

1. Haga clic en el menú desplegable *Serial Port* y seleccione *Enabled/Disabled*.
2. Haga clic en el menú desplegable *Baud Rate* y seleccione el valor de *Baud Rate*.
3. Haga clic en *SAVE*.

Figura 5.55 Menú desplegable del sistema: *Serial Port*



5.7.10 Email

La unidad tiene capacidad para enviar notificaciones de correo electrónico a un máximo de diez (10) direcciones de correo electrónico cuando se produce un evento de alarma o de advertencia.

Figura 5.56 Página *Email Configuration*

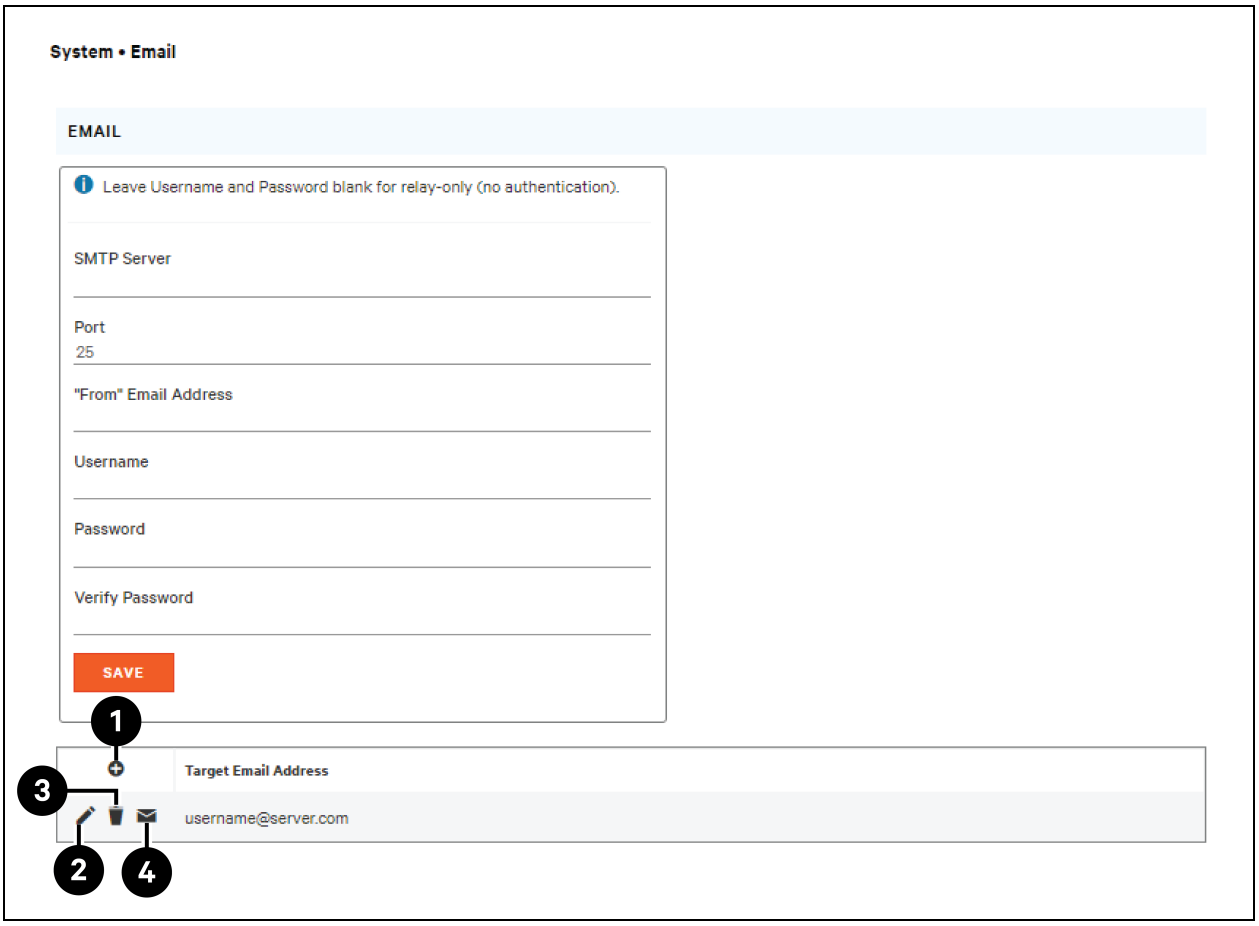


Tabla 5.10 Descripciones de la página *Email Configuration*

Elemento	Descripción
1	Agregar nueva dirección de correo electrónico de destino.
2	Modificar dirección de correo electrónico de destino existente.
3	Eliminar dirección de correo electrónico de destino existente.
4	Enviar correo electrónico de prueba.

Para enviar correos electrónicos, la unidad debe estar configurada para acceder al servidor de correo, de la siguiente manera:

- *SMTP Server*: el nombre o la dirección IP de un servidor SMTP o ESMTP adecuado.
- *Port*: el puerto TCP que el servidor SMTP utiliza para proporcionar servicios de correo. Los valores típicos serían Port 25 para una conexión no cifrada o 465 y 587 para una conexión cifrada mediante TLS/SSL, pero estos pueden variar dependiendo de la configuración del servidor de correo.
- *"From" Email Address*: dirección de la que parecen proceder los correos electrónicos de la unidad. Muchos servicios de correo electrónico hospedados, como Gmail, requieren que sea la cuenta de correo electrónico de un usuario válido.
- *Username and Password*: las credenciales de inicio de sesión para el servidor de correo electrónico. Si el servidor no requiere autenticación (relé abierto), pueden dejarse en blanco.

Los servidores de Microsoft Exchange deben estar configurados para permitir el relé SMTP desde la dirección IP de la unidad. Además, el servidor de Exchange debe estar configurado para permitir una autenticación básica, de modo que la unidad pueda iniciar sesión con el método AUTH LOGIN para enviar sus credenciales de inicio de sesión. Otros métodos, como AUTH PLAIN y AUTH MD5 no son compatibles.

Para agregar o modificar una dirección de correo electrónico de destino:

1. Haga clic en el ícono *Add or Modify*.
2. Ingrese la dirección de correo electrónico y luego haga clic en *Save*.

Para eliminar una dirección de correo electrónico de destino:

1. Haga clic en el ícono *Delete* situado junto a la dirección que desee eliminar.
2. Haga clic en *Delete* en la ventana emergente para confirmar.

Para enviar un correo electrónico de prueba:

1. Haga clic en el ícono *Test email* situado junto a la característica que desee probar.
2. Una ventana emergente indica que se está enviando el correo electrónico de prueba; haga clic en *OK* para descartar la ventana emergente.

5.7.11 *SNMP*

El protocolo simple de administración de red (SNMP) se puede usar para monitorear las mediciones y el estado de la unidad. Se admiten SNMP V1, V2c y V3. Además, se pueden enviar trampas de alarma a un máximo de diez direcciones IP.

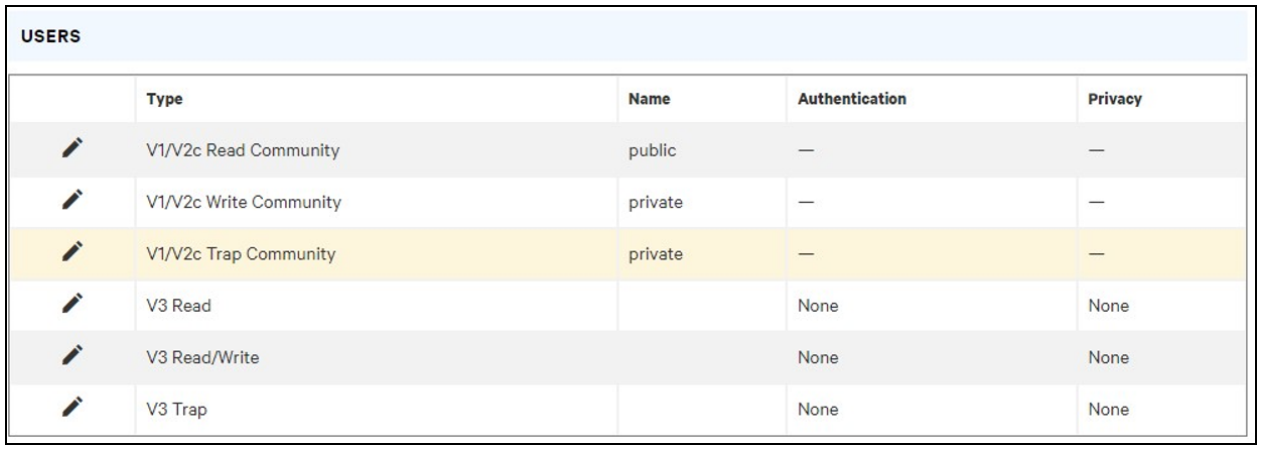
Haga clic en *ZIP* para descargar el archivo *mib.zip* que contiene tanto el archivo MIB como la hoja de cálculo con formato CSV.

El servicio de SNMP-V1/V2c y SNMP-V3 se puede habilitar o deshabilitar de forma independiente. El servicio escucha las solicitudes de lectura de datos en el puerto 161, que es el valor predeterminado habitual para los servicios SNMP. Esto también se puede cambiar.

La Base de datos de información de administración (MIB) se puede descargar desde la unidad a través del enlace al archivo ZIP en la parte superior de la página web. Al hacer clic en este vínculo, se descarga un archivo .Zip que contiene tanto el archivo MIB como una hoja de cálculo en formato CSV que describe los OID disponibles en lenguaje natural para ayudarlo a ajustar su administrador SNMP para que lea los datos de la unidad.

Figura 5.57 Página *SNMP Configuration*

Figura 5.58 Página *SNMP Users Configuration*



La sección *Users* permite configurar las distintas comunidades *Read*, *Write* y *Trap* para los servicios SNMP. Si lo desea, también puede configurar los tipos de autenticación y los métodos de cifrado que se utilizan para SNMP V3. Haga clic en el ícono *Modify* para cambiar la configuración.

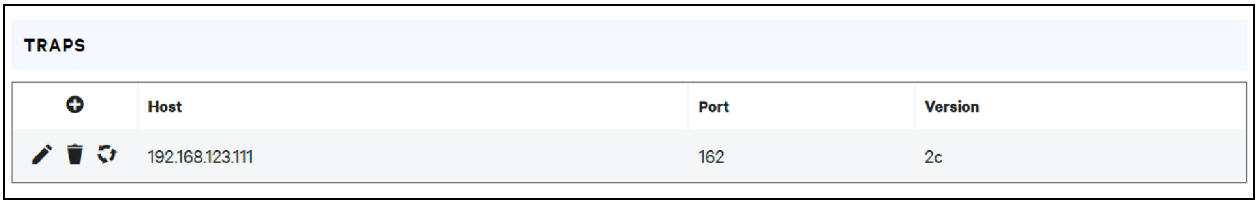
Las trampas permiten definir los tipos de SNMP que desea enviar y las direcciones IP de los destinatarios.

Para configurar un destino de trampa:

1. Localice la sección *Traps* de la página SNMP y haga clic en el ícono Add.
2. Introduzca la dirección IP a la que se debe enviar la trampa en el campo *Host*.
3. Si lo desea, cambie el número de puerto.
4. Seleccione la versión de la trampa que se utilizará (V1, V2c o V3) y haga clic en *SAVE*.

Se puede enviar una trampa de prueba haciendo clic en el ícono *Test* junto a la dirección IP del host. También puede actualizar/cambiar los ajustes de *Trap*. Haga clic en el ícono *Modify* junto a la dirección IP del host.

Figura 5.59 *Trap*



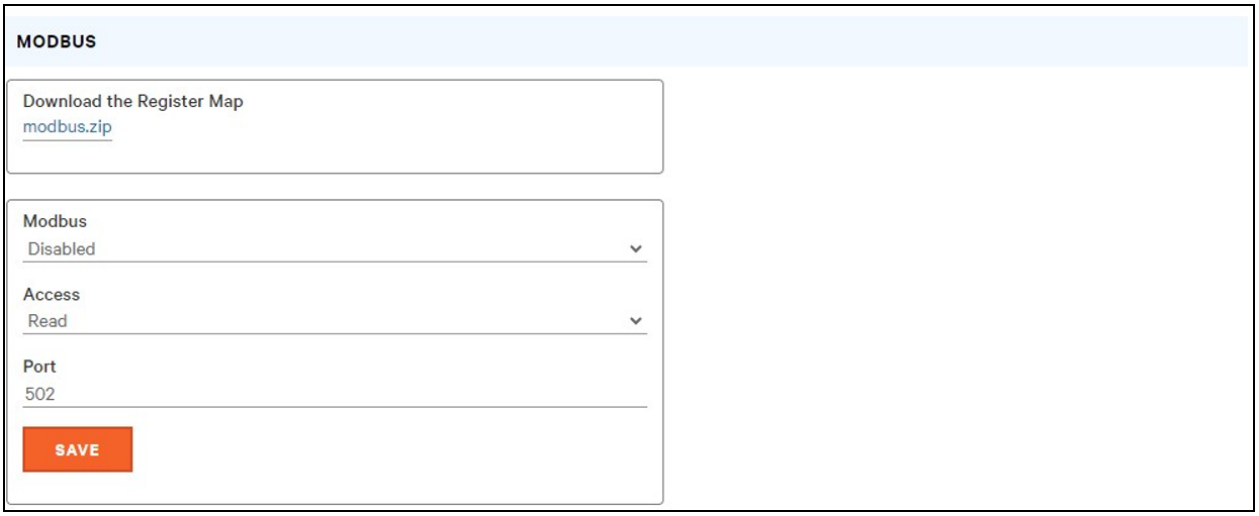
5.7.12 Modbus

El protocolo de comunicación Modbus TCP se puede usar para monitorear las mediciones y el estado de la unidad. También permite al usuario ajustar la configuración de la unidad.

El mapa de registro se puede descargar desde la unidad a través del vínculo ZIP en la parte superior de la página web. Al hacer clic en este vínculo, se descarga un archivo .zip que contiene una hoja de cálculo en formato CSV que describe la asignación Modbus disponibles en lenguaje legible para el ser humano para ayudarlo a ajustar su administrador Modbus para que lea/escriba los datos en la unidad.

El protocolo de comunicación Modbus se puede activar o desactivar. El acceso de Modbus a la unidad puede ser *Read* o *Read/Write*, según sea para lectura o para lectura y escritura. Las solicitudes de lectura o escritura de datos se realizan en el puerto 502, que es el parámetro predeterminado habitual para el protocolo Modbus; este puerto también se puede cambiar.

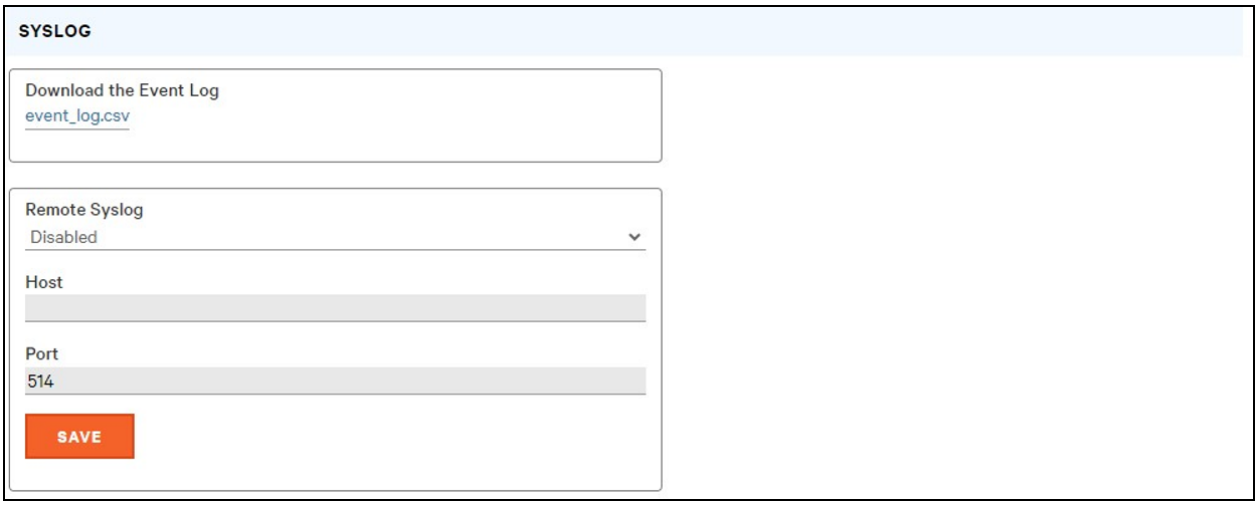
Figura 5.60 Modbus



5.7.13 *Syslog*

Los datos de Syslog se pueden capturar de forma remota, pero primero se deben configurar y habilitar a través de la página SYSLOG.

Figura 5.61 SYSLOG



NOTA: Esta función es principalmente útil para fines de diagnóstico y normalmente debe dejarse deshabilitada, a menos que la asistencia técnica de Vertiv aconseje habilitarla para resolver problemas específicos.

Para poder usar el botón *Download the Event Log CSV*, el usuario debe tener acceso de administrador.

5.7.14 Página *Admin*

La página *Admin* permite al administrador del dispositivo guardar su información de contacto junto con la descripción y la ubicación del dispositivo. En cuanto un administrador guarde la información, otros usuarios (no administradores) podrán verla. Además, en esta página se puede modificar la etiqueta *System Label*. Esta etiqueta suele aparecer en la barra de título de la ventana del navegador web o en las pestañas del navegador en el que se está viendo el dispositivo.

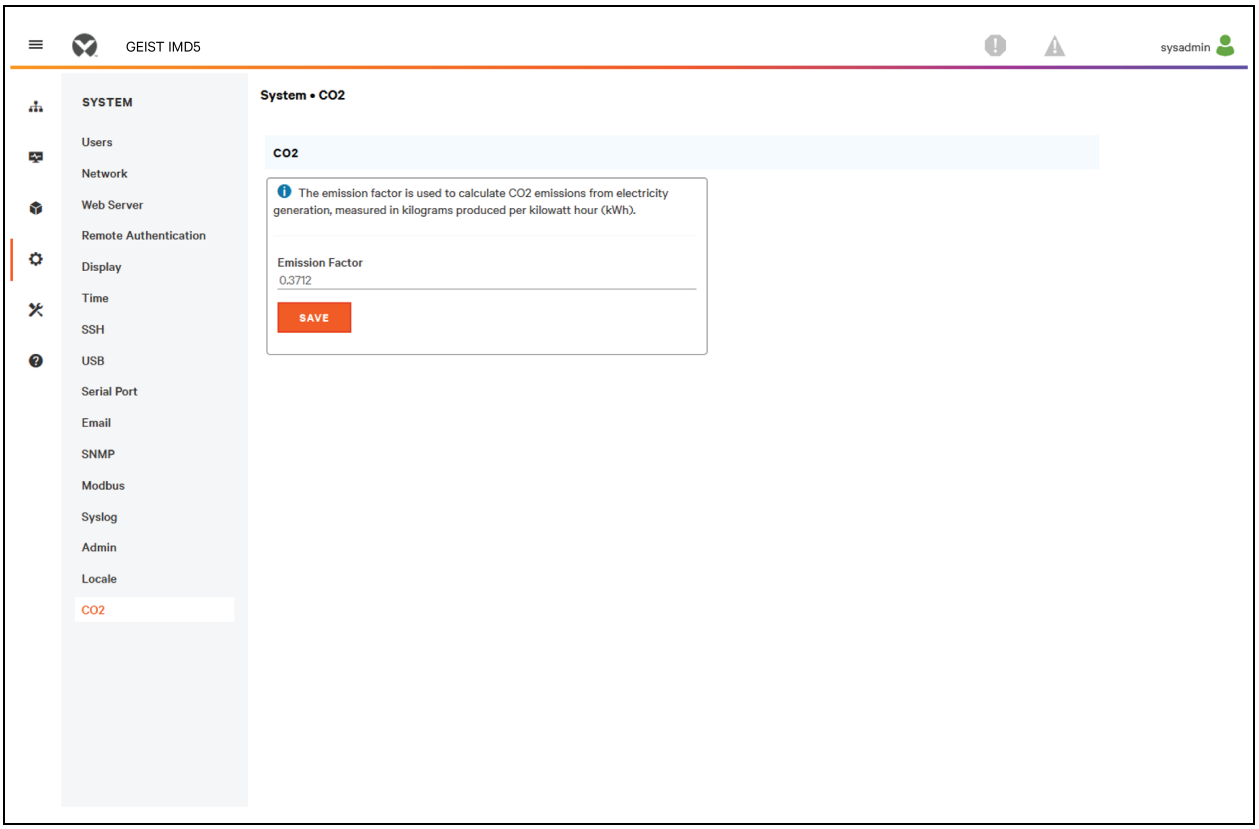
5.7.15 Página *Locale*

La página *Locale* establece el idioma y las unidades de temperatura predeterminados para el dispositivo. Esta configuración se convertirá en las opciones de visualización predeterminadas del dispositivo, aunque los usuarios individuales pueden cambiar estas opciones para sus propias cuentas. La cuenta de invitado solo podrá ver el dispositivo con las opciones establecidas aquí.

5.7.16 CO2

La página CO2 permite al usuario guardar el factor de emisión. El factor de emisión se utiliza para calcular las emisiones de CO2 procedentes de la generación de electricidad, medidas en kilogramos producidos por kilovatio hora (kWh).

Figura 5.62 CO2



5.8 Submenú *Utilities*

El submenú *Utilities* del menú *System* ofrece la posibilidad de restaurar los valores predeterminados, reiniciar el sistema de comunicación y realizar actualizaciones de firmware.

5.8.1 Página *Configuration Backup and Restore*

Guarde los ajustes de la configuración actual y restaure los ajustes de la configuración anterior, si es necesario.

Tabla 5.11 Opciones de copia de seguridad y restauración

Opción	Descripción
Página *Download Configuration Backup File*	Las descargas no requieren autenticación del usuario. El nombre del archivo descargado es **backup_XXX.bin**, donde XXX es una representación de cadena de la dirección MAC para la interfaz **Ethernet** de la unidad sin los caracteres :.
Página *Backup File*	Carga el archivo de copia de seguridad de configuración. Se requiere autenticación del usuario, y el usuario debe tener privilegios de administrador. Un archivo de copia de seguridad solo se puede usar para cargar la configuración en unidades con el mismo número de modelo.

Para guardar los ajustes de la configuración actual:

1. Seleccione *Download Configuration Backup File*.

2. Haga clic en *BIN*.

NOTA: Para guardar la configuración no se requiere la autenticación del usuario.

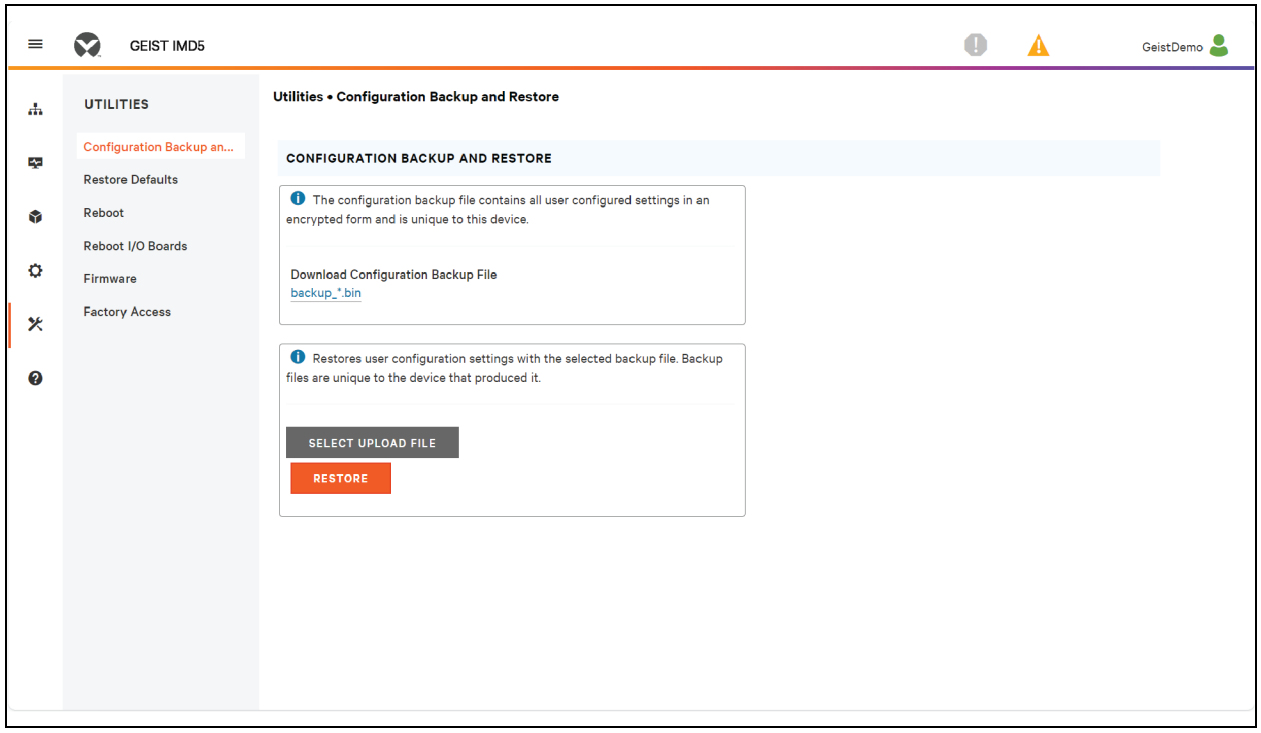
Para restaurar los ajustes de la configuración actual:

1. Haga clic en *Backup File*.
2. Haga clic en *SELECT UPLOAD FILE*.
3. Seleccione el archivo de copia de seguridad.
4. Haga clic en *RESTORE*.

NOTA: Para restaurar la configuración, se requiere autenticación del usuario, y el usuario debe tener privilegios de administrador.

NOTA: Un archivo de copia de seguridad solo se puede usar para cargar la configuración en unidades con el mismo número de modelo.

Figura 5.63 Información general de copia de seguridad y restauración de la configuración



5.8.2 Página *Restore defaults*

Permite restaurar los ajustes predeterminados.

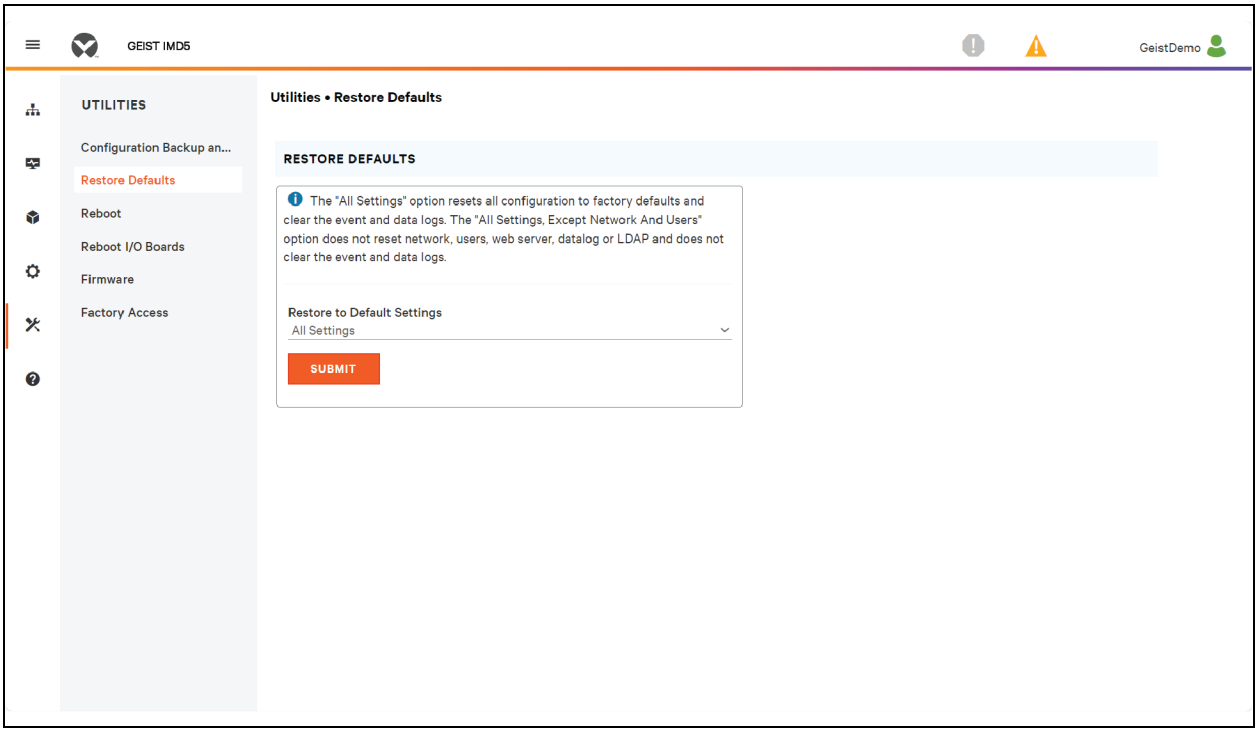
Tabla 5.12 Opciones de *Restore Defaults*

Opción	Descripción
Página *All Settings*	Restablece toda la configuración de /conf, /alarm y /dev a los valores de fábrica. También se borrarán el registro de eventos y el registro de datos, y se ejecutará el comando de eliminación en cualquier dispositivo con estado **unavailable**. Esto hará que partes del sistema se reinicialicen. Se realizará correctamente y le seguirá un breve periodo en el que no se podrá acceder al sistema.
Página *All Settings, Except Networks And Users*	Como la opción **defaults** anterior, pero no restablece /conf/network, /conf/http, /conf/datalog, /auth ni /conf/ldap, y no borra el registro de eventos ni el registro de datos. Esto hará que partes del sistema se reinicialicen. Se realizará correctamente y le seguirá un breve periodo en el que no se podrá acceder al sistema.

Para restaurar la configuración predeterminada:

1. Seleccione una de las opciones *All Settings* o *All Settings, Except Networks And Users* en el menú desplegable.
2. Haga clic en *SUBMIT*.

Figura 5.64 Información general de *Restore defaults*



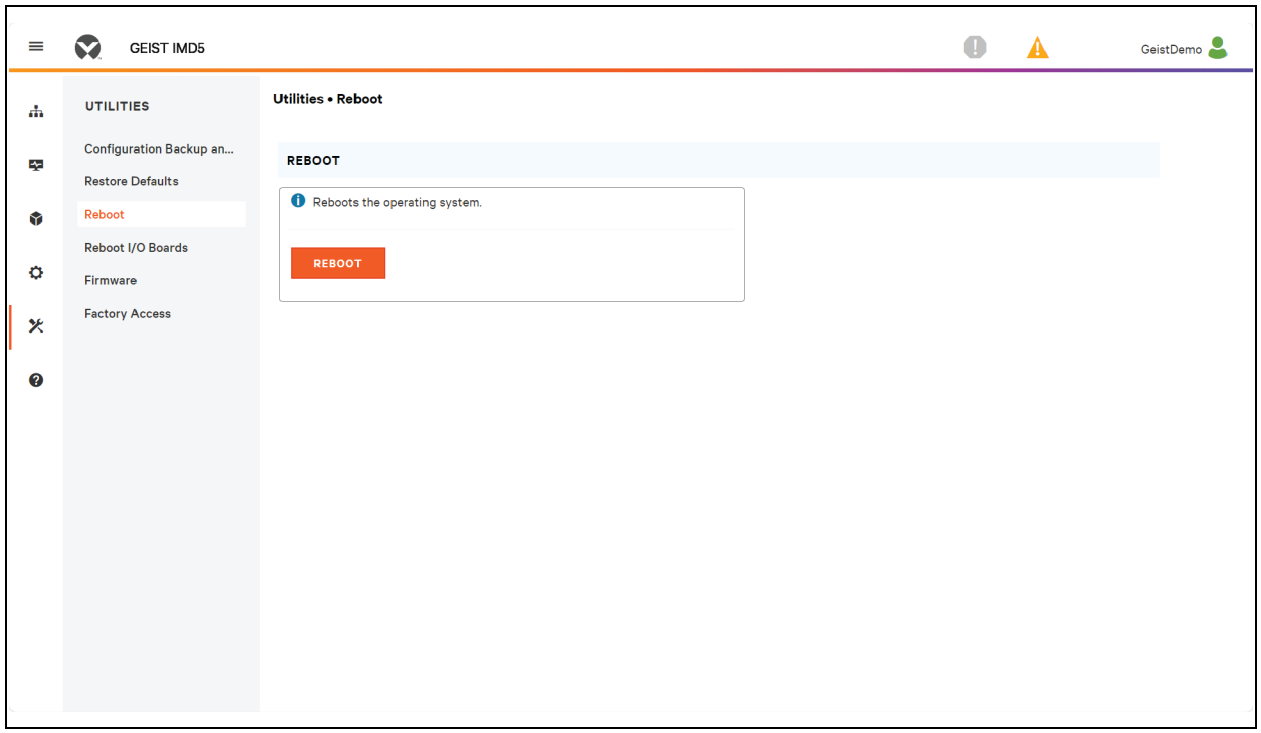
5.8.3 Página *Reboot*

Permite reiniciar el sistema operativo. Restablece el procesador del IMD, lo que hace que el IMD se reinicie.

Haga clic en *REBOOT* para reiniciar el sistema operativo.

NOTA: La potencia de los dispositivos conectados no se ve afectada.

Figura 5.65 Información general de la página *Reboot*



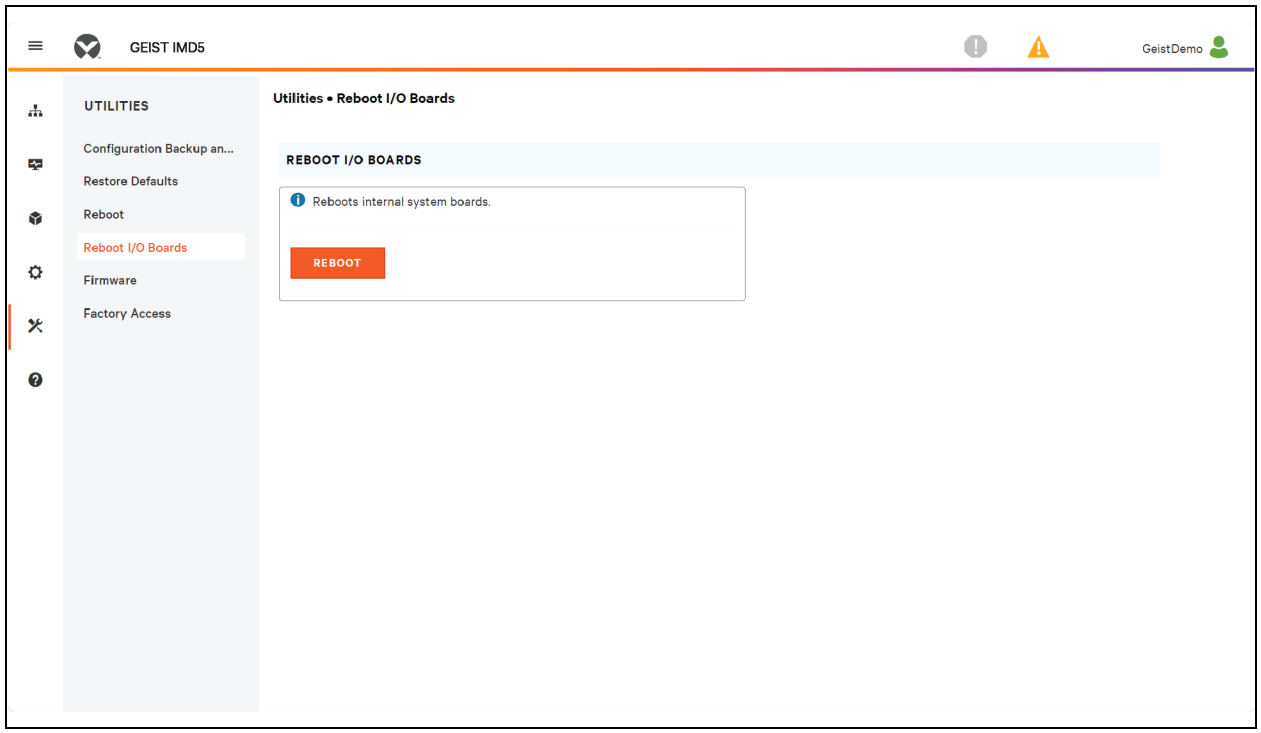
5.8.4 Página *Reboot I/O Boards*

Si el conmutador de transferencia de rack Vertiv™ Geist™ no responde o no muestra todos los valores, el reinicio de las placas internas hará que se reinicie el sistema. De este modo, se restablecerán los procesadores de la placa de entrada interna y de las placas de los tomacorrientes, lo que hará que se reinicien.

Haga clic en *REBOOT* para reiniciar las placas internas del sistema.

NOTA: La potencia de los dispositivos conectados no se ve afectada.

Figura 5.66 Información general de la página *Reboot I/O Boards*



5.8.5 Actualizaciones del firmware

Carga un archivo de firmware que actualiza el sistema. Esta acción requiere autenticación del usuario, y el usuario debe tener privilegios de administrador. Las actualizaciones de firmware normalmente se incluyen en un archivo .zip que contiene varios archivos, incluido el propio paquete de firmware, una copia del MIB de SNMP, un archivo de texto Léame donde se explica cómo instalar el firmware y varios otros archivos de soporte, según sea necesario. Asegúrese de descomprimir el archivo y siga las instrucciones incluidas.

Para actualizar el firmware a través del archivo del paquete de firmware:

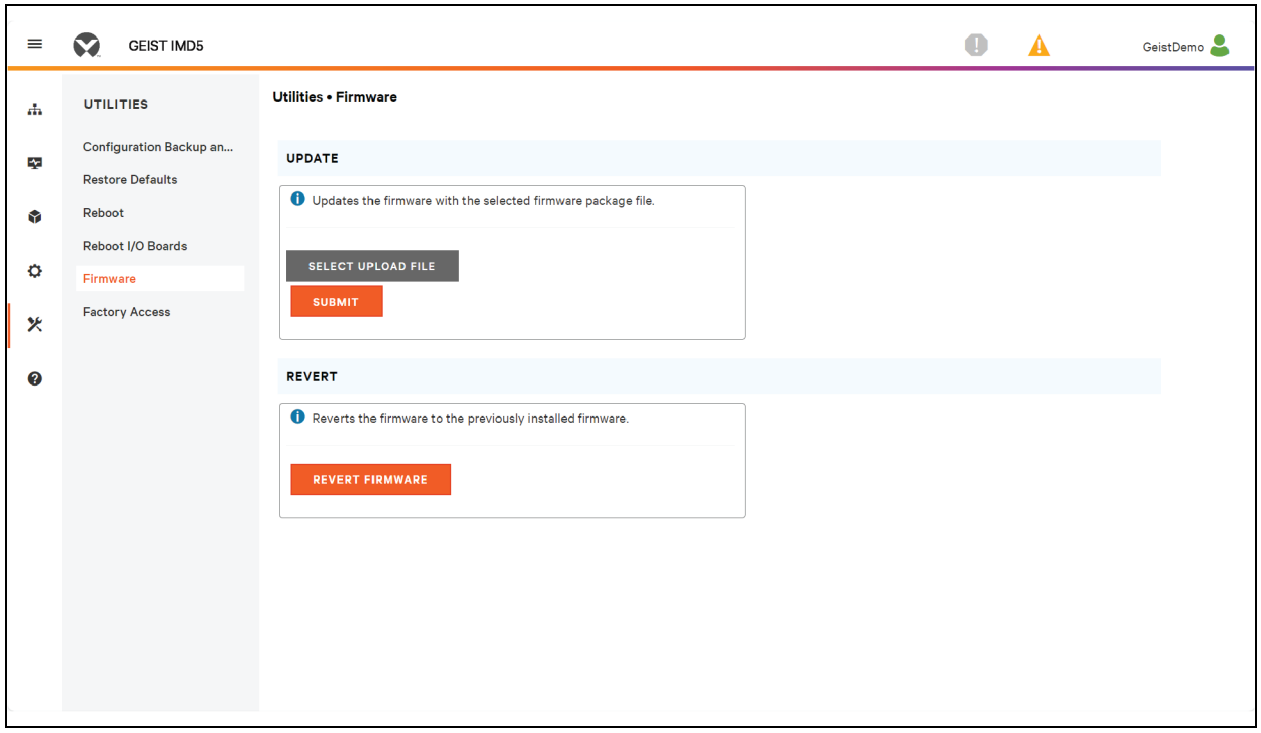
1. Haga clic en *SELECT UPLOAD FILE* y seleccione el archivo .***firmware*** en la ventana *Open*.
2. Haga clic en *SUBMIT*.
3. Si se detecta algún problema (la unidad no se comporta correctamente) después de haber instalado correctamente el firmware, haga clic en *REVERT FIRMWARE*.

Para actualizar el firmware a través de una unidad flash USB:

1. Descargue el firmware más reciente en *https://www.vertiv.com/en-us/support/software-download/power-distribution/geist-upgradeable-series-v5-firmware/* y descomprima la carpeta.
2. Obtenga una unidad flash USB y aplíquele el formato FAT32.
3. Cree un directorio en la unidad flash USB llamado *FIRMWARE* (no es necesario que esté en mayúsculas).
4. Abra la carpeta del firmware descomprimido y copie el archivo .firmware.
5. Pegue este archivo en la carpeta *FIRMWARE* de la unidad flash.
6. Conecte la unidad flash USB en la PDU.

Durante la actualización, el IMD dejará de desplazar datos. Una vez completada la actualización, aparecerá un mensaje de inicio en la pantalla. Después del reinicio, el IMD reanudará el desplazamiento de datos en la pantalla.

Figura 5.67 Información general de *Firmware*



5.8.6 Página *Factory Access*

Factory Access proporciona información para el servicio técnico.

Tabla 5.13 Opciones de *Factory Access*

Opción	Descripción
Download Factory Support Package	Descarga un paquete de diagnóstico cifrado que se puede enviar al personal de asistencia técnica.
Página *Factory Access*	Permite el acceso de fábrica a la unidad a través de SSH (para propósitos de depuración).

Para descargar un paquete de soporte de fábrica:

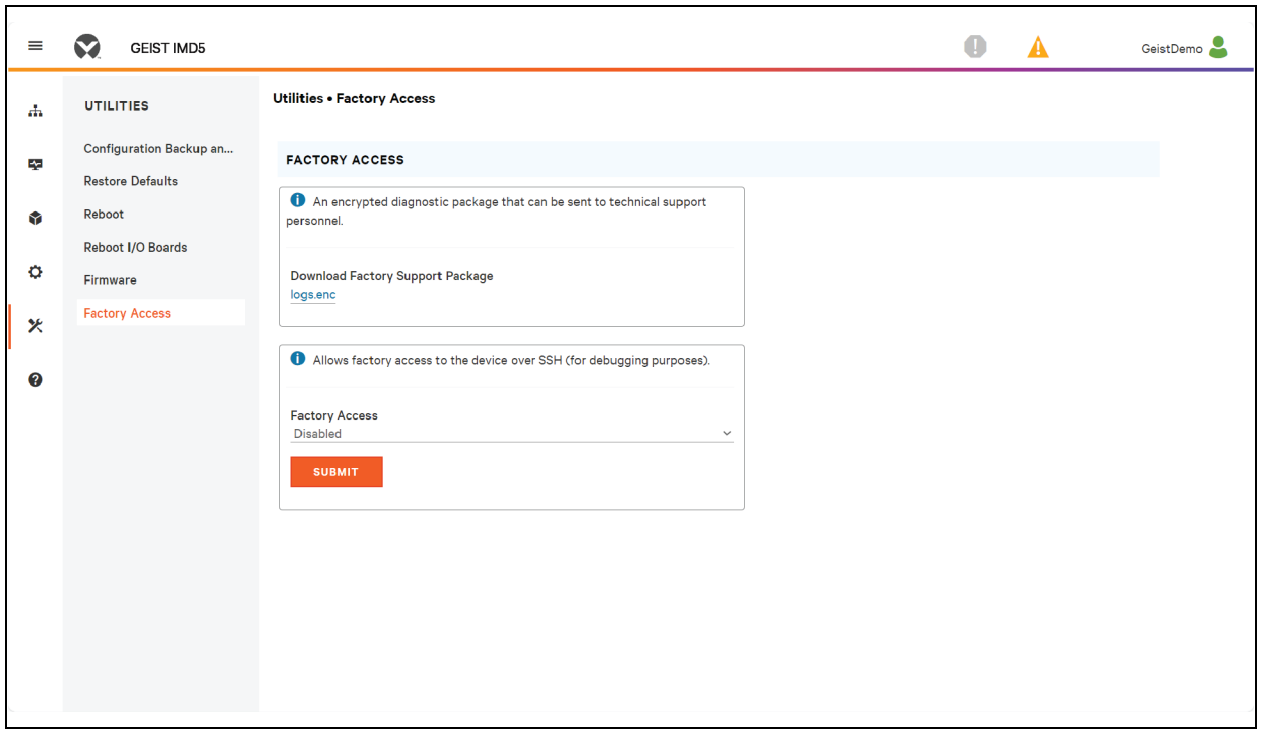
1. Haga clic en *Download Factory Support Package*.
2. Haga clic en *ENC*.

Para habilitar/deshabilitar el acceso de fábrica:

1. Seleccione *Enable* o *Disable* en el menú desplegable.
2. Haga clic en *SUBMIT*.

NOTA: Se requiere autenticación del usuario, y el usuario debe tener privilegios de administrador.

Figura 5.68 Información general de *Factory Access*

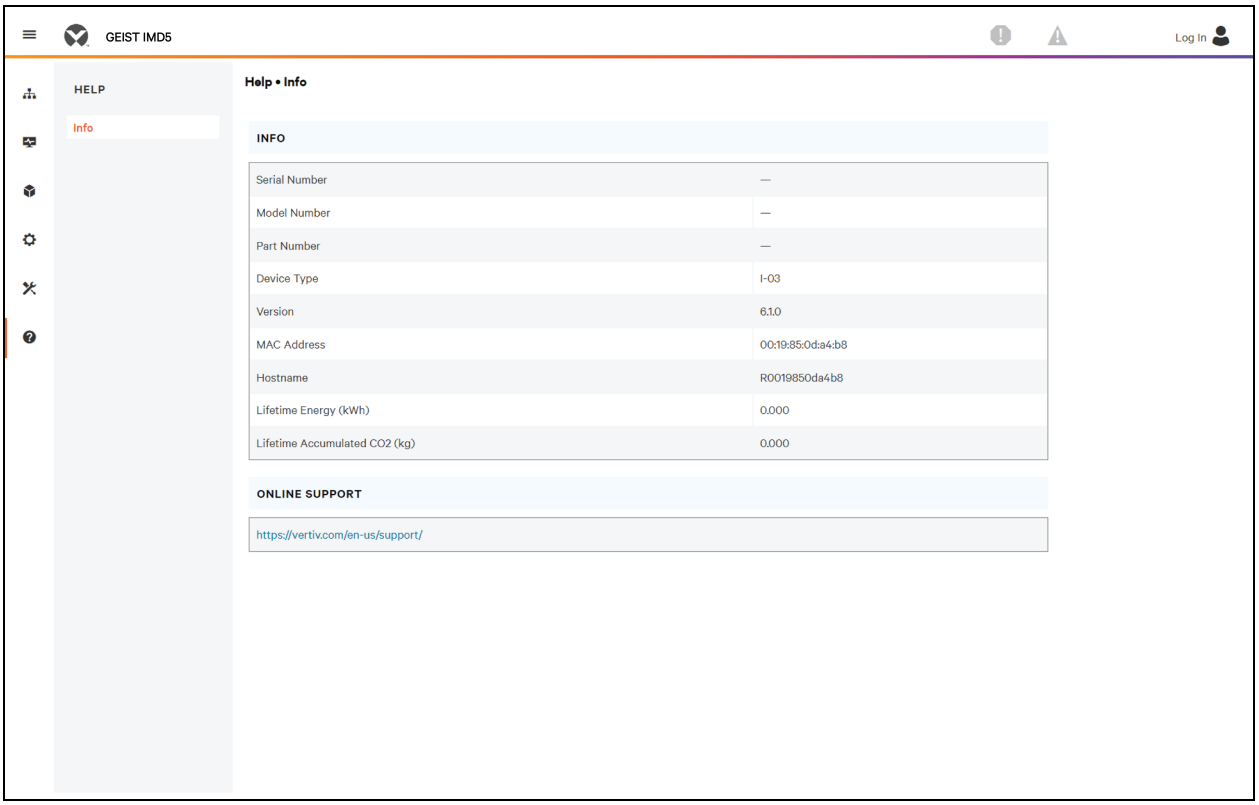


5.9 Submenú *Help*

Página *Info*

La página *Info* muestra la información de configuración actual de la unidad, incluidos el nombre y el ID del dispositivo, el tipo de IMD instalado, la versión del firmware actual de la unidad y la información de red. La información de soporte del fabricante también está aquí.

Figura 5.69 Página *Info*



6 Vertiv™ Intelligence Director

Vertiv Intelligence Director incorpora una capa de visualización única y unificada para pequeñas instalaciones de unidades de RTS/rPDU Vertiv™ Geist™, los UPS de Vertiv™, los sensores medioambientales y los tomacorrientes del RTS Geist™. Una vez instalado, Vertiv Intelligence Director ofrece una funcionalidad mejorada a través del RTS Geist™, no como un dispositivo autónomo, sino como una puerta de acceso para comprender el amplio ecosistema de dispositivos en el que está instalado.

6.1 *Aggregation*

El elemento inicial de Vertiv Intelligence Director, disponible con las unidades de RTS Geist™ que ejecutan la versión de firmware 5.3.0 o posterior, se denomina *Aggregation*. Este elemento único permite lo siguiente:

- Utilizar la agregación para reducir el número de direcciones IP, agregar datos de varias unidades de RTS y permitir la gestión de grupos de tomacorrientes de las PDU para rack.
- Las PDU para rack se conectan mediante una cadena margarita Ethernet, como en el ejemplo de la sección anterior.
- La cabeza del RTS de la cadena está configurada como el gerenciador.
- La red de equipos conectados puede incluir conmutadores de red.
- Se puede utilizar una única dirección IP asignada al gerenciador para acceder hasta a 50 dispositivos (el gerenciador y 49 equipos conectados).
- Los ajustes de red de los equipos conectados se configuran automáticamente.
- El acceso a los equipos conectados se realiza mediante la dirección IP del gerenciador y un número de puerto. El número de puerto se puede obtener desplazándose por la página *Device>List* y desplazando el cursor por encima del dispositivo.
- Los usuarios pueden definir grupos de dispositivos. Por ejemplo, mediante la representación de racks.
- El gerenciador genera medidas agregadas, como la potencia total de grupo y la potencia total, incluidos promedios, mínimos y máximos.
- No se permite la conexión en cadena margarita tolerante a fallas cuando se utiliza Vertiv Intelligence Director.

Figura 6.1 Pestaña *Aggregation*

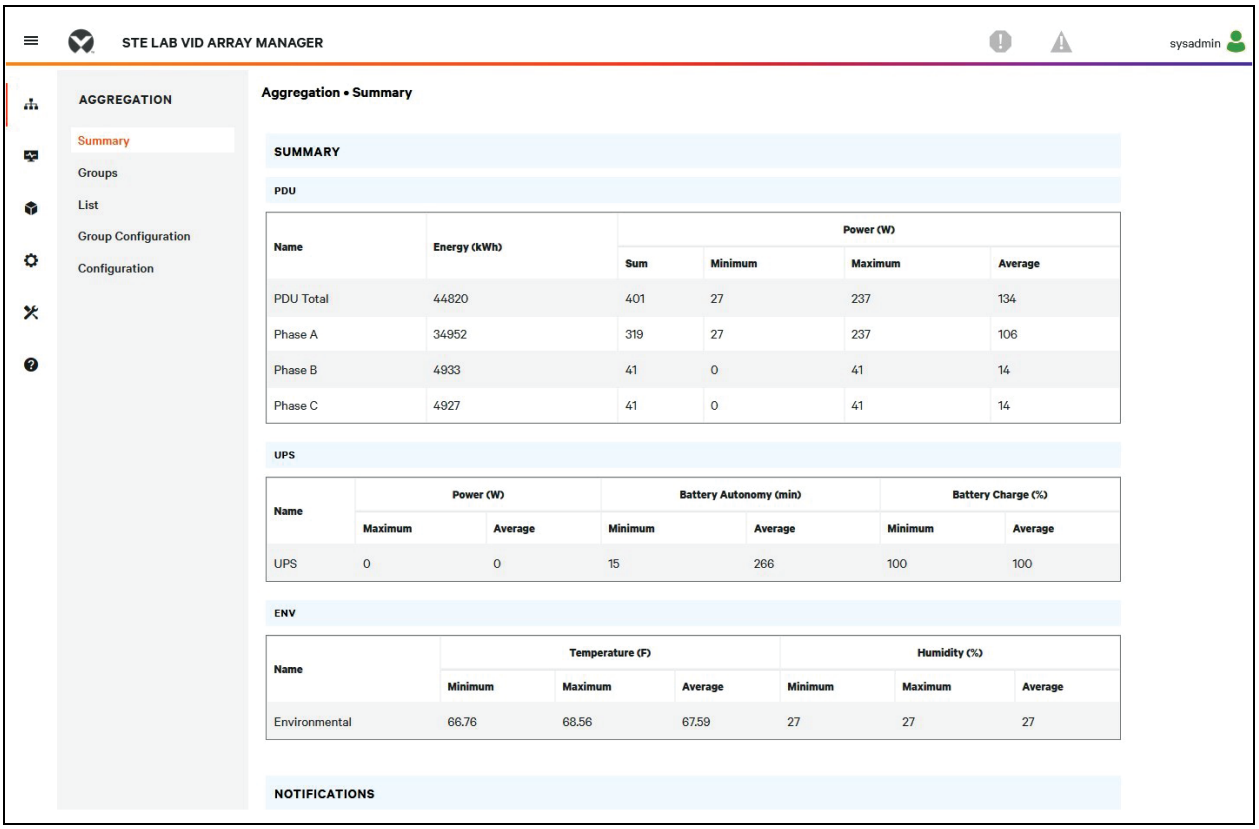
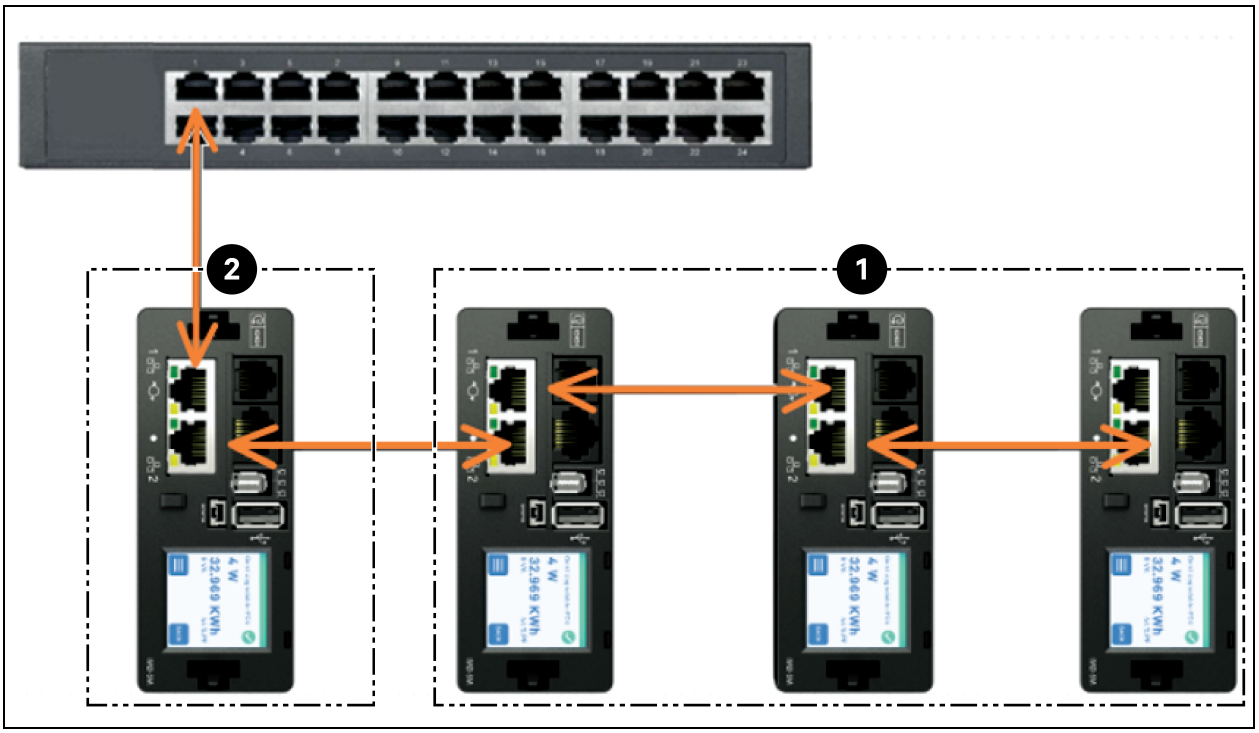


Figura 6.2 Agregación



Elemento	Descripción
1	Equipo conectado
2	Gerenciador

Un elemento adicional de Vertiv Intelligence Director, disponible con las unidades de RTS Vertiv™ Geist™ que ejecutan la versión de firmware 5.7.0 o posterior, es la agrupación de tomacorrientes de PDU para rack. Este elemento permite lo siguiente:

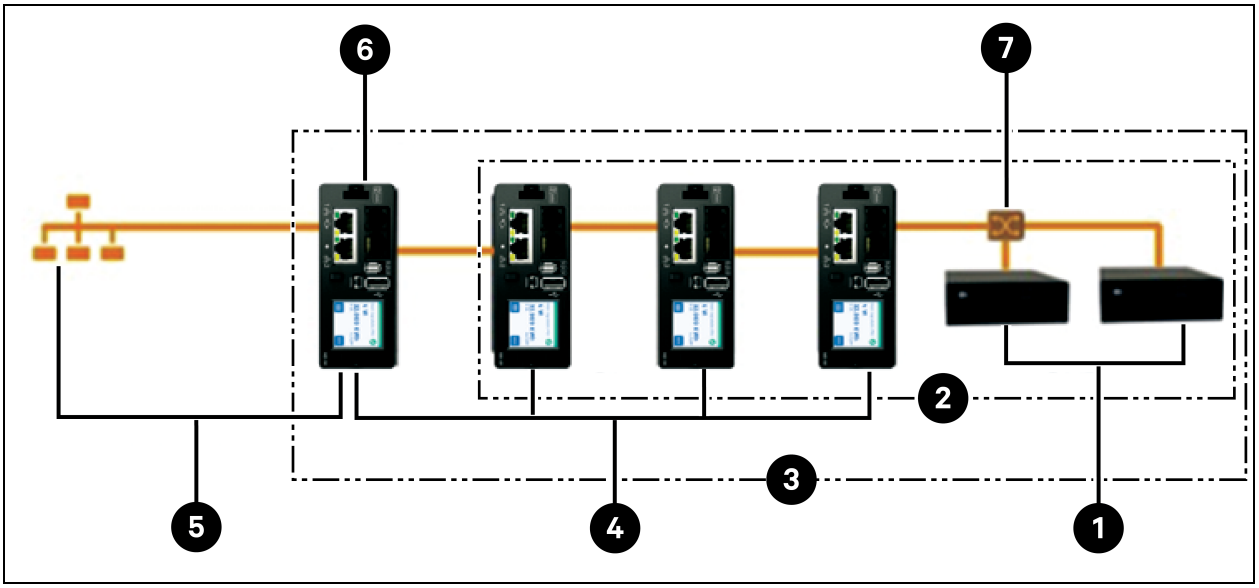
- Crear grupos de tomacorrientes de RTS Geist™ que abarquen una o más unidades de RTS Geist™.
- Notificar la potencia y la energía totales de los grupos de tomacorrientes (con unidades de RTS Geist™ que proporcionan información según las mediciones de los tomacorrientes).
- Ofrecer la posibilidad de apagar, encender o aplicar un ciclo de apagado y encendido del grupo de tomacorrientes con un solo comando (con unidades de RTS Geist™ que permiten la conmutación de tomacorrientes).

Con el firmware 5.10.1 o posterior, la visibilidad completa de los dispositivos de Vertiv Intelligence Director (agregados) está disponible a través de SSH y de las CLI del puerto serie.

6.2 Gerenciador

La agregación requiere la designación de un gerenciador, instalado con PDU para rack Geist™ equipadas con modelos IMD que ejecuten la versión de firmware 6.1.0 o posterior o IMD modelos 3E, 03E, 3E (-S o -G), 03E (-S o -G) o 5M que ejecuten actualmente las versiones de firmware 5.3.0 y posteriores (aunque se recomienda encarecidamente la última versión de firmware). El IMD del gerenciador facilita y configura la red de dispositivos, la matriz interconectada de las rPDU Geist™, los UPS de Vertiv™, los sensores de enfriamiento y entorno del Vertiv™ y los tomacorrientes del conmutador de transferencia de rack Geist™, a la vez que agrega puntos de datos seleccionados de estos dispositivos. También interactúa con la red de administración para su monitoreo y administración propios, así como las de sus equipos conectados.

Figura 6.3 Ejemplo de configuración



Elemento	Descripción
1	Vertiv™ Liebert® GXT4
2	Dispositivos posteriores
3	Red de dispositivos
4	GU
5	Red de gestión
6	Dispositivo maestro (GU2)
7	Conmutador Ethernet

Ya no es posible incorporar nuevas PDU para rack IMD-02x cuando se utiliza un gerenciador con firmware 6.1.0 o posterior.

6.3 Configuración de red

En el lanzamiento inicial de agregación, los equipos conectados se definen como unidades del RTS Vertiv™ Geist™ dentro de las plataformas de productos Vertiv™ Geist™ GU2 así como PDU para rack Vertiv™ MPH2™ y Vertiv™ MPX™, Vertiv™ Liebert® GXT4, Vertiv™ Liebert® GXT5, Vertiv™ Liebert® PSI5, Vertiv™ Liebert® EXM, UPS Vertiv™ Liebert® APM y Vertiv™ Liebert® ITA2, sistema de enfriamiento en fila Vertiv™ Liebert® CRV y enfriamiento Vertiv™ Liebert® VRC con conexión USB. Cada gerenciador puede admitir hasta 49 equipos conectados, por lo que el número de administradores depende del tamaño general de la instalación y de la arquitectura de red de preferencia.

El gerenciador se debe poner en marcha antes de conectarse a la red de administración primaria o a la red de los equipos conectados. Este comisionamiento se realiza habitualmente mediante una computadora portátil o una máquina local conectada directamente al puerto 1 en el IMD.

Una vez establecida la conectividad local, puede poner en marcha el gerenciador.

Para poner en marcha el gerenciador:

1. Desplácese a *System>Locale*. Seleccione los valores pertinentes para *Default Language* y *Temperature Units* en los menús desplegables. Esta configuración se deriva a los equipos conectados de su red.
2. Desplácese a *System>Network*. En el protocolo IPv6, elija *Enabled* en el menú desplegable.
3. Desplácese a *Aggregation>Configuration* y cambie la configuración como desee.
    a. Aggregation: elija *Enabled* en el menú desplegable.
    b. Array device Username: define el nombre de usuario que se configurará en todos los equipos conectados.
    c. Array device Password: define la contraseña que se configurará en todos los equipos conectados.
    - Introduzca la nueva contraseña, confírmela y haga clic en *Submit*. Al configurar la agregación, asegúrese de que la contraseña del dispositivo administrado cumple todas las reglas de complejidad de las contraseñas para equipos conectados. A menos que el usuario las haya cambiado, la contraseña debe tener una longitud mínima de 8 caracteres con las unidades de RTS que ejecuten firmware 5.9.0 o posterior.
4. Haga clic en *Submit*.

Una vez que se active *Aggregation* en el gerenciador, configure los ajustes restantes del gerenciador. Conecte el gerenciador a la red de administración (puerto 1) del IMD y a la red de dispositivos (puerto 2).

NOTA: El gerenciador tiene una red DHCP incorporada para asignar direcciones a sus equipos conectados. Esta red DHCP utiliza direcciones *192.168.123/192.168.124*, que no se pueden utilizar para la red de administración.

Equipos conectados

En el lanzamiento inicial de agregación, los equipos conectados se definen como unidades del RTS Vertiv™ Geist™ dentro de las plataformas de productos Vertiv™ Geist™ GU2 así como PDU para rack Vertiv™ MPH2™ y Vertiv™ MPX™, Vertiv™ MPX™ GXT4, Vertiv™ GXT5, Vertiv™ Liebert® PSI5, Vertiv™ Liebert® EXM, UPS Vertiv™ Liebert® APM y Vertiv™ ITA2, sistema de enfriamiento en fila Vertiv™ Liebert® CRV y enfriamiento Vertiv™ VRC con conexión USB. Todas las rPDU Geist™ GU1 deben ejecutar la versión de firmware 3.4 o posterior; las rPDU Geist™ GU2 deben ejecutar la versión de firmware 5.3.0 o posterior. Los equipos conectados GU1 no se pueden integrar con controladores de matriz con firmware 6.1.0 o posterior. En todos los casos, se recomienda encarecidamente que todas las rPDU y las unidades de RTS se actualicen a la última versión de firmware disponible. Si las rPDU Geist™ se instalan por primera vez y nunca se han configurado, ya están listas para la agregación. Si las rPDU Geist™ se instalaron en un entorno de computación y se pusieron en marcha con la configuración de la LAN y las cuentas de usuario locales, cada rPDU del conmutador de transferencia de rack Geist™ se debe restablecer a sus valores de fábrica mediante *Utilities>Restore Defaults*. Seleccione *All Settings* y haga clic en *Submit*. A continuación, el gerenciador enviará los datos de configuración a los equipos conectados.

Para configurar una nueva instalación con un gerenciador:

1. Instale los gerenciadores en racks y encienda los racks.
2. Cuando sea apropiado, conecte los equipos conectados en cadena margarita utilizando los puertos con las etiquetas 1 y 2 en el IMD.
    - Si se utilizan conexiones del conmutador de transferencia de rack Geist™ en cadena margarita, asegúrese de que ninguna cadena sea más larga que 20 rPDU.
    - Los equipos conectados se pueden conectar en red mediante conexiones en cadena margarita, en estrella o una combinación de ambas.
3. Instale el gerenciador en un rack. Mediante un portátil o una máquina local, conéctelo al puerto 1 para configurar *Aggregation*.
4. Conecte el gerenciador a la red de administración a través del puerto 1.
5. Conecte el gerenciador a la red de equipos conectados a través del puerto 2.

Para configurar una instalación existente con un gerenciador:

NOTA: Utilice las siguientes instrucciones si ya hay unidades de RTS y rPDU Geist™ conectadas en cadena margarita.

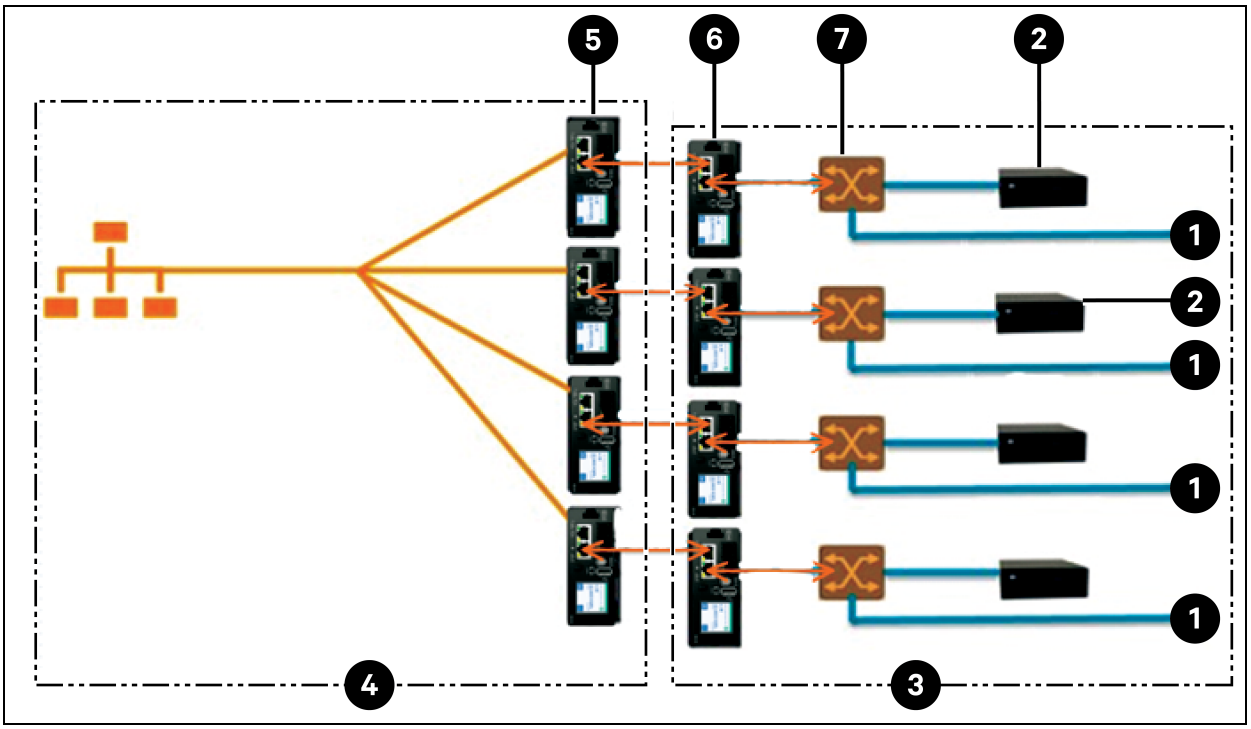
1. Designe un gerenciador y desconéctelo de la red de administración.
2. Reajuste todos los equipos conectados a los valores predeterminados de fábrica. Las conexiones físicas de Ethernet en la conexión de cadena margarita pueden ser las mismas; sin embargo, si se conectan previamente en una configuración en bucle, el RTS Geist™ final de la cadena se debe desconectar del conmutador de red.
3. Habilite la agregación en el gerenciador.
4. Conecte el gerenciador a la red de administración a través del puerto 1.

5. Conecte el gerenciador a la red de matrices a través del puerto 2.

Múltiples gerenciadores

Para instalaciones con varios gerenciadores, tenga en cuenta que cada red de dispositivos debe funcionar como una red autónoma y aislada. Considere un ejemplo de 200 RTS, que se representa en la Figura 6.4 abajo. Esta instalación requeriría un mínimo de cuatro gerenciadores, cada uno de los cuales administra su propia red de dispositivos. Cada gerenciador es visible en la red de administración y actúa como un servidor DHCP para sus equipos conectados. Un usuario de la red de administración puede desplazarse a través de cada gerenciador para llegar a la interfaz de un equipo conectado. Otras consideraciones pueden afectar a la cantidad de gerenciadores. Si tiene una arquitectura de red en filas, es posible que prefiera un gerenciador al comienzo de cada fila, en lugar de un gerenciador que atraviese varias filas. Dependiendo de cómo estén divididos estos 200 gabinetes en filas, puede que tenga más de cuatro gerenciadores. Una vez decidida la configuración, siga el proceso correspondiente para la agregación.

Figura 6.4 Ejemplo de configuración de red



Elemento	Descripción
1	Otros dispositivos
2	UPS
3	Red de dispositivos
4	Red de administración
5	Dispositivo maestro (GU2)
6	rPDU posterior
7	Conmutador Ethernet

NOTA: Solo se requerirá un conmutador de red Ethernet de red de dispositivos cuando se conecte más de un dispositivo de puerto de red único al final de una conexión en cadena margarita del RTS o cuando no se utilicen conexiones en cadena margarita.

6.4 Vistas

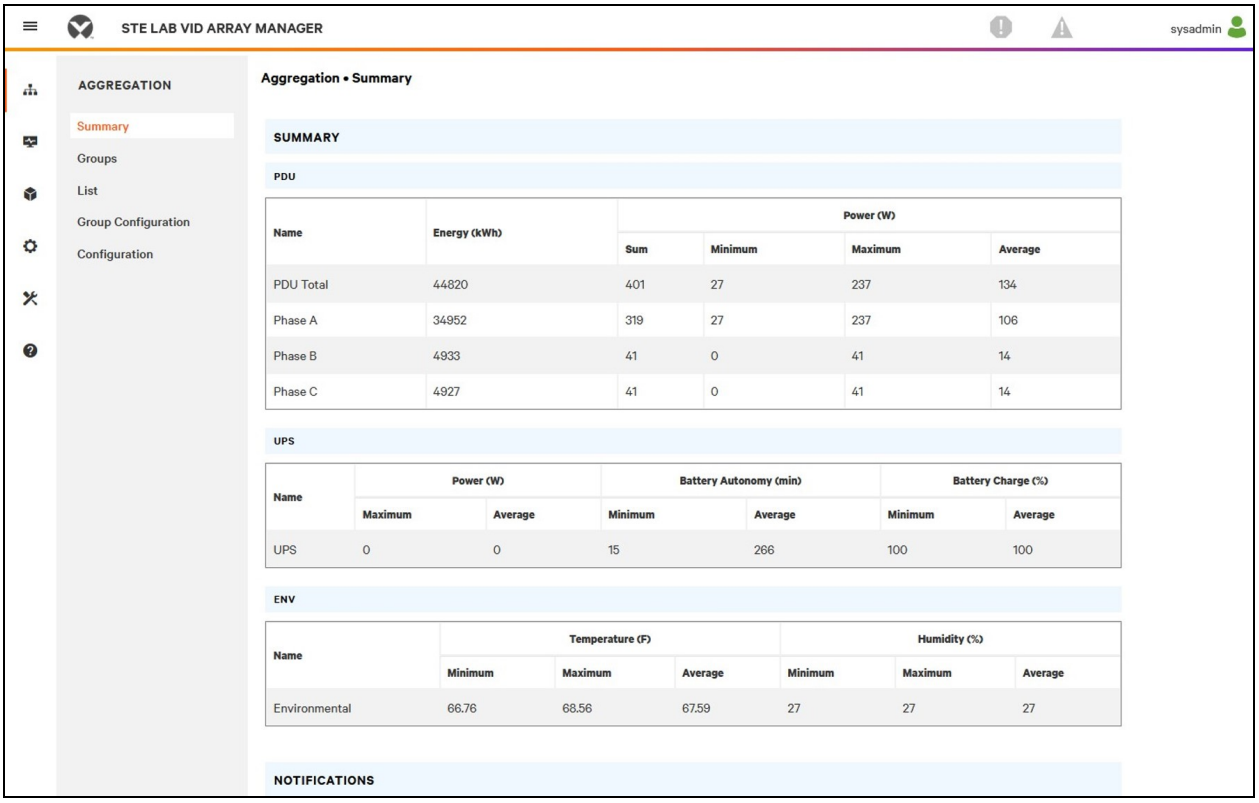
Cuando se establece la comunicación entre el gerenciador y los equipos conectados, se rellenan automáticamente varias vistas en la interfaz del usuario. Estas son las nuevas vistas en la pestaña *Device* de la barra de navegación superior:

- Vista *Summary*
- Vista *Groups*
- Vista *List*
- Vista *Group Configuration*
- Vista *Configuration*

6.4.1 Vista *Summary*

La vista *Summary* recopila los datos de todos los equipos conectados, y presenta un esquema conciso de los detalles de energía, entorno y alarmas.

Figura 6.5 Vista *Summary*



Unidades de conmutadores de transferencia de rack

La red del RTS Vertiv™ Geist™ se resume en los siguientes puntos de datos:

- Energy (kWh): la energía total del RTS Geist™ dentro de la red de dispositivos.
- Power (W) Sum: la carga energética total del RTS Geist™ dentro de la red de dispositivos.
- Power (W) Minimum: la carga energética más baja de grupo del RTS Geist™ dentro de la red de dispositivos.
- Power (W) Maximum: la carga energética más alta del RTS Geist™ dentro de la red de dispositivos.
- Power (W) Average: la carga energética promedio del RTS Geist™ dentro de la red de dispositivos.

NOTA: Estas lecturas se repiten por fase (se muestran cuando solo hay unidades de RTS Geist™ trifásicas).

UPS

La red de UPS se resume en los siguientes puntos de datos:

- Power (W) Maximum: la carga energética más alta del UPS dentro de la red de dispositivos.
- Power (W) Average: la carga energética promedio del UPS dentro de la red de dispositivos.
- Battery Autonomy (min) Minimum: el tiempo de autonomía más bajo de la batería del UPS dentro de la red de dispositivos.
- Battery Autonomy (min) Average: el tiempo de autonomía promedio de la batería del UPS dentro de la red de dispositivos.
- Battery Charge (%) Minimum: la carga más baja de la batería del UPS dentro de la red de dispositivos.
- Battery Charge (%) Average: la carga promedio de la batería del UPS dentro de la red de dispositivos.

Sensores medioambientales (ENV)

La categoría de ENV se resume en los siguientes puntos de datos:

NOTA: Los valores de humedad estarán en blanco cuando se utilicen sensores solo de temperatura.

- Temperature (F) Minimum: la temperatura más baja dentro de la red de dispositivos.
- Temperature (F) Maximum: la temperatura más alta dentro de la red de dispositivos.
- Temperature (F) Average: la temperatura promedio dentro de la red de dispositivos.
- Humidity (%) Minimum: la humedad más baja dentro de la red de dispositivos.
- Humidity (%) Maximum: la humedad más alta dentro de la red de dispositivos.
- Humidity (%) Average: la humedad promedio dentro de la red de dispositivos.

Refrigeración térmica

- Fan Speed (%) Minimum: la velocidad más baja del ventilador del dispositivo térmico dentro de la red de dispositivos.

- Fan Speed (%) Maximum: la velocidad más alta del ventilador del dispositivo térmico dentro de la red de dispositivos.
- Fan Speed (%) Average: la velocidad promedio del ventilador del dispositivo térmico dentro de la red de dispositivos.
- Temperature (F) Minimum: la temperatura más baja del dispositivo térmico entro de la red de dispositivos.
- Temperature (F) Maximum: la temperatura más alta del dispositivo térmico dentro de la red de dispositivos.
- Temperature (F) Average: la temperatura promedio del dispositivo térmico dentro de la red de dispositivos.
- Capacity (%) Minimum: la capacidad más baja del dispositivo térmico dentro de la red de dispositivos.
- Capacity (%) Maximum: la capacidad más alta del ventilador del dispositivo térmico dentro de la red de dispositivos.
- Capacity (%) Average: la capacidad promedio del dispositivo térmico dentro de la red de dispositivos.

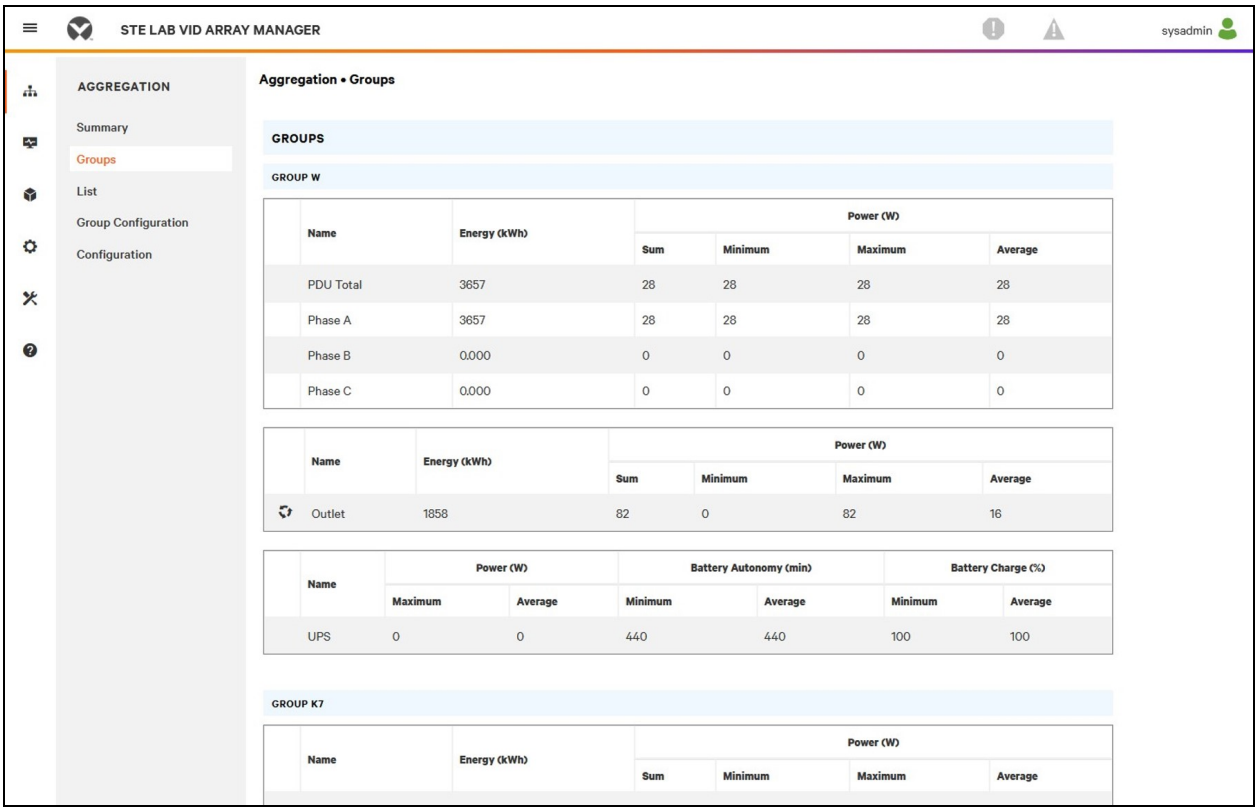
Notifications

Aquí se muestran alarmas pendientes de los dispositivos de la red de dispositivos.

6.4.2 Vista *Groups*

Una vez establecidos los grupos dentro de *Group Configuration,* la vista *Groups* resume los datos de potencia y entorno.

Figura 6.6 Pestaña *Groups*



Los puntos de datos disponibles son:

RTS del grupo

- Energy (kWh): la energía total del conmutador de transferencia de rack Geist™ de Vertiv™ dentro del grupo.
- Power (W) Sum: la carga energética total del conmutador de transferencia de rack Geist™ dentro del grupo.
- Power (W) Minimum: la carga energética más baja del conmutador de transferencia de rack Geist™ dentro del grupo.
- Power (W) Maximum: la carga energética más alta del conmutador de transferencia de rack Geist™ dentro del grupo.
- Power (W) Average: la carga energética promedio del conmutador de transferencia de rack Geist™ dentro del grupo.

NOTA: Estas lecturas se repiten por fase (se muestran cuando solo hay rPDU trifásicas).

Tomacorriente del RTS de grupos

- Energy (kWh): la energía total del tomacorriente del conmutador de transferencia de rack Geist™ dentro del grupo.
- Power (W) Sum: la carga energética total del tomacorriente del conmutador de transferencia de rack Geist™ dentro del grupo.

- **Power (W) Minimum:** la carga energética más baja del tomacorriente del conmutador de transferencia de rack Geist™ dentro del grupo.
- **Power (W) Maximum:** la carga energética más alta del tomacorriente del conmutador de transferencia de rack Geist™ dentro del grupo.
- **Power (W) Average:** la carga energética promedio del tomacorriente del conmutador de transferencia de rack Geist™ dentro del grupo.

Estas lecturas se repiten para cada grupo de tomacorrientes del conmutador de transferencia de rack Vertiv™ Geist™ presente en el grupo cuando hay por lo menos un tomacorriente monitoreado. Si en el grupo existe una combinación de PDU para rack con y sin monitoreo de tomacorrientes, las lecturas solamente proporcionarán el total de las PDU para rack con tomacorrientes monitoreados.

Estas lecturas se repiten por cada fase (se muestran cuando solo hay rPDU trifásicas).

NOTA: Las lecturas de energía reflejan la suma de las lecturas de energía de los tomacorrientes; y, al restablecer la lectura de energía de cada tomacorriente, también se restablecerá la energía total del grupo de tomacorrientes.

El ícono *Operations*  se muestra para cada grupo que incluya, por lo menos, un tomacorriente de PDU para rack con capacidad de conmutación.

Para cambiar la operación del grupo de tomacorrientes:

1. Haga clic en el ícono *Operation*.
2. Seleccione la operación que se debe realizar (se aplica solo a los tomacorrientes de la PDU para rack con capacidad de conmutación asignadas al grupo):
   - **On/Off:** activa o desactiva todos los tomacorrientes.
   - **Reboot:** para los tomacorrientes que están activados, esta opción inicia un clico de desactivación/activación después del retardo de espera de reinicio.

     Los tomacorrientes que estén desactivados se activan tras el reinicio.
   - **Cancel:** cancela la operación en curso, si no se ha completado.
3. Para las operaciones relacionadas con el estado de los tomacorrientes, al configurar *Delay* como *True*, se utiliza la configuración de retardo actual para cada tomacorriente.
4. Seleccione *Submit* para iniciar la acción.

UPS del grupo

- **Power (W) Maximum:** la carga energética más alta del UPS dentro del grupo.
- **Power (W) Average:** la carga energética promedio del UPS dentro del grupo.
- **Battery Autonomy (min) Minimum:** el tiempo de autonomía más bajo de la batería del UPS dentro del grupo.
- **Battery Autonomy (min) Average:** el tiempo de autonomía promedio de la batería del UPS dentro del grupo.
- **Battery Charge (%) Minimum:** la carga más baja de la batería del UPS dentro del grupo.
- **Battery Charge (%) Average:** la carga promedio de la batería del UPS dentro del grupo.

Parámetros ambientales del grupo

- Temperature (F) Minimum: la temperatura más baja dentro del grupo.
- Temperature (F) Maximum: la temperatura más alta dentro del grupo.
- Temperature (F) Average: la temperatura promedio dentro del grupo.
- Humidity (%) Minimum: la humedad más baja dentro del grupo.
- Humidity (%) Maximum: la humedad más alta dentro del grupo.
- Humidity (%) Average: la humedad promedio dentro del grupo.

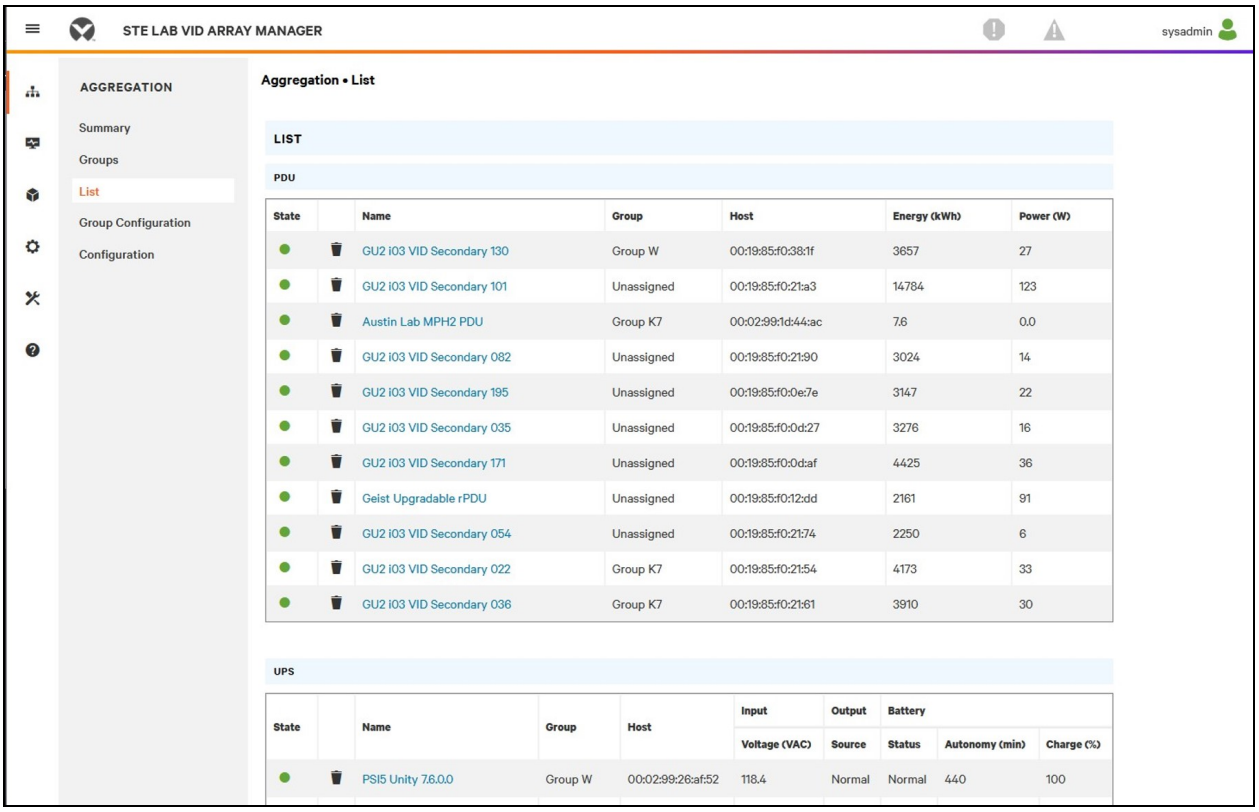
Refrigeración térmica del grupo

- Fan Speed (%) Minimum: la velocidad del ventilador del dispositivo térmico más baja dentro del grupo.
- Fan Speed (%) Maximum: la velocidad del ventilador del dispositivo térmico más alta dentro del grupo.
- Fan Speed (%) Average: la velocidad del ventilador del dispositivo térmico promedio dentro del grupo.
- Temperature (F) Minimum: la temperatura del dispositivo térmico más baja dentro del grupo.
- Temperature (F) Maximum: la temperatura del dispositivo térmico más alta dentro del grupo.
- Temperature (F) Average: la temperatura del dispositivo térmico promedio dentro del grupo.
- Capacity (%) Minimum: la capacidad del dispositivo térmico más baja dentro del grupo.
- Capacity (%) Maximum: la capacidad del dispositivo térmico más alta dentro del grupo.
- Capacity (%) Average: la capacidad del dispositivo térmico promedio dentro del grupo.

6.4.3 Vista *List*

La vista *List* presenta un inventario de todos los dispositivos dentro de la red de dispositivos del gerenciador.

Figura 6.7 Pestaña *List*



El inventario se subdivide en las siguientes categorías:

PDU para rack

Todas las unidades RTS Vertiv™ Geist™ de la red de dispositivos entran en esta categoría y presentan los siguientes puntos de datos:

- State: el estado del RTS Geist™. El estado es *Normal* o *Unavailable* (pérdida de conectividad).
- Name: etiqueta del RTS Geist™. Al hacer clic en el nombre, se abre una pestaña del navegador para acceder al dispositivo.
- Group: el nombre del grupo. Si no hay un grupo creado por el usuario, el nombre del grupo es *Unassigned*.
- Energy: energía del RTS Geist™.
- Power: carga energética total del RTS Geist™.

UPS

Todos los dispositivos UPS de la red de dispositivos entran en esta categoría y presentan los siguientes puntos de datos:

- State: el estado del UPS. El estado es *Normal* o *Unavailable* (pérdida de conectividad).
- Name: etiqueta del UPS. Al hacer clic en el nombre, se abre una pestaña del navegador para acceder al dispositivo.

- **Group:** el nombre del grupo. Si no hay un grupo creado por el usuario, el nombre del grupo es *Unassigned*.
- **Input Voltage:** voltaje de entrada del UPS.
- **Output Source:** el modo de funcionamiento del UPS, que puede ser: *Normal, Bypass, Battery, Booster, Reducer, Off,* u *Other*.
- **Status:** el estado de la batería, que puede ser: *Normal, Low, Depleted, o Unknown*.
- **Battery Autonomy:** tiempo de funcionamiento de la batería del UPS.
- **Charge:** carga de la batería del UPS.

Sensores medioambientales (ENV)

Todos los sensores medioambientales de la red de dispositivos entran en esta categoría y presentan los siguientes puntos de datos:

- **State:** el estado del sensor. El estado es *Normal* o *Unavailable* (pérdida de conectividad).
- **Name:** etiqueta del sensor. Al hacer clic en el nombre, se abre una pestaña del navegador para acceder al dispositivo.
- **Group:** el nombre del grupo. Si no hay un grupo creado por el usuario, el nombre del grupo es *Unassigned*.
- **Device:** muestra la dirección MAC y la etiqueta del RTS Vertiv™ Geist™ primaria del sensor.
- **Temperature (F):** lectura de la temperatura (temperatura principal solo con sensores GT3HD).
- **Humidity (%):** lectura de humedad. Este campo está en blanco si solo se despliegan los sensores de temperatura SRT.

Los sensores medioambientales comunican sus valores a través del MIB de las unidades de RTS Geist™ a las que están conectados. No son sensores independientes con sus propias direcciones IP. En esta versión, los únicos sensores válidos son los sensores SRT, GTHD o GTHD3 Geist™ conectados al RTS Geist™.

NOTA: La etiqueta de cualquier dispositivo se puede personalizar iniciando sesión en el dispositivo y editándolo a través del ícono *Configuration*.

NOTA: Para eliminar un dispositivo que se ha quitado de la red, seleccione el ícono *Trash* situado junto al dispositivo. Al seleccionar el ícono *Delete*, se eliminan el dispositivo y los sensores medioambientales conectados a él.

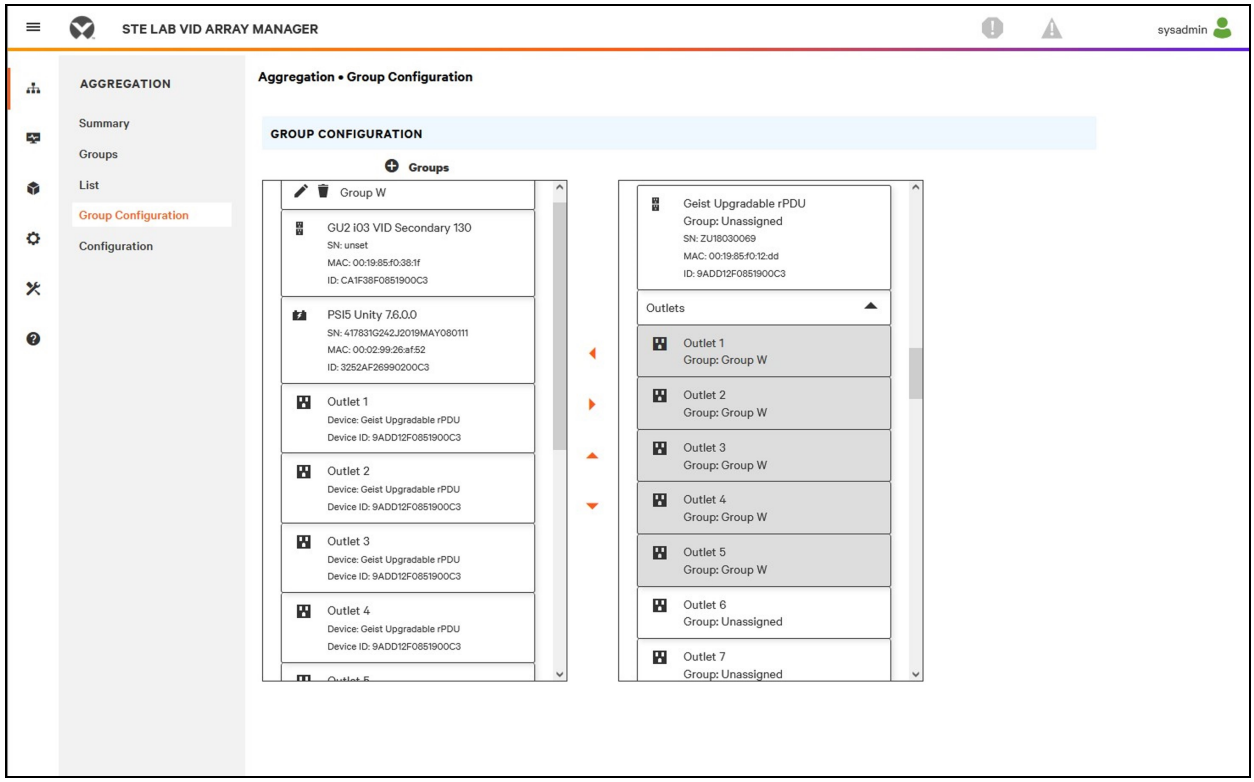
Refrigeración térmica

- **State:** el estado de la refrigeración. El estado es *Normal* o *Unavailable* (pérdida de conectividad).
- **Name:** etiqueta del dispositivo de refrigeración térmica. Al hacer clic en el nombre, se abre una pestaña del navegador para acceder al dispositivo.
- **Group:** el nombre del grupo. Si no hay un grupo creado por el usuario, el nombre del grupo es *Unassigned*.
- **Host:** dirección MAC
- **Fan Speed (%):** velocidad del ventilador del dispositivo térmico.
- **Temperature (F):** temperatura del dispositivo térmico.
- **Capacity (%):** capacidad del dispositivo térmico.

6.4.4 Vista *Group Configuration*

En la página *Group Configuration*, puede definir grupos de dispositivos con fines de agregación y analítica de datos. Un grupo a menudo hace referencia a una unidad de medida dentro de un entorno de computación que incluye varios equipos conectados, como un rack con dos unidades de RTS Geist™, dispositivos UPS y sensores medioambientales o una fila que incluye varios racks.

Figura 6.8 ***Group Configuration***



La página *Group Configuration* muestra una lista de los dispositivos detectados automáticamente bajo la columna *Unassigned*, que muestra:

- Uno o varios íconos que definen el tipo de dispositivo, como RTS Vertiv™ Geist™, sensor medioambiental, UPS o tomacorriente de rPDU Geist™.
- Etiqueta del dispositivo
- Número de serie
- Dirección MAC
- ID

A la izquierda se muestran los grupos de dispositivos configurados (que normalmente representan racks).

Para crear un nuevo grupo:

1. Haga clic en el signo más *(+)* a la izquierda de *Groups*, para agregar un nuevo grupo, bajo *Groups*.
2. Haga clic en el ícono *Configuration* para cambiar el nombre de la etiqueta de grupo.

3. Edite la etiqueta, si lo desea, y haga clic en *Save*.
4. Para asignar dispositivos al grupo, resalte el grupo deseado (dentro de la categoría *Groups*) y resalte los dispositivos deseados dentro de la categoría *Unassigned*.

NOTA: Debe hacer clic en la flecha hacia abajo que se encuentra debajo de la PDU para ver la lista de tomacorrientes.

5. Haga clic en la *flecha derecha* para asignar los dispositivos al grupo.
6. Repita el proceso para otros grupos, según sea necesario.

NOTA: Los grupos se pueden reordenar haciendo clic en las flechas hacia arriba o hacia abajo.

Para quitar dispositivos de un grupo:

Resalte los dispositivos y haga clic en la *flecha derecha*.

Para eliminar un grupo:

Haga clic en el ícono *Trash* situado junto al nombre del grupo.

NOTA: Al eliminar un grupo, todos sus dispositivos vuelven al grupo *Unassigned*.

6.5 Interfaces

Los equipos conectados se combinan para formar grupos; cada dispositivo conserva su propia interfaz de usuario y datos de SNMP independientes.

Para acceder a la interfaz de usuario del equipo conectado:

1. En la vista *List*, use el *mouse* para desplazar el cursor por encima de las entradas de la tabla. Al pausar los dispositivos, aparecen un resaltado amarillo y un cuadro de texto. El cuadro de texto revela la dirección IP del dispositivo y el número de puerto del dispositivo.
2. Navegue hasta una dirección IP y un número de puerto para acceder a la interfaz del servidor web del dispositivo.

   - o -

3. Haga clic en el nombre del dispositivo para acceder al hipervínculo a la interfaz web del dispositivo.

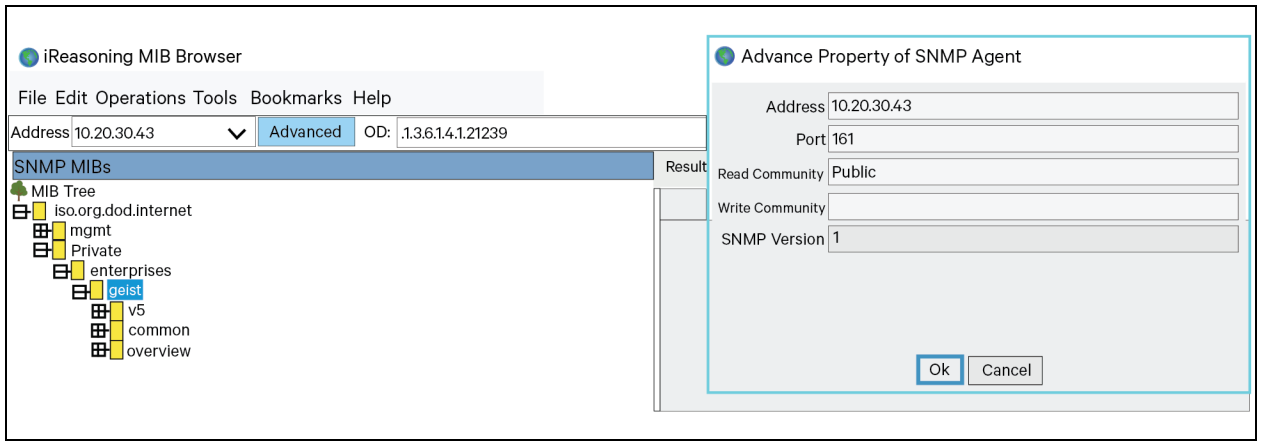
Para acceder a los datos de SNMP del equipo conectado:

Los datos de SNMP de la PDU para rack Geist™ están disponibles mediante el acceso mapeado de puertos a través de la dirección IP del dispositivo gerenciador utilizando la MIB v5 de Geist™. El archivo MIB se puede descargar desde la página SNMP del gerenciador.

1. En la vista *List*, use el *mouse* para desplazar el cursor por encima de las entradas de la tabla. Al pausar un dispositivo, aparecen un resaltado amarillo y un cuadro de texto con el puerto SNMP del dispositivo.
2. En el navegador de MIB, introduzca el puerto SNMP que aparece en la lista.

NOTA: El software para monitorear los dispositivos de matriz individuales debe poder admitir un número de puerto SNMP único por cada dispositivo monitoreado.

Figura 6.9 Navegador de MIB



6.5.1 Datos SNMP del grupo

Los datos agregados, tanto de resumen (como kWH totales y kW máximos) como de grupo, están disponibles a través de la dirección IP del RTS Vertiv™ Geist™ principal y el puerto SNMP 161 predeterminado. Hay dos MIB disponibles para la PDU para rack Geist del controlador de la matriz:

- v5: contiene puntos de datos del RTS Geist™ principal individual.
- Oneview: contiene puntos de datos para datos agregados en todos los equipos conectados.

6.5.2 Consejos y resolución de problemas

- Se recomienda actualizar todos los dispositivos a la última versión del *firmware* antes de configurar la agregación.
- Antes de conectar cualquier gerenciador, asegúrese de que la PDU para rack designada como gerenciador esté totalmente configurada y la agregación esté habilitada.
- Antes de conectarlos al gerenciador, asegúrese de que todos los gerenciadores tengan el estado predeterminado de fábrica. Si los ajustes se han modificado previamente o si se ha definido algún usuario en un dispositivo, el dispositivo debe restablecerse a sus valores predeterminados de fábrica antes de conectarlo al gerenciador.
- Si se restablece una PDU para rack a los valores predeterminados de fábrica, asegúrese de utilizar la función *Utilities>Restore defaults>All Settings*. El uso del interruptor de restablecimiento de *pinhole* del IMD bajo el puerto de red 1 para restablecer los ajustes no restablece todos los ajustes y puede hacer que los equipos conectados no se identifiquen correctamente.
- Después de restablecer una PDU para rack a los ajustes predeterminados de fábrica y antes de conectarla como equipo conectado, desconecte la PDU para rack de la red y reiníciela mediante el botón situado debajo del puerto de red 1. Esto garantiza que se libere cualquier dirección DHCP asignada durante el procedimiento de restablecimiento de los valores predeterminados de fábrica.
- Se puede tardar hasta 20 minutos en reconocer los equipos conectados tras la configuración inicial.
- Los datos agregados, tanto resumidos como de grupo, no se pueden utilizar para generar alarmas.

- La herramienta *Provisioner* (*Provisioner>Discovery and Provisioner>File Management*) se puede utilizar para actualizar fácilmente el firmware del gerenciador y el firmware de la PDU para rack del equipo conectado.
- Los datos agregados, tanto resumidos como de grupo, no se pueden utilizar para generar trampas de SNMP.
- Los nombres de la comunidad SNMP están configurados en cada dispositivo. Siga los vínculos de los dispositivos que se muestran en la página *List* en el menú *Devices* e inicie sesión en cada dispositivo para configurar el SNMP.
- No cambie el número de puerto SNMP predeterminado, la configuración de red ni la configuración del servidor Web cuando haya iniciado sesión en un equipo conectado.
- Las trampas y alarmas de SNMP se enrutan desde un dispositivo a la red de administración a través del dispositivo principal.

Apéndices

Apéndice A: Asistencia técnica

A.1 Restablecimiento de un conmutador de transferencia de rack (RTS) Vertiv™Geist™

Si un RTS Geist™ pierde la comunicación, el procesador se puede reiniciar manualmente sin afectar la alimentación de los tomacorrientes. Si se pulsa el botón de reinicio en la parte frontal del IMD, se reiniciará el procesador. La interfaz web permanecerá desconectada durante el arranque. Para obtener más información, consulte Dispositivo de monitoreo intercambiable en la página 18.

A.2 Servicio y mantenimiento

No se necesita servicio ni mantenimiento. La apertura del RTS Geist™ puede anular la garantía. En el interior del RTS Geist™ no hay piezas que pueda reparar el usuario, salvo el dispositivo de monitoreo intercambiable (IMD), que se puede remplazar sobre el terreno. Geist™ recomienda desconectar la alimentación de la unidad antes de instalar o quitar cualquier equipo.

El IMD está diseñado para que su remplazo sobre el terreno lo realice únicamente personal de servicio debidamente capacitado y cualificado. El IMD está diseñado para ser remplazado mientras el RTS Geist™ sigue conectado a la alimentación. Para obtener más información, consulte la Guía de remplazo de módulos IMD del RTS Geist™.

A.3 Más asistencia técnica

Para obtener asistencia técnica, visite *www.Vertiv.com/support*.

América

- Sitio web: *www.Vertiv.com/geist*
- Correo electrónico: geistsupport@vertiv.com
- Teléfono: 1-888-630-4445

Europa y Oriente Medio

- Asistencia técnica: *www.Vertiv.com/en-emea/support*
- Correo electrónico: eoc@Vertiv.com
- Teléfono: 44 1823 275100

Asia

- Teléfono (inglés): 1-888-630-4445 (número de los EE. UU.)
- Teléfono (chino): +86 755 23546462

A.4 Uso de Microsoft Exchange como servidor SMTP

Si su centro utiliza un servidor de correo electrónico de Microsoft Exchange, el RTS Geist™ del IMD puede utilizarlo para enviar correos electrónicos de notificación de alarma y advertencia. Sin embargo, puede ser necesario configurar Exchange Server para permitir primero las conexiones SMTP de la unidad, ya que las versiones posteriores de Exchange Server suelen tener los servicios SMTP o la autenticación básica desactivados de forma predeterminada. Si tiene dificultades para que el RTS Geist™ del IMD envíe correos electrónicos a través de su servidor de Exchange, las siguientes notas pueden ser de utilidad.

NOTA: Estas sugerencias solo son válidas si utiliza su propio servidor físico de Exchange. El servicio de Office 365 hospedado de Microsoft no es compatible con el RTS Vertiv™ Geist™ del IMD que utilice versiones de firmware anteriores a la v3.0.0, ya que Office 365 requiere una conexión StartTLS. Las versiones de firmware 3.0.0 y posteriores tienen soporte para StartTLS y son compatibles con Office 365.

En primer lugar, dado que el RTS Geist™ del IMD no puede utilizar IMAP ni los protocolos patentados de Microsoft MAPI/RPC Exchange/Outlook para enviar mensajes, debe habilitar SMTP configurando un conector de envío SMTP en el servidor de Exchange. Si desea obtener más información sobre la configuración de un conector de envío SMTP en Exchange, consulte este artículo de Microsoft TechNet: *http://technet.microsoft.com/en-us/library/aa997285.aspx*

En segundo lugar, es posible que necesite configurar su servidor de Exchange para permitir la retransmisión de mensajes desde la unidad de monitoreo. Habitualmente, esto implicará activar la opción *Redirigir el correo SMTP entrante* en las propiedades de enrutamiento del servidor de Exchange, y luego agregar la dirección IP del RTS Geist™ del IMD como un dominio al que se permite retransmitir el correo a través del servidor de Exchange. Si desea obtener más información sobre la activación y configuración de la retransmisión SMTP en Exchange, consulte este artículo de Microsoft TechNet: *http://technet.microsoft.com/en- us/library/dd277329.aspx*

Los métodos de autenticación SMTP AUTH PLAIN y AUTH LOGIN para iniciar sesión en el servidor ya no suelen estar habilitados de forma predeterminada en Exchange Server; solo está habilitado el método de autenticación NTLM patentado de Microsoft.

Para volver a habilitar el método AUTH LOGIN:

1. En la consola de Exchange, seleccione *Server Configuration - Hub Transport*.
2. Haga clic con el botón derecho del ratón en *Client Server* y seleccione *Properties*.
3. Seleccione la pestaña *Authentication* y active la casilla *Basic Authentication*.
4. Anule la selección de la casilla *Offer Basic only after TLS*.
5. Haga clic en *Apply* o en *Save* y haga clic en *Exit*.

NOTA: Es posible que tenga que reiniciar el servidor de Exchange después de hacer estos cambios.

Por último, una vez que haya activado el SMTP, la retransmisión y el método de autenticación básica AUTH LOGIN, es posible que también tenga que crear una cuenta de usuario específicamente para que se conecte el RTS Geist™ del IMD. Si creó una cuenta antes de habilitar el conector de envío SMTP o si intenta utilizar una cuenta creada para otro usuario y el RTS Geist™ del IMD aún no puede conectarse al servidor de Exchange, es probable que la cuenta no haya heredado correctamente los nuevos permisos al habilitarlos como se indicó anteriormente. Esto tiende a ser más frecuente en los servidores de Exchange que se han actualizados desde que se creó la cuenta que intenta utilizar, pero a veces puede suceder con las cuentas cuando se agregan nuevos conectores y complementos, independientemente de la versión de Exchange. Elimine las cuentas de usuario y, a continuación, cree una nueva para que la utilice la unidad de monitoreo, y la nueva cuenta debería heredar correctamente la autenticación SMTP y los permisos de retransmisión de correo.

Si ninguna de las sugerencias anteriores logra que el RTS Geist™ del IMD envíe correo a través del servidor de Exchange, es posible que tenga que ponerse en contacto con el soporte técnico de Microsoft, a fin de que le ayude a configurar el servidor de Exchange para permitir el envío de correos electrónicos SMTP desde un dispositivo de terceros, que no sea de Windows, a través de su red.

Apéndice B: Sensores disponibles

B.1 Sensores remotos

- SRT: temperatura remota inoxidable.
- GTHD: temperatura/humedad/punto de condensación.
- GT3HD: temperatura/humedad/punto de condensación con dos sensores SRT.
- RTAFHD3: temperatura/flujo de aire/humedad/punto de condensación.
- A2D: convierte los sensores de E/S analógicos en sensores digitales remotos.

B.2 Sensores de E/S analógicos

- FS-15: sensor de inundación (agua).
- PFS-100 US / PFS-100 UN: sensor de falla de potencia.
- RPDS: juego de interruptor de puerta.

B.3 Sensores integrados y modulares de Liebert®

NOTA: Se requiere un adaptador para usar cualquiera de los sensores siguientes.

- SN-T: una sonda de temperatura.
- SN-TH: una sonda de temperatura y otra de humedad.
- SN-Z01: cable integrado con una sonda de temperatura.
- SN-Z02: cable integrado con tres sondas de temperatura.
- SN-Z03: cable integrado con cuatro sondas (tres de temperatura y una de humedad).
- SN-2D: sensor monitor del conmutador de dos puertas.

B.4 Conexión con sensores remotos

Se pueden conectar hasta 16 sensores remotos de tipo *plug-and-play* a la unidad en cualquier momento, a través de los conectores RJ-12 situados en la parte delantera de la unidad. En algunos casos, es posible que se necesiten divisores para agregar sensores adicionales. Cada sensor tiene un número de serie único y se detecta y agrega automáticamente a la página web. El número de serie de los sensores determina su orden de visualización en la web. Los nombres de los sensores se pueden personalizar en la página *Sensors Overview*.

NOTA: Los sensores utilizan Cat 5, cable CMP y conectores RJ-12. El cableado debe ser directo. La polaridad invertida desactiva temporalmente todos los sensores hasta que se corrige. Los sensores utilizan un protocolo de comunicaciones en serie y están sujetos a restricciones de señalización de la red que dependen del blindaje, el ruido ambiental y la longitud del cable. Las instalaciones típicas permiten tendidos de hasta 600 ft (180 m) de cable del sensor.

Apéndice C: Adaptadores USB inalámbricos TP-Link

- Archer T2U Nano (adaptador USB inalámbrico AC600 Nano)
- Archer T2U Plus (adaptador USB inalámbrico de doble banda y alta ganancia AC600)
- Archer T2U v3 (adaptador USB inalámbrico de doble banda AC600)
- Archer T3U (adaptador USB inalámbrico mini MU-MIMO AC1300)
- Archer T3U Plus (adaptador USB inalámbrico de doble banda y alta ganancia AC1300)
- Archer T4U v3 (adaptador USB inalámbrico de doble banda AC1300)

NOTA: Estos dispositivos se detectan automáticamente cuando se conectan y pueden configurarse como una interfaz de red adicional.

Apéndice D: LED de los tomacorrientes

NOTA: Este apéndice se aplica solamente a los conmutadores de transferencia de rack Vertiv™ Geist™ con monitoreo de tomacorrientes/tomacorrientes conmutados.

Los LED de los tomacorrientes proporcionan una indicación visual del estado de potencia del tomacorrientes (*On*, *Off* o *Error*). Los LED están numerados secuencialmente con números blancos fáciles de leer sobre un fondo negro. Dependiendo del estado de alimentación de los tomacorrientes, los LED se iluminan en colores sólidos o en colores intermitentes.

Tabla 7.1 Tomacorrientes LED

LED	Descripción
Verde	El voltaje del tomacorriente está presente y por encima del límite de umbral mínimo
Rojo	El voltaje del tomacorriente no está presente
Ámbar	Se ha detectado un condición de error en la salida de potencia

Tabla 7.2 Descripción del estado del LED

Voltaje medido	Estado de relé	Estado	LED	
On	Activado o desconocido	Sólido	Verde	
Off	Apagado o desconocido	Sólido	Rojo	
Off	Encendido	Intermitente [1]	Ámbar	Rojo
On	Apagado	Intermitente [2]	Ámbar	Verde

[1] El tomacorriente se detecta como *Off* pero debería estar en *On*.

[2] El tomacorriente se detecta como *On* pero debería estar en *Off*.

Código de error

Los LED se iluminan en ámbar sólido durante las siguientes situaciones:

- Falla de potencia (se fuerza la apertura de todos los relés en caso de falla de potencia para permitir la secuencia de encendido)
- Disyuntor abierto
- No se detecta voltaje de entrada

Apéndice E: Códigos de pantalla del IMD

Tabla 7.3 Códigos de pantalla del IMD

Pantalla	Tipo de IMD	Explicación
Err1	IMD-01 (solo medido)	El IMD no descubrió ninguna placa de entrada, o descubrió más de una. Esto se puede deber a problemas de cableado interno o a una placa de entrada que no responde. Esto también se muestra si la placa de entrada comunica un error de medición.
8888	IMD-02, IMD-03, IMD-3	El IMD se está iniciando y aún no ha detectado la pantalla simple y muestra *boot*. Si se muestra durante más de unos segundos, hay un problema en la placa de la pantalla o con el cableado interno.
-- (dos guiones en la posición más a la derecha de la pantalla)	IMD-02, IMD-03, IMD-3	El IMD no puede comunicarse con la placa de entrada. Esto también se puede mostrar de forma intermitente para mediciones individuales. Hay un problema con la placa de entrada o con el cableado interno.
boot	IMD-01	El IMD se está iniciando y detectando la placa de entrada.
boot	IMD-02, IMD-03, IMD-3	El firmware se está inicializando. Se mostrará mientras se actualiza el firmware en las placas internas.
updt	IMD-02, IMD-03, IMD-3	Actualización del firmware en curso.
rset dflt	IMD-02, IMD-03, IMD-3	Después de la acción del usuario, aparecerá *rset* (*Reset*) durante una secuencia de restablecimiento de parámetros. Durante el restablecimiento de un parámetro, aparecerá brevemente *dflt* (*Default*).
bcup	IMD-02, IMD-03, IMD-3	*bcup* (*Backup*) aparecerá durante una copia de seguridad de la configuración.
rest conf	IMD-02, IMD-03, IMD-3	*rest* (*Restore*) y *Conf* (*Configuration*) aparecerán durante una restauración de la configuración.
____ (cuatro guiones bajos en la parte inferior de la pantalla)	IMD-03 IMD-3	La pantalla del IMD se ha configurado de modo que las opciones *Total Power*, *Voltage* y *Current* están desactivadas.

NOTA: El IMD-5M no tiene códigos de pantalla; la pantalla táctil muestra información de estado.

Apéndice F: Aprovisionador: formato del archivo de ajustes de configuración

NOTA: A continuación se describe el formato del archivo de ajustes de configuración usado por el aprovisionador. En los ejemplos se siguen, a grandes rasgos, los ajustes disponibles en la interfaz del usuario web del RTS Vertiv™ Geist™.

1. En los ejemplos que aparecen a continuación, el texto en azul se puede copiar en un archivo de texto y actualizarse según sea necesario. A continuación, el archivo de texto se puede cargar en la herramienta de aprovisionamiento.
2. Cuando edite archivos de configuración, use un editor de texto, por ejemplo, el Bloc de notas que pueda guardar archivos en formato .txt.
3. Las sangrías que se muestran en los ejemplos se pueden omitir.
4. Asegúrese de utilizar las comillas dobles correctas al editar la configuración.
5. Si se omite un ajuste en el archivo de configuración, el valor de ese ajuste permanecerá inalterado.
6. Cuando se configure un RTS Geist™ no configurado anteriormente (es decir, nuevo de fábrica), el primer ajuste de configuración debe ser la definición de un usuario administrador; consulte Usuarios locales abajo.
7. Para combinar varios ajustes (que no sean usuarios locales) en un solo archivo (consulte también el Ejemplo 1 en la página 132 al final de este documento):
   - Combine los ajustes necesarios en un solo archivo.
   - Elimine todas las ocurrencias de {"conf":{ excepto en la primera línea del archivo.
   - Remplace todas las líneas que contengan solo }} por una , (coma) excepto en la última línea del archivo.
8. Si se combinan ajustes de usuario local con otros ajustes en un mismo archivo, consulte el Ejemplo 2 en la página 133 al final de este documento.
9. Después de seleccionar *Provisioner>Discovery>Update*, ingrese el nombre de usuario y la contraseña solo cuando configure las unidades de RTS Geist™ que se hayan configurado anteriormente (el nombre de usuario y la contraseña son los de las unidades de RTS Geist™ que se están aprovisionando). No ingrese un usuario y una contraseña cuando configure unidades nuevas de fábrica (identificadas por el atributo *Provisioned* igual a *False*).

Usuarios locales

```
{ "auth": {
"username": {
"password": "userpw",
"enabled": true,
"control": false,
"admin": false,
"language": "en"}
}}
```

username	El nombre de usuario que se debe crear (entre comillas)
password	Contraseña (entre comillas)
enabled	Las opciones *true* o *false* determinan si el usuario está activado
control	Las opciones *true* o *false* determinan si el usuario tendrá privilegios de control
admin	Las opciones *true* o *false* determinan si el usuario tendrá privilegios de administrador
language	Anula el idioma predeterminado para este usuario; las opciones válidas son "de", "en", "es", "fr", "ja", "ko", "pt" y "zh"

LDAP

```
{"conf":{
"remoteAuth": {
"mode": "ldap",
"ldap": {
"host": "192.168.123.1",
"port": 389,
"mode": "activeDirectory",
"securityType": "ssl",
"bindDn": "",
"password": null,
"baseDn": "",
"userFilter": "(objectClass=posixAccount)",
"userId": "uid",
"userIdNum": "uidNumber",
"groupFilter": "(objectClass=posixGroup)",
"groupId": "gidNumber",
"groupMemberUid": "memberOf",
"enabledGroup": "enabled",
"controlGroup": "control",
"adminGroup": "admin"}}
}}
```

host	URL de LDAP (ref. RFC4516 > RFC2255) (entre comillas); es necesario si LDAP está activado.
port	Puerto para la comunicación del protocolo
mode	Determina la compatibilidad predeterminada entre los diferentes tipos de LDAP; las opciones son "openLdap" o "activeDirectory".
securityType	Cifrado que se debe usar en la conexión con el servidor LDAP; las opciones son "ssl" y "starttls".
bindDn	Nombre distintivo (entre comillas) (ref. RFC4514 > RFC2253); se usa como enlace al servidor de directorios y una cadena en blanco significa un enlace anónimo
password	Contraseña (entre comillas) utilizada como enlace al servidor de directorios
baseDn	Nombre distintivo (entre comillas) (ref. RFC4514 > RFC2253) que se usará para la base de búsqueda
userFilter	Filtro de búsqueda LDAP (entre comillas) (ref. RFC4515 > RFC2254), objectClass equivalente a posixAccount (ref. RFC2307)
userId	Equivalente al atributo "uid" (entre comillas) ref. (RFC2307)
userIdNum	Equivalente al atributo "uidNumber" (entre comillas) (ref. RFC2307)
groupFilter	Filtro de búsqueda LDAP (entre comillas) (ref. RFC4515 > RFC2254), objectClass equivalente a posixGroup (RFC2307)
groupId	Equivalente al atributo "gidNumber" (ref. RFC2307) (entre comillas)
groupMemberUid	Equivalente al atributo "memberUid" (ref. RFC2307) (entre comillas)
enabledGroup	El usuario (entre comillas) de este grupo tendrá el privilegio "enabled”
controlGroup	El usuario (entre comillas) de este grupo tendrá el privilegio "control"
adminGroup	El usuario (entre comillas) de este grupo tendrá el privilegio "admin"


```
{"conf":{
"remoteAuth": {
"mode": "tacacs",
"tacacs": {
"authenticationServer1": "10.20.30.21",
"authenticationServer2": "10.20.30.70",
"accountingServer1": "10.20.30.21",
"accountingServer2": "10.20.30.70",
"sharedSecret": "secret",
"service": "raccess",
"adminAttribute": "admin=true",
"controlAttribute": "control=true",
"enabledAttribute": "enabled=true"}}
}}
```

authenticationServer1	Servidor de autenticación/autorización primario (entre comillas)
authenticationServer2	Servidor de autenticación/autorización alternativo (entre comillas)
accountingServer1	Servidor de contabilidad primario (entre comillas)
accountingServer2	Servidor de contabilidad alternativo (entre comillas)
sharedSecret	El secreto (entre comillas) compartido por el cliente y el servidor (con el valor nulo se elimina el secreto)
service	Valor que se debe utilizar para el campo de servicio en las solicitudes TACACS+. Las opciones válidas son "ppp" y "raccess".
adminAttribute	El usuario (entre comillas) con este par atributo-valor tendrá el privilegio "admin"
controlAttribute	El usuario (entre comillas) con este par atributo-valor tendrá el privilegio "control"
enabledAttribute	El usuario (entre comillas) con este par atributo-valor tendrá el privilegio "enabled"

Radius

```
{"conf":{
"remoteAuth": {
"mode": "radius",
"radius": {
"authenticationServer1": "",
"authenticationServer2": "",
"accountingServer1": "",
"accountingServer2": "",
"sharedSecret": "Secret",
"groupAttribute": "filter-id",
"adminGroup": "admin",
"controlGroup": "control",
"enabledGroup": "enabled"}}
}}
```

authenticationServer1	Servidor de autenticación primario (entre comillas)
authenticationServer2	Servidor de autenticación alternativo (entre comillas)
accountingServer1	Servidor de contabilidad primario (entre comillas)
accountingServer2	Servidor de contabilidad alternativo (entre comillas)
sharedSecret	Secreto compartido por el cliente y el servidor (entre comillas)
groupAttribute	Identifica el AVP que indica a qué grupo de acceso pertenece el usuario; los valores válidos son "filter-id" y "management-privilege-level".
adminGroup	El usuario (entre comillas) que pertenece a este grupo tiene el privilegio de "admin"
controlGroup	El usuario (entre comillas) que pertenece a este grupo tiene el privilegio "control"
enabledGroup	El usuario (entre comillas) que pertenece a este grupo tendrá el privilegio "enabled"

Direcciones IP y nombre de host de la red

```
{"conf":{
"system": {
"hostname": "rPDUhostname",
"ip6Enabled": true},
"network": {
"ethernet": {
"label": "Bridge 0",
"enabled": true,
"dhcpOn": false,
"address": {
"0": {"address": "192.168.123.123","prefix": 24},
"1": {"address": "10.20.30.43","prefix": 24}}}}
}}
```

Hostname	Nombre (entre comillas) para identificar la unidad en una red
ip6Enabled	Las opciones son *true* o *false* para activar o desactivar la compatibilidad con IPV6
label	Etiqueta del puente (entre comillas)
enabled	Las opciones son *true* o *false* para activar o desactivar el puente de red
dhcpOn	Las opciones son *true* o *false* para activar o desactivar DHCP
address	Dirección IP (entre comillas) de la interfaz
prefix	Prefijo de la dirección IP de la interfaz

Puertos de red

```
{"conf":{
"network": {
"port0": {
"label": "Port 0",
"enabled": true,
"stp": {"cost": 0}},
"port1": {
"label": "Port 1",
"enabled": true,
"stp": {"cost": 0}}}
}}
```

label	Etiqueta del puerto (entre comillas)
enabled	Las opciones son *true* o *false* para determinar si el puerto está activado
cost	Costo del árbol de expansión para este puerto

Rutas de red

```
{"conf":{
"network": {
"ethernet": {
"route": {
"0": {
"gateway": "10.20.30.254",
"prefix": 0,
"destination": "0.0.0.0"}}}}
}}
```

gateway	Dirección de la puerta de enlace (entre comillas) para la ruta
prefixDestination	Prefijo de red; 0 para la puerta de enlace predeterminada
destination	Dirección de red de destino (entre comillas); "0.0.0.0" para la red predeterminada

DNS de red

```
{"conf":{
"network": {
"ethernet": {
"dns": {
"0": {"address": "8.8.8.8"},
"1": {"address": "8.8.4.4"}}}}
}}
```

address	La dirección del servidor DNS (entre comillas). La segunda ocurrencia es para el servidor DNS alternativo.

RSTP de red

```
{"conf":{
"network": {
"ethernet": {
"stp": {
"enabled": false,
"mode": "rstp",
"bridgePriority": 24576,
"helloTime": 2,
"maxAge": 40,
"maxHops": 40,
"forwardDelay": 21}}}
}}
```

enabled	Las opciones son *true* o *false*; determina si el protocolo de árbol de expansión está activado
mode	Las opciones son "stp" o "rstp"; el modo RSTP permite volver a STP cuando sea necesario
bridgePriority	La prioridad del puente del árbol de expansión de esta interfaz
helloTime	Intervalo en segundos entre las transmisiones periódicas del mensaje de configuración
maxAge	Antigüedad máxima de la información transmitida por esta interfaz, cuando sirve como puente de raíz. Se usa cuando "mode" está configurado como "stp". Debe ser al menos 2 * (helloTime + 1)
maxHops	Número máximo de cruces del puente de la información transmitida por esta interfaz cuando sirve como puente raíz; se usa cuando "mode" está configurado como "rstp"
forwardDelay	El retardo utilizado por los puentes para la transición del puente raíz y los puertos designados al modo de reenvío; debe ser como mínimo (maxAge / 2) + 1

Servidor web

```
{"conf":{
"http": {
"httpEnabled": true,
"httpPort": 80,
"httpsPort": 443}
}}
```

httpEnabled	Las opciones son *true* o *false* para permitir las comunicaciones no cifradas
httpPort	Número de puerto para la comunicación HTTP
httpsPort	Número de puerto para la comunicación HTTPS

Informes

```
{"conf":{
"report": {
"0": {
"start": "00:00",
"days": "MTWTFSS",
"targets": ["1","2"],
"interval": 1},
"1": {
"start": "00:00",
"days": "MT-----",
"targets": ["1"],
"interval": 1}}
}}
```

start	Hora del día a partir de la cual se aplica el intervalo. El formato es "(00-23):(00-59)", configurable en incrementos de 15 minutos
days	Primera letra de los días seleccionados (entre comillas) en orden de lunes a domingo. Se usa un '-' para representar destinos de días no seleccionados
	Lista de claves que hacen referencia a los destinos de correo electrónico (entre comillas)
interval	Número de horas entre informes; el valor puede ser 1, 2, 3, 4, 6, 8, 12 y 24

Pantalla

```
{"conf":{
"display": {
"gmsd": {
"mode": "currentAndTotalPower",
"inverted": false,
"vlc": {"enabled": false}}}
}}
```

mode	Selecciona un conjunto de datos para presentar en la pantalla; las opciones son "current", "totalPower" y "currentAndTotalPower"
inverted	Las opciones son *true* o *false* para describir la orientación actual de la pantalla
enabled	Las opciones son *true* o *false* para determinar el modo de pantalla de VLC de la rPDU

Fecha y hora

```
{"conf":{
"time": {
"mode": "ntp",
"datetime": "2021-03-09 12:05:36",
"zone": "UTC",
```

```
"ntpServer1": "0.pool.ntp.org",
"ntpServer2": "1.pool.ntp.org"}
}}
```

mode	El modo; las opciones válidas son "ntp" y "manual"
datetime	Fecha y hora. El formato es "AAAA-MM-DD HH:MM:SS". Las horas van de 0-23 (este campo se muestra en hora local). Solo debe usarse con el modo="manual"
Zone	Debe ser un nombre válido (entre comillas) de la base de datos tz
ntpServer1	Dirección del servidor NTP primario (entre comillas); solo debe utilizarse con el modo="ntp"
ntpServer2	Dirección del servidor NTP de reserva (entre comillas); solo debe utilizarse con el modo="ntp"

SSH

```
{"conf":{
"ssh": {
"enabled": true,
"port": 22}
}}
```

enabled	Las opciones son *true* o *false* para activar o desactivar SSH
port	Número de puerto para la comunicación SSH

USB

```
{"conf":{
"usb": {"enabled": true}
}}
```

enabled	Las opciones son *true* o *false* y activa o desactiva el puerto USB

Puerto serie

```
{"conf":{
"serial": {
"baudRate": 115200,
"dataBits": 8,
"enabled": true,
"parity": "none",
"stopBits": 1}
}}
```

baudRate	Velocidad en baudios; las opciones son 1200, 2400, 4800, 9600, 19200, 38400, 57600 y 115200
dataBits	Número de bits de datos en una trama; las opciones son 7 y 8
enabled	Las opciones son *true* o *false*; activa o desactiva la CLI serie en un dispositivo
parity	Tipo de bit de paridad utilizado en la trama; las opciones son "none", "even" y "odd"
stopBits	Número de bits de parada usados para terminar cada trama; las opciones son *1* y *2*

Correo electrónico

```
{"conf":{
"email": {
"server": "Example-server",
"port": 25,
"sender": "From email address",
"username": "username",
"password": "password",
"target": {
"0": {"name": "email1@domain.com"},
"1": {"name": "email2@domain.com"}}}
}}
```

Server	Dirección del servidor SMTP (entre comillas)
port	Número de puerto SMTP
sender	Dirección de correo electrónico del remitente (entre comillas)
username	Nombre de usuario SMTP (entre comillas)
password	Contraseña SMTP (entre comillas)
name	Dirección de correo electrónico de destino (entre comillas)

SNMP v1 o v2c

```
{"conf":{
"snmp": {
"v1v2cEnabled": true,
"port": 161,
"readCommunity": "public",
"writeCommunity": "private",
"trapCommunity": "private",
"target": {
"0": {
"port": 162,
"name": "10.20.30.10",
"trapVersion": "1"},
"1": {
"port": 162,
"name": "10.20.30.11",
```

```
"trapVersion": "1"},
"2": {
"port": 162,
"name": "10.20.30.12",
"trapVersion": "2c"}}}
}}
```


v1v2cEnabled	Las opciones son *true* o *false*; activa o desactiva SNMP (versión 1 y 2c)
port	Número de puerto para la comunicación SNMP
readCommunity	Nombre de la comunidad de lectura (entre comillas); debe ser diferente de *writeCommunity*
writeCommunity	Nombre de la comunidad de escritura (entre comillas); debe ser diferente de *readCommunity*
trapCommunity	Nombre de comunidad de trampa (entre comillas)
port	Número de puerto para las trampas de SNMP
name	Dirección (entre comillas) para el destino de las trampas de SNMP
trapVersion	Versión de trampa de SNMP, "1" o "2c"

SNMP v3


```
{"conf":{
"snmp": {
"v3Enabled": true,
"port": 161,
"user": {
"0": {
"privPassword": "password",
"type": "read",
"username": "name",
"privType": "aes",
"authPassword": "password",
"authType": "sha1"},
"1": {
"privPassword": "password",
"type": "write",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"},
"2": {
"privPassword": "password",
"type": "trap",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"}}}
}}
```

v3Enabled	Las opciones son *true* o *false*; activa o desactiva SNMP (versión 1 y 2c)
port	Número de puerto para la comunicación SNMP
type	Tipo de permiso: los valores posibles son "read", "write" o "trap"
username	Nombre de usuario de SNMPv3 (entre comillas)
privPassword	Contraseña de privacidad (entre comillas)
privType	Tipo de cifrado de privacidad; los valores son "aes", "des" o "none"
authPassword	Contraseña de autenticación (entre comillas)
authType	Tipo de autenticación; los valores son "sha1", "md5" o "none"

Syslog

```
{"conf":{
"syslog": {
"enabled": true,
"target": "10.20.30.40",
"port": 514}
}}
```

enabled	Las opciones son *true* o *false*; permite activar la transmisión de mensajes de syslog a un destino remoto
target	Dirección (entre comillas) del destino remoto de los mensajes de syslog
port	Número de puerto de destino para los mensajes

Admin

```
{"conf":{
"contact": {
"description": " Geist GU PDU ",
"location": "Example Location",
"contactName": "Example Contact",
"contactEmail": "email@example.com",
"contactPhone": "123 456 789"},
"system": {"label": "System Label"}
}}
```

description	Descripción de la unidad (entre comillas)
location	Ubicación de la unidad (entre comillas)
contactName	Nombre de contacto de la unidad (entre comillas)
contactEmail	Correo electrónico de contacto de la unidad (entre comillas)
contactPhone	Número de teléfono de contacto de la unidad (entre comillas)
label	Etiqueta del sistema de la unidad (entre comillas)

Locale

```
{"conf":{
"locale": {
"defaultLang": "en",
"units": "metric"}
}}
```

defaultLang	Idioma; las opciones válidas son "de", "en", "es", "fr", "ja", "ko", "pt" y "zh"
units	Unidades; las opciones válidas son "metric" e "imperial"

Intervalo de registro de datos

```
{"conf":{
"datalog": {"interval": 15}
}}
```

interval	Intervalo en minutos para el registro de datos

Agregación

```
{"conf":{
"oneview": {
"enabled": true,
"username": "x",
"password": "pass"}
}}
```

enabled	Las opciones son *true* o *false*; determina si la agregación está activada
username	Nombre de usuario (entre comillas) para establecer dispositivos de matriz
password	Contraseña (entre comillas) a establecer para los dispositivos de matriz (con un valor nulo se elimina la contraseña)

Ejemplo 1

Archivo para configurar un nombre de host, la dirección IP, la puerta de enlace, los nombres de comunidad de SNMP v1 y la configuración regional:

```
{"conf":{
"system": {
"hostname": "hostname1"},
"network": {
"ethernet": {
"dhcpOn": false,
```

```
"address": {
"0": {"address": "10.20.30.40","prefix": 24}}}}
,
"network": {
"ethernet": {
"route": {
"0": {
"gateway": "10.20.30.254",
"prefix": 0,
"destination": "0.0.0.0"}}}}
,
"network": {
"ethernet": {
"dns": {
"0": {"address": "8.8.8.8"},
"1": {"address": "8.8.4.4"}}}}
,
"snmp": {
"v1v2cEnabled": true,
"port": 161,
"readCommunity": "public",
"writeCommunity": "private",
"trapCommunity": "private",
"target": {
"0": {
"port": 162,
"name": "10.20.30.60",
"trapVersion": "1"}}}
,
"locale": {
"defaultLang": "en",
"units": "metric"}
}}
```

Ejemplo 2

Archivo para configurar un usuario administrador, desactivar HTTP y configurar un servidor NTP:

```
{ "auth": {
"username": {
"password": "userpw",
"enabled": true,
"control": false,
"admin": false,
"language": "en"}
},
"conf":{
"http": {
"httpEnabled": false}
,
"time": {
"mode": "ntp",
"zone": "UTC",
```

```
"ntpServer1": "0.pool.ntp.org", "ntpServer2": "1.pool.ntp.org"} }}
```


Ajustes y alarmas del sensor


```
{"dev": {
    "0000000000000000": {
        "label": "PDU 22A",
        "type": "i03",
        "conf": {"outletControlEnabled": true},
        "outlet": {
            "0": {
                "poaAction": "last",
                "rebootHoldDelay": 10,
                "rebootDelay": 5,
                "poaDelay": 1.25,
                "onDelay": 5,
                "mode": "manual",
                "offDelay": 5,
                "label": "Outlet 1"
            },
            "1": {
                "poaAction": "last",
                "rebootHoldDelay": 10,
                "rebootDelay": 5,
                "poaDelay": 1.50,
                "onDelay": 5,
                "mode": "manual",
                "offDelay": 5,
                "label": "Outlet 2"
            }
        },
        "entity": {
            "total0": {"label": "Total"},
            "breaker0": {"label": "Circuit 1"},
            "breaker1": {"label": "Circuit 2"},
            "phase0": {"label": "Phase A"},
            "phase1": {"label": "Phase B"},
            "phase2": {"label": "Phase C"},
            "line3": {"label": "Neutral Line"}
        }
    }
},
"alarm": {
    "action": {
        "0": {
            "target": "trap0",
            "delay": 0,
            "repeat": 0
        },
        "1": {
            "target": "email0",
            "delay": 0,
            "repeat": 0
```

```
        }
    },
     "trigger": {
        "0": {
            "path": "0000000000000000/entity/phase0/measurement/0",
            "severity": "alarm",
            "type": "high",
            "threshold": 222.0,
            "tripDelay": 0,
            "clearDelay": 1,
            "latching": false,
            "selectedActions": ["0","1"]
        },
        "1": {
            "path": "0000000000000000/outlet/0/measurement/0",
            "severity": "alarm",
            "type": "low",
            "threshold": 55.0,
            "tripDelay": 2,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        },
        "2": {
            "path": "0000000000000000/entity/breaker0/measurement/4",
            "severity": "alarm",
            "type": "high",
            "threshold": 12.0,
            "tripDelay": 0,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        },
        "3": {
            "path": "0000000000000000/entity/total0/measurement/0",
            "severity": "alarm",
            "type": "high",
            "threshold": 7200.0,
            "tripDelay": 0,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        }
    }
}}
```

0000000000000000	El ID del dispositivo (que se encuentra en la página *Sensors>Overview*) del RTS que se va a configurar. Si este ID del dispositivo no coincide con ninguno de los dispositivos seleccionados que se están aprovisionando, se aprovisionarán todos los dispositivos seleccionados. La configuración del ID del dispositivo como 0000000000000000 garantiza la configuración de todos los dispositivos seleccionados.
label	La etiqueta del RTS (que se encuentra en la página *Sensors>Overview*)
type	Para configurar alarmas en las mediciones internas del RTS, el valor "type" debe coincidir con el IMD que se esté utilizando en la PDU, por lo que debe ser "i03" para las PDU que utilicen cualquier IMD-03x o IMD-3x, e "i05" para las unidades de RTS que utilicen el IMD-5M. Para configurar alarmas en sensores externos, "type" debe ser el tipo del sensor externo. Los valores válidos son "remotetemp", "afht3", "thd", "t3hd", "a2d", "snt", "snh", "snd". Al omitirse, se evita que se configuren las unidades de RTS seleccionadas cuando el ID del dispositivo no coincida con el de ningún RTS.
outletControlEnabled	Se aplica solo a las unidades de RTS con conmutación de tomacorrientes y determina si es posible controlar los tomacorrientes en un RTS de este tipo. El valor *true* permite controlar los tomacorrientes, el valor *false* impide controlar los tomacorrientes.
outlet	La sección de tomacorrientes se aplica solo a las unidades de RTS con conmutación de tomacorriente y define los ajustes para cada tomacorriente del RTS. Tenga en cuenta que la numeración de los tomacorrientes empieza por 0 (tomacorriente del RTS número 1). Si estos ajustes no requieren cambios, se pueden omitir los tomacorrientes individuales (o toda la sección de tomacorrientes).
poaAction	Define el estado en que se iniciará el tomacorriente cuando se encienda ("on", "off" o "last").
rebootHoldDelay	Tiempo, en segundos, que la unidad espera después de apagar el tomacorriente antes de volver a encenderlo durante un reinicio. Puede ser cualquier número entero entre 0 y 14.400.
rebootDelay	Tiempo, en segundos, que la unidad espera antes de reiniciar un tomacorriente. Puede ser cualquier número entero entre 0 y 14.400.
poaDelay	Tiempo, en segundos, que la unidad espera después del encendido y antes de activar el tomacorriente. Puede ser cualquier número entero entre 0 y 14.400.
onDelay	Tiempo, en segundos, que la unidad espera antes de encender un tomacorriente. Puede ser cualquier número entero entre 0 y 14.400.
mode	Debe tener el valor "manual" para los tomacorrientes controlados por el usuario.
offDelay	Tiempo, en segundos, que la unidad espera antes de apagar un tomacorriente. Puede ser cualquier número entero entre 0 y 14.400.
label	La etiqueta del tomacorriente.

entity	La sección entity se utiliza para etiquetar las mediciones que no son de tomacorrientes en la página *Sensors>Overview*.
total0 label	La etiqueta para el total de RTS en la página *Sensors>Overview*
breaker0 label	Etiqueta para el primer circuito (si está presente). Otros circuitos, si los hubiera, se pueden etiquetar como *breaker1*, *breaker2*, y así sucesivamente.
phase0 label	Etiqueta de la primera fase. Otras fases, si las hubiera, se pueden etiquetar como *phase1* y *phase2*.
line3 label	Etiqueta para la línea neutra.
alarm	En la sección alarm se definen los métodos que se pueden usar para enviar alarmas. Cada método se enumera a partir de 0 y define lo siguiente:
target	Para el envío de alarmas de trampa SNMP, *target* puede tener los valores "trap0", "trap1" y subsiguientes, que hacen referencia a la primera, segunda y subsiguientes trampas SNMP definidas en la página *System>SNMP*. Para el envío de alarmas por correo electrónico, *target* puede tener los valores "email0", "email1" y subsiguientes, que hacen referencia al primer, segundo y subsiguientes correos electrónicos, según se define en la página *System>Email*. Tenga en cuenta que target no debe especificar trampas SNMP ni correos electrónicos que no se hayan configurado.
delay	Determina el tiempo durante el que este evento debe permanecer activado antes de que se envíe la primera notificación vertical de esta acción.
repeat	Determina si se enviarán varias notificaciones para esta acción de evento.
trigger	En esta sección se definen las alarmas que se han configurado, comenzando por la primera, que está numerada con 0.
path	Define la medida en la que se activará la alarma. El formato de este campo es: "0000000000000000/entity/phase0/measurement/0", que define las alarmas para las mediciones de la fase de entrada del RTS; donde phase0 se refiere a la primera fase de entrada del RTS, phase1 se refiere a la segunda fase (si está presente) y así sucesivamente. El número que sigue inmediatamente a la medición indica el tipo de medición que va a activar la alarma, según se define a continuación: 0: Voltaje 4: Corriente 8: Potencia real 9: Potencia aparente 10: Factor de potencia 11: Energía 14: Factor de cresta de corriente

	"0000000000000000/outlet/0/measurement/0" define las alarmas de tomacorrientes para las unidades de RTS con monitoreo de tomacorrientes; donde el número que sigue inmediatamente al tomacorriente especifica su número (comenzando por cero). El número que sigue inmediatamente a la medición indica el tipo de medición que va a activar la alarma, según se define a continuación: 0: Voltaje 4: Corriente 8: Potencia real 9: Potencia aparente 10: Factor de potencia 11: Energía 12: Equilibrio 14: Factor de cresta de corriente "0000000000000000/entity/total0/measurement/0" define alarmas para mediciones de entrada total de fase del RTS. El número que sigue inmediatamente a la medición indica el tipo de medición que va a activar la alarma, según se define a continuación: 0: Potencia real 1: Potencia aparente 2: Factor de potencia 3: Energía "0000000000000000/entity/breaker0/measurement/4" define las alarmas para las alarmas de circuito del RTS, en las que el primer circuito se indica con *breaker0*, el segundo con *breaker1* y así sucesivamente. El número que sigue inmediatamente a la medición indica el tipo de medición que va a activar la alarma, según se define a continuación: 4: Corriente "0000000000000000/entity/line3/measurement/4" define alarmas para las alarmas de corriente neutra del RTS. El número que sigue inmediatamente a la medición indica el tipo de medición que va a activar la alarma, según se define a continuación: 0: Corriente
severity	Describe la gravedad de la alarma generada, y los valores pueden ser "warning" o "alarm".
type	Define si se trata de un umbral alto o bajo, y los valores pueden ser "high" o "low".

threshold	Valor umbral que puede ser cualquier número entre –999,0 y 999,0. La corriente de línea neutra se puede especificar con hasta dos decimales.
tripDelay	La medición debe superar el umbral durante este número de segundos antes de que se dispare el evento. Puede ser cualquier número entero entre 0 y 14.400.
clearDelay	La medición debe volver a la normalidad durante este número de segundos antes de que el evento se borre y se restablezca. Puede ser cualquier número entero entre 0 y 14.400.
latching	Los valores pueden ser *true* o *false*. Si el valor es *true*, el evento y sus acciones asociadas permanecen activos hasta que se reconoce el evento, incluso si la medición vuelve posteriormente a la normalidad.
selectedActions	Especifica cuáles de las acciones definidas anteriormente se pueden usar para enviar la alarma. Por ejemplo ["0","1"] determina las acciones 0 y 1, que se definen como acciones, y usan los valores *trap0* y *email0* en el ejemplo anterior.

Apéndice G: Códigos de error de API/CLI

G.1 Operación exitosa

Código	Explicación
Success	La operación se ha realizado correctamente

Errores de autenticación

Código	Explicación
No Admin user configured	Debe configurarse por lo menos un usuario administrador en el sistema
Not Authorized	El usuario actual no está autorizado
Not Authorized: Session expired	El token utilizado ya no es válido
Not Authorized: Not enough permissions	El usuario actual no tiene permisos suficientes para realizar la operación
Invalid credential combination	Se proporcionaron tanto el nombre de usuario/contraseña como el token o solo se proporcionó el nombre de usuario o la contraseña.
Must have at least one admin user	Debe configurarse por lo menos un usuario administrador en el sistema

Errores de formato JSON

Código	Explicación
Malformed JSON	El JSON recibido no es válido o está dañado
Missing field	No se ha encontrado un campo esperado en la estructura JSON
Duplicate fields	El mismo campo se ha establecido varias veces, por ejemplo en el cuerpo HTTP y en la cadena de consulta

Errores en la ruta

Código	Explicación
Invalid path	La ruta indicada no cumple los requisitos del sistema
Path not found	La ruta indicada no se ha encontrado
Identifier not found	Uno de los campos de la estructura JSON recibida no existe
Field not applicable	Un campo de la estructura JSON existe pero no se debería haber enviado

Errores de validación de datos

Código	Explicación
Invalid input	Un campo de entrada no es válido pero no se ajusta a otras categorías de validación de datos
Input too long	Un campo de entrada supera la longitud máxima permitida
Invalid characters	Un campo de entrada contiene caracteres no válidos para el campo
Invalid serial	Un campo de entrada es un número de serie no válido
Invalid Boolean	Un campo de entrada es un valor booleano no válido
Out of range	Un campo de entrada está fuera del intervalo válido para el campo
Invalid integer	Un campo de entrada no es un entero cuando se espera uno
Invalid number	Un campo de entrada no es un número cuando se espera uno
Invalid URL	Un campo de entrada no es una URL válida cuando se espera una
Invalid IP	Un campo de entrada no es una dirección IP válida cuando se espera una
Paths not allowed	Un campo de entrada contiene una ruta de acceso cuando no se espera una
Invalid username	Un campo de entrada es un nombre de usuario no admisible
Invalid email address	Un campo de entrada no es una dirección de correo electrónico válida cuando se espera una
Invalid option	Un campo de entrada contiene una selección de opción no válida
Invalid datetime	Un campo de entrada no es una fecha u hora válida cuando se espera una
Out of bounds	Un campo de entrada está fuera de los límites permitidos para el campo
Invalid week	Un campo de entrada representa una selección de días de la semana no válida
Duplicate entry	Un campo de entrada crearía un duplicado cuando no se permite uno
Invalid Route	Una ruta de red se ha configurado de forma incorrecta

Otros errores

Código	Explicación
Unknown error	Se ha producido un error del sistema para el que no es aplicable ningún otro código de error
Command not allowed	El comando recibido no está permitido en la ruta de acceso especificada
System busy	La acción que se ha intentado no se puede ejecutar en este momento y se debe reintentar

Errores de coherencia de datos

Código	Explicación
Inconsistent state	El comando dejará el sistema en un estado incoherente, por lo que se ha rechazado
Syslog enabled requires target	La activación de syslog remoto requiere que se especifique un host de destino
NTP mode requires servers	La activación de NTP requiere servidores para consultas
Start time must come before end time	Se ha recibido una hora para la que el final llegó antes del inicio
Invalid SNMPv3 auth/priv combination	La privacidad de SNMPv3 no se puede usar sin autenticación
Port not available	Se ha intentado establecer un número de puerto que ya se encuentra en uso
Vertiv Intelligence Director missing credentials	Para habilitar Vertiv Intelligence Director es necesario establecer un nombre de usuario y una contraseña
Time not settable	Para poder ajustar la fecha y la hora se necesita el modo de hora manual

Errores de carga

Código	Explicación
Invalid firmware package	El paquete tiene un formato incorrecto o está dañado
Invalid file key	El paquete especifica una clave OEM incorrecta y no se puede usar con esta unidad
Invalid version	La versión es demasiado antigua o no es compatible
Producto no válido	El paquete se ha diseñado para una arquitectura de hardware diferente
Invalid certificate file	El certificado SSL proporcionado no se ha podido analizar
Invalid certificate password	La contraseña no ha funcionado con el certificado SSL proporcionado

Apéndice H: Un ejemplo de configuración de LDAP para credenciales de *Active Directory*

H.1 Información general

La integración de *Active Directory* con el dispositivo de monitoreo intercambiable (IMD) de la marca Vertiv y de la marca Geist permite la autenticación y autorización de los usuarios en la interfaz CLI y en la web del IMD utilizando sus credenciales empresariales de *Active Directory*. También se autorizará al usuario para uno de los tres roles del IMD basados en un grupo de seguridad de *Active Directory* del que el usuario es miembro. Estos roles son:

- *Admin*: derechos de configuración totales, incluidos los permisos de rol *Control*.
- *Control*: capacidad de controlar el estado del tomacorriente, si corresponde, cambiar los nombres de los dispositivos y los ajustes de alarmas/eventos.
- *Enabled*: solo lectura de los ajustes de configuración y ninguno de los derechos de configuración de tomacorrientes.

H.2 Requisitos generales y notas

- IMD v5.3.3 o el nuevo firmware se pueden usar para este procedimiento.
- Los ejemplos se representan en verde.

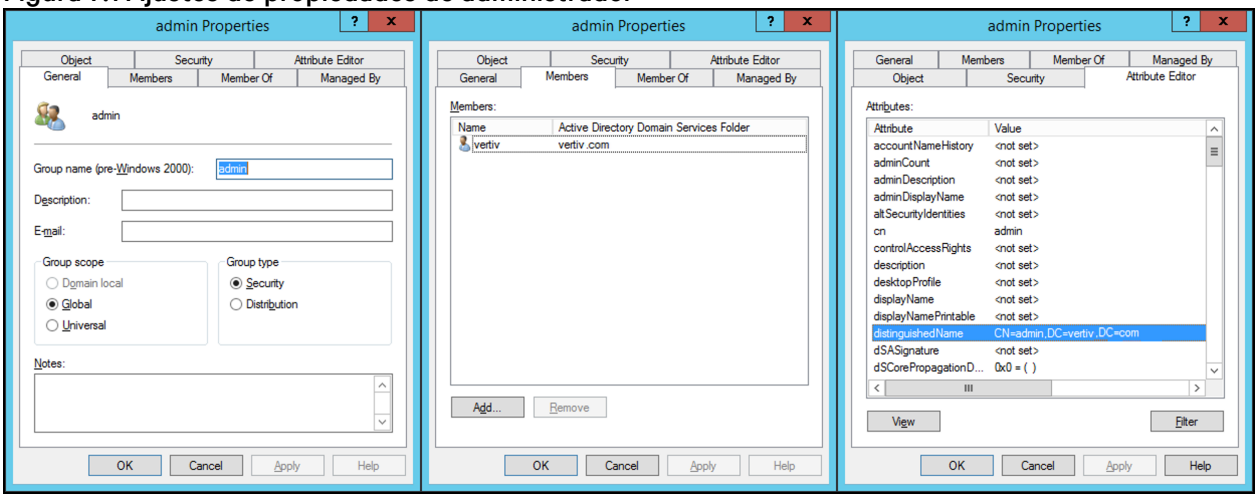
H.3 Procedimiento de configuración de *Active Directory*

- Cree o utilice una cuenta *AD bind* existente para el IMD. El IMD utilizará esta cuenta para buscar en el dominio AD y autenticar a los usuarios. La contraseña de esta cuenta debe estar configurada para que no caduque nunca.
- Cree uno o más grupos de seguridad de AD para representar los roles del IMD: *Admin, Control* y *Enabled*.
- Incluya al usuario de AD como miembro del grupo de seguridad aplicable.
    - En el ejemplo que se muestra a continuación, a la cuenta de AD vertiv se le asignó un miembro del grupo de seguridad admin. Como resultado, la cuenta de usuario de AD vertiv asumirá el rol *Admin* del IMD al iniciar sesión.

NOTA: El nombre del grupo de seguridad es a su discreción. El nombre del grupo de seguridad y el DN deben coincidir con lo definido en la sección Group de LDAP del IMD.

NOTA: Un usuario de AD que pertenezca a más de uno de estos grupos de seguridad asignados a los roles del IMD heredará los privilegios de rol más elevados.

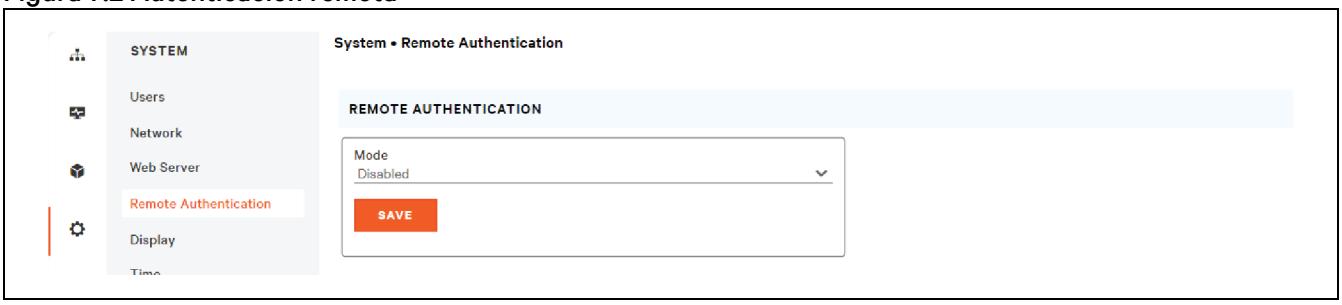
Figura 7.1 Ajustes de propiedades de administrador



H.4 Procedimiento de configuración del IMD (interfaz web)

- Abra un navegador web con la IP o el nombre DNS del IMD e inicie sesión como la cuenta de administrador local.
- Desplácese a *System>Remote Authentication*.
- Establezca el modo de autenticación remota en LDAP y guarde.

Figura 7.2 Autenticación remota



- Consulte la ilustración siguiente para ver las descripciones de los ajustes de la sección de LDAP.

Figura 7.3 Ajustes de LDAP

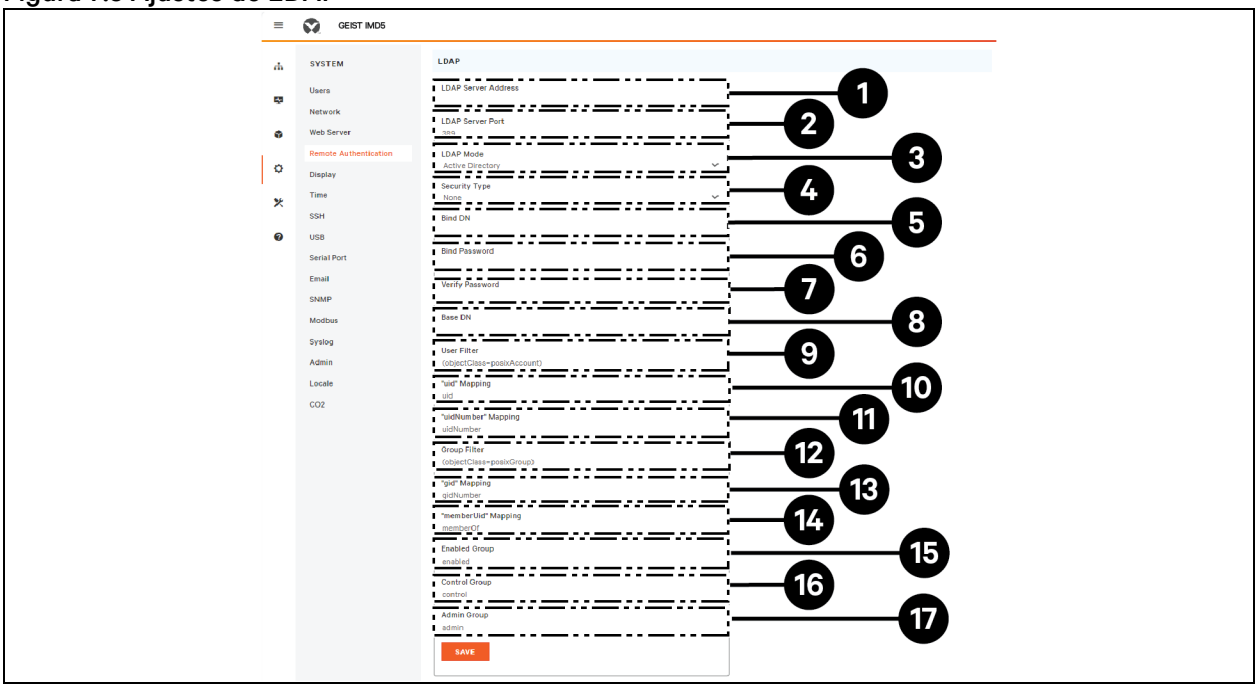


Tabla 7.4 Ajustes de LDAP

Elemento	Descripción
1	Dirección IP del servidor de *Active Directory*
2	Puerto TCP de *Active Directory*[2] 389 - Non SSL 636 - SSL
3	Modo LADAP OpenLDAP - *Active Directory*
4	Seguridad de *Active Directory*[2] None - SSL - StartTLS
5	Cuenta de AD usada para enlazar al servidor de AD Debe estar en notación de ruta de DN completo CN=adbindacct,CN=Usuarios,DC=vertiv,DC=com La contraseña de la cuenta no debe caducar
6	Establecer contraseña de cuenta de enlace de AD
7	Verificar contraseña
8	Ruta de dominio base para buscar usuarios de AD[1] Debe estar en notación de ruta de DN completo DC=vertiv, DC=com
9	Filtro de atributo ObjectClass de usuario de AD (objectClass=usuario)

Tabla 7.4 Ajustes de LDAP

Elemento	Descripción
10	Filtro de nombre de cuentas de usuario de AD samaccountname
11	Asignación de "uidNumber" uidNumber
12	Filtro de atributo ObjectClass de grupo de AD (objectClass=grupo)
13	Asignación de "gid" gidNumber
14	Ajuste requerido memberOf
15	Asignación del grupo de seguridad de AD al rol *Enabled* Debe estar en notación de ruta de DN completo CN=habilitado, DC=vertiv, DC=com
16	Asignación del grupo de seguridad de AD al rol *Control* Debe estar en notación de ruta de DN completo CN=control, DC=vertiv, DC=com
17	Asignación del grupo de seguridad de AD al rol *Admin* Debe estar en notación de ruta de DN completo CN=administrador, DC=vertiv, DC=com
NOTA: [1]La mejor práctica es reducir el alcance de cruce del dominio de AD para buscar usuarios autenticados. Intente no especificar solo el dominio base si hay un esquema de AD grande y anidado. • Ideal: OU=usuarios habilitados, Ou=cuentas de usuarios, DC=vertiv, DC=com • No ideal: DC=vertiv, DC=com	
NOTA: [2]StartTLS utiliza el puerto TCP 389. Inicialmente, establece la sesión no cifrada, pero cifrará la sesión a partir de ese momento si el servidor de *Active Directory* acepta la solicitud LDAP_START_TLS_OID.	

Conectar con Vertiv en las redes sociales

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

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

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

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

Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 EE. UU.

SL-71272_REVA_08-24