Unidade de distribuição de energia no rack Geist™

Guia do Usuário/Instalador

Série M e série D com e sem upgrade (equipadas com Firmware 6.x.x)

As informações contidas neste documento estão sujeitas a alterações sem notificação prévia e podem não ser adequadas a todas as aplicações. Embora toda precaução tenha sido tomada para garantir a precisão e a abrangência deste documento, a Vertiv não assume qualquer responsabilidade e isenta-se de toda responsabilidade civil por danos resultantes do uso destas informações ou por quaisquer erros ou omissões.

Consulte os regulamentos locais e os códigos de construção referentes a aplicação, instalação e operação deste produto. O engenheiro de consultoria, o instalador e/ou o usuário final é responsável pela conformidade com todas as leis e os regulamentos vigentes relacionados a aplicação, instalação e operação deste produto.

Os produtos cobertos por este manual de instruções são fabricados e/ou vendidos pela Vertiv. Este documento é de propriedade da Vertiv e contém informações confidenciais e proprietárias da Vertiv. É estritamente proibido copiá-lo, usá-lo ou divulgá-lo sem a permissão por escrito da Vertiv.

Nomes de empresas e produtos são trademarks ou trademarks registradas das respectivas empresas. Qualquer dúvida sobre o uso de nomes de trademarks deve ser direcionada ao fabricante original.

Site do Suporte técnico

Se você encontrar algum problema de instalação ou operacional com o seu produto, verifique a seção pertinente deste manual para ver se o problema pode ser resolvido seguindo os procedimentos descritos.

Visite https://www.vertiv.com/pt-latam/suporte/ para obter mais ajuda.

SUMÁRIO

Esta página foi deixada intencionalmente em branco

1 Instruções importantes de segurança

Conformidade com normas

Os produtos da Vertiv são regulamentados para conformidade de segurança, emissões e impacto ambiental de acordo com os órgãos e as normas a seguir.

Underwriters Laboratories (UL)

Os padrões UL são usados para avaliar produtos; testar componentes, materiais, sistemas e desempenho e avaliar produtos sustentáveis ao meio ambiente, energias renováveis, produtos alimentícios e que utilizam água, sistemas de reciclagem e outras tecnologias inovadoras.

Os padrões UL específicos deste equipamento estão descritos na placa de identificação do dispositivo.

CE

A posição da marca CE no produto significa que ele está em conformidade com as normas de proteção ambiental, saúde e segurança aplicáveis da Europa (EU), incluindo a legislação e as diretivas de produtos da EU. A marca CE é obrigatória para produtos comercializados no Espaço Econômico Europeu (EEE).

As regulamentações, as diretivas e as normas específicas aplicáveis a cada produto estão especificadas na Declaração de Conformidade.

Comissão Federal de Comunicações (FCC)

A Comissão Federal de Comunicações (FCC) regulamenta as comunicações interestaduais e internacionais por rádio, televisão, meios eletrônicos, satélite e cabo em todos os 50 estados, no Distrito de Colúmbia e nos territórios americanos. A FCC é uma agência independente governamental dos EUA, supervisionada pelo Congresso e a principal autoridade do país para leis, regulamentos e inovação tecnológica de comunicações.

Os padrões FCC específicos deste equipamento são:

- Este dispositivo Classe A está em conformidade com a parte 15 das Normas FCC.
- A operação está sujeita às duas condições a seguir:
  - Este dispositivo não pode causar interferências prejudiciais.
  - Este dispositivo deve aceitar qualquer interferência recebida, incluindo aquela que pode provocar uma operação indesejada.
- Este aparelho digital de Classe A está em conformidade com a norma ICES-003 do Canadá.
- Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ADVERTÊNCIA! As alterações ou modificações nesta unidade não aprovadas expressamente pela parte responsável pela conformidade poderão invalidar a autoridade do usuário de operar este equipamento.

NOTA: Visite *http://www.Vertiv.com/ComplianceRegulatoryInfo* para obter informações importantes sobre segurança antes da instalação.

Esta página foi deixada intencionalmente em branco

2 Visão geral

A Unidade de distribuição de energia no rack Geist™ Vertiv™ (rPDU) oferece aos gerentes de data center a flexibilidade de instalação exigida atualmente. Da potência básica ao monitoramento de potência e o chaveamento de tomada, a linha de produtos rPDU Geist™ atende às necessidades das empresas agora e no futuro.

Para estabelecer esse caminho de atualização, os engenheiros da Vertiv utilizaram o design robusto da rPDU Geist™ e incorporaram um Dispositivo de monitoramento intercambiável (IMD). As PDUs duram muitos anos e, com o design do IMD, as empresas poderão atualizá-las para tecnologias de monitoramento mais recentes no futuro sem precisar substituir toda a rPDU Geist™. O IMD intercambiável a quente é alterado em algumas etapas simples, sem interromper a alimentação dos servidores críticos.

2.1 Ambiental

Os limites ambientais e operacionais referentes à temperatura, umidade e elevação seguem as definições apresentadas nas tabelas abaixo.

Tabela 2.1 Limites de temperatura

Descrição	Mínimo	Máximo
Durante a operação	10 °C (50 °F)	60 °C (140 °F)
Armazenamento	-40 °C (-40 °F)	70 °C (158 °F)

Tabela 2.2 Limites de umidade

Descrição	Mínimo	Máximo
Durante a operação	5%	95% (sem condensação)
Armazenamento	5%	95% (sem condensação)

Tabela 2.3 Limites de elevação

Descrição	Mínimo	Máximo
Durante a operação	0 m (0 pés)	3.050 m (10.000 pés)
Armazenamento	0 m (0 pés)	15.240 m (50.000 pés)

2.2 Configurações elétricas

As características e o desempenho dos produtos elétricos estão definidos na Tabela 2.4 abaixo. Consulte também a placa de identificação do produto para saber outros limites de classificação.

Tabela 2.4 Classificações do receptáculo

Tipo	Classificações
Combinação C13/C19	250 VCA, 16 A (UL & CSA 16 A, 250 VCA) com cabo C20 250 VCA, 10 A (UL & CSA 12 A, 250 VCA) com cabo C14 **NOTA: Cada bateria de tomada de combinação C13/C19 está restrita a no máximo 32 A por banco.**
German Schuko	250 VAC, 16 A
IEC-60320 C13	250 VAC, 10 A (UL e CSA 12 A, 250 VAC)
IEC-60320 C19	250 VAC, 16 A (UL e CSA 16 A, 250 VAC)
IEC309 PS6	230 VAC, 16 A
IEC309 PS56	230/400 VCA, 32 A
NEMA 5-15R ou L5-15R	125 VAC, 12 A
NEMA 6-15R ou L6-15R	250 VAC, 12 A
NEMA 5-20R ou L5-20R	125 VAC, 16 A
NEMA 6-20R ou L6-20R	250 VAC, 16 A
NEMA L5-30R	125 VAC, 24 A
NEMA L6-30R	250 VAC, 24 A
NEMA L7-15R	277 VAC, 12 A
NEMA L7-20R	277 VAC, 16 A
Saf-D-Grid	277 VAC, 16 A
IEC-60320 C13 com trava U-Lock	250 VAC, 10 A (UL e CSA 12 A, 250 VAC)
IEC -60320 C19 com trava U-Lock	250 VAC, 16 A (UL e CSA 16 A, 250 VAC)
Reino Unido BS1363	250 VAC, 13 A

2.3 Redes

Os requisitos de comunicação do produto estão definidos nas seções a seguir.

2.3.1 ETHERNET

A velocidade da conexão ETHERNET deste produto é: 10/100/1000 Mb, full duplex.

2.3.2 Protocolos

Os protocolos de comunicação aceitos neste produto incluem: ARP, IPv4, IPv6, ICMP, ICMPv6, NDP, TCP, UDP, RSTP, STP, DNS, HTTP, HTTPS (TLSv1.3), SMTP, SMTPS, Modbus TCP/IP, DHCP, SNMP (V1/V2c/V3), LDAP, TACACS+, RADIUS, NTP, SSH, RS232 e Syslog.

2.3.3 Interfaces do usuário

Este produto é compatível com as seguintes interfaces do usuário: SNMP, GUI da Web baseada em JSON, API JSON e interface de linha de comando por SSH ou serial (RS232).

Esta página foi deixada intencionalmente em branco

3 Instalação

Consulte as imagens na seção de montagem para instalar a rPDU Geist™.

NOTA: Visite http://www.Vertiv.com/ComplianceRegulatoryInfo para obter informações importantes sobre segurança antes da instalação.

Para instalar sua unidade:

1. Use equipamentos de proteção individual (EPI).
2. Usando o hardware adequado, encaixe a unidade no rack.
3. Conecte a rPDU Geist™ a um receptáculo de circuito da ramificação com proteção e valor nominal adequados.
4. Conecte os dispositivos que serão ligados pela rPDU Geist™.
5. Ligue cada dispositivo conectado à rPDU Geist™.

NOTA: É recomendado ligá-los na sequência para evitar corrente de partida.

3.1 Montagem

Os suportes opcionais são vendidos separadamente.

Figura 3.1 Suportes de comprimento completo

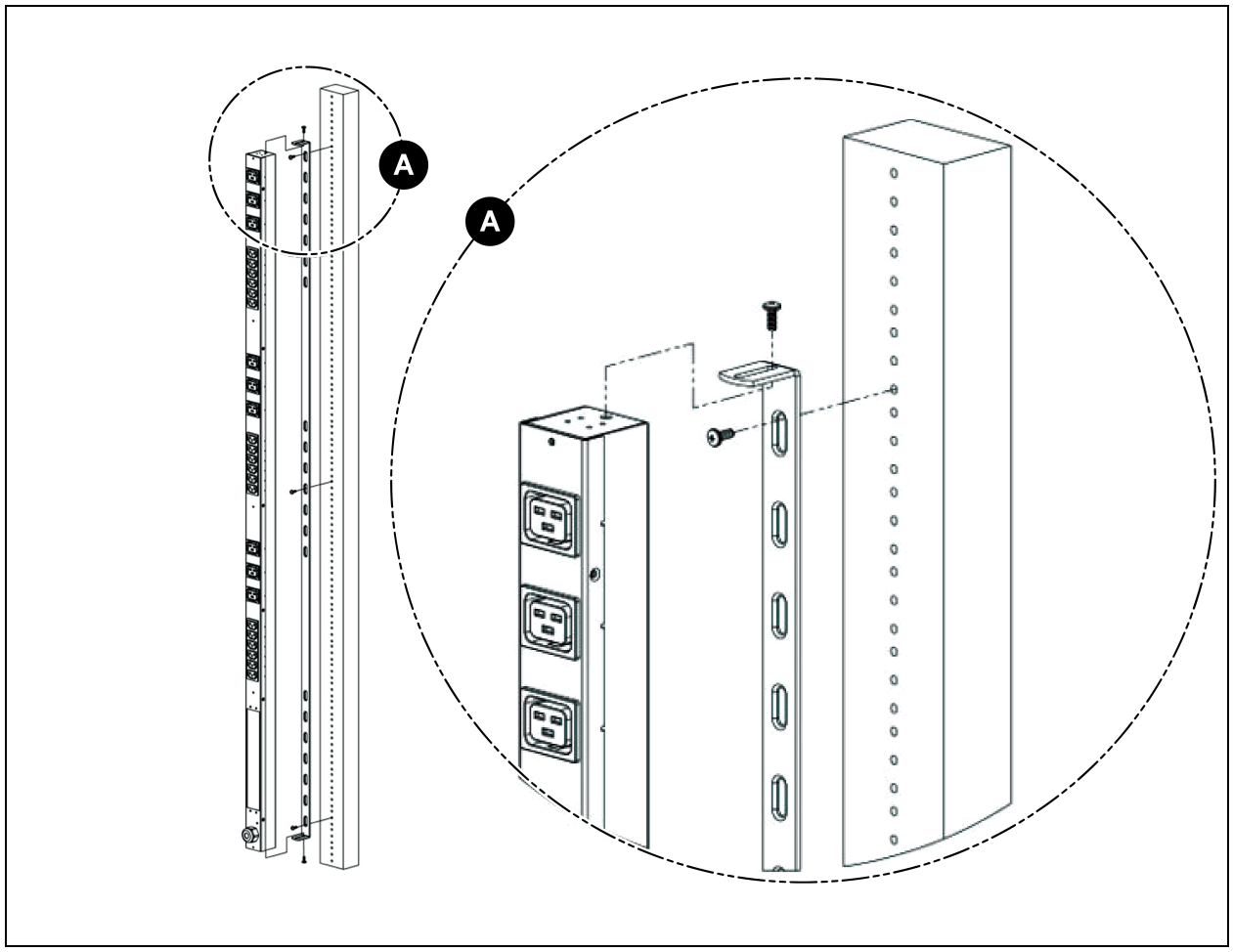


Figura 3.2 Suportes mini em L

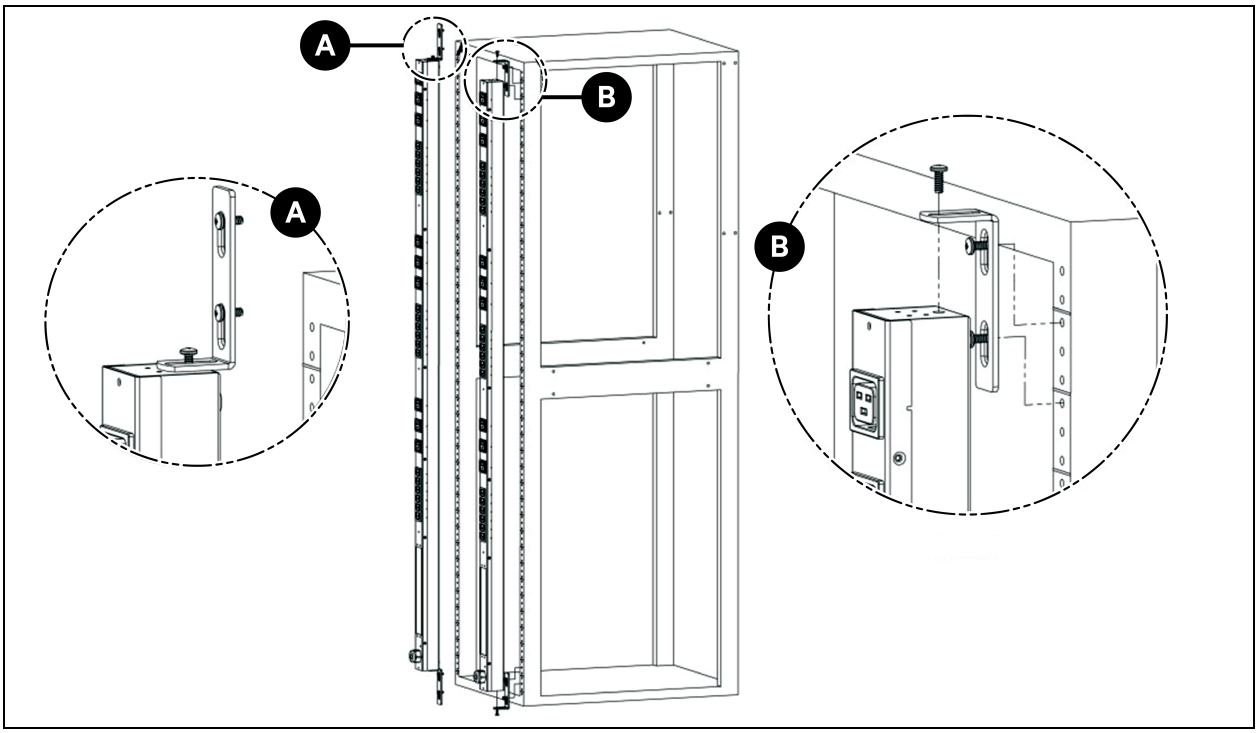


Figura 3.3 Suportes de extensão vertical

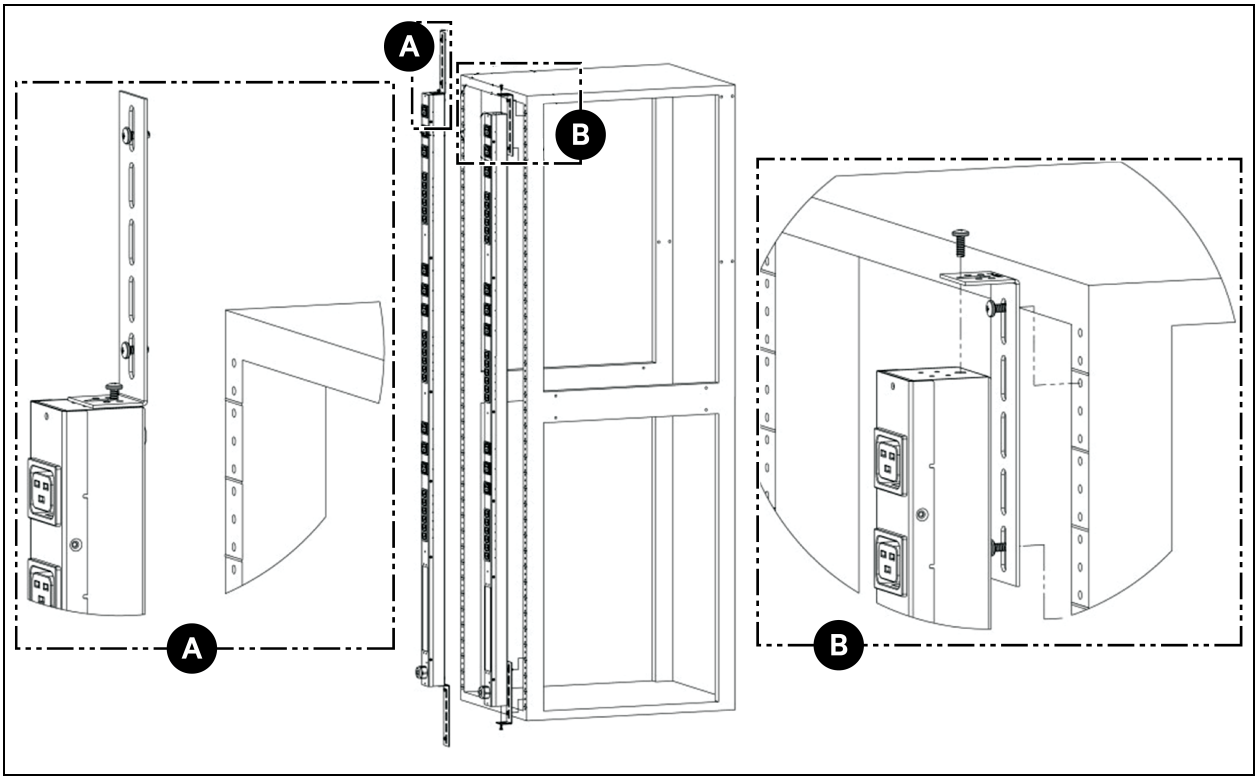


Figura 3.4 Hardware de montagem sem ferramentas

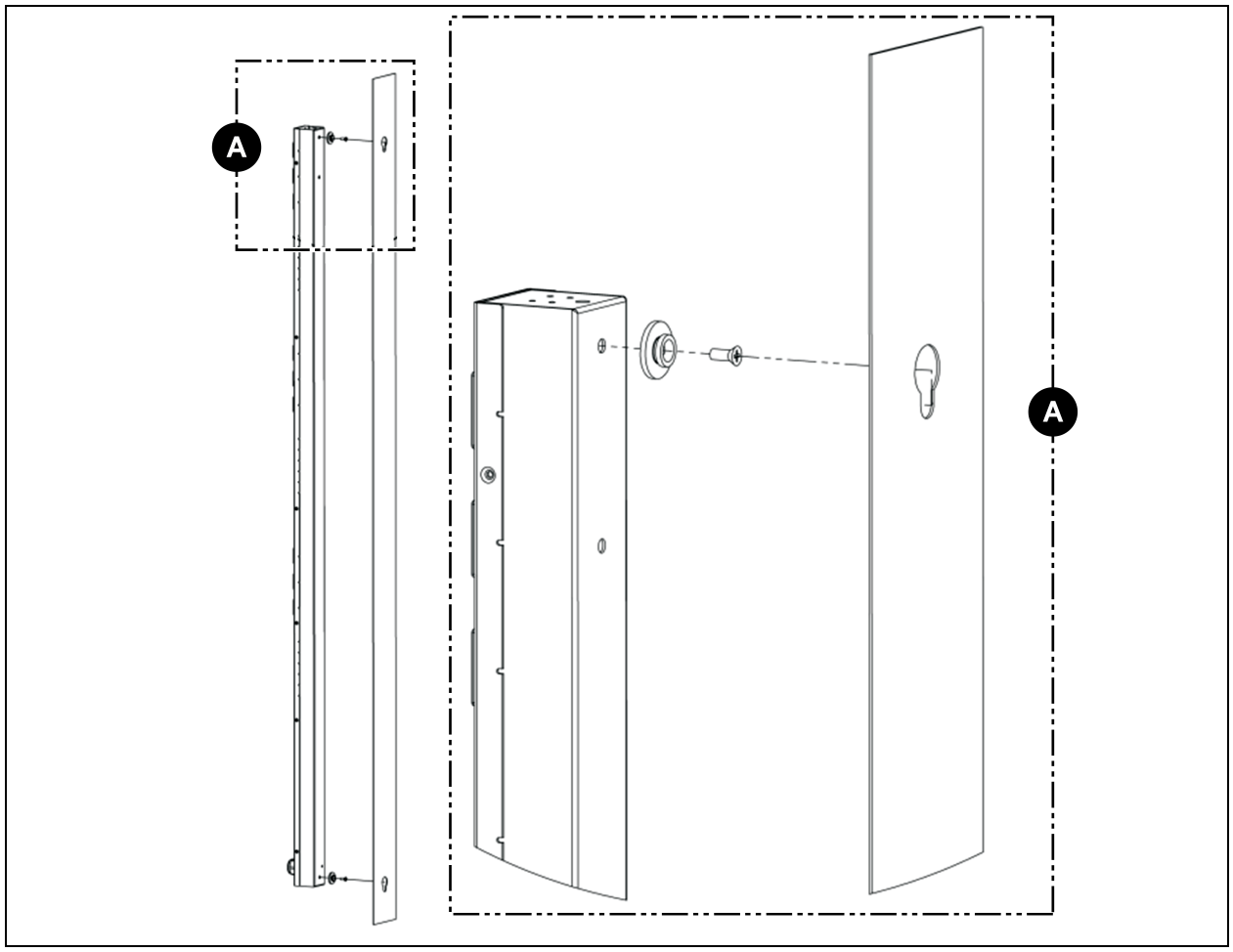
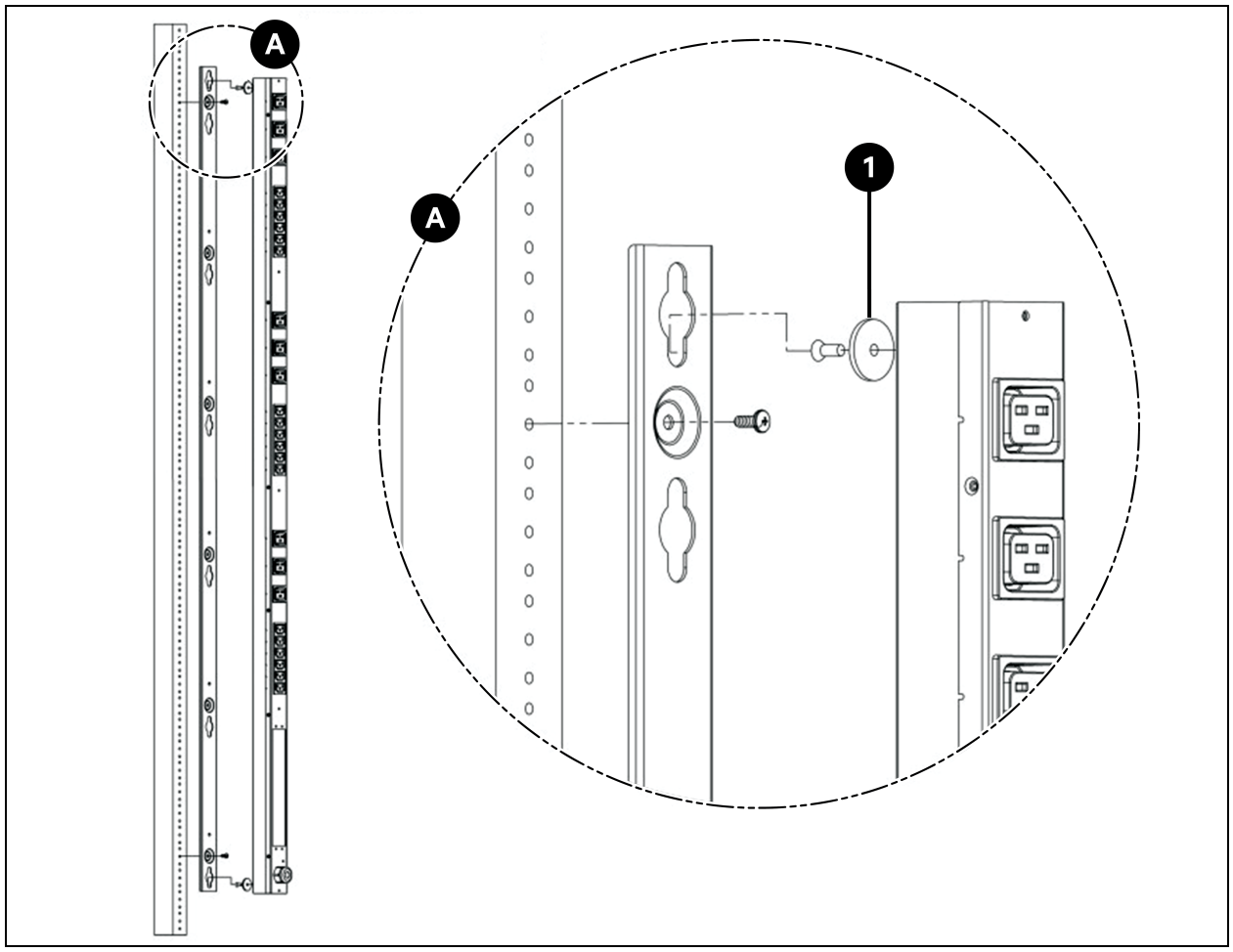


Figura 3.5 Suportes de comprimento completo sem ferramentas



Item	Descrição
1	Arruela de entalhe sem ferramentas

Figura 3.6 Suportes simples de montagem lateral para duas unidades

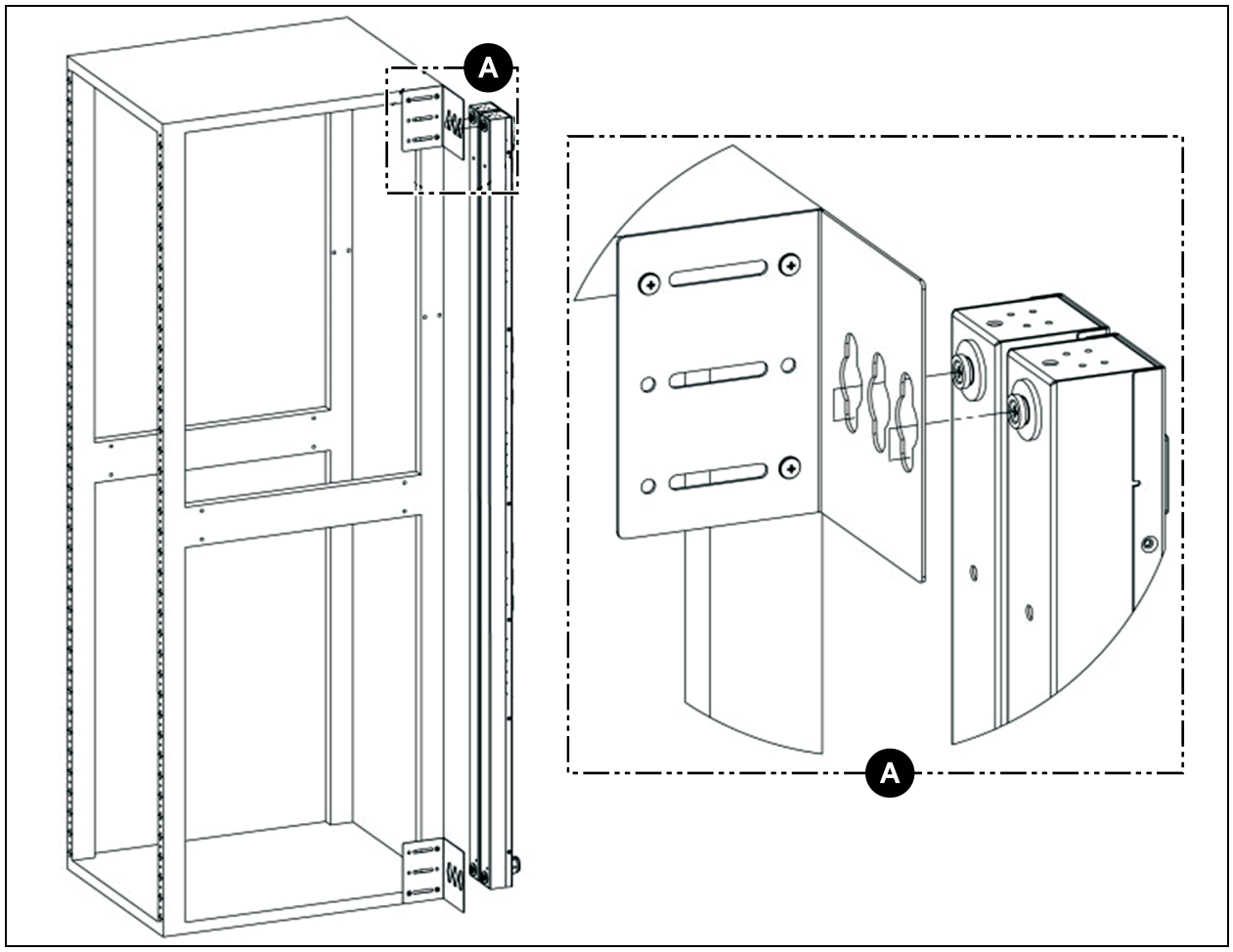
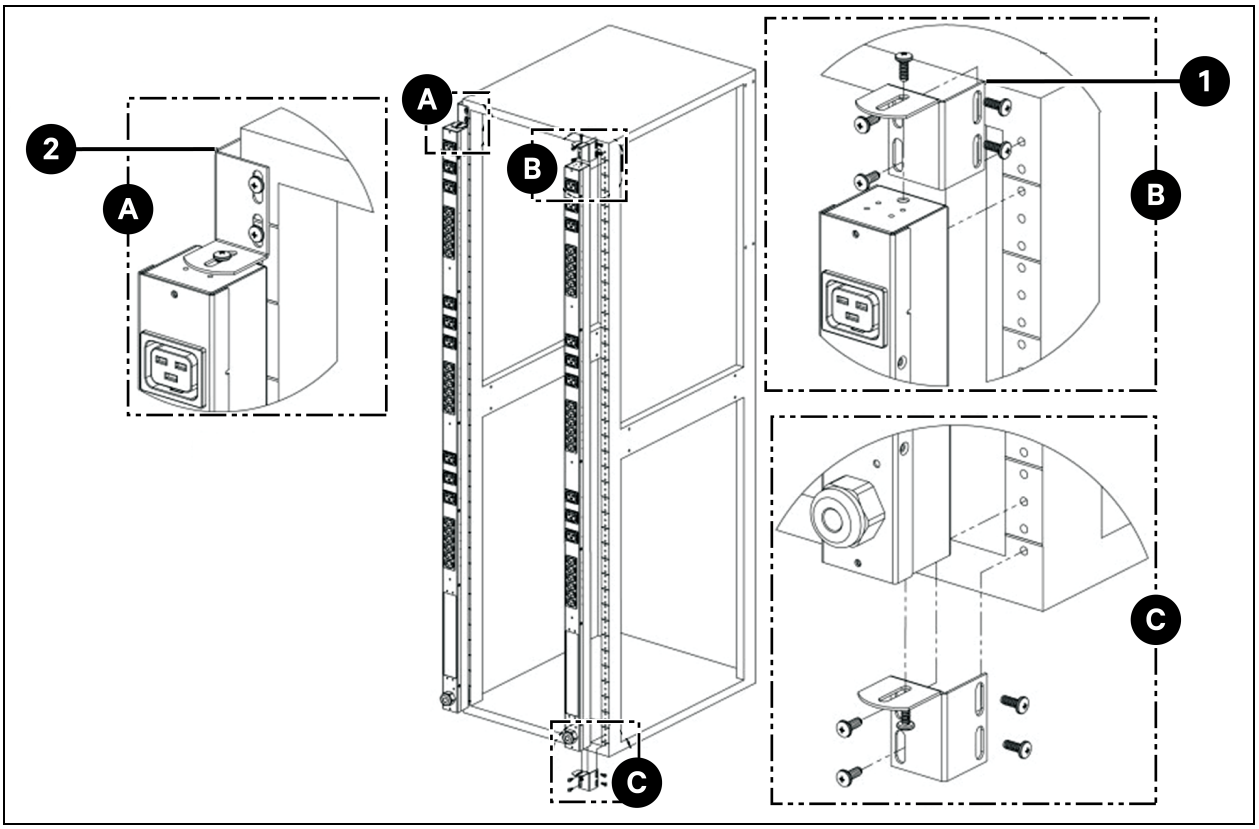


Figura 3.7 Suportes de montagem lateral/deslocamento



Item	Descrição
1	Opção do lado direito
2	Opção do lado esquerdo

Figura 3.8 Suportes de extensão de 7" (polegadas)

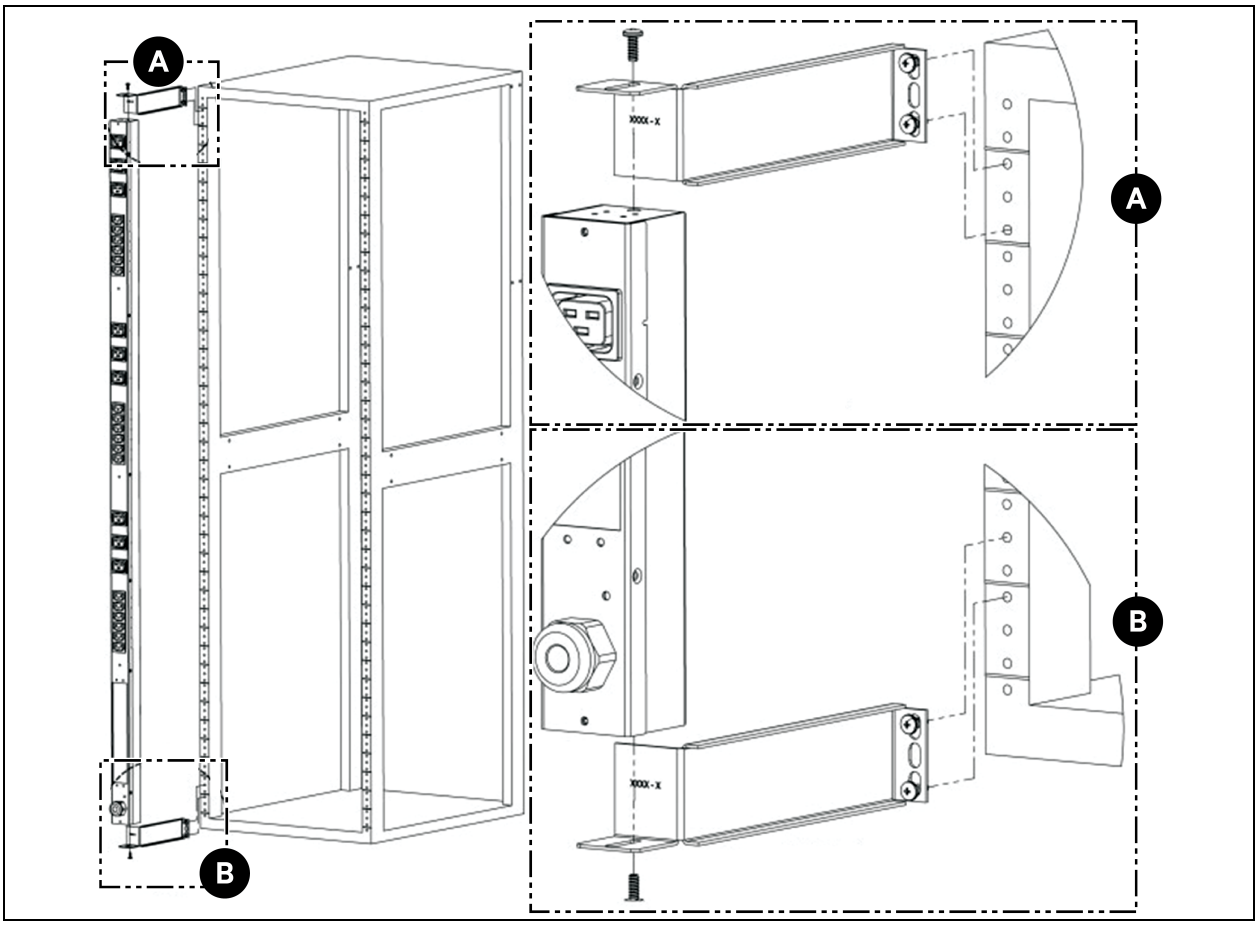


Figura 3.9 Suporte de montagem embutido

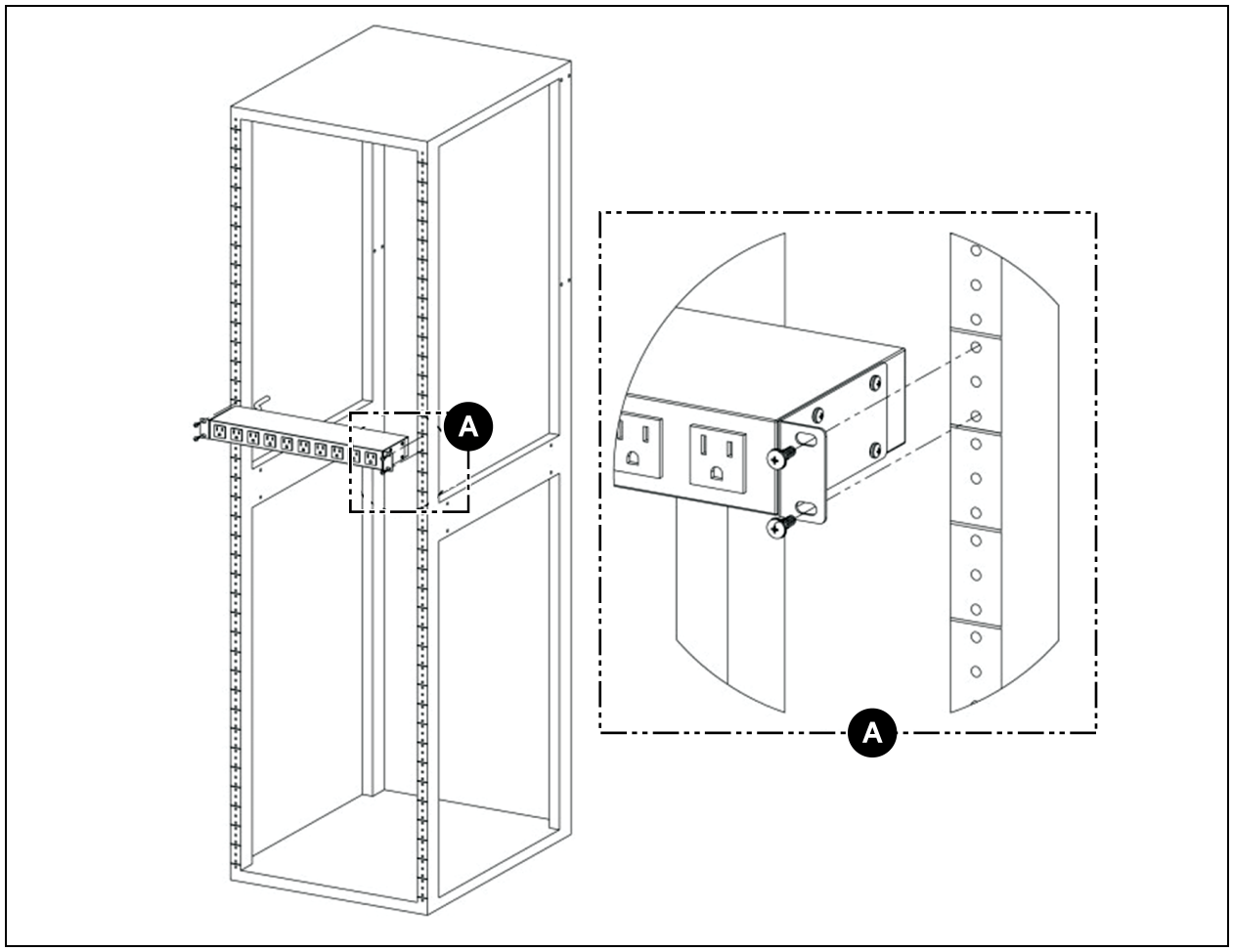


Figura 3.10 Suporte de montagem ajustável

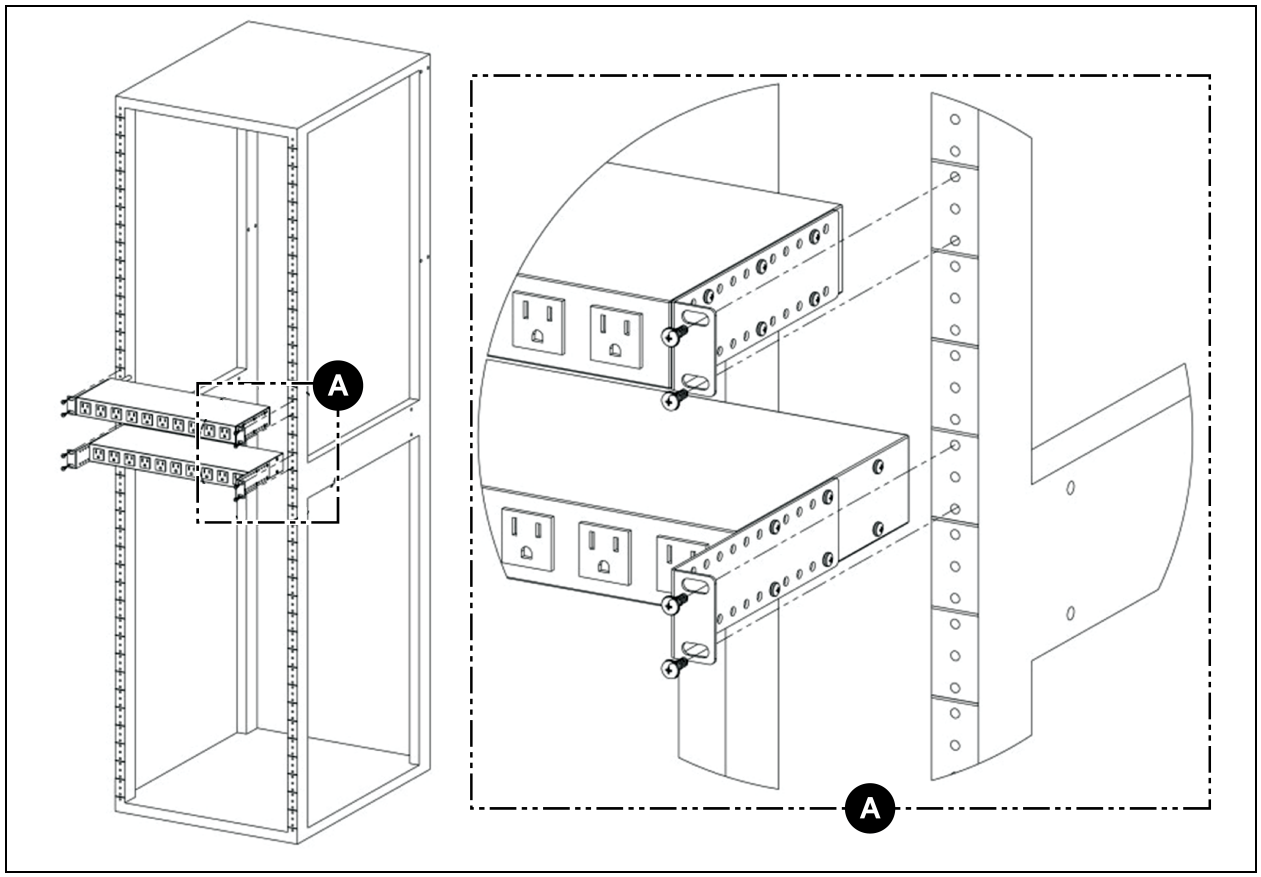


Figura 3.11 Suporte de montagem no painel

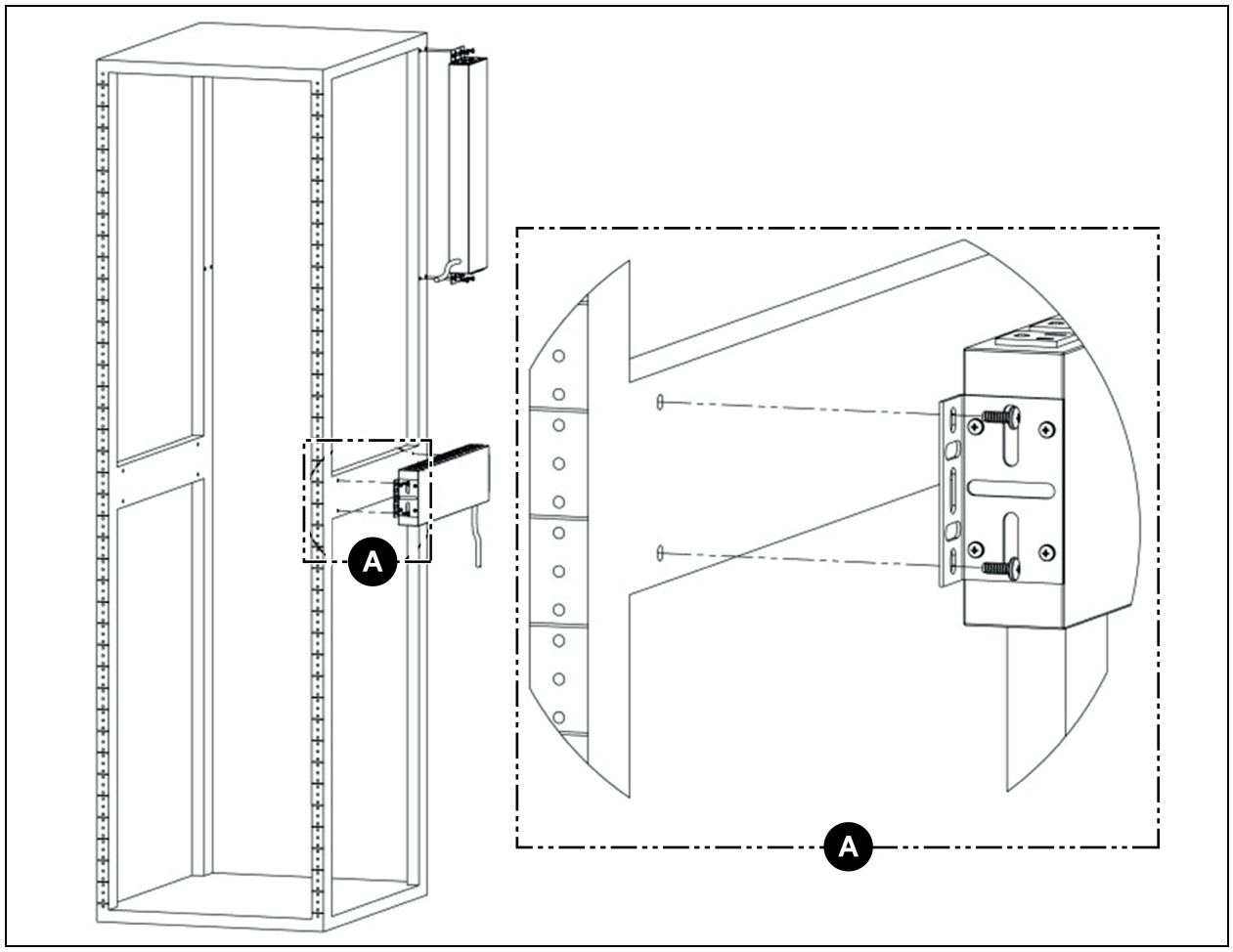


Figura 3.12 Suportes de montagem-conversão de 23" (polegadas)

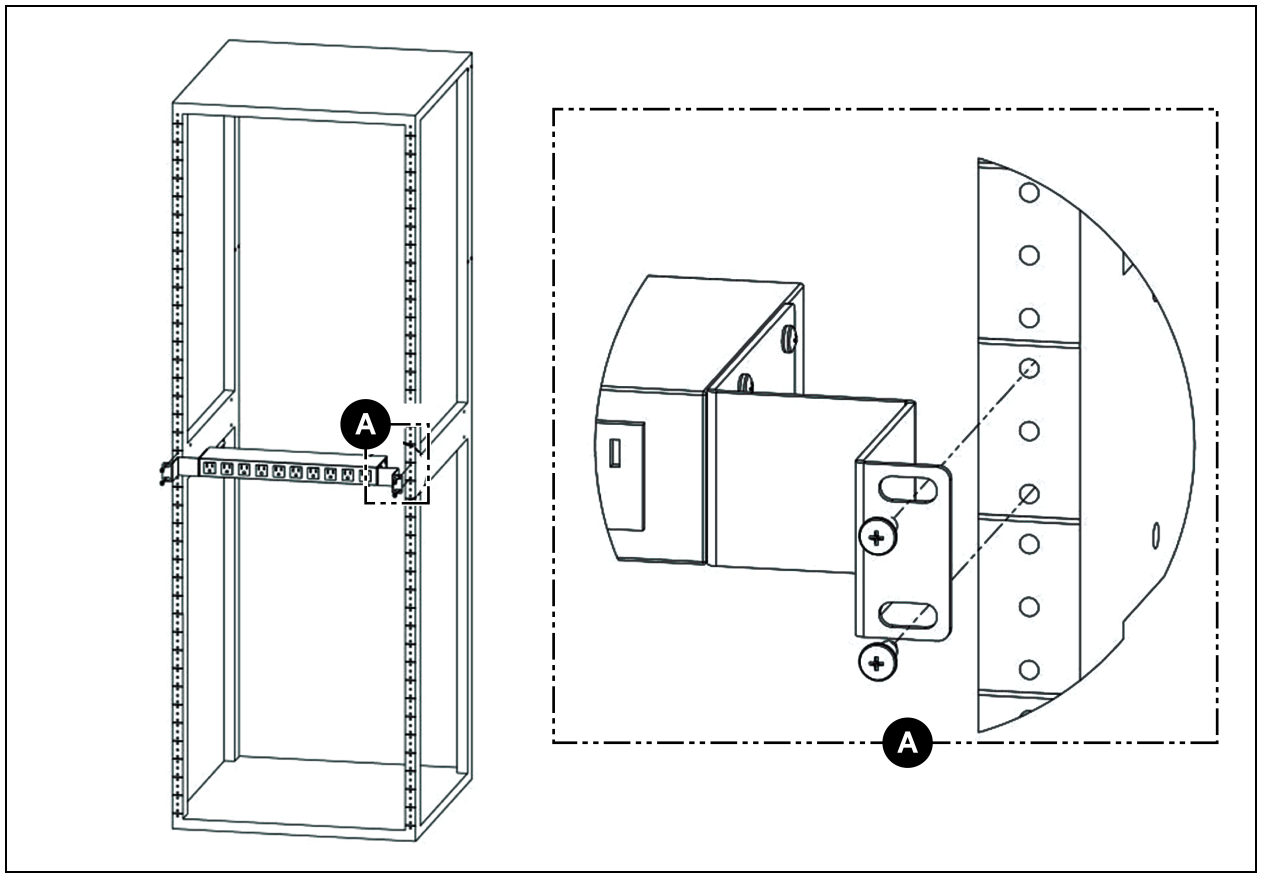


Figura 3.13 Suportes de montagem horizontal/no painel de 19" (polegadas)

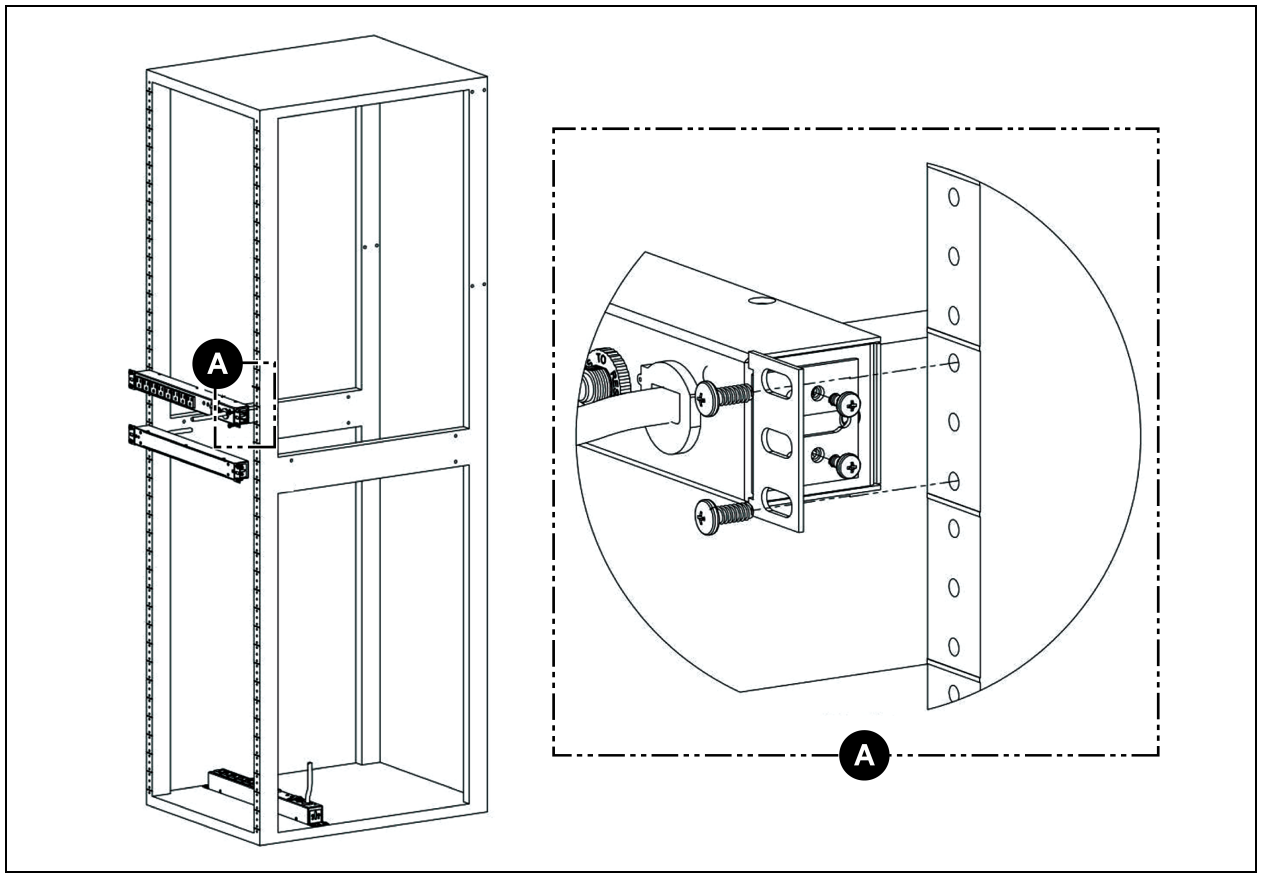
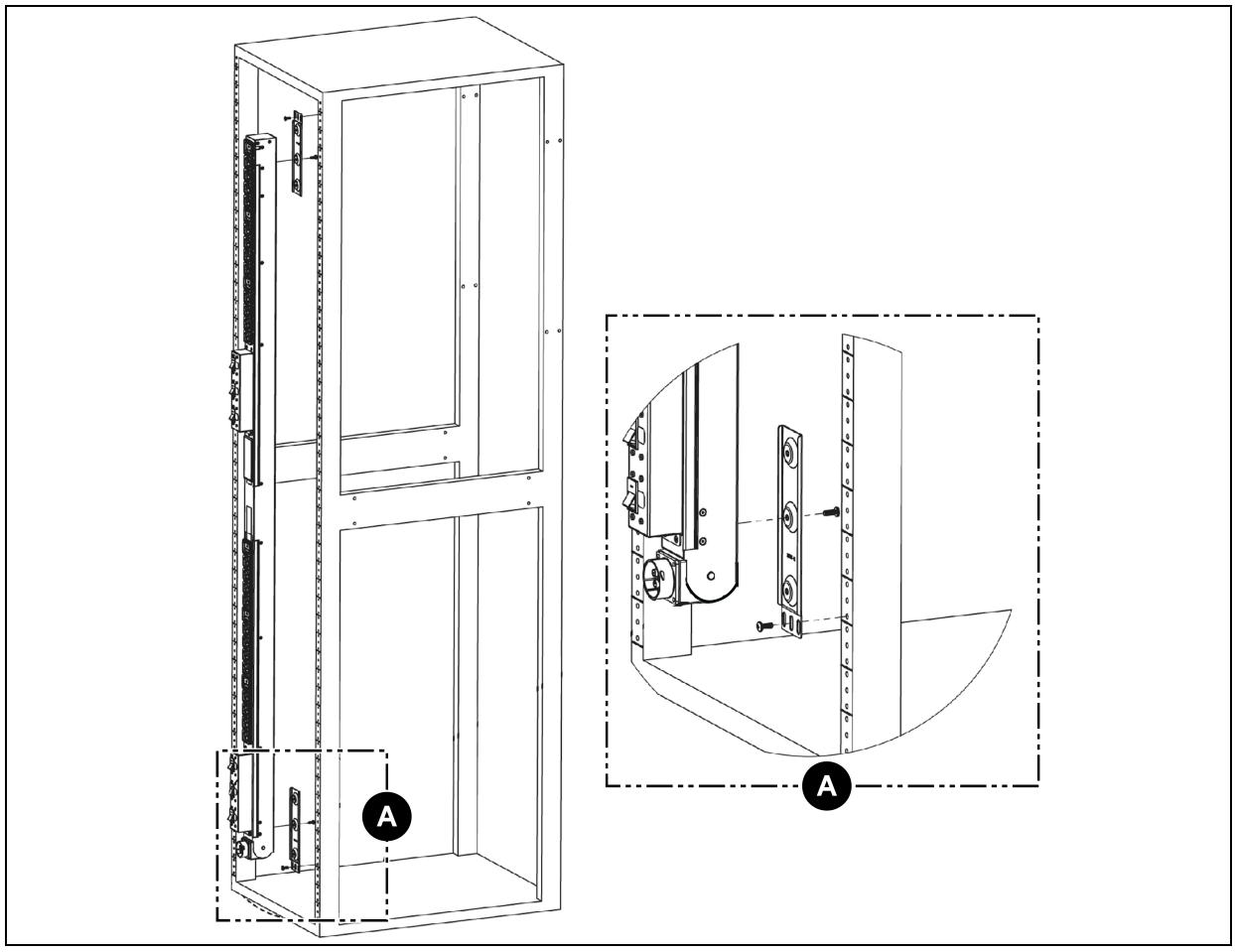


Figura 3.14 Suportes de montagem para a unidade de distribuição de energia universal Geist™ Vertiv™ (UPDU) com extremidade giratória



3.2 Conexão elétrica

Conecte a rPDU Geist™ Vertiv™ a um receptáculo de circuito da ramificação com proteção e valor nominal adequados. Verifique se o cabo de força não excede o raio de curvatura (10X) do fabricante.

3.2.1 Operação de U-Lock

Conecte os dispositivos que serão ligados pela rPDU Geist™.

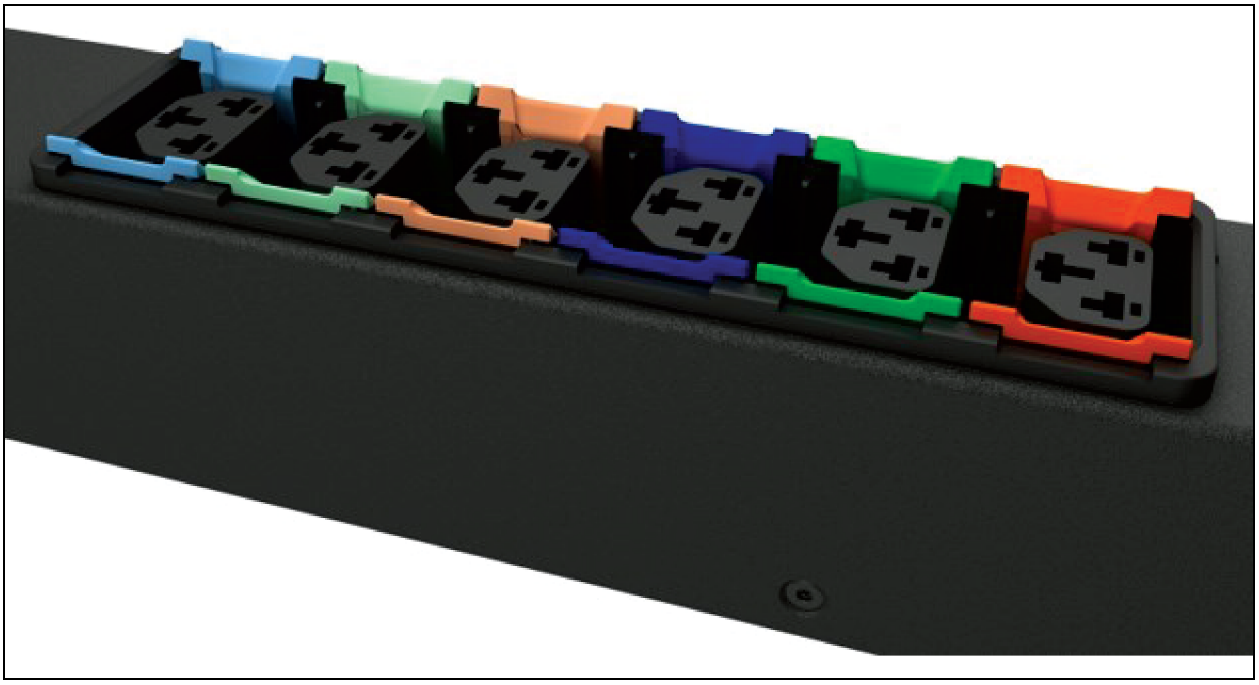
- Retenção de cabo de alimentação U-Lock com patente da Vertiv.
- Usa cabos de alimentação padrão.
- Sistema de bloqueio ativado pela inserção do cabo.
- Recurso de desbloqueio por bisel fácil de empurrar e segurar.

Figura 3.15 Operação de retenção de cabo U-Lock

3.2.2 Operação de P-Lock

- Conecte os dispositivos que serão ligados pela rPDU Geist™.
- Vertiv™ Tomada combinada C13/C19 com retenção do cabo de alimentação P-Lock.
- Compatível com cabos de alimentação P-Lock.
- Use as abas do tipo pressionar e segurar no cabo P-Lock para soltar da tomada.

Figura 3.16 Operação de retenção de cabo P-Lock



4 Práticas recomendadas de segurança

As configurações padrão no suporte de cartão servem para garantir a segurança durante a implementação. A segurança adequada de equipamentos de infraestrutura crítica exige a configuração adequada de TODOS os serviços de comunicação. Esta seção resume as configurações.

Por meio do ciclo de vida SEGURO do produto da Vertiv, estamos comprometidos com a redução do risco à segurança cibernética em nossos produtos ao implementar práticas recomendadas de segurança cibernética no design de engenharia de produtos e soluções, tornando-os mais seguros, confiáveis e competitivos para nossos clientes.

Consulte abaixo algumas recomendações de segurança cibernética do ciclo de vida. As recomendações de segurança cibernética não devem ser um guia abrangente sobre esse assunto, mas sim um complemento aos programas de segurança cibernética dos clientes. Os sites a seguir contêm mais informações sobre as práticas recomendadas e diretrizes gerais sobre segurança cibernética:

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

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

A **Tabela 4.1** abaixo apresenta uma lista de itens. Cada um deve ser analisado e configurado com base nas necessidades operacionais de gerenciamento do equipamento. As configurações devem apoiar a funcionalidade operacional desejada sem adicionar acesso desnecessário ou não autorizado aos equipamentos de infraestrutura crítica. Oferecemos uma referência à seção adequada para configurar cada item.

Tabela 4.1 Configurações de análise e verificação de redução do risco de acesso não autorizado

Item	Descrição	Referência
Contas e senhas	Altere imediatamente os nomes das contas de administrador e usuário para eliminar o acesso com credenciais padrão.	Consulte Users na página 62.
Acesso à rede IP	Ative/Desative o acesso à rede IPV4 e IPV6 do cartão (desative o acesso a redes não utilizadas).	Consulte Network na página 66.
Acesso SSHv2	Ative/Desative o acesso SSHv2 para suporte de diagnóstico e configuração (desative quando não estiver em uso).	Consulte SSH na página 84.
Protocolo de serviço da Web	Selecione HTTPS para usar a criptografia SSL ao acessar dados pela interface de usuário da Web.	Consulte Servidor Web na página 76.
Certificados TLS	Ao usar HTTPS, instale seus próprios certificados TLS de uma autoridade confiável de certificados ou gere certificados autoassinados alternativos.	Consulte SSL Certificate: permite carregar seu próprio arquivo de certificado SSL assinado para substituir o padrão. O certificado pode ser autoassinado ou assinado por uma autoridade de certificação. O certificado SSL deve estar no formato PEM ou PFX

Tabela 4.1 Configurações de análise e verificação de redução do risco de acesso não autorizado (continuação)

Item	Descrição	Referência
		(PKCS12) na página 77.
Acesso remoto à gravação na Web	Para controlar/gravar pela interface da Web, é preciso fazer login remotamente e ter uma conta de usuário de administrador ou controle. Para proibir o acesso remoto, desative HTTP e HTTPS. **ADVERTÊNCIA! A desativação do HTTP e HTTPS encerrará imediatamente esta conexão e o acesso remoto estará disponível apenas por meio do SSH.**	Consulte Servidor Web na página 76.
Protocolos de comunicação	Ative/desative SNMP (desative os protocolos não utilizados).	Consulte Modbus na página 90.
Configurações da versão do SNMP	Ative/desative as versões do SNMP desejadas (use SNMPv3 com autenticação e criptografia do usuário).	Consulte SNMP na página 88.
Configurações da tabela de acesso SNMP	Para cada entrada da tabela de acesso SNMPv1/v2c, configure o tipo de acesso SNMP como somente leitura para evitar que os hosts identificados na entrada da tabela alterem o dispositivo.	Consulte SNMP na página 88.
Strings da comunidade SNMP	Use valores fortes adequados para a comunicação SNMP de acordo com a política de senhas da sua organização.	Consulte SNMP na página 88.
Configurações SNMPv3	Use algoritmos adequados de hash e criptografia para as configurações de autenticação e privacidade SNMPv3 a fim de deixar as comunicações SNMPv3 mais seguras.	Consulte SNMP na página 88.
Conta de usuário convidado	Essa conta deve permanecer desativada, exceto mediante solicitação de ativação, pois ela fornece acesso somente leitura ao dispositivo e pode dar mais contexto sobre as configurações do dispositivo se ativada.	Consulte a Users na página 62.

Para maior segurança, o firewall e o gateway da rede local podem ser restritos para permitir apenas o tráfego necessário nas portas de rede exigidas. As portas usadas pelo cartão MRIC-RP são definidas na tabela a seguir. O administrador pode alterar algumas configurações de portas.

Tabela 4.2 Portas usadas pelo cartão MRIC-RP (v6.1 ou mais recente)

Serviço de rede	Porta usada	Padrão	Modificação necessária
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
SNMP	UDP 161, 162	N	Apenas a porta trap 162 pode ser alterada.
Modbus	TCP 502	N	S

Tabela 4.2 Portas usadas pelo cartão MRIC-RP (v6.1 ou mais recente) (continuação)

Serviço de rede	Porta usada	Padrão	Modificação necessária
VID/VIP	GDP/HTTP	N	N
Cliente DHCP	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
Syslog remoto	TCP 514	N	S

Os detalhes da configuração de todas as opções são apresentados no restante deste guia.

4.1 Avaliação de risco

A Vertiv recomenda realizar uma avaliação de risco para identificar e analisar riscos internos e externos previsíveis em relação à segurança, disponibilidade e integridade do sistema e seu ambiente. Isso deve ser realizado de acordo com as estruturas técnicas e regulatórias aplicáveis, como IEC 62443 e NERC-CIP. A avaliação de risco deve ser realizada periodicamente.

4.2 Segurança física

O IMD5 foi criado para ser implantando e operado em um local fisicamente seguro. A Vertiv recomenda a revisão da segurança física e do ambiente operacional da unidade. Como um invasor ou uma ameaça interna pode causar interrupções graves, estas são algumas das práticas recomendadas:

- Restrição de acesso a áreas, racks e unidades com RFID de cartão criptografado/crachás, autenticação de código de acesso multifator exclusivo para acesso, armadilhas e scanners biométricos para acesso físico ao equipamento.
- Guardas confiáveis e com histórico verificado com presença física 24 horas por dia, 7 dias por semana, 365 dias por ano, e registros escritos para ajudar a documentar e anotar o acesso físico a um data center, prédio e rack.
- Acesso físico restrito a equipamentos de telecomunicações e cabeamento de rede. O acesso físico a linhas de telecomunicações e cabeamento de rede deve ser restrito para proteger contra tentativas de interceptação ou sabotagem das comunicações. As práticas recomendadas incluem o uso de conduítes de metal para o cabeamento da rede entre os gabinetes do equipamento.
- Todas as portas USB, RJ45 e outras portas físicas devem ser restritas nas unidades.
- Não conecte mídias removíveis, como dispositivos USB e cartões SD, durante operações de upgrade de firmware, alteração de configuração ou alteração de aplicativo de inicialização, a menos que a origem da mídia seja conhecida e confiável. Antes de conectar dispositivos portáteis em uma porta USB ou slot de cartão SD, escaneie o dispositivo para ver se há malware e vírus.

4.3 Acesso à conta

Os privilégios de acesso à conta do IMD5 devem ser administrados para fornecer o mínimo de funções da conta para permitir que o usuário final realize suas tarefas. O login no IMD5 deve ser restrito a usuários legítimos. Algumas destas práticas recomendadas devem ser adotadas pelos procedimentos escritos da organização para acesso à rede e a equipamentos:

- O primeiro login no IMD5 exige a criação de credenciais.
- Não é permitido compartilhar contas/logins. Cada usuário deve ter sua própria conta e senha específica. As funções de login do IMD5 esperam que cada conta seja um usuário exclusivo e não compartilhado.
- Os administradores devem restringir o acesso e os privilégios às funções exigidas para as tarefas do usuário.
- Restrinja todos os privilégios de administradores, como atualizações de firmware, ativação/desativação de protocolo, apenas aos administradores aprovados.
- A senha deve ser forte, complexa e seguir os requisitos de comprimento de acordo com o nível mais alto conforme a política de TI da empresa.
- Os funcionários demitidos deve ser removidos imediatamente do acesso à unidade. Alguns exemplos incluem o processo de autenticação de usuários AAA, TACACS+.
- A sessão deve ser encerrada após um período de inatividade.
- Use a instalação syslog remota para receber alertas sobre eventos do sistema e da rede, ameaças à segurança e visibilidade do dispositivo para resolver problemas. (Isso também pode ser exigido em seu ambiente para conformidade PCI-DSS/SOX/HIPAA).

5 Configuração

5.1 Dispositivo de monitoramento intercambiável

O Dispositivo de monitoramento intercambiável (IMD) é o principal componente da linha de produtos de energia atualizáveis da rPDU Geist™. É possível substituir ou atualizar o IMD para permitir que os data centers preparem seus locais para o futuro. A instalação do IMD incorreto para substituição em uma rPDU pode provocar danos no IMD.

5.1.1 Básica

A rPDU Geist™ básica atualizável é a base da linha de produtos GU. Ela foi criada com o módulo IMD-01X e oferece distribuição de energia de baixo custo com a opção de atualização para incluir medição local, monitoramento remoto e outros recursos no futuro.

5.1.2 Medida

A rPDU Geist™ medida atualizável é uma opção com medição local disponível na linha de produtos GU. Ela foi criada com o módulo IMD-01D e tem uma tela local para visualização do consumo de corrente (amperes) com a opção de atualização para incluir monitoramento e outros recursos no futuro.

Figura 5.1 Módulo IMD-01D

Tabela 5.1 Descrições do módulo IMD-01D

Item	Nome	Descrição
1	Tela local	A tela local mostra os valores de corrente da fase, da linha e do circuito (em amperes).
2	Botões da tela	Há três botões perto da tela do IMD: um para voltar, um para avançar e um para centralizar. As funções desses botões estão definidas na **Tabela 5.2** na página seguinte.

Tabela 5.2 Funções dos botões da tela

Botão	Símbolo	Descrição
Botão para voltar		Voltar para o canal anterior.
Botão para avançar		Avançar para o próximo canal.
Botão para centralizar		Alternar entre os modos da tela de rolagem e estático. Manter esse botão pressionado por 10 segundos executa uma redefinição de rede, restaurando o endereço IP padrão e redefinindo as informações de conta de usuário.
Botão para centralizar 3 vezes		Pressione esse botão três vezes em dois segundos para ativar o modo VLC. Pressione o botão com o modo VLC ativo para reverter a unidade à tela atual padrão.
Botões para voltar e avançar	e	Pressione os dois botões ao mesmo tempo para girar a tela 180 graus.

NOTA: A funcionalidade do botão da tela pode variar de acordo com a configuração da unidade.

5.1.3 Unidade monitorada

As versões anteriores das rPDUs Geist™ Vertiv™ de monitoramento no nível da unidade Vertiv™ foram enviadas com o módulo IMD-03E-G.

Figura 5.2 Módulo IMD-03E-G

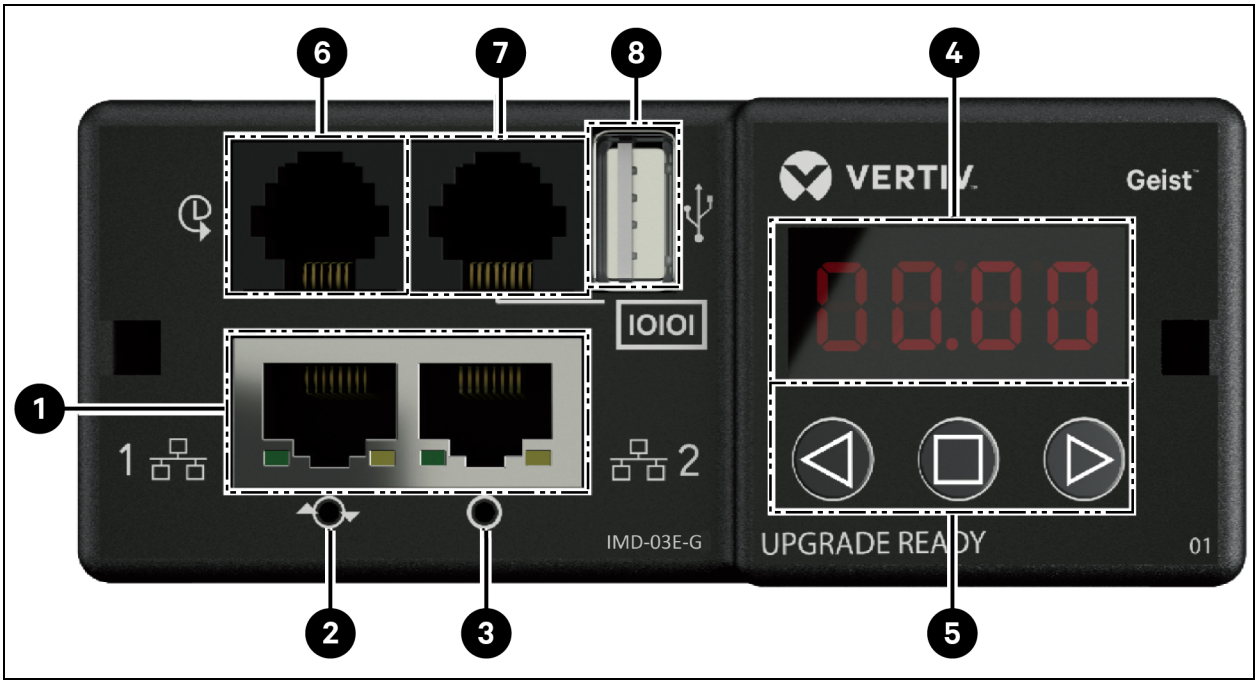


Tabela 5.3 Descrições do módulo IMD-03E-G

Número	Nome	Descrição
1	Portas ETHERNET duplas	As portas ETHERNET duplas funcionam como um comutador ETHERNET de duas portas, permitindo a conexão de vários dispositivos em cadeia. É possível configurar as portas ETHERNET duplas de forma independente das interfaces de rede ETHERNET duplas, o que permite a conexão da rPDU com duas redes diferentes.
2	Botão de reinicialização forçada	Pressione o botão de reinicialização forçada para reinicializar o IMD. Esse procedimento funciona como um ciclo de alimentação para o IMD e não altera ou remove nenhuma informação do usuário.
3	Botão de redefinição de rede	Manter o botão de redefinição de rede pressionado por 5 segundos durante a operação normal restaura o endereço IP padrão e redefine as contas de usuário.
4	Tela local	A tela local mostra os valores de corrente da fase, da linha e do circuito (em amperes).
5	Botões da tela	Há três botões perto da tela do IMD: um para voltar, um para avançar e um para centralizar. As funções desses botões estão definidas na **Tabela 5.4** na página seguinte.
6	Porta do sensor remoto	Porta RJ-12 para conexão de sensores digitais remotos plug-and-play da Vertiv™ (vendidos separadamente). Cada sensor digital tem um número de série exclusivo e é detectado automaticamente. As PDUs GU2 comportam até 16 sensores. É possível adicionar o conversor A2D Vertiv™ opcional para auxiliar no sensoriamento analógico. É possível adicionar o SN-ADAPTER opcional para auxiliar os sensores Liebert integrados e modulares. Para obter mais informações, consulte Sensores disponíveis na página 123.
7	Porta serial	RS-232 pela porta RJ-45.
8	Porta USB	Porta USB usada para carregar a configuração do firmware e do dispositivo de backup/restauração, para expandir a capacidade de gravação de logs por meio do dispositivo de armazenamento USB ou para permitir adaptadores USB sem fio TP-Link. A porta USB deve ser ativada. Consulte USB na página 85. Fornece até 100 mA de capacidade de energia para dispositivos conectados por USB.

NOTA: A conexão serial não permite controle de fluxo.

Tabela 5.4 Funções dos botões da tela

Botão	Símbolo	Descrição
Botão para voltar		Pressione para retroceder ao canal anterior. Ao segurar o botão por 3 segundos, um backup da configuração é iniciado. A tela mostra uma mensagem **bcup** durante a geração do backup e depois volta à operação normal. O backup é armazenado nos dispositivos de armazenamento USB disponíveis, e a operação não fará nada se não houver unidades disponíveis.
Botão para avançar		Pressione para avançar ao próximo canal. Ao segurar esse botão por 3 segundos, uma restauração da configuração é iniciada. A tela mostra a mensagem **load** seguida da mensagem **conf** e de uma contagem regressiva de 3 segundos. Depois que a contagem regressiva termina, uma mensagem **8888** aparece e o backup é usado. O backup será lido dos dispositivos de armazenamento USB. Se você soltar o botão a qualquer momento durante esta sequência, a restauração será cancelada. Depois que o backup é aplicado, ou se não houver imagens de backup nem dispositivos de armazenamento USB conectados, a tela voltará à operação normal.
Botão para centralizar		Alternar entre os modos da tela de rolagem e estático. Manter esse botão pressionado por 3 segundos inicia uma sequência de redefinições de parâmetros. Essa sequência consiste na mensagem **rset** seguida da mensagem **dflt** e de uma contagem regressiva de 3 segundos. Depois que a contagem regressiva termina, uma mensagem **8888** aparece, e as informações de rede, *http*, contas de usuário e *LDAP/RADIUS* são redefinidas aos valores padrão. Se você soltar o botão a qualquer momento durante esta sequência, a redefinição será cancelada.
Botão para centralizar 3 vezes		Pressione esse botão 3 vezes em 2 segundos para ativar o modo VLC. Pressione o botão com o modo VLC ativo para reverter a unidade à tela atual padrão.
Botões para voltar e avançar		Pressione os dois botões ao mesmo tempo para girar a tela 180 graus.
Botões para voltar e centralizar		Pressione os dois botões ao mesmo tempo para exibir o endereço IPv4 principal da unidade.

5.1.4 Monitoramento chaveado e da tomada

As versões anteriores das rPDUs Geist™ Vertiv™ de monitoramento no nível da unidade chaveada, de monitoramento no nível da tomada e de monitoramento no nível da tomada chaveada já vêm com o módulo IMD-03E-G.

Figura 5.3 Módulo IMD-03E-G

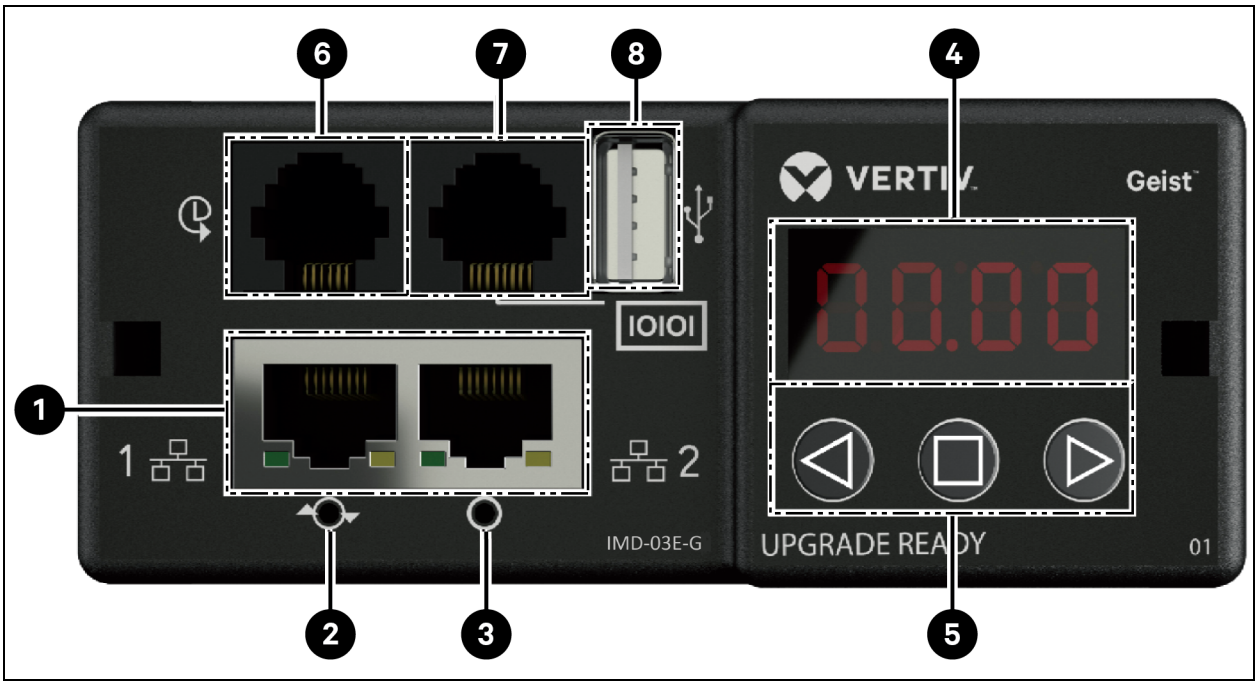


Tabela 5.5 Descrições do módulo IMD-03E-G

Número	Nome	Descrição
1	Portas ETHERNET duplas	As portas ETHERNET duplas funcionam como um comutador ETHERNET de duas portas, permitindo a conexão de vários dispositivos em cadeia. É possível configurar as portas ETHERNET duplas de forma independente das interfaces de rede ETHERNET duplas, o que permite a conexão da rPDU com duas redes diferentes.
2	Botão de reinicialização forçada	Pressione o botão de reinicialização forçada para reinicializar o IMD. Esse procedimento funciona como um ciclo de alimentação para o IMD e não altera ou remove nenhuma informação do usuário.
3	Botão de redefinição de rede	Manter o botão de redefinição de rede pressionado por 5 segundos durante a operação normal restaura o endereço IP padrão e redefine as contas de usuário.
4	Tela local	A tela local mostra os valores de corrente da fase, da linha e do circuito (em amperes).
5	Botões da tela	Há três botões perto da tela do IMD: um para voltar, um para avançar e um para centralizar. As funções desses botões estão descritas em Funções dos botões da tela na página seguinte.
6	Porta do sensor remoto	Porta RJ-12 para conexão de sensores digitais remotos plug-and-play da Vertiv (vendidos separadamente). Cada sensor digital tem um número de série exclusivo e é detectado automaticamente. As PDUs GU2 comportam até 16 sensores. É possível adicionar o conversor A2D Vertiv™ opcional para auxiliar no sensoriamento analógico. É possível adicionar o SN-ADAPTER opcional para auxiliar os sensores Liebert integrados e modulares. Para obter mais informações, consulte Sensores disponíveis na página 123.
7	Porta serial	RS-232 pela porta RJ-45.
8	Porta USB	Porta USB usada para carregar a configuração do firmware e do dispositivo de backup/restauração, para expandir a capacidade de gravação de logs por meio do dispositivo de armazenamento USB ou para permitir adaptadores USB sem fio TP-Link. A porta USB deve ser ativada. Consulte USB na página 85. Fornece até 100 mA de capacidade de energia para dispositivos conectados por USB.

NOTA: Os dispositivos USB MSC, como pen drives ou unidades de disco rígido externas, são compatíveis. Os dispositivos de armazenamento USB devem ser formatados como FAT32.

NOTA: A conexão serial não permite controle de fluxo.

Botões da tela

Há três botões perto da tela do IMD: um para voltar, um para avançar e um para centralizar. As funções desses botões estão descritas na tabela a seguir.

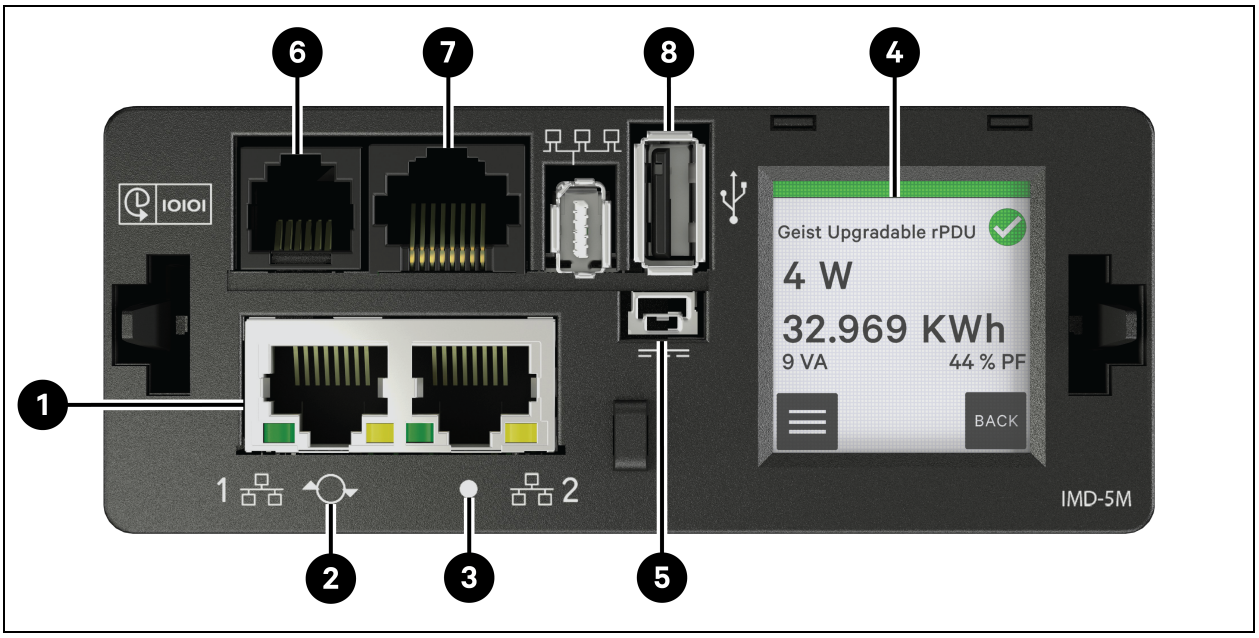
Tabela 5.6 Funções dos botões da tela

Botão	Símbolo	Descrição
Botão para voltar		Pressione para retroceder ao canal anterior. Ao segurar esse botão por 3 segundos, um backup da configuração é iniciado. A tela mostra uma mensagem **bcup** durante a geração do backup e depois volta à operação normal. O backup é armazenado nos dispositivos de armazenamento USB disponíveis, e a operação não fará nada se não houver unidades disponíveis.
Botão para avançar		Pressione para avançar ao próximo canal. Ao segurar esse botão por 3 segundos, uma restauração da configuração é iniciada. A tela mostra a mensagem **load** seguida da mensagem **conf** e de uma contagem regressiva de 3 segundos. Depois que a contagem regressiva termina, uma mensagem **8888** aparece e o backup é usado. O backup será lido dos dispositivos de armazenamento USB. Se você soltar o botão a qualquer momento durante esta sequência, a restauração será cancelada. Depois que o backup é aplicado, ou se não houver imagens de backup nem dispositivos de armazenamento USB conectados, a tela voltará à operação normal.
Botão para centralizar		Alternar entre os modos da tela de rolagem e estático. Manter esse botão pressionado por 3 segundos inicia uma sequência de redefinições de parâmetros. Essa sequência consiste na mensagem **rset** seguida da mensagem **dflt** e de uma contagem regressiva de 3 segundos. Depois que a contagem regressiva termina, uma mensagem **8888** aparece, e as informações de rede, http, contas de usuário e LDAP/RADIUS são redefinidas aos valores padrão. Se você soltar o botão a qualquer momento durante esta sequência, a redefinição será cancelada.
Botão para centralizar 3 vezes		Pressione esse botão três vezes em 2 segundos para ativar o modo VLC. Pressione o botão com o modo VLC ativo para reverter a unidade à tela atual padrão.
Botões para voltar e avançar		Pressione os dois botões ao mesmo tempo para girar a tela 180 graus.
Botões para voltar e centralizar		Pressione os dois botões ao mesmo tempo para exibir o endereço IPv4 principal da unidade.

5.1.5 Monitoramento e comutação (IMD-5M)

Todas as rPDUs Geist™ Vertiv™ monitoradas e comutadas são enviadas com o módulo IMD-5M.

Figura 5.4 Módulo IMD-5M



Item	Nome	Descrição
1	Portas ETHERNET duplas	As portas ETHERNET duplas funcionam como um comutador ETHERNET de duas portas, permitindo a conexão de vários dispositivos em cadeia. É possível configurar as portas ETHERNET duplas de forma independente das interfaces de rede ETHERNET duplas, o que permite a conexão da rPDU com duas redes diferentes.
2	Botão de reinicialização/redefinição	Mantenha pressionado o botão por 10 segundos para reinicializar o IMD. Esse procedimento funciona como um ciclo de alimentação para o IMD e não altera ou remove nenhuma informação do usuário. Mantenha pressionado o botão por 25 segundos durante a operação normal para restaurar o endereço IP padrão e redefinir as contas de usuário.
3	LED de status RGB	LED verde: unidade em funcionamento. LED amarelo: unidade inicializando.
4	Menu da tela sensível ao toque	Use o menu da tela sensível ao toque para encontrar os valores de corrente da fase, da linha e do circuito (em amperes).
5	Potência de entrada redundante	Se o cabo de conexão opcional estiver conectado na segunda unidade, o IMD continuará ligado quando a rPDU ficar sem energia.

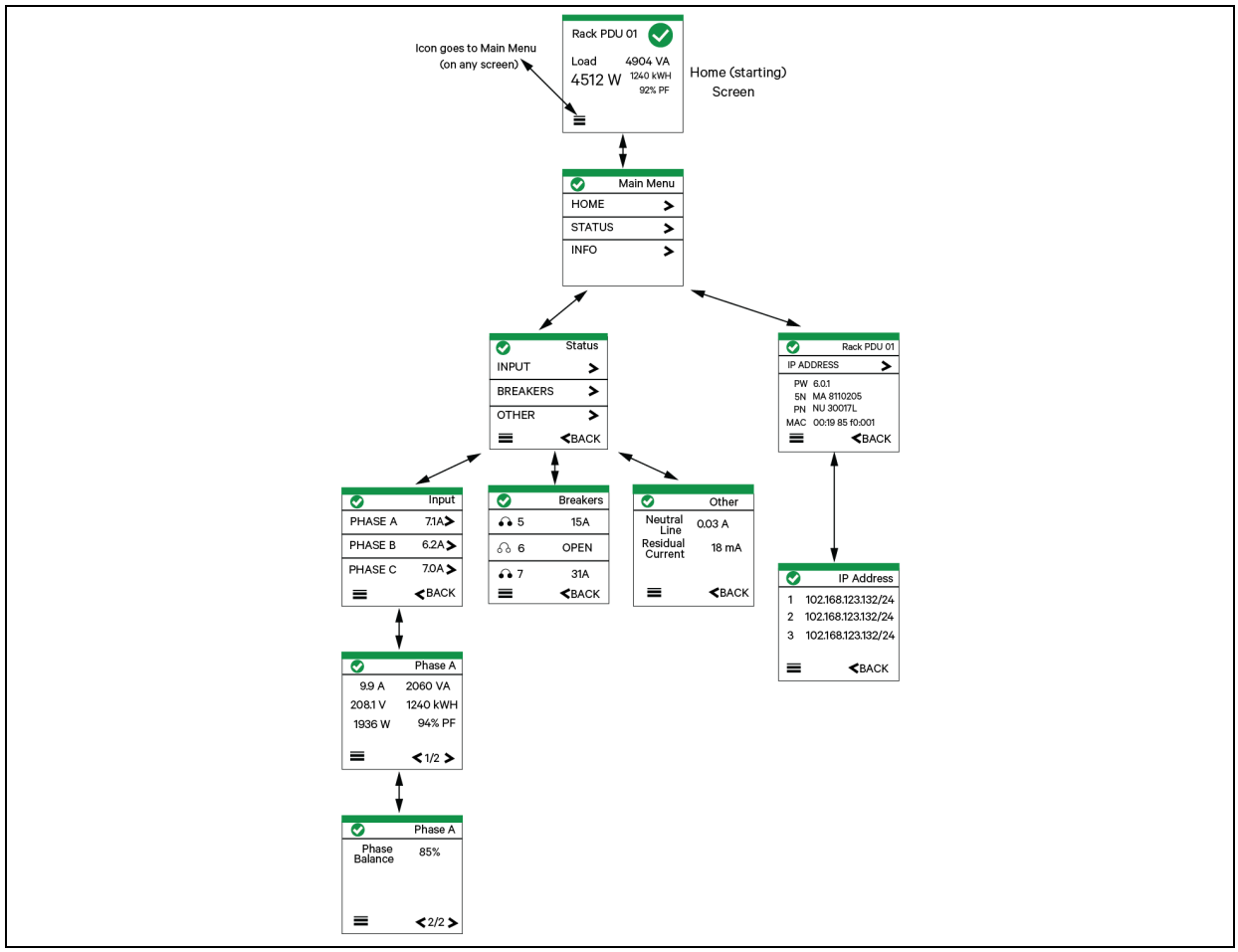
Item	Nome	Descrição
6	Porta do sensor remoto	Porta RJ-12 para conexão de sensores digitais remotos plug-and-play da Vertiv™ (vendidos separadamente). Cada sensor digital tem um número de série exclusivo e é detectado automaticamente. As PDUs GU2 comportam até 16 sensores. É possível adicionar o conversor A2D Vertiv™ opcional para auxiliar no sensoriamento analógico. É possível adicionar o SN-ADAPTER opcional para auxiliar os sensores Liebert® integrados e modulares. Para obter mais informações, consulte Sensores disponíveis na página 123.
7	Porta serial	RS-232 pela porta RJ-45.
8	Porta USB	Porta USB usada para carregar a configuração do firmware e do dispositivo de backup/restauração, para expandir a capacidade de gravação de logs por meio do dispositivo de armazenamento USB ou para permitir adaptadores USB sem fio TP-Link. A porta USB deve ser ativada. Consulte USB na página 85. Fornece até 0,5 watt para o nível monitorado da unidade e 5 watts para o nível da tomada monitorada/nível da unidade comutada/nível da tomada comutada.

NOTA: A conexão serial não permite controle de fluxo.

Fluxo de trabalho do menu da tela sensível ao toque

A tela de inicialização mostrará a carga de voltagem, tensão, kilowatts/hora e a porcentagem do PF. Clique no botão de hambúrguer no canto inferior direito para acessar o menu principal independentemente de onde você estiver no fluxo. No menu principal, há três opções. Home retornará para a primeira página com as estatísticas mencionadas acima. Status levará para outra página do menu onde há acesso a páginas com informações sobre fase, disjuntor ou linha, respectivamente. O botão INFO mostrará a página do endereço IP.

Figura 5.5 Diagrama do fluxo de trabalho do menu da tela sensível ao toque



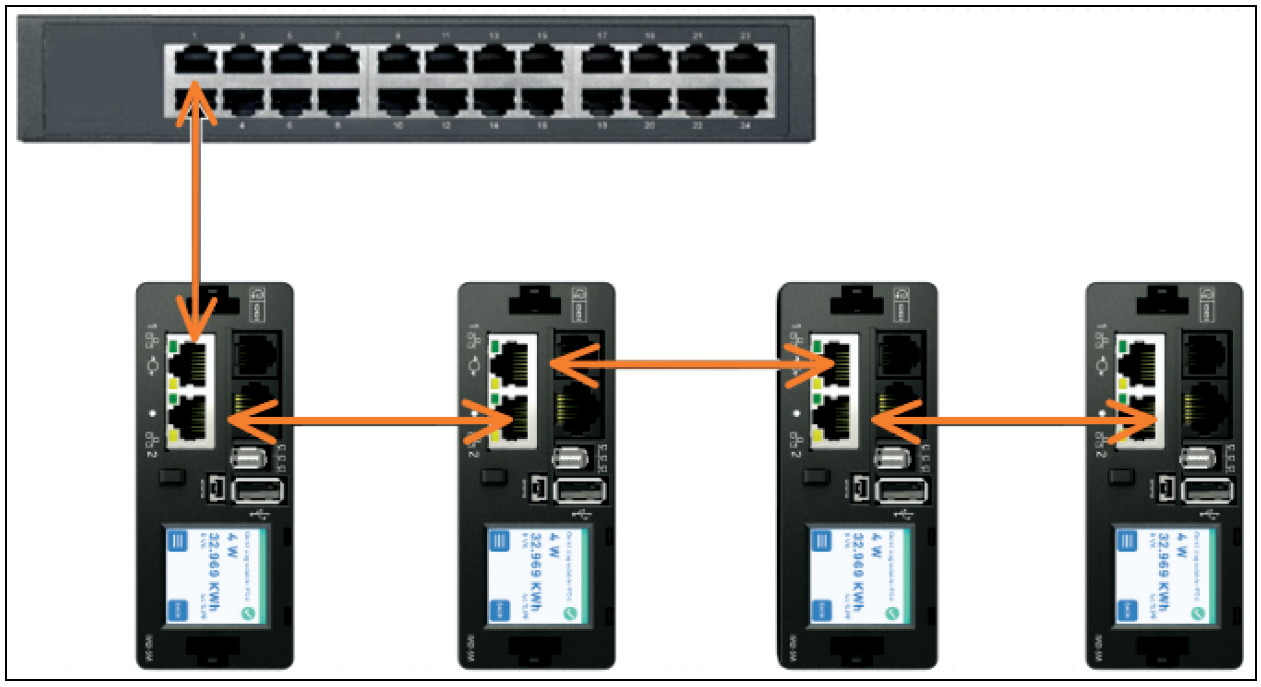
5.1.6 Rapid Spanning Tree Protocol (RSTP)

Os dispositivos monitorados atualizáveis, com o IMD-5M integrado, incluem duas portas ETHERNET que funcionam juntas como uma ponte ETHERNET interna. É possível usar uma dessas portas para conectar o IMD a uma rede existente ou as duas portas ao mesmo tempo para conectar um IMD a outro em uma configuração em cadeia.

Encadeamento em cascata

- Use o encadeamento em cascata para reduzir o número de portas no comutador de rede.
- As PDUs de rack são conectadas usando cadeia ETHERNET.
- A parte da frente da PDU de rack em cadeia é conectada à porta do comutador de rede.
- Cada PDU de rack tem o próprio endereço IP exclusivo.

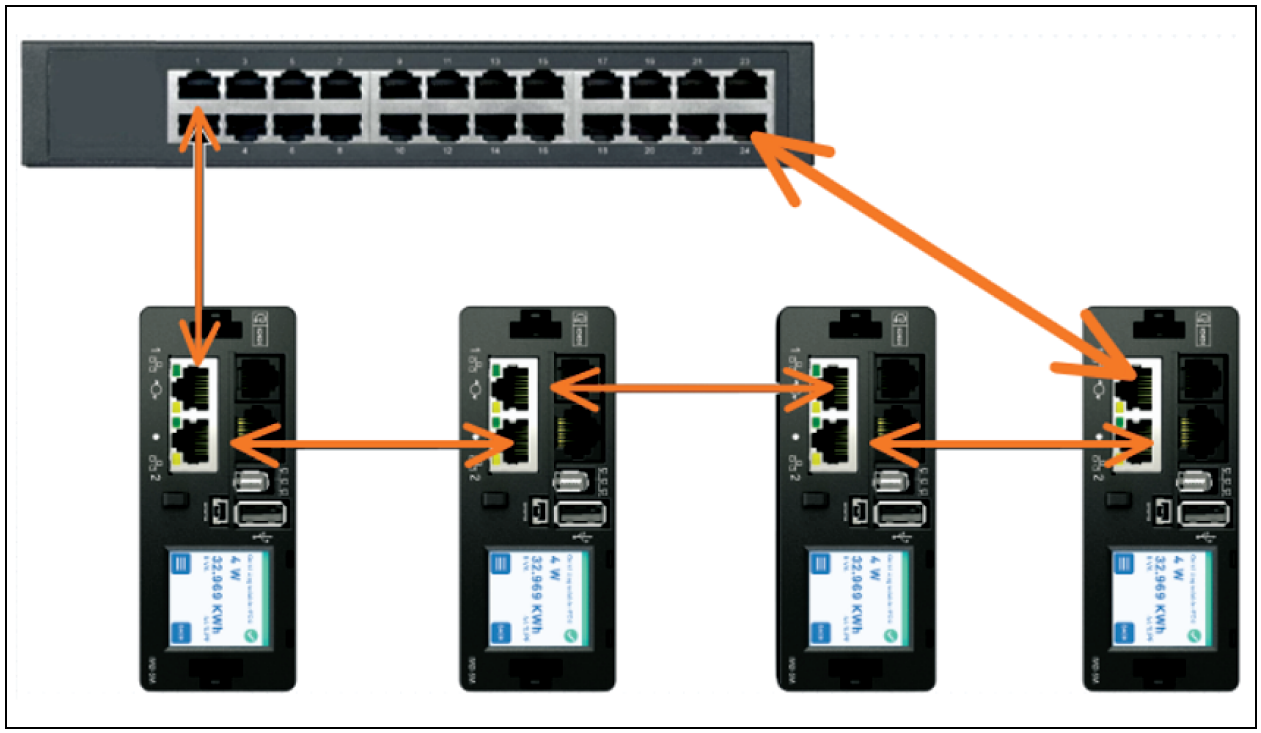
Figura 5.6 Encadeamento em cascata



Encadeamento em cascata tolerante a falhas

- Use o encadeamento em cascata tolerante a falhas para oferecer conectividade de rede resiliente.
- As PDUs de rack são conectadas usando cadeia ETHERNET.
- As partes tanto da frente quanto de trás das PDUs de rack em cadeia são conectadas às portas do comutador de rede.
- Cada PDU de rack tem o próprio endereço IP exclusivo.
- É necessário configurar o Rapid Spanning Tree Protocol (RSTP) para gerenciar a tolerância a falhas e manter a conectividade em caso de falha em um cabo ou de perda de energia da PDU de rack.

Figura 5.7 Encadeamento em cascata tolerante a falhas



Quando as duas interfaces de rede estão conectadas, o IMD implementa um protocolo de ponte de rede denominado Rapid Spanning Tree Protocol (RSTP). RSTP é um padrão da IEEE implementado por todas as pontes gerenciadas. Por meio do RSTP, acesse as informações de rede do Exchange para encontrar caminhos ou loops redundantes. O IPv6 deve ser desativado ao usar conectividade de rede redundante.

Quando um loop é detectado, as pontes na rede trabalham juntas para desativar temporariamente os caminhos redundantes. Dessa forma, a rede pode evitar broadcast storms provocados por loops. O RSTP também verifica regularmente se há alterações na topologia da rede. Quando uma conexão é perdida, o RSTP permite que as pontes alternem rapidamente para um caminho redundante.

NOTA: O protocolo RSTP impõe um limite de 40 ligações entre as pontes, incluindo os IMDs.

NOTA: O Vertiv Intelligence Director não pode ser usado junto com RSTP e conectividade de rede redundante.

5.2 Configuração de rede

O IMD atualizável tem um endereço IP padrão para configuração e acesso iniciais.

Para restaurar o endereço IP padrão e redefinir todas as informações da conta do usuário:

1. Em caso de perda ou esquecimento de endereços ou senhas atribuídos pelo usuário, pressione e segure o botão de redefinição de rede localizado abaixo da porta ETHERNET por 15 segundos.
2. Se você segurar o botão para centralizar da tela de LED por 10 segundos, as informações da conta da rede e do usuário também serão redefinidas.

A página Network, localizada abaixo da guia System, permite atribuir as propriedades de rede manualmente ou usar DHCP para conexão com sua rede. Para acessar a unidade, é necessário saber o endereço IP. É recomendado o uso de um IP estático ou DHCP reservado. O endereço padrão é exibido na parte frontal da unidade.

- IP Address: *192168123123*
- Subnet Mask: *255.255.255.0*
- Gateway: *192.168.123.1*

Para acessar a unidade pela primeira vez, você deve alterar temporariamente as configurações de rede do seu computador para corresponder à sub-rede 192.168.123. xxx. Para configurar a unidade, conecte-a à porta ETHERNET do seu computador e siga as instruções apropriadas ao sistema operacional do seu computador.

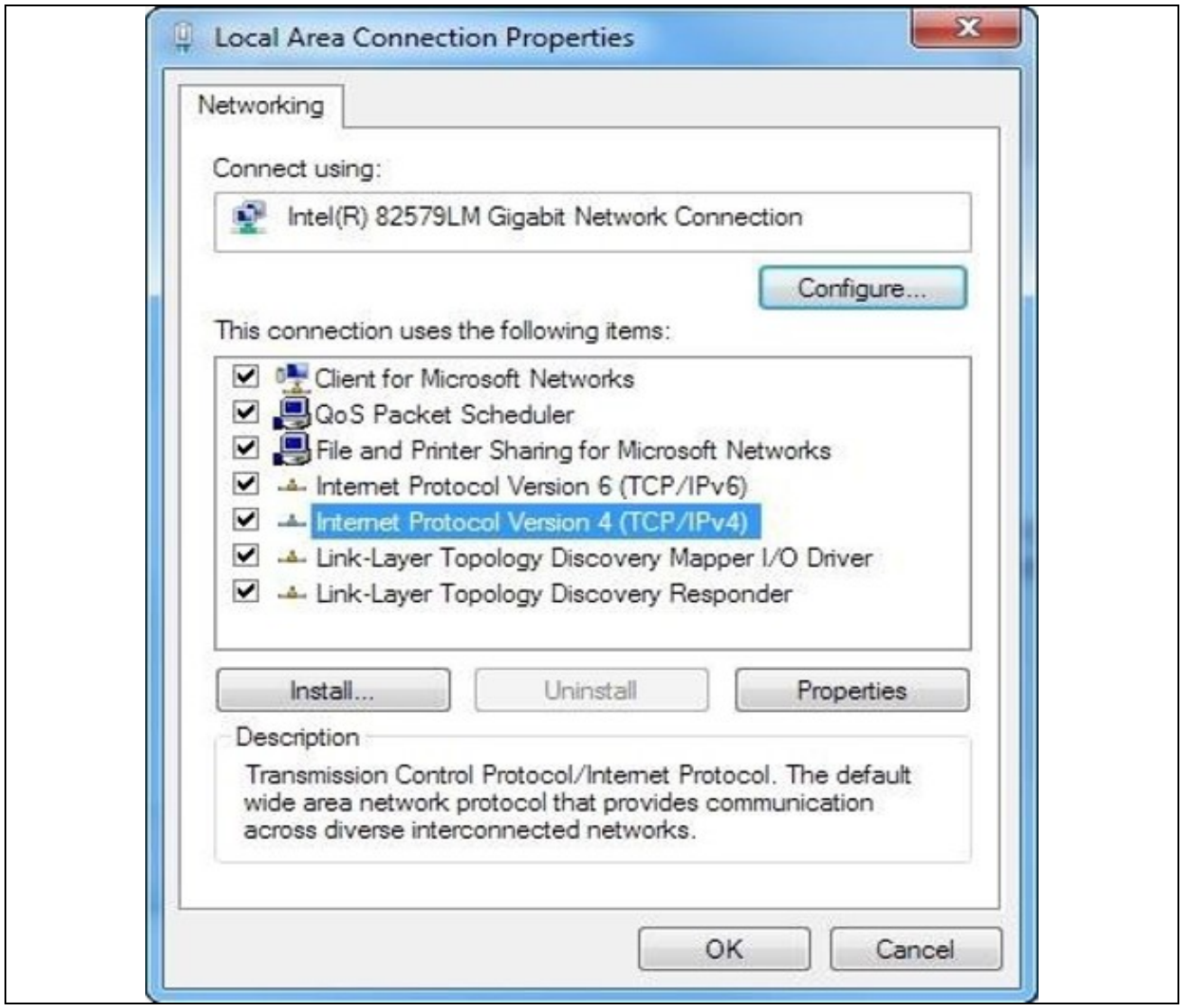
Para configurar a rede no sistema operacional Windows:

1. Acesse as configurações de rede do seu sistema operacional.
   - Windows Server 2022 e 2019.
   - No Microsoft Windows 10, clique em *Start>Network and Internet>Change Adapter Settings*.
   - No Microsoft Windows 11, clique em *Start>Network and Internet>Change Adapter Settings*.
2. Localize a entrada em Rede Local ou de Alta Velocidade com a Internet ou Conexão Local que corresponda à placa de rede (NIC). Clique duas vezes na entrada do adaptador de rede na lista de conexões de rede.

NOTA: A maioria dos computadores tem uma única NIC ETHERNET instalada, mas um adaptador Wi-Fi ou de dados do celular também aparece como NIC nesta lista. Certifique-se de escolher a entrada correta.

3. Clique em *Properties* para abrir a janela Local Properties.

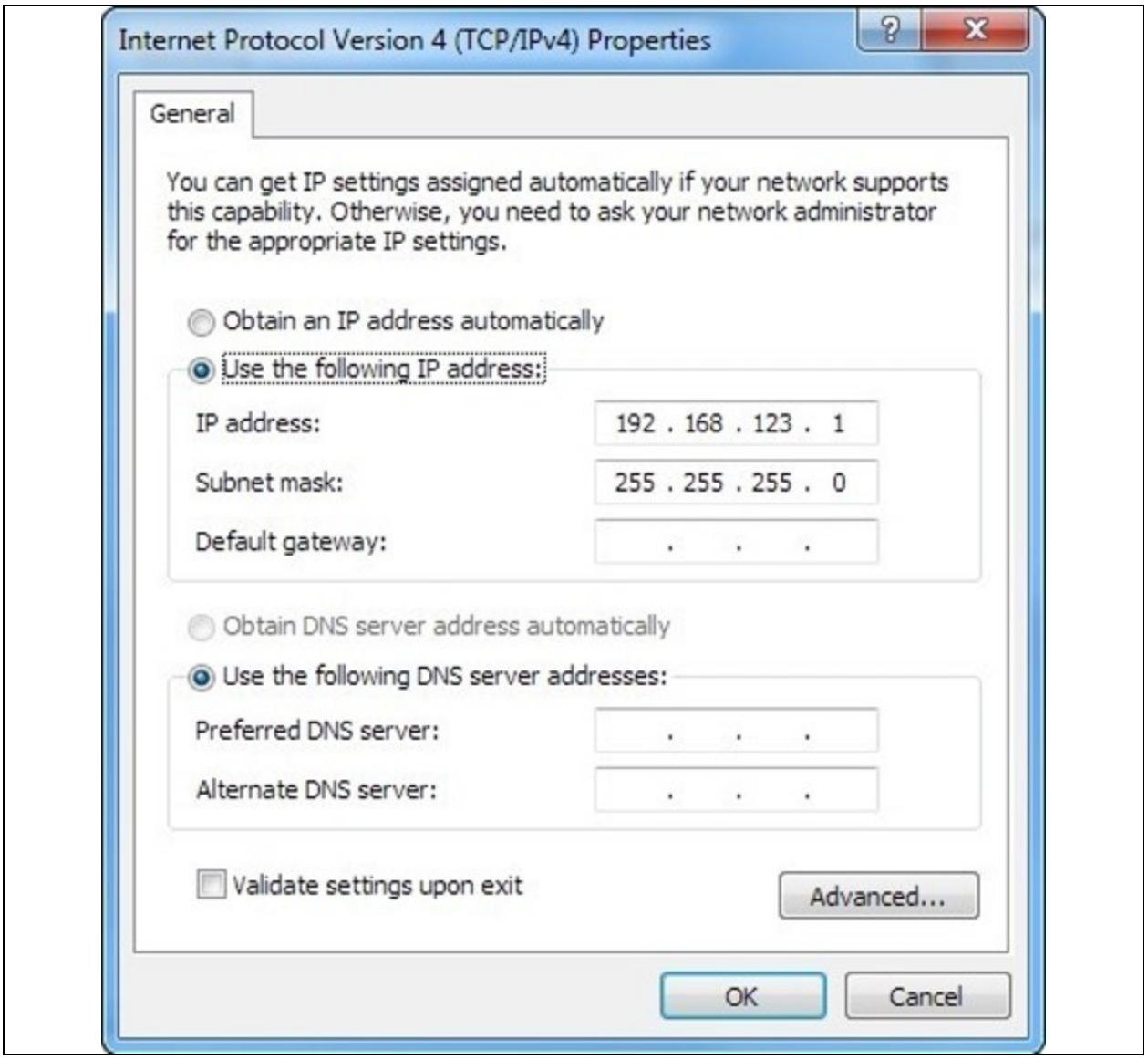
Figura 5.8 Local Area Connection Properties



4. Selecione *Internet Protocol Version 4 (TCP/IPv4)* na lista e clique em *Properties*.

NOTA: Se aparecer mais de uma entrada TCP/IP, como no exemplo acima, talvez o computador esteja configurado para suporte a IPv6 e também a IPv4. Certifique-se de selecionar a entrada referente ao protocolo IPv4. Anote as configurações atuais da placa NIC para que você possa restaurá-las ao estado normal depois de concluir o procedimento de configuração.

Figura 5.9 Internet Protocol Version 4



5. Selecione *Use the following IP address*, defina o endereço IP como **192.168.123.1** e a máscara de sub-rede como **255.255.255.0** . Na configuração inicial, gateway padrão e servidor DNS podem ficar em branco. Selecione *OK* - *OK* para fechar as duas janelas de propriedades do protocolo de Internet e de propriedades locais.
6. Em um navegador da Web, insira **http://192.168.123.123** para acessar a unidade. Se você está configurando a unidade pela primeira vez, é necessário criar uma conta e uma senha de Admin antes de continuar.
7. Após a criação da conta de administrador, faça login na unidade.
8. Por padrão, a página de sensores padrão é exibida. Navegue até a *guia System* e a *página Network* para configurar as propriedades de rede do dispositivo. É possível atribuir as configurações de endereço IP, máscara de sub-rede, Gateway e DNS da unidade manualmente ou adquiri-las por DHCP.

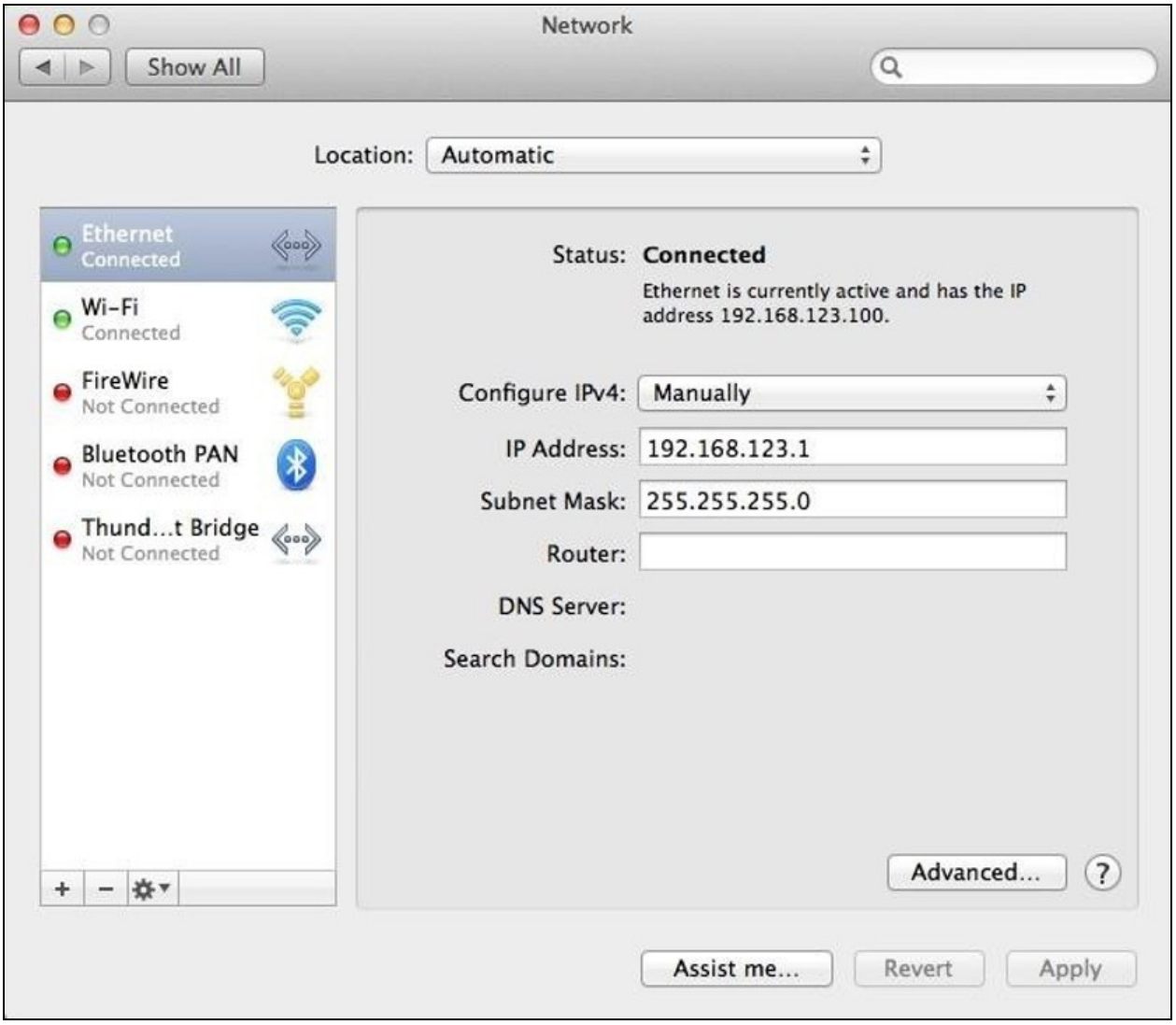
9. Clique em *Save*.

NOTA: Depois que as alterações forem salvas, o navegador não poderá mais recarregar a página da Web do endereço 192.168.123.123 e exibirá as mensagens Page not Found ou Host Unavailable, o que é normal. Depois que você terminar de configurar o endereço IP da unidade, repita as etapas acima alterando as configurações de placa NIC ETHERNET do computador para aquelas que você anotou antes de alterá-las.

Para configurar a rede no MAC:

1. Clique no ícone de Preferências do sistema no Dock e escolha *Network*.

Figura 5.10 Preferências do sistema MAC



2. Verifique se ETHERNET está destacado na lateral esquerda da janela da NIC. Na maioria dos casos, haverá uma entrada ETHERNET no Mac. Anote as configurações atuais para que você possa restaurá-las ao estado normal depois de concluir o procedimento de configuração.
3. Selecione *Manually* na lista suspensa Configure IPv4, defina o endereço IP como 192.168.123.1 e a máscara de sub-rede como 255.255.255.0 e clique em *Apply*.

NOTA: É possível deixar as configurações Router e DNS Server em branco para esta configuração inicial. Em um navegador da Web, insira http://192.168.123.123 para acessar a unidade. Se você está configurando a unidade pela primeira vez, é necessário criar uma conta e uma senha de Admin antes de continuar.

4. Após a criação da conta de administrador, faça login na unidade.
5. Por padrão, a página de sensores padrão é exibida. Navegue até a guia *System* e a página *Network* para configurar as propriedades de rede do dispositivo. É possível atribuir as configurações de endereço IP, máscara de sub-rede, Gateway e DNS da unidade manualmente ou adquiri-las por DHCP.
6. Clique em *Save*.

NOTA: Depois que as alterações forem salvas, o navegador não poderá mais recarregar a página da Web do endereço 192.168.123.123 e exibirá as mensagens Page not Found ou Host Unavailable, o que é normal. Depois que você terminar de configurar o endereço IP da unidade, repita as etapas acima alterando as configurações de placa NIC ETHERNET do computador para aquelas que você anotou antes de alterá-las.

5.3 Interface de usuário da Web

A unidade pode ser acessada por uma conexão HTTP padrão não criptografada e também por uma conexão HTTPS (TLS) criptografada. As unidades terão com padrão o HTTP e serão redirecionadas para HTTPS, exceto se o administrador ativar explicitamente o HTTP.

NOTA: É necessário criar uma conta de administrador (nome de usuário e senha) ao fazer login no dispositivo pela primeira vez.

NOTA: Se aparecer Clock not set na parte inferior da página, siga os procedimentos em Time na página 84.

5.3.1 Menu principal

O menu principal está localizado na vertical do lado esquerdo. Consulte a Figura 5.11 na página oposta para ver o menu principal.

ADVERTÊNCIA! Não conecte aquecedores elétricos, aparelhos elétricos de aquecimento ou outros aparelhos elétricos que possam provocar incêndio, choque elétrico e ferimentos quando operados sem supervisão.

Figura 5.11 Menu principal

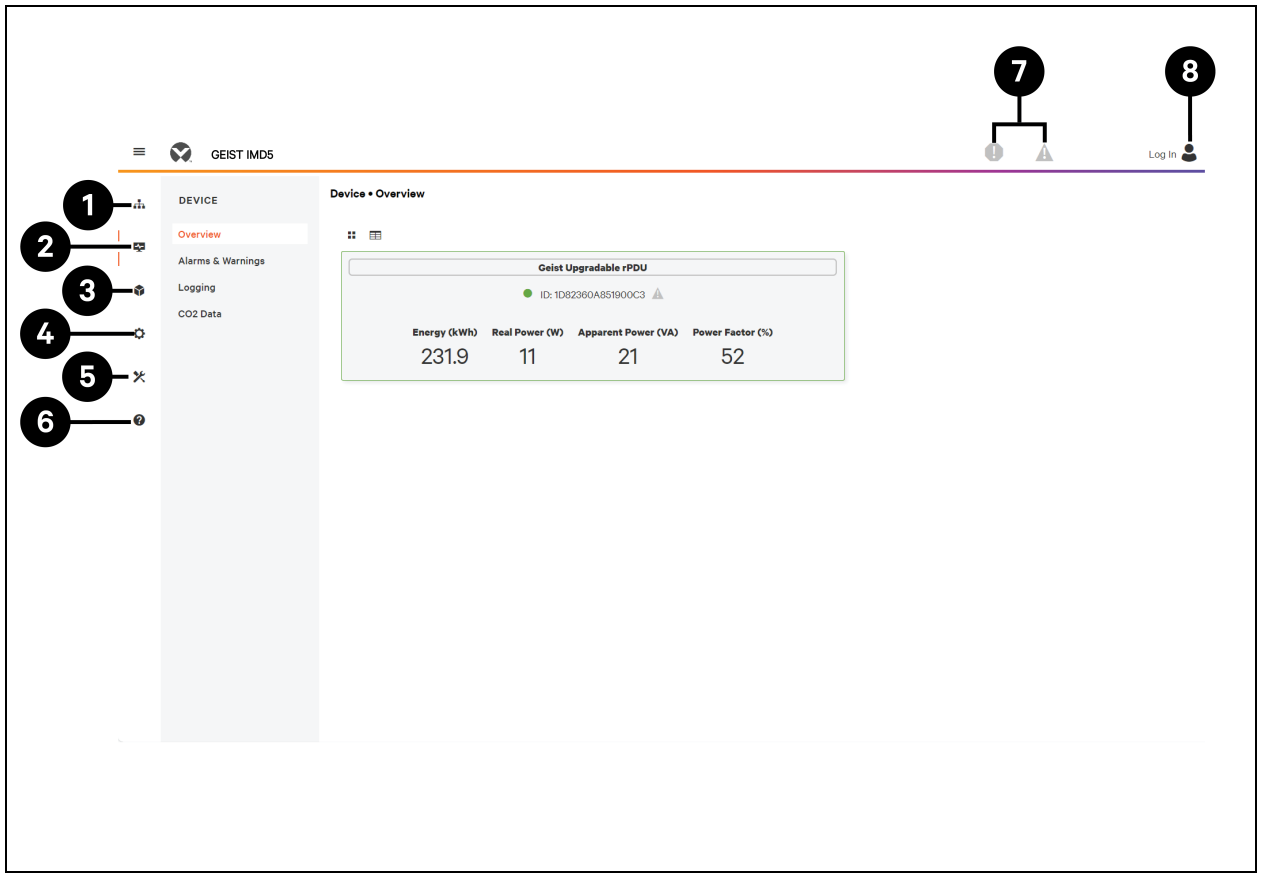


Tabela 5.7 Descrições do menu principal

Item	Descrição
1	Aggregation
2	Device
3	Provisioner
4	System
5	Utilities
6	Help
7	Alarms & Warnings
8	Login/Logout

5.4 Submenu Device

Clique no submenu Device para acessar os menus *Overview, Alarms & Warnings, Logging* e *CO2 Data*.

5.4.1 Overview

Você deve fazer login antes de implementar alterações. Somente usuários com autorizações de nível de controle ou superiores podem acessar essas configurações.

Figura 5.12 Descrições do submenu Device Overview

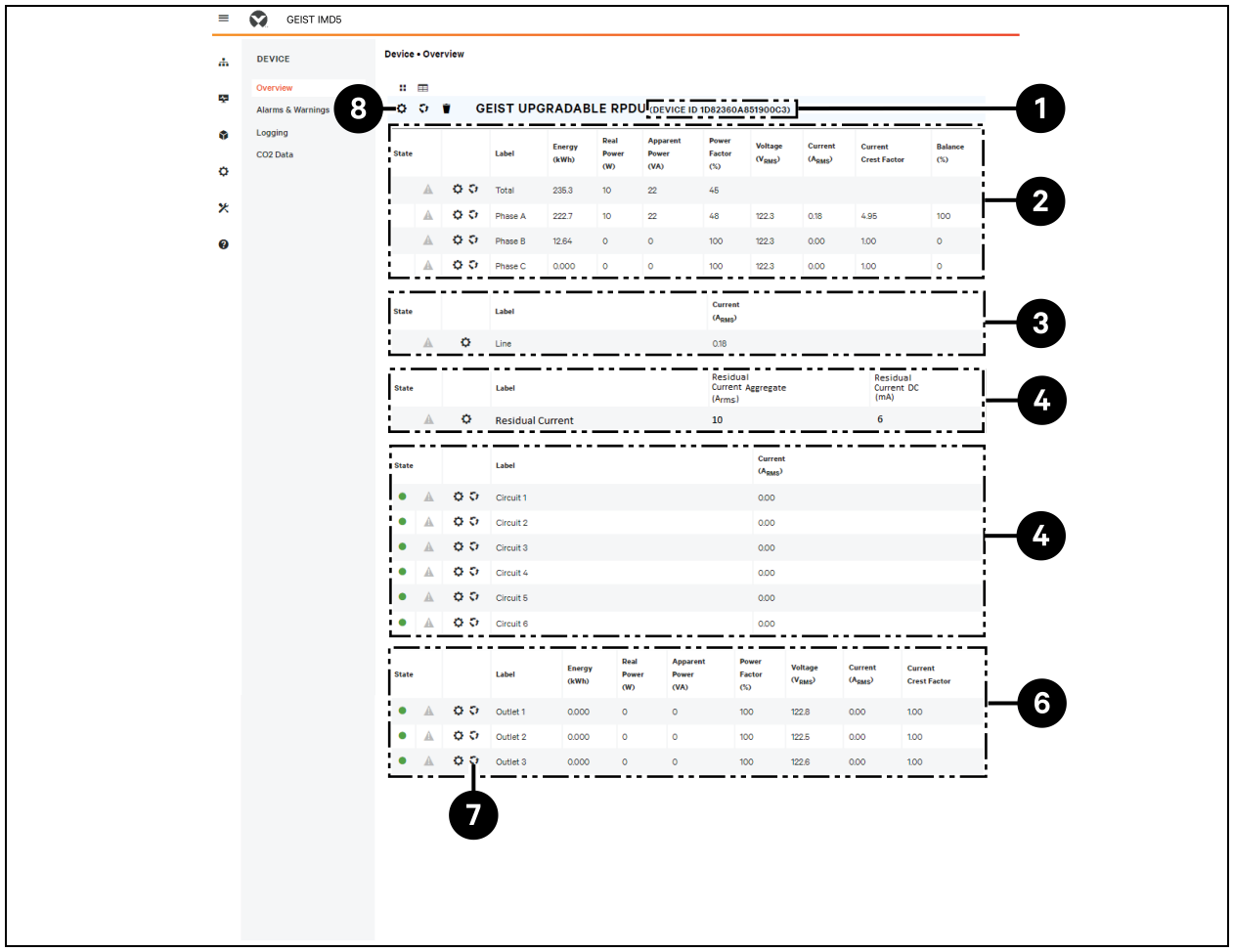


Tabela 5.8 Descrições do submenu Device Overview

Número	Nome	Descrição
1	ID do dispositivo	Identificação exclusiva do produto que não pode ser alterada. Talvez seja necessário para suporte técnico.
2	Monitor de fase total e individual	Exibe as estatísticas de corrente CA, tensão e potência de cada fase e do total das fases combinadas. O fator de pico da corrente e o equilíbrio de fases (%) também estão indicados.
3	Linha	Exibe a corrente (RMS em amperes) nas unidades Wye trifásicas. Isso não aparece nas unidades Delta monofásicas e trifásicas.
4	Corrente residual	Somente para rPDUs com o recurso RCM-B. Exibe a agregação da corrente residual (mA) e a DC da corrente residual (mA). Quando aplicável, mostra a corrente residual de cada fase.

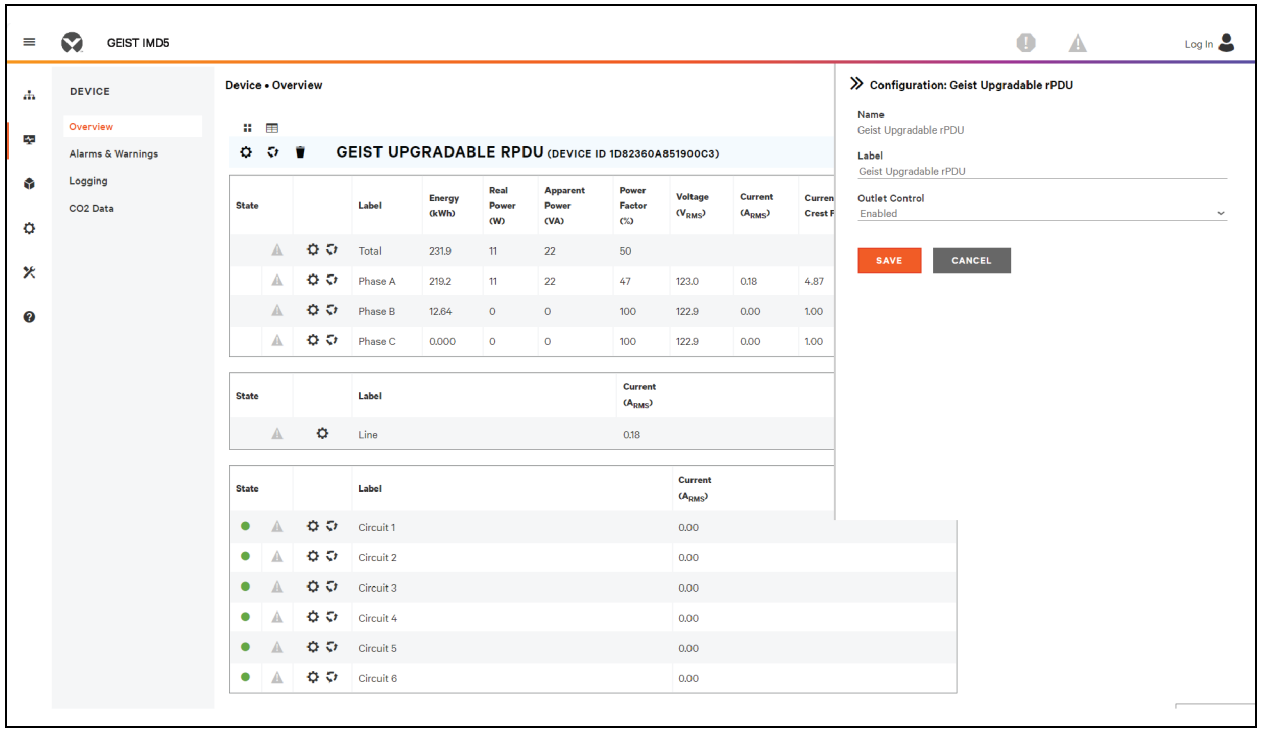
Tabela 5.8 Descrições do submenu Device Overview (continuação)

Número	Nome	Descrição
5	Monitor de corrente	Exibe as estatísticas de consumo de corrente CA de cada circuito na rPDU.
6	Monitor de tomada	Aplicável SOMENTE a rPDUs monitoradas/comutadas de tomada - Exibe as estatísticas de corrente CA, tensão e potência de cada circuito e tomada. O fator de pico da corrente também está indicado. (Somente monitoramento de potência no nível da tomada e monitoramento no nível da tomada chaveada.) Exibe o status da tomada. (Somente monitoramento no nível chaveado e da tomada chaveada).
7	Ícone de operação	Aplicável SOMENTE a rPDUs monitoradas/comutadas de tomada - Modifique as configurações.
8	Ícone de configuração	Aplicável SOMENTE a rPDUs monitoradas/comutadas de tomada - Modifique o nome do rótulo.

Para alterar o rótulo de um dispositivo:

1. Clique no ícone de configuração da rPDU Geist™ Vertiv™ e altere o rótulo. Name é o nome ou o modelo de fábrica da rPDU e não pode ser alterado.
2. Clique em *SAVE*.

Figura 5.13 Alterar o rótulo do dispositivo



Para alterar a operação de um dispositivo:

1. Clique no ícone de operação .
2. Selecione a operação que será executada:
   - **On/Off:** liga ou desliga todas as tomadas.
   - **Reboot:** para tomadas ligadas, a reinicialização desliga e depois liga as tomadas após o atraso durante a reinicialização. Para as tomadas que estão desligadas, a reinicialização as liga.
   - **Cancel:** cancela a operação atual se ainda não foi concluída.
   - **Reset Energy:** redefine a energia total medida em kWH.
   - **Restore Defaults:** restaura as configurações do dispositivo ao padrão de fábrica. Dentre elas: rótulos, atrasos e ações de ativação do dispositivo.

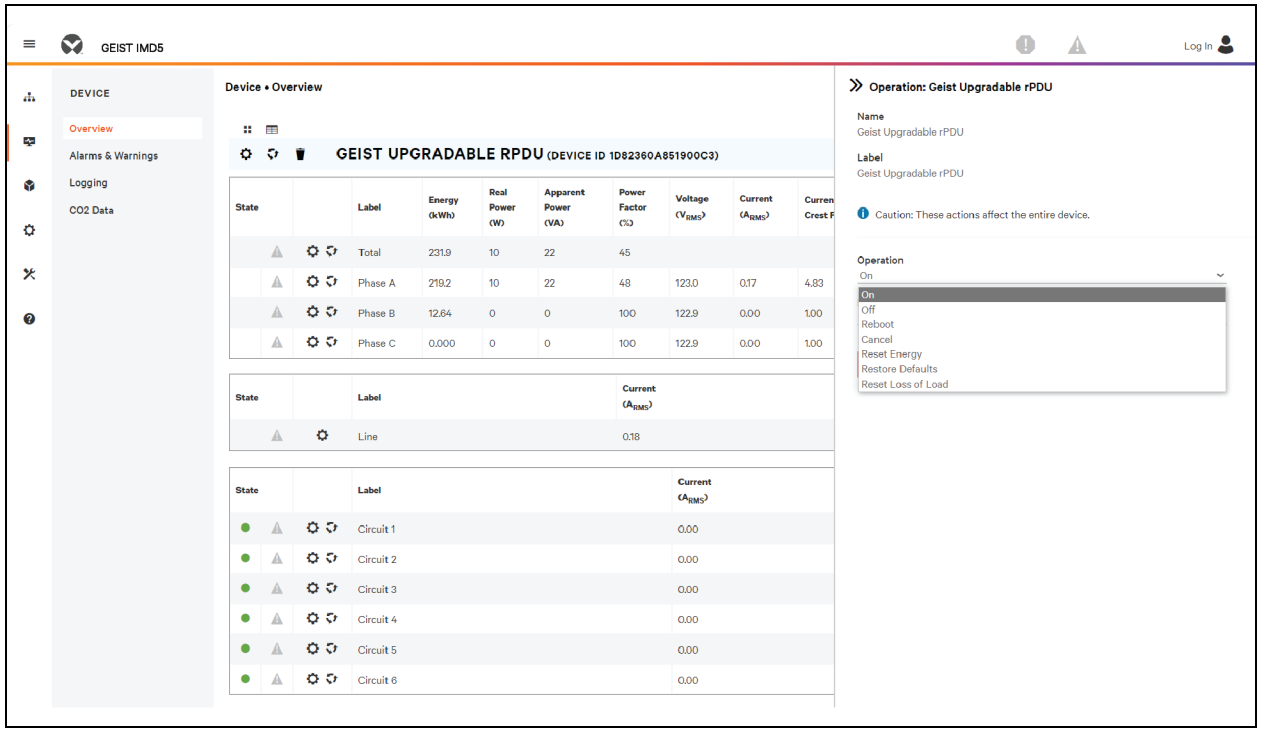
NOTA: Essas ações afetam todo o dispositivo.

NOTA: As operações On/Off e Reboot são aplicadas somente a rPDUs Geist™ chaveadas de tomada.

3. Para operações que envolvem o estado das tomadas, a definição de Delay como *True* usa a configuração de atraso atual de cada tomada ao executar a operação selecionada.
4. Clique em *SAVE* para emitir a ação.

NOTA: Os atrasos da ação de ativação referem-se ao momento desde que a unidade foi ligada, e não desde que ela foi completamente inicializada. Eles podem ser executados antes da inicialização completa da unidade.

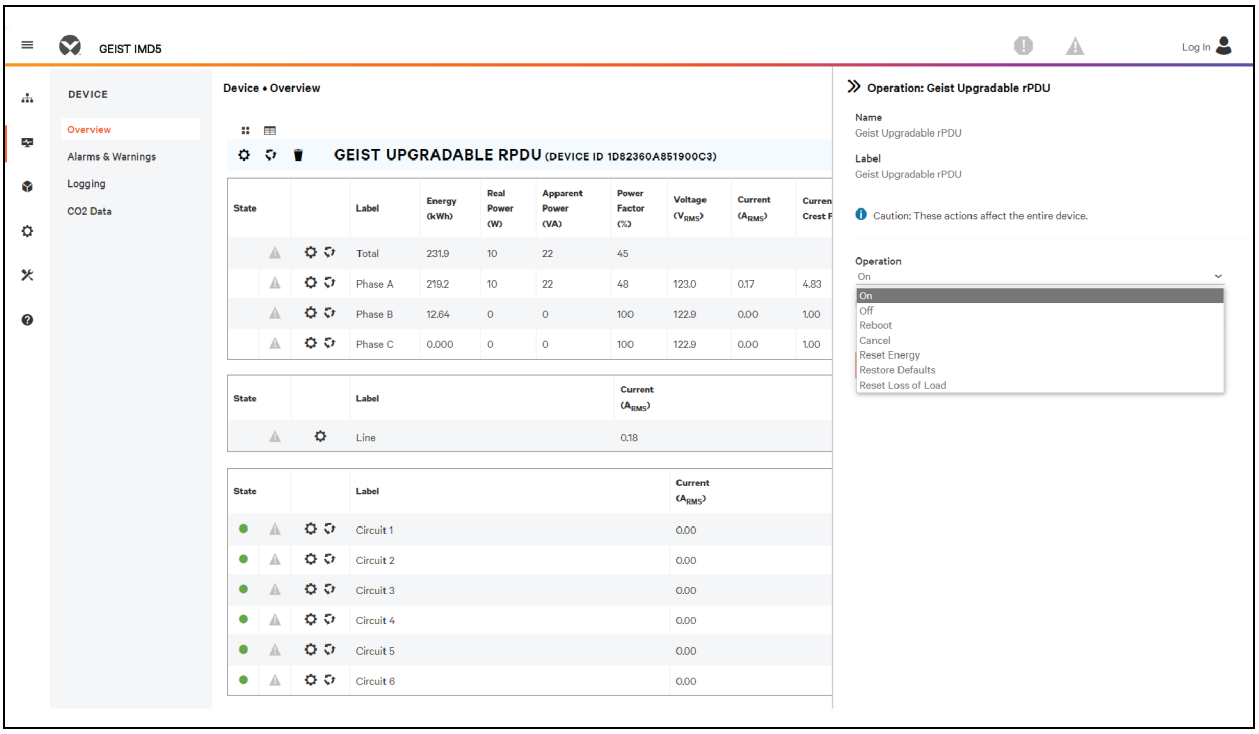
Figura 5.14 Operação de alteração do dispositivo



Para alterar o rótulo de uma fase ou um circuito:

1. Clique no ícone de configuração da fase ou do circuito e altere o rótulo. Name é o nome do circuito ou da fase física e não pode ser alterado.
2. Clique em *SAVE*.

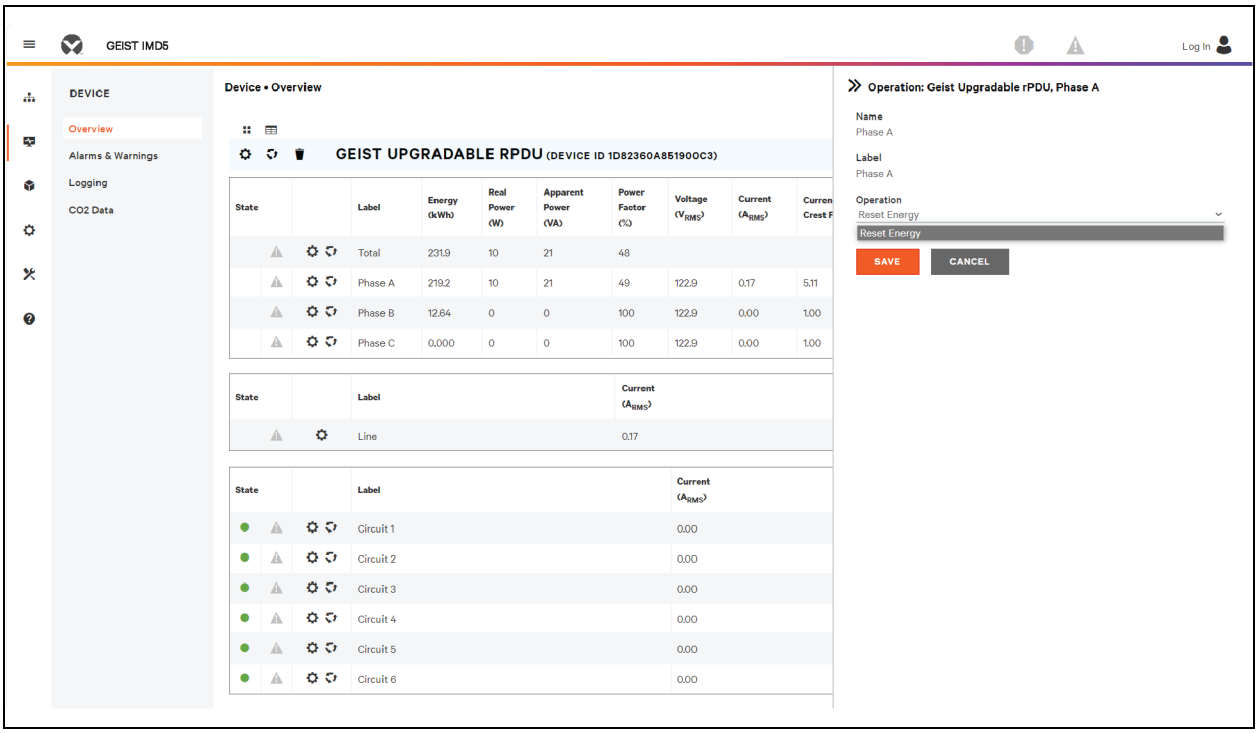
Figura 5.15 Alterar o rótulo de uma fase ou um circuito



Para alterar a operação de uma fase:

1. Clique no ícone de operação.
2. Selecione *Reset Energy* para redefinir a energia total medida em kWH referente à fase selecionada.
3. Clique em *SAVE* para emitir a ação.

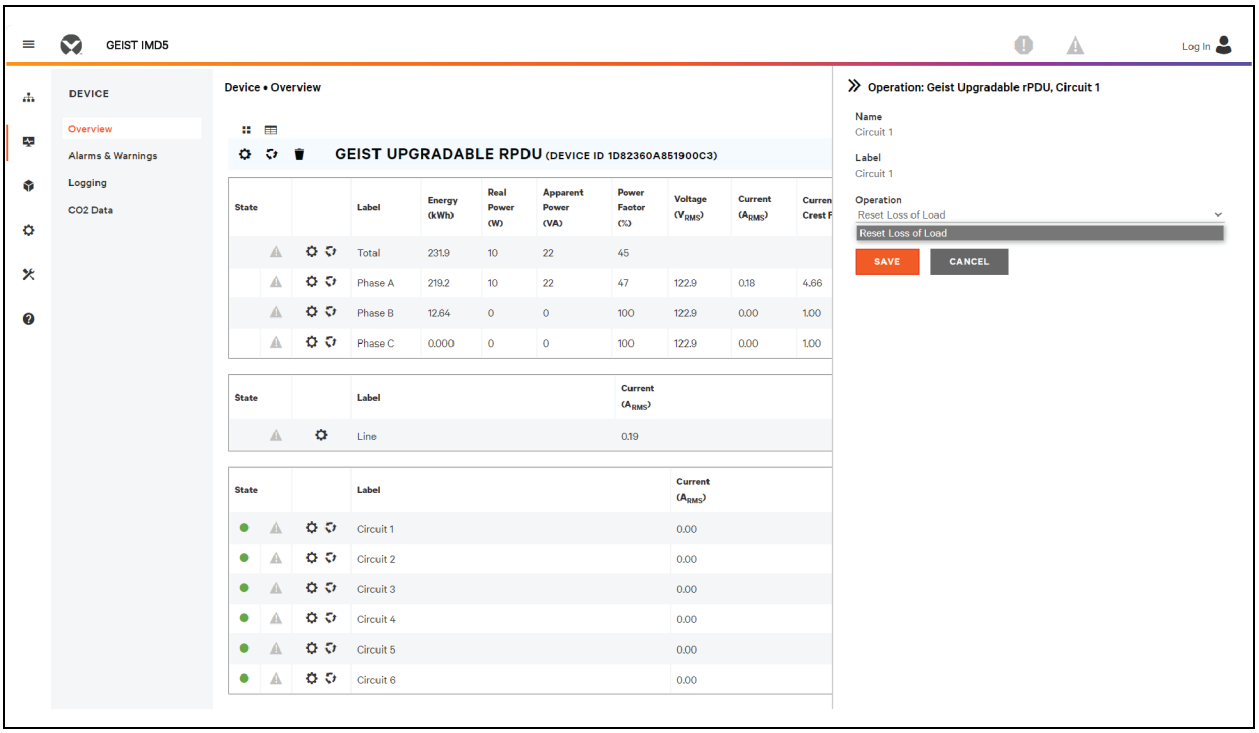
Figura 5.16 Alterar a operação da fase



Para alterar a operação do circuito:

1. Clique no ícone de operação .
2. Selecione *Reset Loss of Load* para redefinir o alarme Loss of Load.
3. Clique em *SAVE* para emitir a ação.

Figura 5.17 Alterar a operação do circuito



NOTA: Essa etapa é necessária quando o estado mostra um alarme de perda de carga e o problema foi resolvido. O alarme de perda de carga é acionado por uma queda repentina da corrente detectada pelo transdutor que faz a medição da corrente do disjuntor quando a operação se aproxima do limite de carga do circuito. Para as unidades horizontais atualizáveis com chaveamento, o alarme de perda de carga é também acionado pela perda de tensão do disjuntor (seja qual for a carga do circuito).

Para configurar uma tomada:

NOTA: Aplicável somente a rPDUs Geist™ Vertiv™ monitoradas/comutadas de tomada.

1. Clique no ícone de configuração da tomada .
2. Altere as configurações, conforme necessário.
   a. Rótulo da tomada.

NOTA: As etapas 2b a 2k são relevantes apenas a tomadas chaveadas.

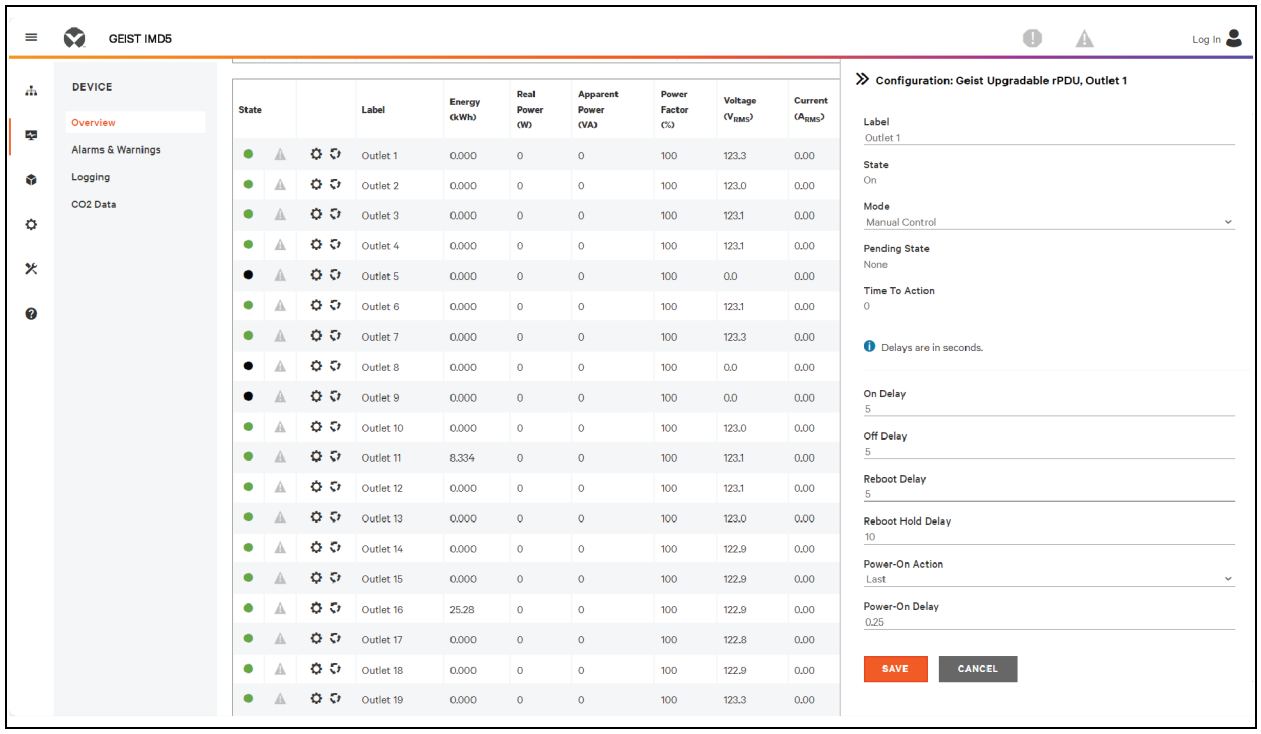
   b. State: o estado da corrente da tomada (On ou Off).
   c. Mode: como a tomada será controlada.
      - Manual Control: o estado da tomada é controlado é controlado usando a interface de usuário da Web, o SNMP ou a API.
      - Alarm Control (normalmente desligado, ligado quando qualquer alarme associado é ativado): normalmente, o estado da tomada é definido como Off e será ligado quando qualquer evento de alarme da tomada for ativado.
      - Alarm Control (normalmente ligado, desligado quando qualquer alarme associado é ativado): normalmente, o estado da tomada é definido como On e será desligado quando qualquer evento de alarme da tomada for ativado.

- **Alarm Control (normalmente desligado, ligado quando todos os alarmes associados são ativados):** normalmente, o estado da tomada é definido como Off e será ligado quando todos os eventos de alarme da tomada fores ativados.
- **Alarm Control (normalmente ligado, desligado quando todos os alarmes associados são ativados):** normalmente, o estado da tomada é definido como On e será desligado quando todos os eventos de alarme da tomada fores ativados.

d. **Pending State:** o estado da tomada está em transição.
e. **Time To Action:** o tempo restante antes que a ação pendente ocorra. Isso é ajustado em Delays.
f. **On Delay:** quanto tempo, em segundos, a unidade aguarda para ligar uma tomada.
g. **Off Delay:** quanto tempo, em segundos, a unidade aguarda para desligar uma tomada.
h. **Reboot Delay:** tempo, em segundos, que a unidade aguarda para reinicializar uma tomada.
i. **Reboot Hold Delay:** tempo, em segundos, que a unidade aguarda depois que desliga a tomada e antes de ligá-la novamente durante uma reinicialização.
j. **Power-On Action:** descreve o estado inicial da tomada quando ela é ligada ("on", "off" ou "last").
k. **Power-On Delay:** tempo, em segundos, que a unidade aguarda depois de ser ligada e antes de ligar a tomada.

3. Clique em *SAVE*.

Figura 5.18 Configuração da tomada



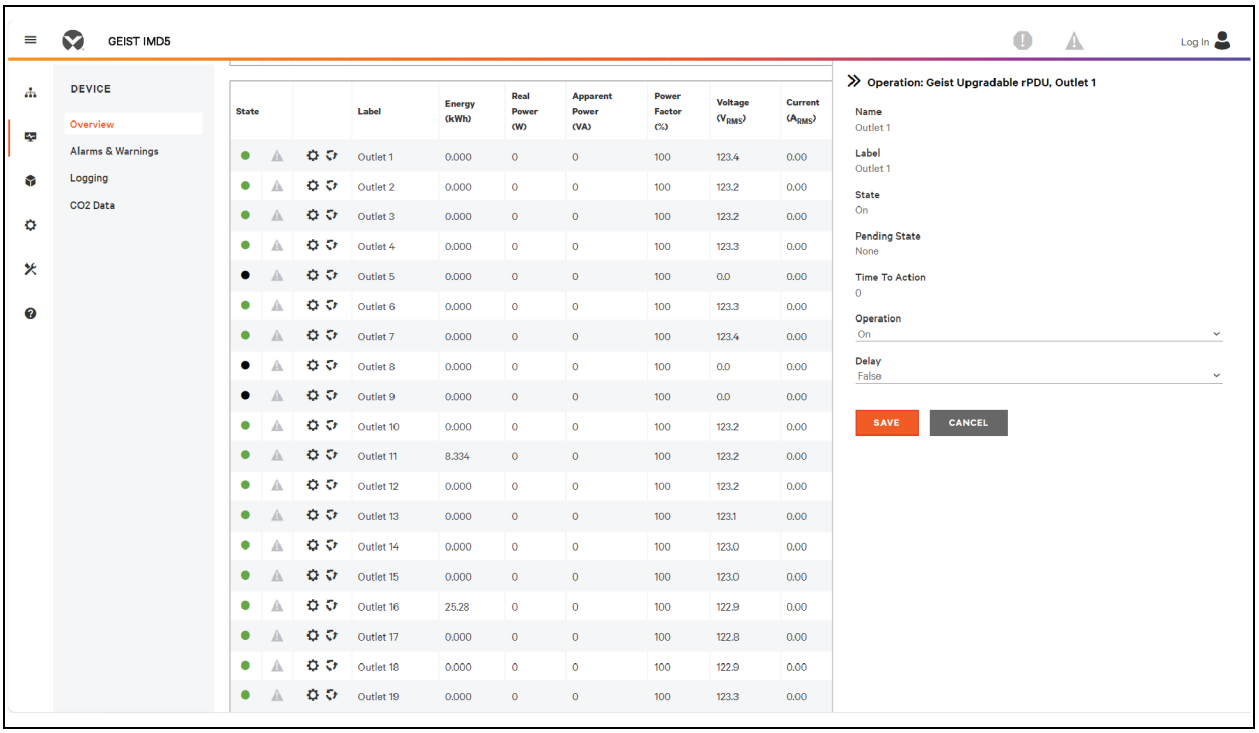
Para alterar a operação de uma tomada:

NOTA: Aplicável somente a rPDUs Geist™ Vertiv™ monitoradas/comutadas de tomada.

1. Clique no ícone de operação  da tomada desejada.

2. Selecione a operação que será executada:
   - **On/Off:** liga ou desliga a tomada selecionada.
   - **Reboot:** Para tomadas ligadas, a reinicialização desliga e depois liga as tomadas após o atraso durante a reinicialização. Para as tomadas que estão desligadas, a reinicialização as liga.
   - **Cancel:** cancela a operação atual se ainda não foi concluída.
   - **Reset Energy:** redefine a energia total medida em kWH referente à tomada selecionada.
3. Para operações que envolvem o estado das tomadas, a definição de Delay como *True* usa a configuração de atraso atual de cada tomada ao executar a operação selecionada.
4. Selecione *SAVE* para emitir a ação.

Figura 5.19 Alterar a operação de uma tomada



5.4.2 Alarms & Warnings

A página Alarms & Warnings permite estabelecer condições (eventos) de alarme ou de advertência para cada leitura de potência e circuito. Os eventos são disparados quando a medição excede um limite definido pelo usuário, seja acima (trip alto) ou abaixo (trip baixo) do limite. Os eventos são exibidos em seções diferentes, com base no dispositivo ou na medida a que eles estão associados. Cada evento pode ter uma ou mais ações que serão executadas quando ele ocorrer.

Figura 5.20 Página Alarms & Warnings

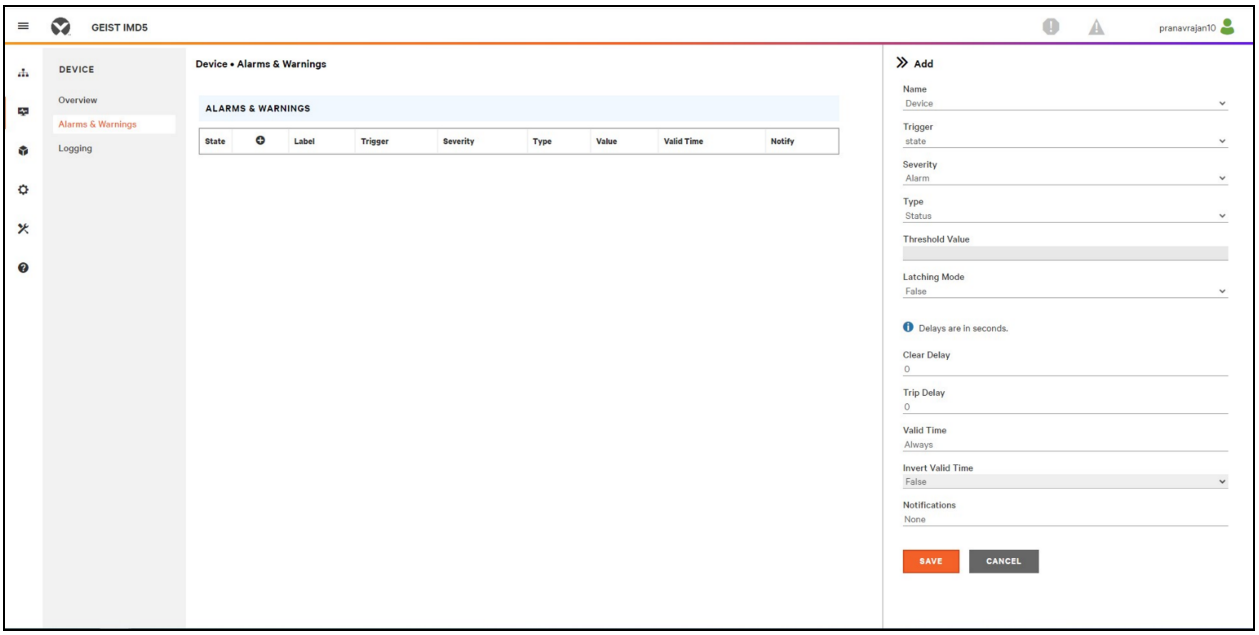


Tabela 5.9 Descrições de alarmes e advertências

Número	Descrição	Símbolo	Descrição
1	Status de cada evento.		Símbolo de advertência. O evento é exibido em laranja.
			Símbolo de alarme. O alarme é exibido em vermelho.
			Símbolo de evento confirmado. O símbolo permanece até a condição medida voltar ao normal.
2	Adicionar/Excluir/Modificar alarmes e advertências.		Adicionar novos alarmes e advertências.
			Modificar alarmes e advertências existentes.
			Excluir alarmes e advertências existentes.
3	Notificar o usuário sobre os eventos ativados e solicitar confirmação.	N/A	Vazio, se não houver condição de alerta.
			Quando há um evento de alarme ou de advertência, você pode clicar nesse símbolo para confirmar o evento e fazer com que a unidade pare de enviar notificações sobre isso. **NOTA: Clicar nesse símbolo não apaga o evento de advertência ou de alarme, apenas para de repetir as notificações.**
4	Exibe as condições das configurações de alarmes e de advertências.		

Para adicionar um novo evento de alarme ou de advertência:

1. Clique nos botões *Add/Modify Alarms* e *Warnings*.
2. Defina as condições desejadas para este evento da seguinte maneira:
   a. Nas listas suspensas, selecione o nome da fase ou do circuito, a medida do acionador, a gravidade e o tipo.

NOTA: Trips altos se a medição ficar acima do limite e trips baixos se a medição ficar abaixo do limite.

   b. Insira o valor de limite desejado (qualquer número entre -999,0 e 999,0).
   c. Insira o tempo desejado de Clear Delay em segundos. Qualquer valor diferente de *0* indica que, quando este evento for ativado, a medição deverá voltar ao normal por esse número de segundos antes que o evento seja apagado e redefinido. Clear Delay pode ser de até 14.400 segundos (4 horas).
   d. Insira o tempo desejado de Trip Delay em segundos. Qualquer valor diferente de *0* indica que a medição deve exceder o limite por esse número de segundos antes de o evento ser ativado. Trip Delay pode ser de até 14.400 segundos (4 horas).
   e. No modo de travamento, se ativado, este evento e suas ações associadas continuarão ativas até a confirmação do evento, mesmo que a medição seguinte volte ao normal.
   f. Para especificar para onde as notificações de alerta serão enviadas quando houver este evento de alarme ou de advertência, clique no ícone Add para criar uma nova ação.
   g. Selecione as opções desejadas no menu suspenso:
      - Destino é o endereço de e-mail ou gerenciador SNMP ao qual as notificações são enviadas quando um evento é ativado. Para obter mais informações sobre a configuração de um endereço de e-mail de destino, consulte Email na página 86.
      - Ou, quando o número de uma tomada é selecionado como destino, o estado da tomada muda para chaveado quando um evento é ativado e permanece no estado chaveado até a redefinição ou confirmação do evento. Para esta opção, o modo da tomada deve ser configurado como Alarm Control. Consulte Alarms & Warnings na página 51.

NOTA: Os atrasos de destino e as repetições são compartilhados com todos os alarmes. Se forem necessários muitos valores de atraso ou de repetição para destinos específicos, cada um deverá ser adicionado à lista de destinos, e a caixa Enabled adequada de cada alarme deverá ser marcada.

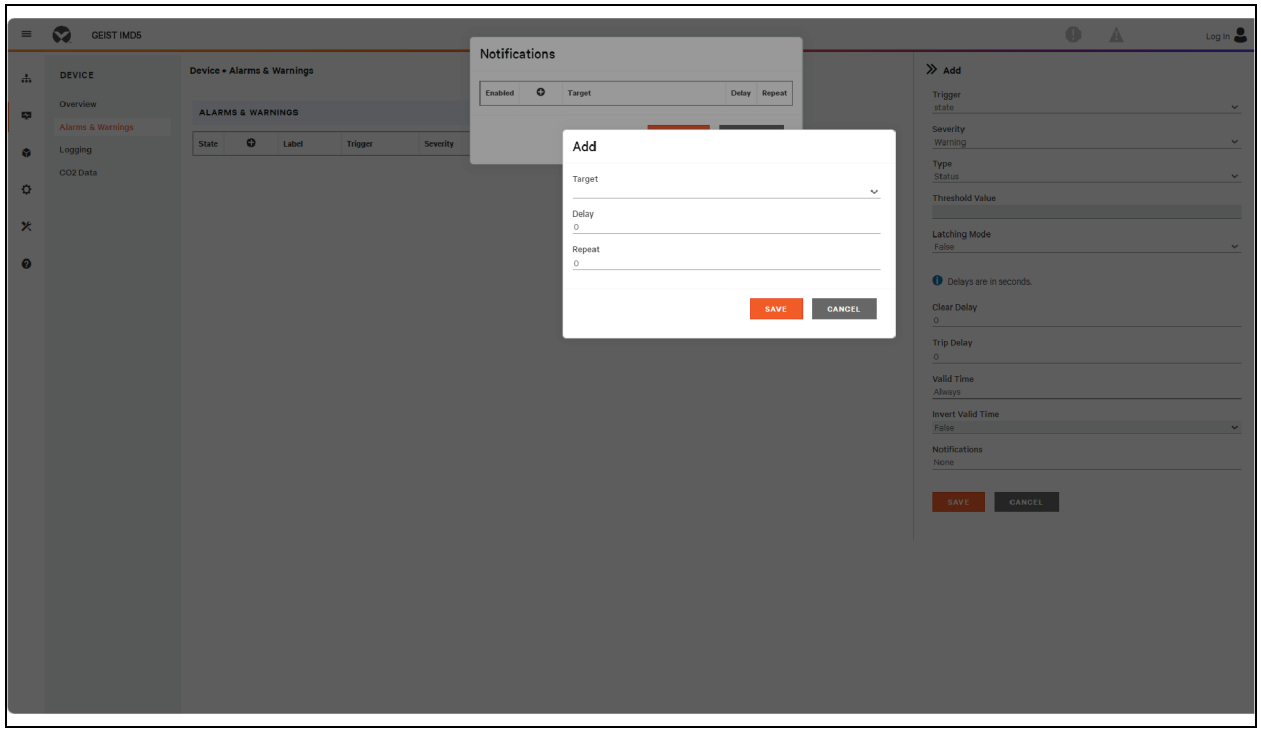
NOTA: Aplicável somente a rPDUs Geist™ Vertiv™ monitoradas/comutadas de tomada.

- Delay determina por quanto tempo este evento deve permanecer ativado antes de enviar a primeira notificação desta ação. Isso é diferente do Trip Delay acima. Trip Delay determina por quanto tempo o valor de limite precisa ser excedido para acionar o evento. Esse atraso determina por quanto tempo o evento deve permanecer ativado antes que esta ação ocorra. Delay pode ser de até 14.400 segundos (4 horas). Se o atraso for *0*, a notificação será enviada imediatamente.
- Repeat determina se várias notificações serão enviadas para esta ação de evento. As notificações repetidas são enviadas em intervalos especificados até o evento ser confirmado ou apagado e redefinido. O intervalo de repetição pode ser de até 14.400 segundos (4 horas). Se a repetição for *0*, este recurso será desativado e apenas uma notificação será enviada.

3. Clique em *SAVE* para salvar esta ação de notificação.

NOTA: É possível definir mais de uma ação para um alarme ou uma advertência. Para adicionar várias ações, apenas clique no ícone Add novamente e defina cada uma conforme desejado. Cada alerta pode ter até 32 ações associadas.

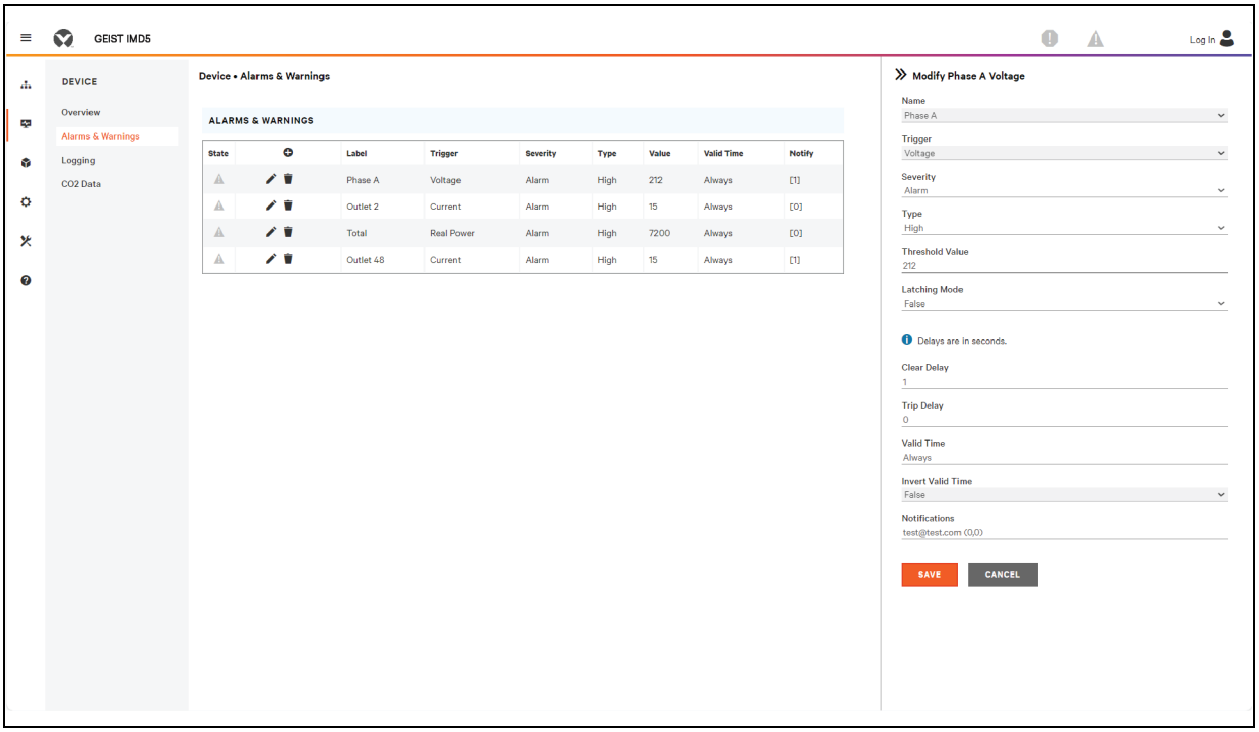
Figura 5.21 Janela de adição de alarmes e advertência



Para alterar um evento de alarme ou de advertência existente:

1. Clique no ícone Modify ao lado do evento de alarme ou de advertência que deseja alterar.
2. Modifique as configurações conforme necessário e clique em *SAVE*.
3. Quando uma ação é adicionada, ela inclui uma caixa de seleção na coluna ativada à esquerda. Por padrão, ela é desmarcada (desativada) quando uma ação é adicionada. Clique na *caixa de seleção* para ativá-la. Permite ativar e desativar seletivamente ações diferentes para teste.

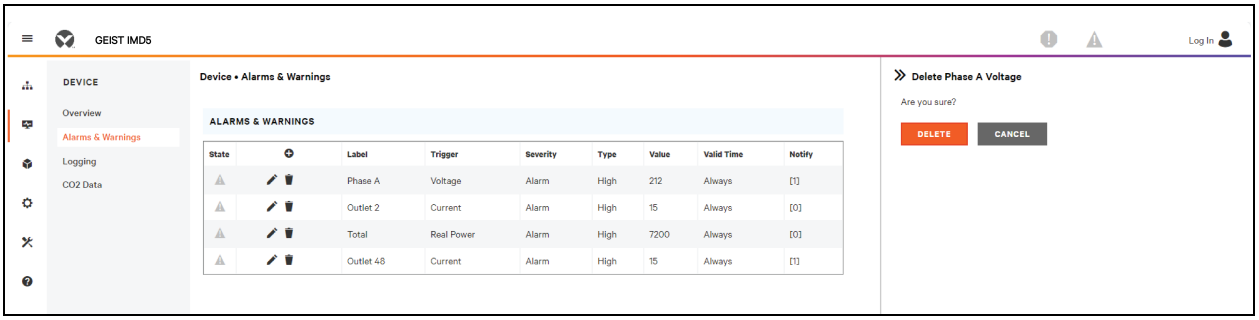
Figura 5.22 Janela de alteração de alarmes e advertência



Para excluir um evento de alarme ou de advertência existente:

1. Clique no ícone de exclusão ao lado do evento de alarme ou de advertência que deseja remover.
2. Clique em *DELETE* e *SAVE* para confirmar.

Figura 5.23 Excluir evento de alarmes e advertência



5.4.3 Logging

A página Logging permite acessar os dados históricos gravados pela rPDU Geist™ Vertiv™, selecionando os sensores desejados e o período de gravação. A página Logging permite selecionar tudo ou nada.

Para selecionar ou remover a seleção do valor da medição:

1. Clique no ícone Device e no submenu Logging.
2. Na página Logging, clique em *Select All* para selecionar o valor da medição e em *Select None* para remover a seleção do valor da medição.

Figura 5.24 Página Logging

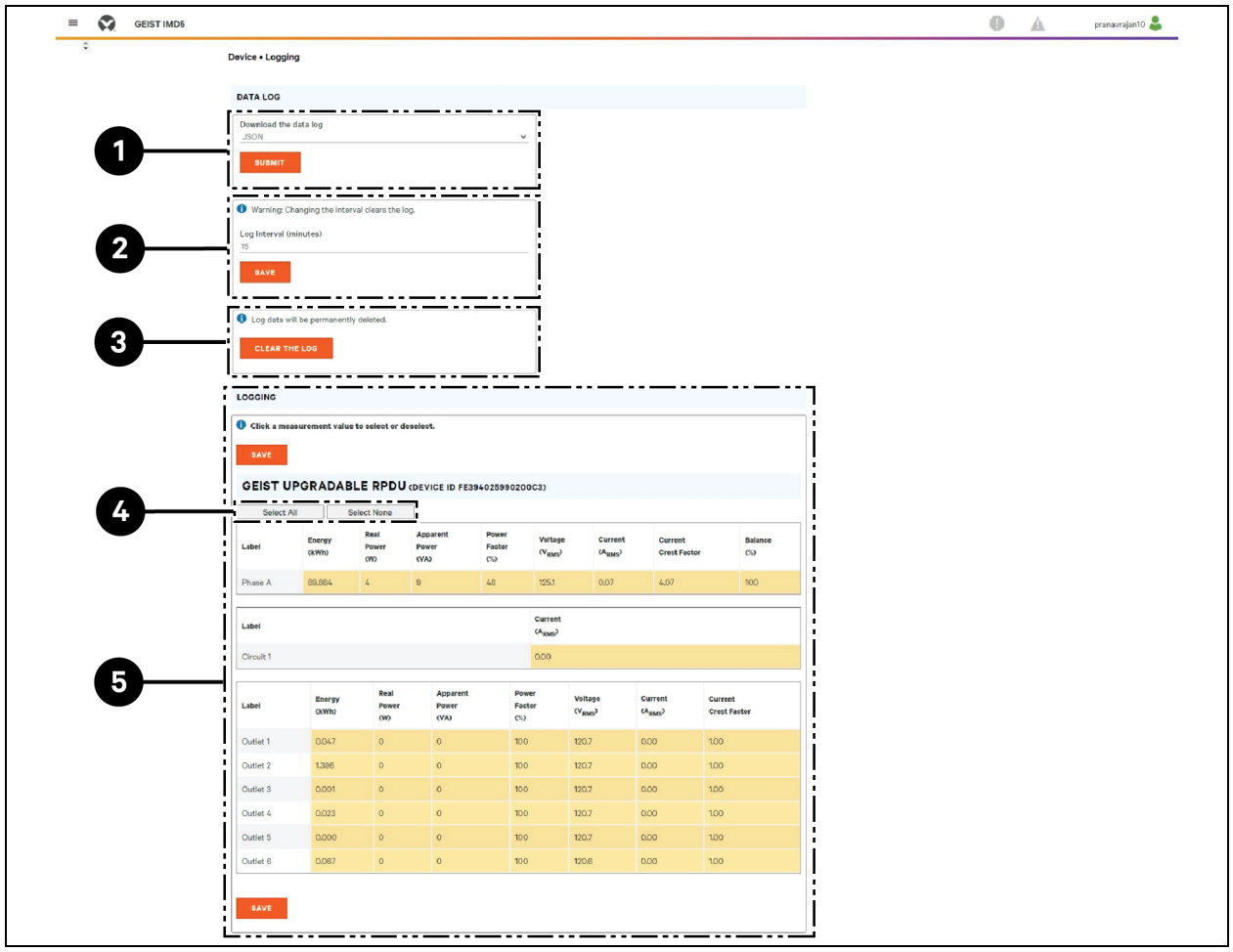


Tabela 5.10 Descrições da página Logging

Item	Nome	Descrição
1	Download the data log	Clique no menu suspenso e selecione uma das opções: *JSON* para o formato *JSON*. CSV para o formato .csv no software de planilha. Clique no botão *SUBMIT* para baixar o log de dados.
2	Log interval	A frequência com que os dados são gravados no arquivo de log. O intervalo de gravação de logs pode ser entre 1 e 600 minutos; a configuração padrão é de 15 minutos. **ADVERTÊNCIA! Os dados do registro serão excluídos permanentemente.**
3	Clear the log	Excluir o arquivo de log. **ADVERTÊNCIA! Os dados do registro serão excluídos permanentemente.**
4	Select All/Select None	Clique em *Select All* para selecionar o valor da medição e em *Select None* para remover a seleção do valor da medição.
5	Logging	Clique no valor da medida para marcar ou desmarcar os parâmetros de gravação de logs desejados. Por padrão, todas as medidas estão selecionadas. Clique em *SAVE* para salvar as alterações.

NOTA: O período máximo para gravação de logs é determinado pelo número de medições que são gravadas em log e pelo intervalo em que os dados são gravados no arquivo de log.

5.4.4 CO2 Data

Figura 5.25 Página inicial de CO2

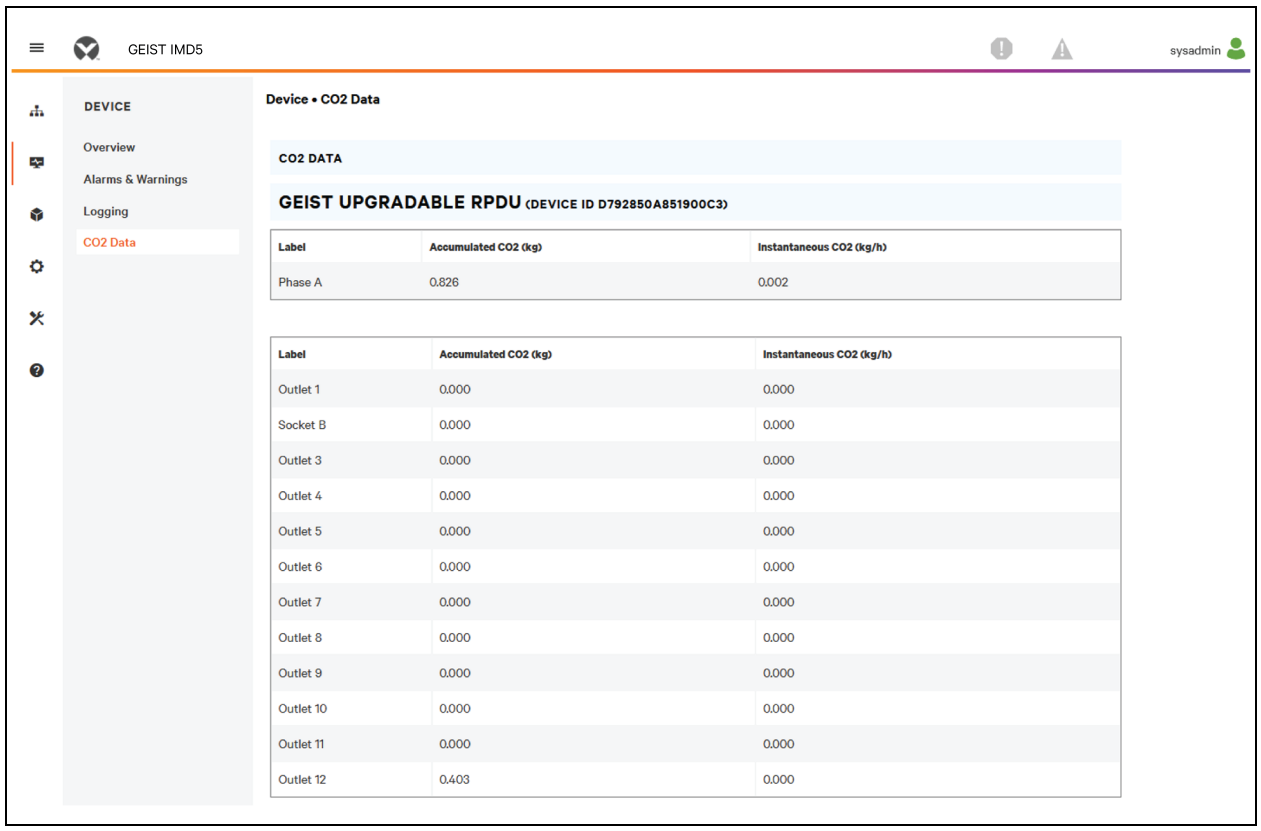
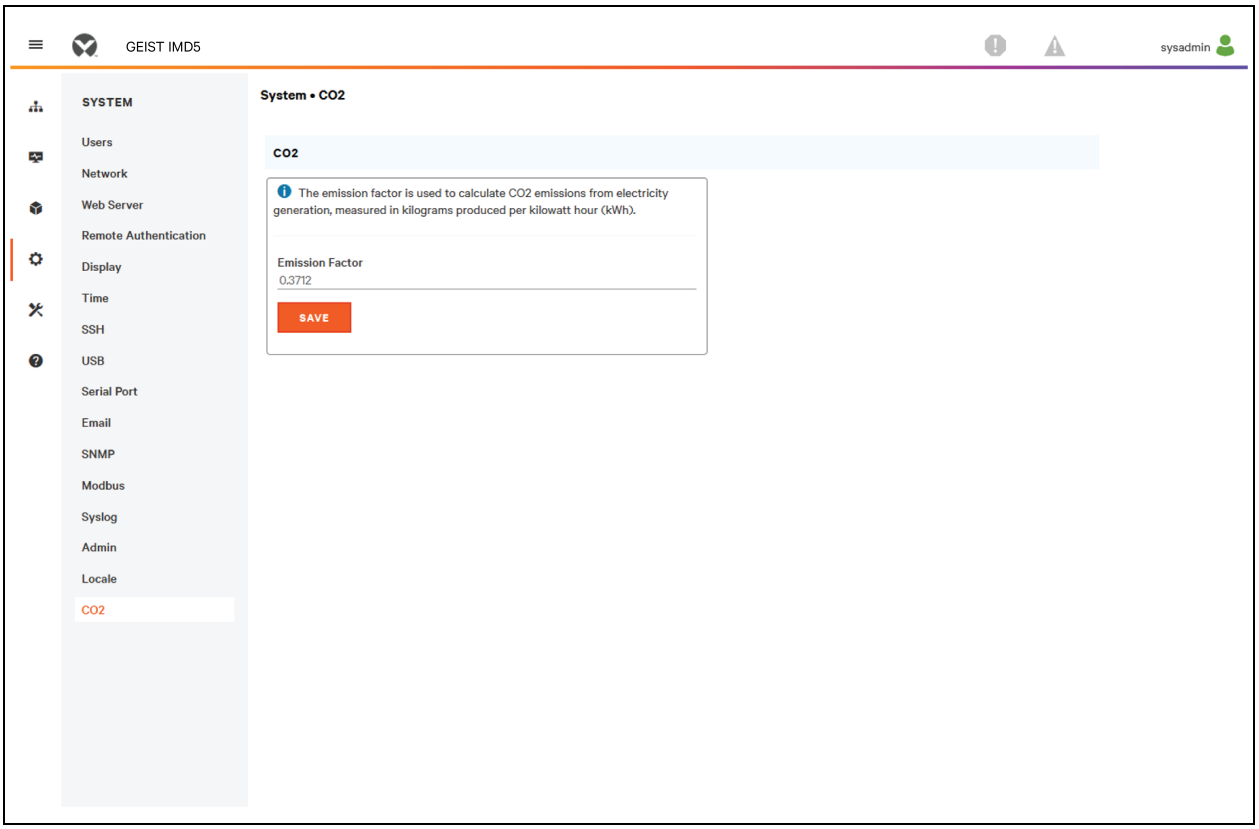


Figura 5.26 Aba System de CO2



NOTA: Essas são as três páginas associadas à página de CO2. A primeira página é a que contém os dados de CO2 em Device (Figura 5.25 na página anterior), que mostra os cálculos acumulados e instantâneos das fases e tomadas. A segunda página é a página de CO2 em System, onde é possível definir o Emission Factor para calcular o CO2 por kWH. O fator de emissão padrão de CO2 será definido como 0,3172. A terceira página está na página de ajuda; o CO2 vitalício é baseado na Lifetime Energy. Se um usuário redefinir o uso de energia em uma PDU ou tomada específica, o valor voltará para 0. No entanto, a energia vitalícia desse componente não voltará para 0.

5.5 Submenu Provisioner

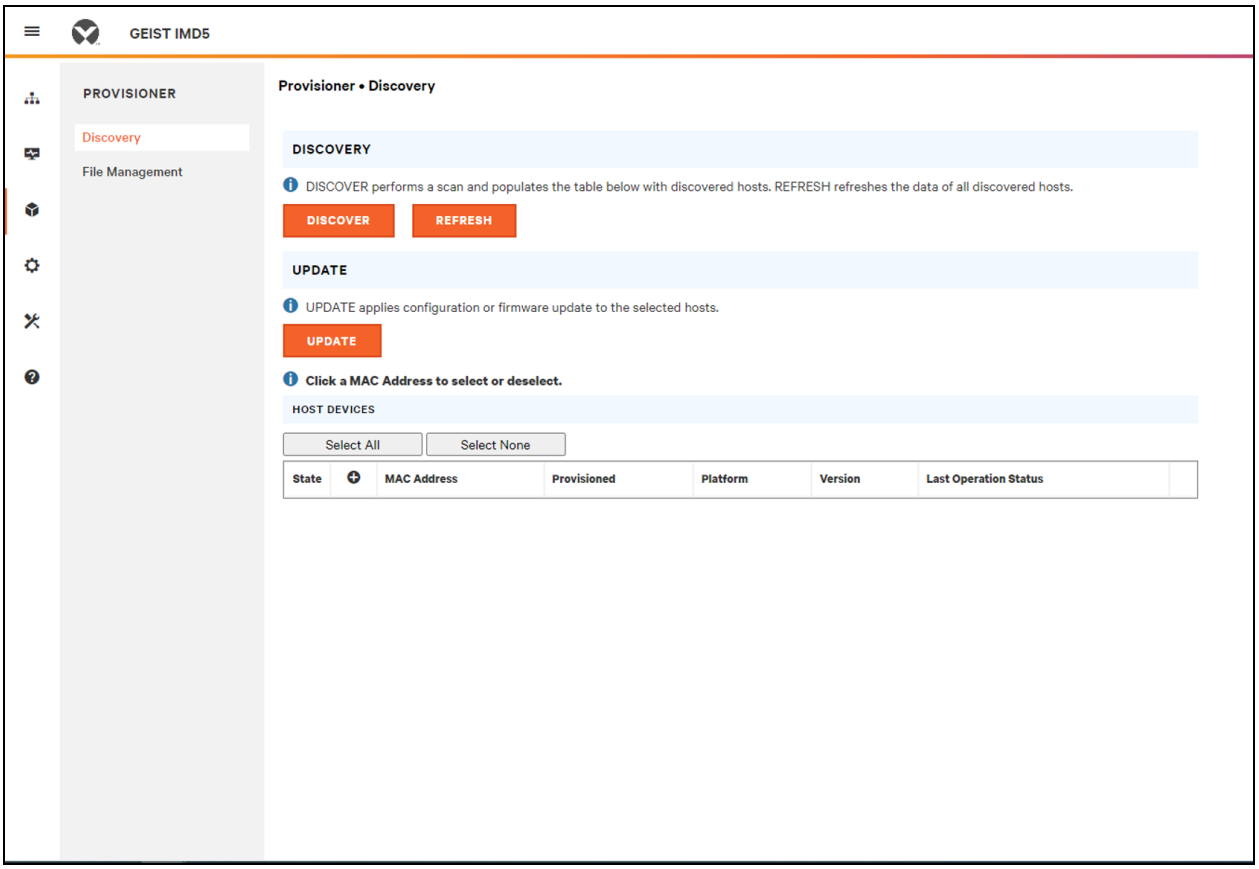
O submenu Provisioner permite que o usuário detecte as rPDUs Geist™ Vertiv™ conectadas localmente. Para atualizar e configurar o firmware, o usuário pode carregar um arquivo de configurações.

O submenu Provisioner permite definir as configurações do dispositivo (por exemplo, alarmes) e do sistema. Esta funcionalidade pode incluir:

- IMD-5M com firmware 6.x.x.
- rPDUs com firmware 5.x.x (modelos IMD 3E, 03E, 3E-S e 03E-S).
- rPDUs Geist™ com 6.1.0, novas de fábrica ou configuradas anteriormente.
- PDUs de rack conectadas diretamente à rede local ou conectadas como parte de uma rede do Vertiv Intelligence Director (agregação).
- Todas ou as rPDUs Geist™ detectadas selecionadas.

NOTA: Você deve estar conectado como usuário no nível de administrador para utilizar o Provisionador. É necessário ativar o IPV6 nas rPDUs Geist™ detectadas. É possível configurar a maioria dos itens no menu da interface de usuário do sistema. Outras configurações, como do sensor e de alarmes, não podem ser definidas com esta versão da ferramenta de instalação.

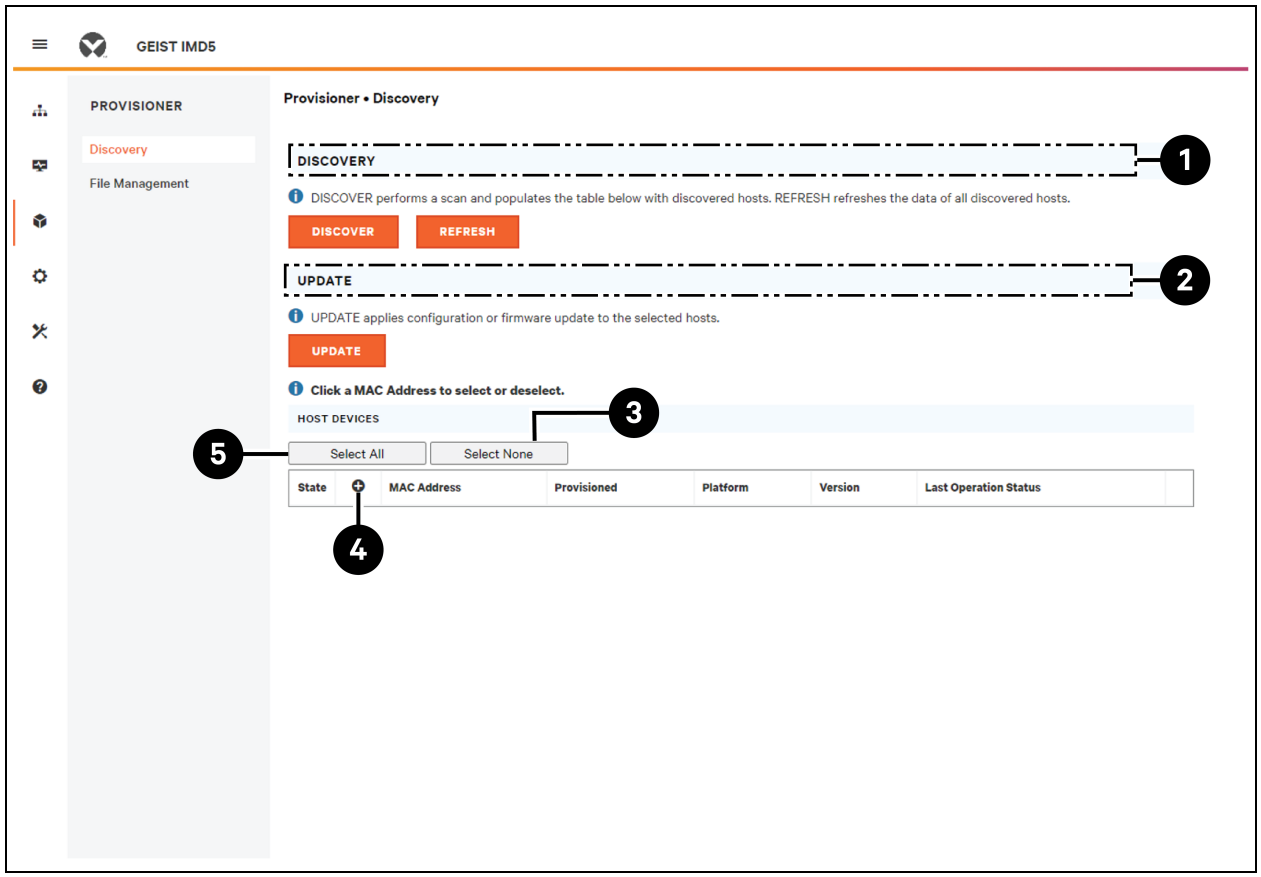
Figura 5.27 Página do submenu Provisioner



5.5.1 Discovery

1. Clique em *DISCOVER* para identificar rPDUS Geist™ Vertiv™ conectadas localmente.
2. Clique em todas as rPDUs Geist™ da lista das quais você deseja atualizar o firmware e/ou a configuração. As unidades selecionadas estarão destacadas em verde. Você também pode clicar em *Select All* para atualizar todas as rPDUs Geist™ da lista.
3. Clique no ícone *UPDATE* para atualizar todas as rPDUs Geist™ selecionadas com o arquivo de firmware e/ou de configuração.

Figura 5.28 Discovery



Número	Nome	Descrição
1	Discover	Identifica o local e a rede das PDUs de rack conectadas
2	Update	Atualiza o firmware e/ou a configuração das rPDUs selecionadas
3	Select None	Selecione None para remover todas as seleções
4	Add MAC address	Permite rPDUs inseridas manualmente pelo endereço MAC
5	Select All	Seleciona todas as rPDUs conectadas

NOTA: Você deve carregar os arquivos de firmware e de configuração antes de executar esta etapa na guia File Management.

5.5.2 File Management

Arquivos de firmware:

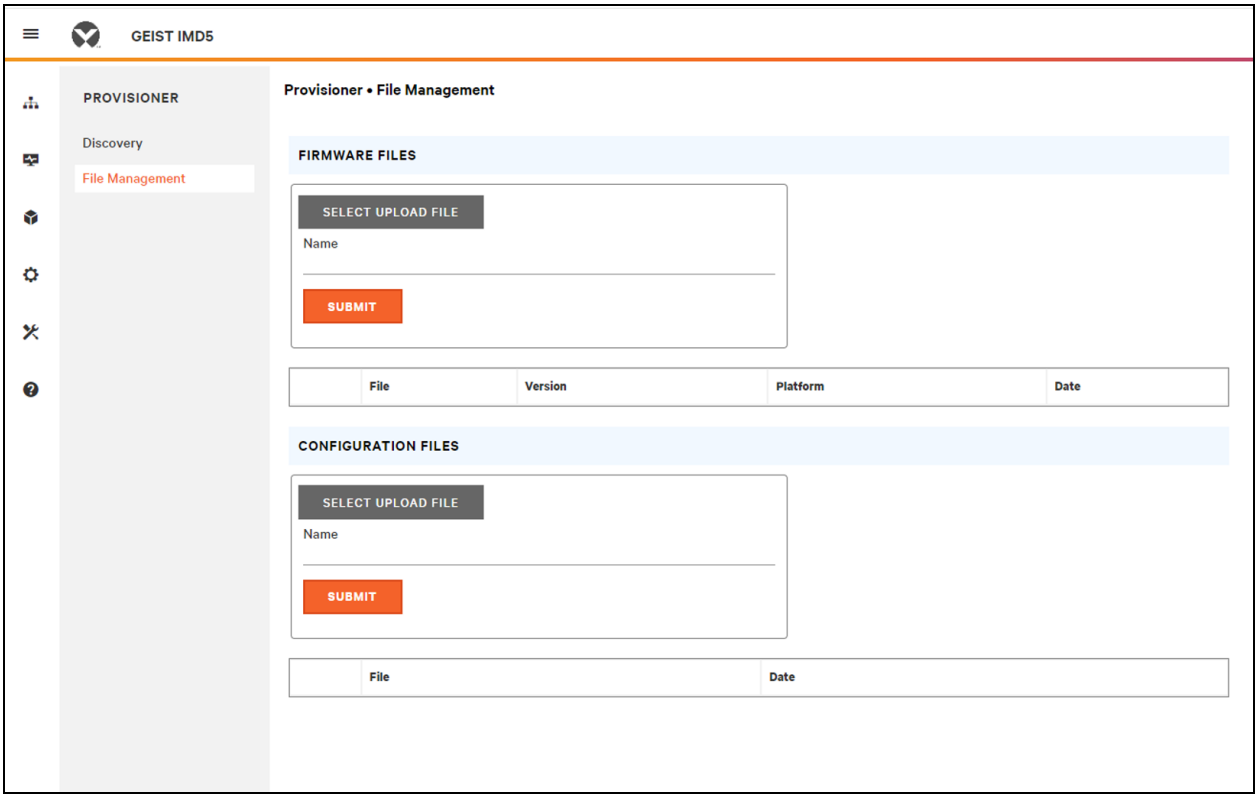
1. Clique em *SELECT UPLOAD FILE* e selecione o ***arquivo .firmware*** na janela Open.
2. Clique em *SUBMIT*. O arquivo de firmware será listado.

Arquivos de configuração:

1. Clique em *SELECT UPLOAD FILE* e selecione o ***arquivo .config*** na janela Open.

2. Clique em *SUBMIT*. O arquivo de configuração será listado.

Figura 5.29 Página File Management



Consulte Provisioner: formato do arquivo de configurações na página 129 para ver exemplos de arquivos de configurações usados pelo Provisionador e o formato necessário do arquivo.

5.6 Submenu System

NOTA: Você deve estar conectado como Administrador para modificar as configurações na guia System.

5.6.1 Users

A página Users no menu System permite gerenciar ou restringir o acesso aos recursos da unidade criando contas para usuários diferentes.

NOTA: Política de bloqueio de conta Web/SSH/CLI: Uma conta é bloqueada por 30 minutos quando 10 tentativas seguidas de login incorreto são feitas dentro de 60 minutos. Isso pode ser editado com a versão mais recente do firmware.

O escopo permite que uma conta no nível de administrador restrinja a visibilidade das informações de tomada especificadas.

Figura 5.30 Página User

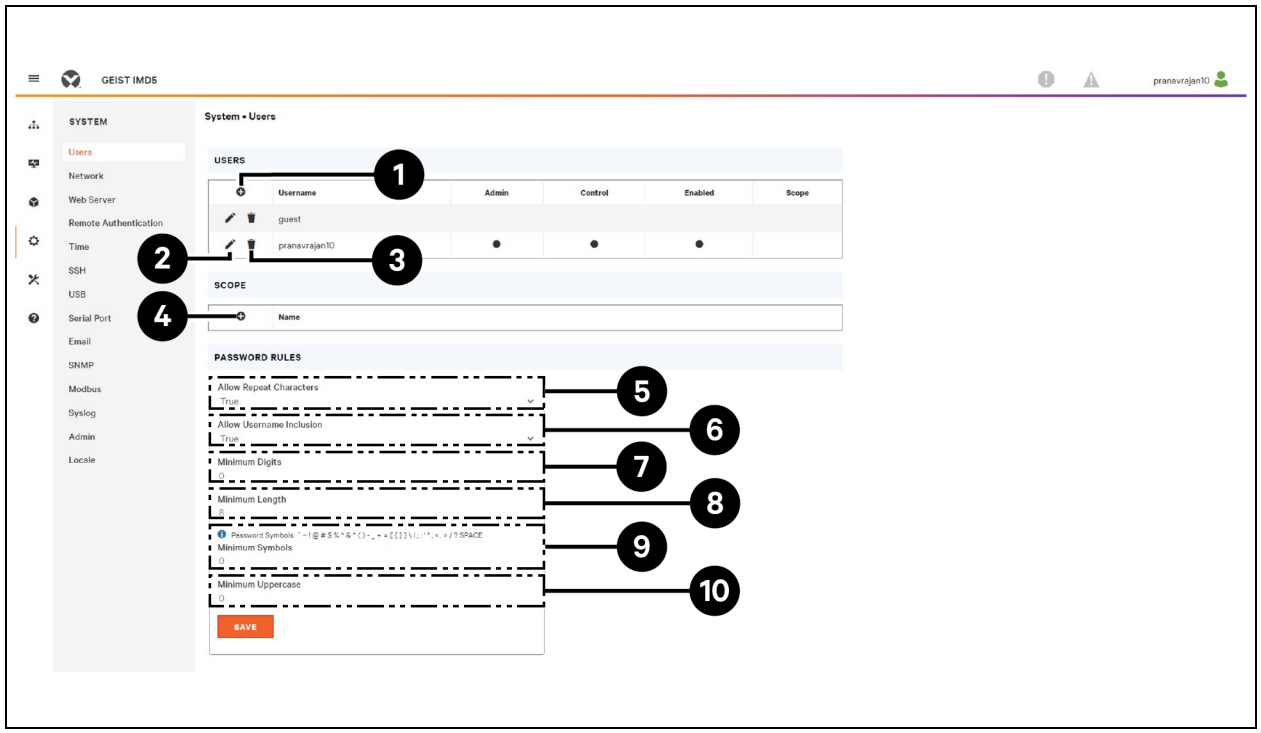


Tabela 5.11 Descrições da página User

Número	Descrições
1	Add new user account
2	Modify user account
3	Delete user account
4	Add user scope : visível somente quando conectado como Administrador*
5	Allow Repeat Characters: restringir o uso de mais do que 2 caracteres repetidos (o padrão é falso)*
6	Allow Username Inclusion: restringir a inclusão do nome de usuário na senha (o padrão é falso)*
7	Minimum Digits: inserir o mínimo de caracteres digitais numéricos (o padrão é 0)*
8	Minimum Length: inserir o número mínimo de caracteres de senha (o padrão é 8, o mínimo é 6)*
9	Minimum Symbols: inserir o mínimo de caracteres de símbolos (o padrão é 0)*
10	Minimum Uppercase: inserir o mínimo de caracteres maiúsculos (o padrão é 0)*
NOTA: *Visível somente quando conectado como Administrador.	

NOTA: Somente uma conta no nível de administrador pode adicionar, modificar ou excluir usuários e escopos. As contas no nível de controle e somente leitura podem alterar suas próprias senhas usando o ícone de modificação de usuário, mas não podem adicionar, excluir ou modificar outras contas. A conta de convidado não pode adicionar, excluir ou modificar nenhuma conta, nem ela própria.

Para adicionar ou modificar uma conta do usuário:

1. Clique no ícone de adição ou modificação de usuário.
2. Crie ou modifique as informações da conta, conforme necessário.
   a. Username: o nome da conta. Os nomes de usuário podem ter até 24 caracteres, diferenciam maiúsculas de minúsculas e não podem incluir espaços ou qualquer um destes caracteres proibidos: $& `:<>[ ] { }"+%@/ ; =?\^|~',

NOTA: Não é possível alterar o nome de usuário depois que a conta é criada.

   b. Administrator: se definido como *True*, esta conta terá acesso no nível de Administrador à unidade e poderá alterar qualquer configuração.
   c. Control: se definido como *True*, está conta terá acesso no nível de Controle. Se Administrator for configurado como *True*, Control também será definido como *True*. Se for configurado como *False*, a conta se tornará Enabled, o que significa somente visualização.
   d. Scope: se um escopo do usuário foi criado, selecione o escopo relevante para a conta. Consulte a etapa Para adicionar ou modificar o escopo de um usuário: na página oposta.
   e. New Password: a senha da conta pode ter até 24 caracteres, diferencia maiúsculas de minúsculas e não pode incluir espaços.
   f. Account Status: defina a conta como *Enabled* ou *Disabled*. A desativação da conta evita que ela seja usada para fazer login, mas não a exclui da lista de contas.
3. Clique em *SAVE*.

Tipos de conta do usuário

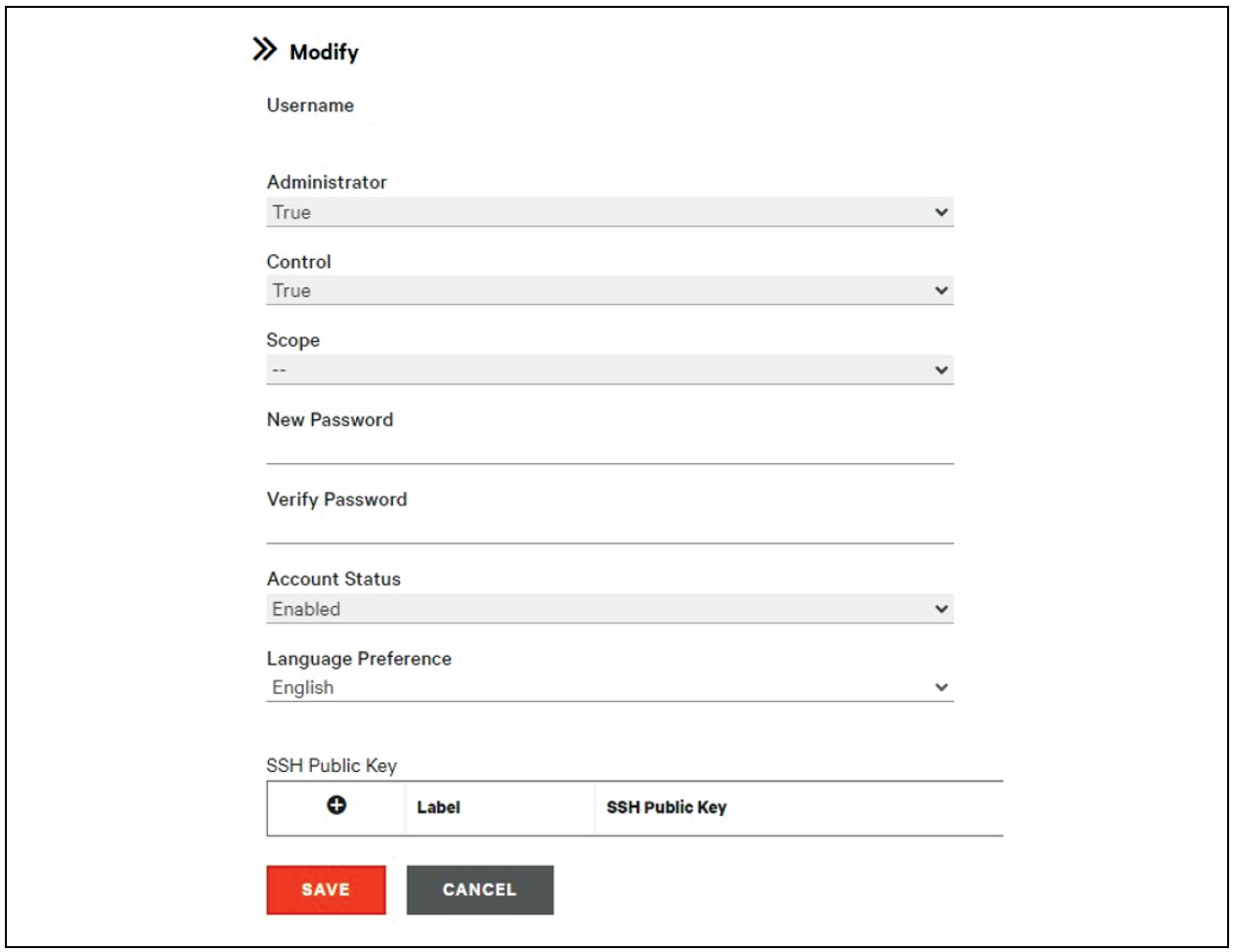
- Administrator: as contas de administrador (contas com administrador e autoridade de controle definidos como *True*, conforme mostrado acima) têm controle total de todas as funções e configurações disponíveis no dispositivo, incluindo a capacidade de modificar as configurações do sistema e de adicionar, modificar ou excluir contas de outros usuários.
- Control: as contas de controle (contas apenas com o controle definido como *True*) têm controle de todas as configurações referentes aos sensores do dispositivo. Elas podem adicionar, modificar ou excluir eventos de alarmes e de advertência e ações de notificação e podem alterar os nomes ou rótulos do dispositivo e de seus sensores. As contas de controle não podem modificar as configurações do sistema nem fazer alterações nas contas de outros usuários.
- View-Only: se tanto administrador quanto controle estiverem definidos como *False*, a conta será somente visualização. As únicas alterações que uma conta somente visualização pode fazer são alterar a senha e o idioma preferencial da própria conta. As contas somente visualização não podem alterar as configurações do dispositivo ou do sistema.
- Guest: qualquer usuário que visualiza a página da Web da unidade sem fazer login está automaticamente visualizando a unidade como convidado. Por padrão, a conta de convidado é uma conta somente visualização e não pode alterar nenhuma configuração nem permitir que alguém altere nomes, rótulos, eventos de alarme e notificações sem fazer login. A conta de convidado não pode ser excluída, mas pode ser desativada para exigir o login e visualizar o status do sistema.

Para alterar uma senha do usuário:

1. Faça login na sua conta.
2. Clique no ícone de modificação de usuário.

3. Clique no nome de usuário no canto superior direito da página.
4. Insira uma nova senha e verifique-a ao reinseri-la no campo Verify password.
5. Clique em *SAVE*.

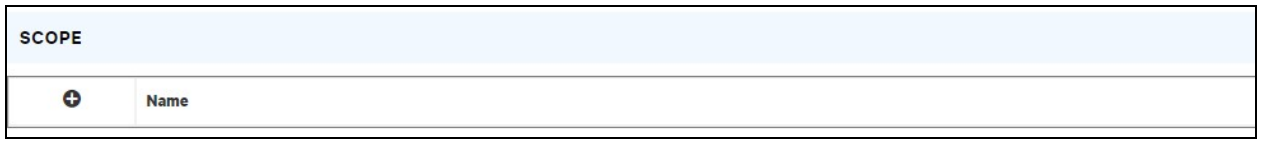
Figura 5.31 Página de alteração de senha do usuário



Para adicionar ou modificar o escopo de um usuário:

1. Clique no ícone de adição ou modificação de escopo. Consulte a Figura 5.32 abaixo.
2. Crie ou modifique as informações do escopo, conforme necessário.
   a. **Label:** insira o nome desejado do escopo selecionado.
   b. **Remote Authentication Attribute:** usado para todos os tipos de autenticação remota.
   c. Clique nas tomadas relevantes ao usuário especificado. (Destaque em verde)
3. Clique em *OK* para salvar as alterações.

Figura 5.32 Adicionar escopo



Configurações de regras de senha e política de conta

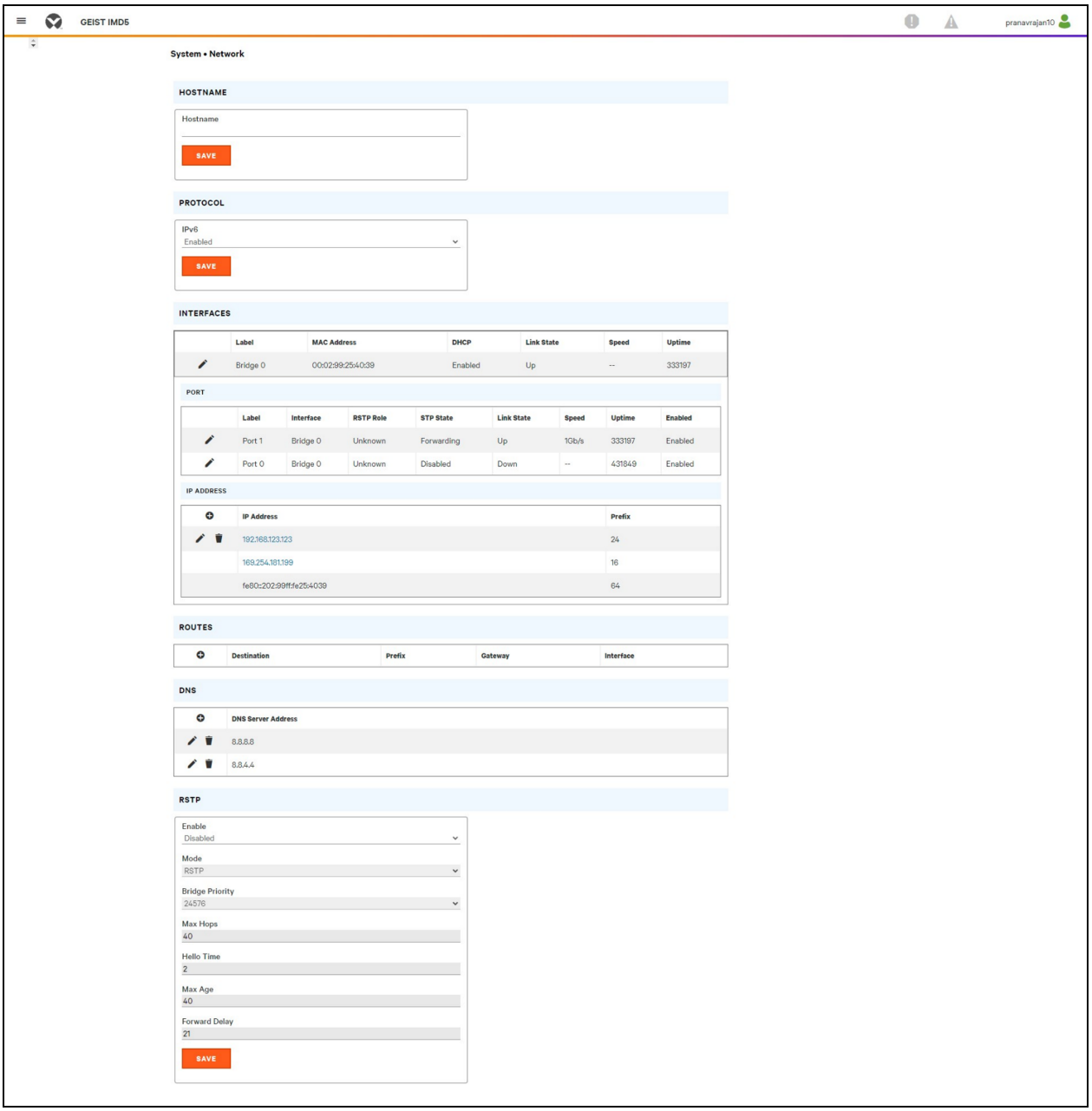
NOTA: O usuário será automaticamente desconectado após 10 minutos de inatividade.

5.6.2 Network

A configuração de rede da unidade é definida na *guia Network* do menu System. As configurações referentes à conexão de rede da unidade são:

- Hostname: o nome do host pode ser usado como um método para identificação do dispositivo na rede.
- Protocol: clique no menu suspenso IPv6, selecione *Enabled* ou *Disabled* e clique em *Save*.
- Interfaces: usadas para configurar o endereço IP da rPDU Geist™ Vertiv™, ativar/desativar o DHCP e visualizar o estado do link, a velocidade e o tempo de atividade. O dispositivo aceita até oito entradas de endereço IP configuradas pelo usuário.
- Ports: usadas para visualizar e/ou modificar as configurações da porta ETHERNET e o status do RSTP, interface, estado do STP, velocidade, tempo de atividade e estado do link e a ativação de cada porta da rPDU Geist™.
- IP Address: usado para adicionar ou modificar os endereços IP.
- Routes: exibem as rotas configuradas e é onde você definirá o endereço gateway para a rPDU Geist™. As rotas padrão são diferenciadas por um *destino* de 0.0.0.0 ou ::, com um Prefixo 0 e Interface all. Só pode haver uma rota padrão para IPv4 e uma para IPv6.
- DNS: permite que a unidade resolva os nomes de host dos servidores de e-mail, NTP e SNMP.
- RSTP: usado para visualizar e modificar o estado do RSTP, modo, prioridade da ponte, máx. de hops, idade máxima (máx.) do tempo de saudação e atraso de encaminhamento.

Figura 5.33 Página de configuração de rede



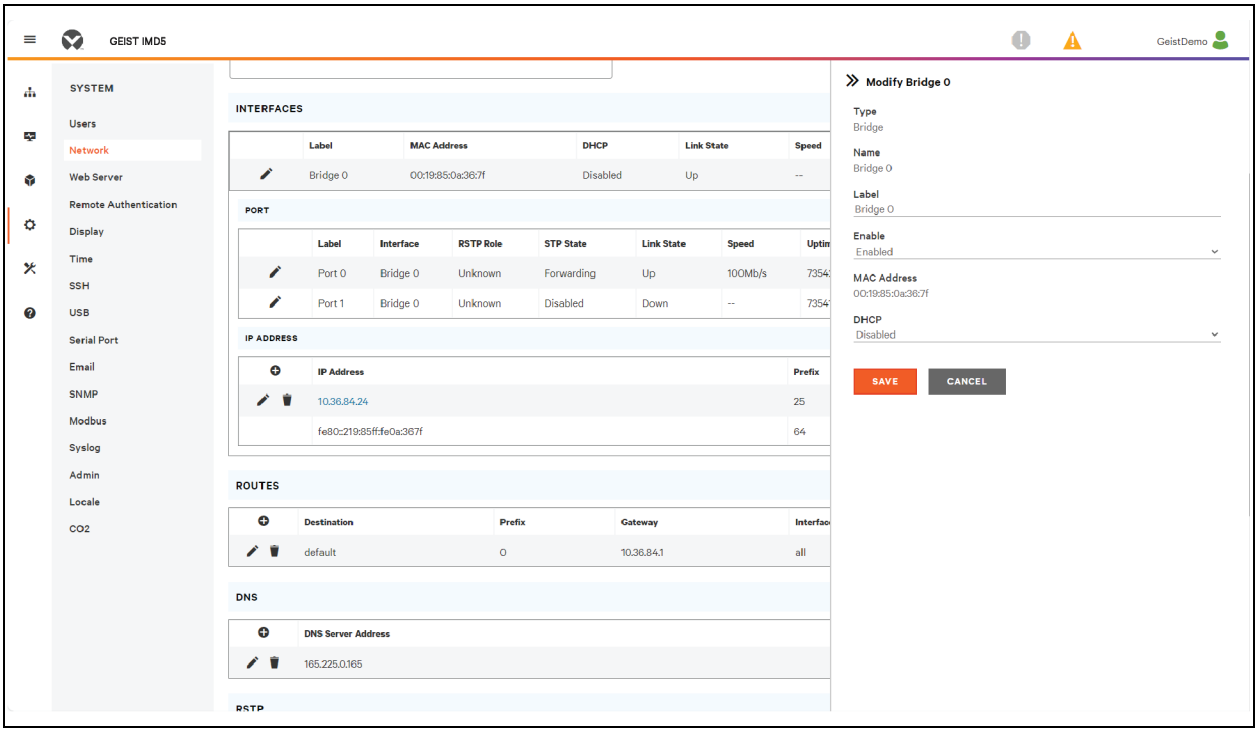
Para editar os parâmetros de interface:

1. Clique no ícone Modify.
2. Modifique os campos desejados.
   a. **Label:** *alterar* o nome desejado da interface selecionada.
   b. **Enable:** *ativar/desativar* a interface selecionada. Se apenas uma interface estiver disponível, sua desativação impedirá o acesso ao dispositivo, exigindo a redefinição da rede.
   c. **DHCP:** *ativar/desativar* DHCP na interface selecionada.

3. Clique em *SAVE*.

NOTA: Todas as alterações feitas nas configurações de interface de rede entram em vigor ao clicar no botão *Save*. Se você alterou o endereço IP, pode parecer que a unidade não responde mais porque o navegador não consegue recarregar a página da Web. Feche a janela do navegador e digite o novo endereço IP na barra de endereço do navegador para acessar a unidade.

Figura 5.34 Parâmetros da interface



Para adicionar uma interface a um adaptador USB sem fio:

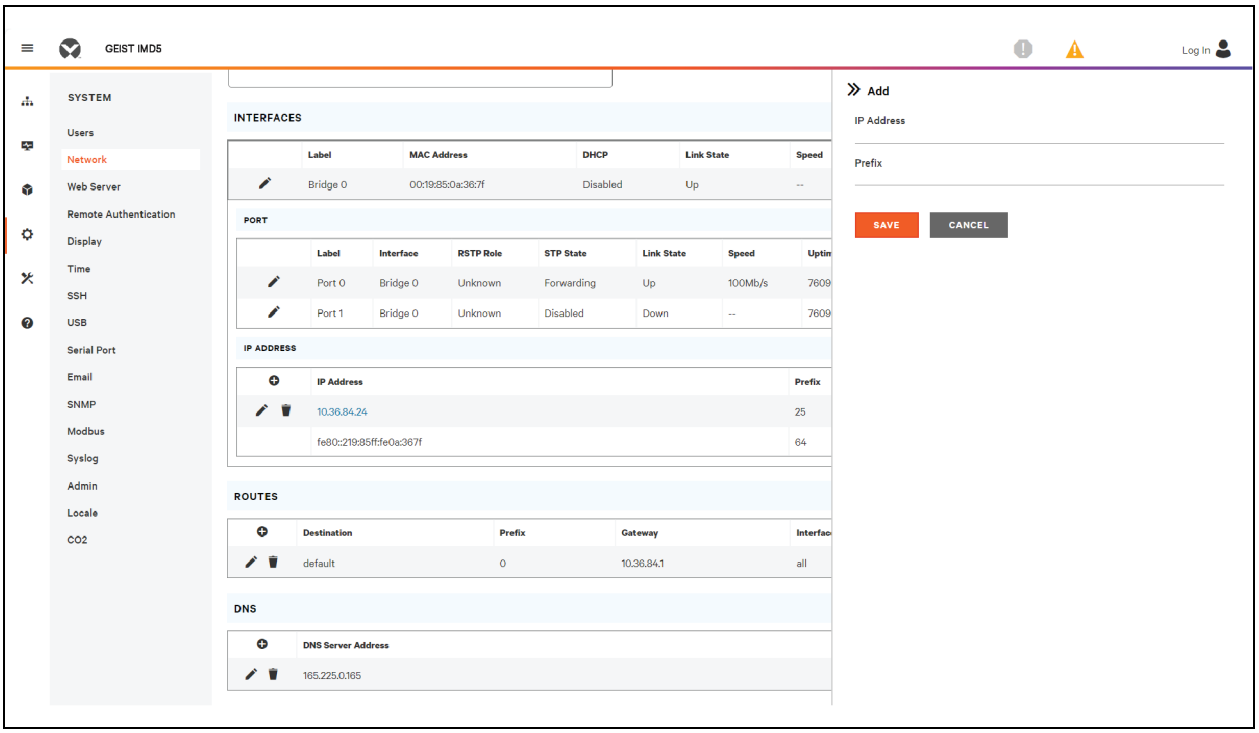
1. Insira o adaptador USB sem fio na porta USB. (A rPDU ficará inacessível por alguns segundos durante a autorreconfiguração da pilha de rede.)
2. Após a detecção automática do adaptador, a interface do Wi-Fi aparecerá.
3. Clique no ícone Modify. Selecione o SSID aplicável no menu suspenso Detected SSIDs.

NOTA: Consulte Adaptadores USB sem fio de TP-Link na página 124 para ver os adaptadores sem fio TP-Link.

Para adicionar um novo endereço IP:

1. Clique no ícone Add.
2. Insira o endereço IPv4 ou IPv6 e o prefixo/máscara de sub-rede nos campos adequados. É possível atribuir até oito endereços IP estaticamente.
3. Clique em *SAVE*.

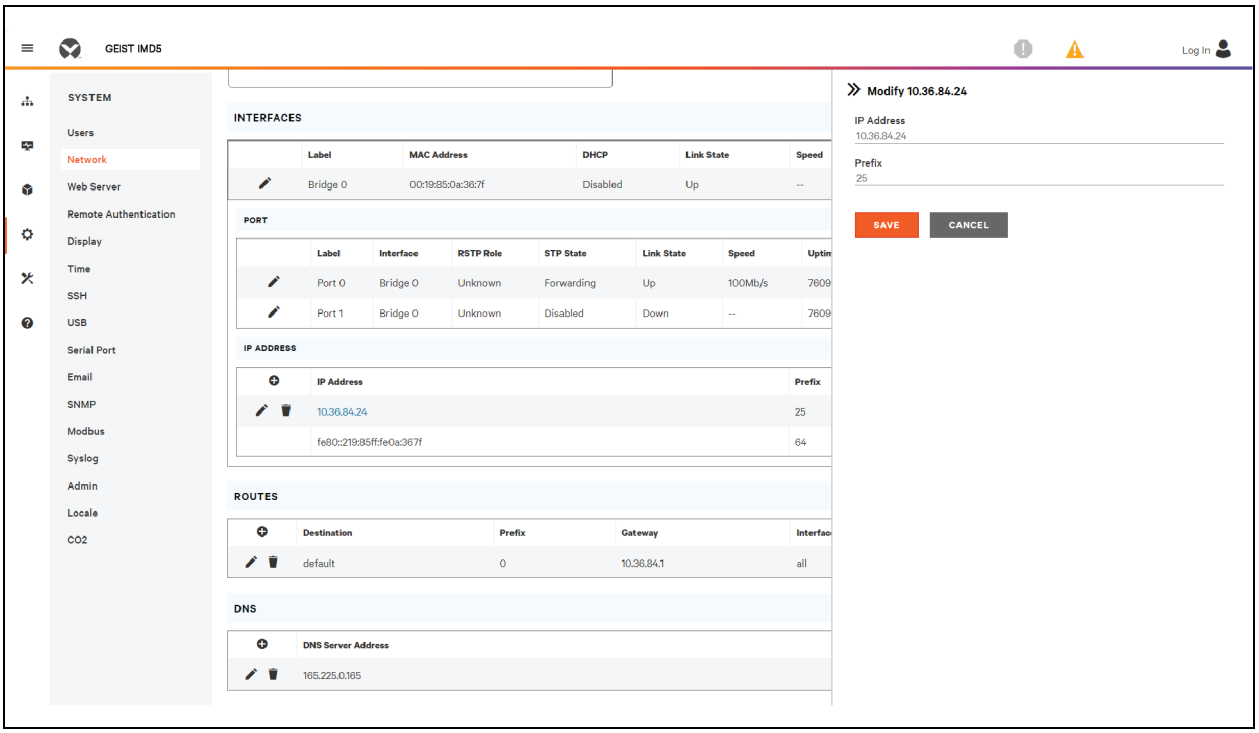
Figura 5.35 Adicionar um novo endereço IP



Para modificar um endereço IP existente:

1. Clique no ícone Modify.
2. Edite os campos IP address e Prefix/Subnet Mask conforme necessário.
3. Clique em *SAVE*.

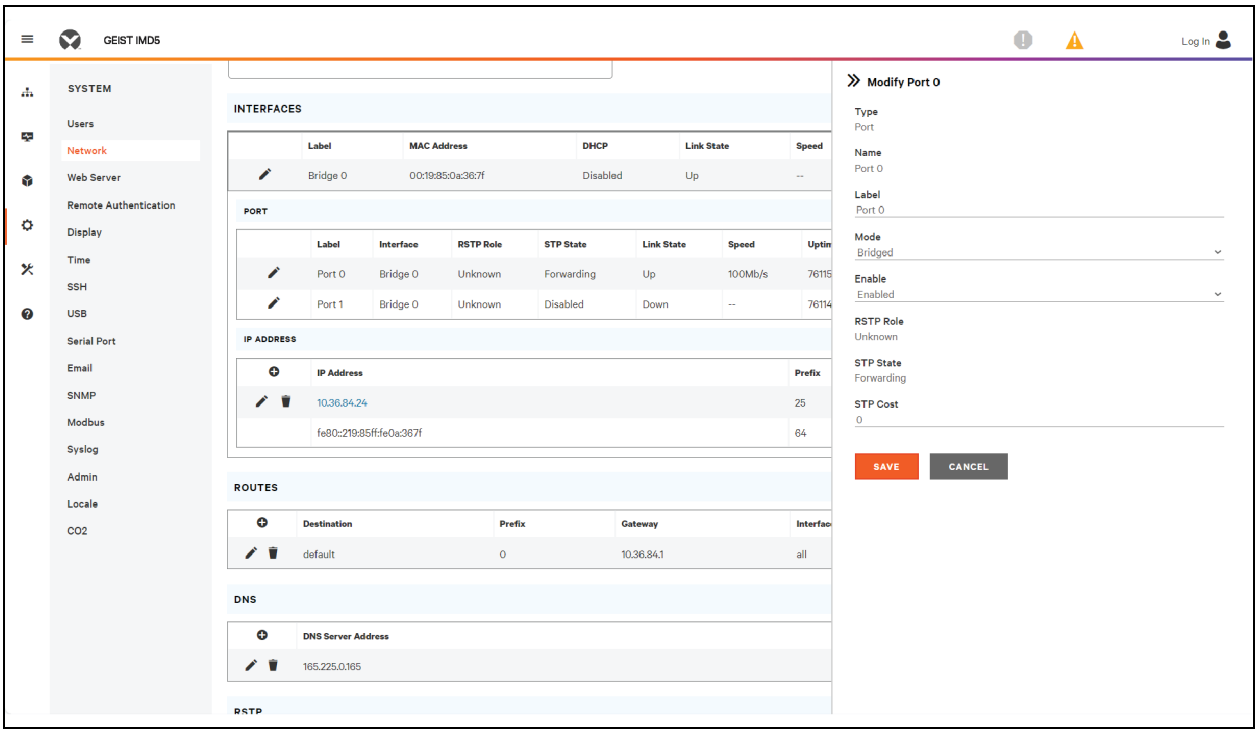
Figura 5.36 Modificar um endereço IP



Para modificar as configurações de porta:

1. Clique no ícone Modify.
2. Insira as informações adequadas.
   a. Se desejado, altere o rótulo da porta.
   b. Selecione o modo Bridged ou Independent.
   c. Ative/Desative a porta.
   d. Atribua o estado doe STP. Isso indica a contribuição desta interface com o custo do caminho raiz quando ela funciona como a porta raiz.
3. Clique em *SAVE*.

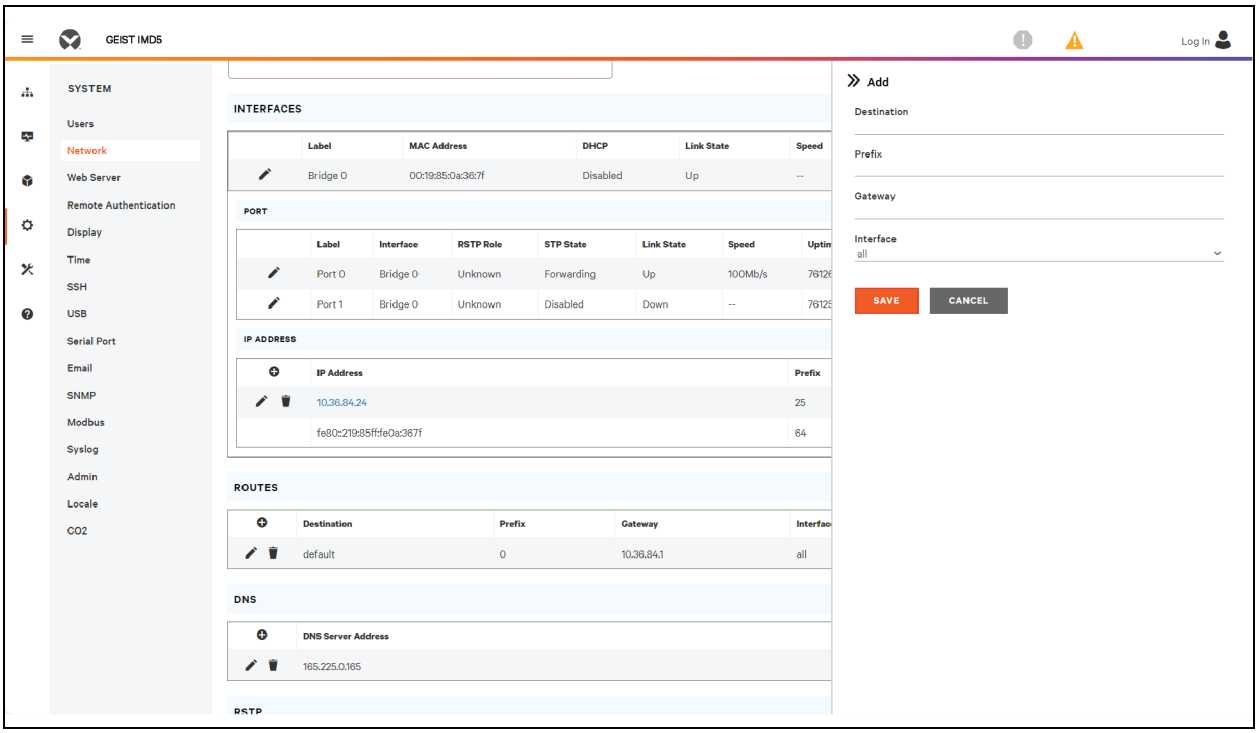
Figura 5.37 Modificar as configurações de porta



Para adicionar uma nova rota:

1. Clique no ícone Add.
2. Insira as informações adequadas.
   a. Endereço IP de destino da rota desejada.
   b. Insira o *Prefix* da rota desejada.
   c. Insira o endereço IP do gateway.
   d. Selecione a *Interface* à qual a rota se aplica.
3. Clique em *SAVE*.

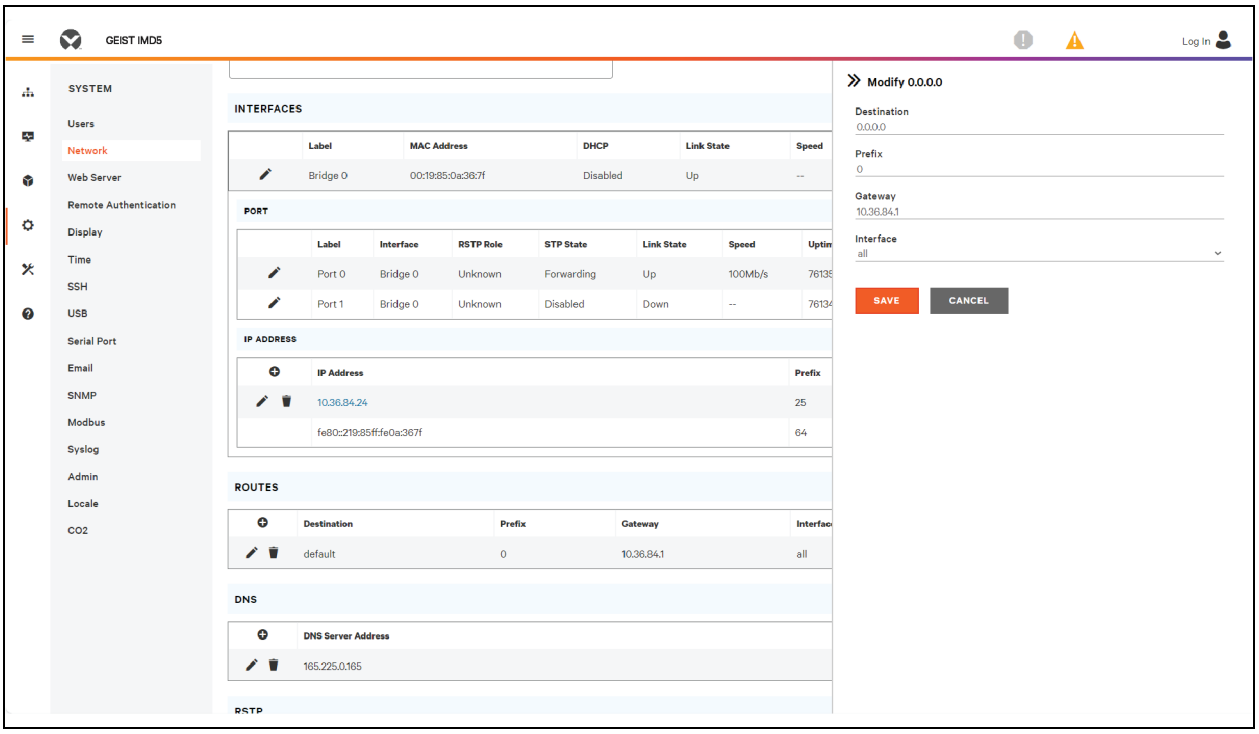
Figura 5.38 Adicionar rota



Para modificar uma rota existente:

1. Clique no ícone Modify.
2. Edite os campos obrigatórios.
3. Clique em *SAVE*.

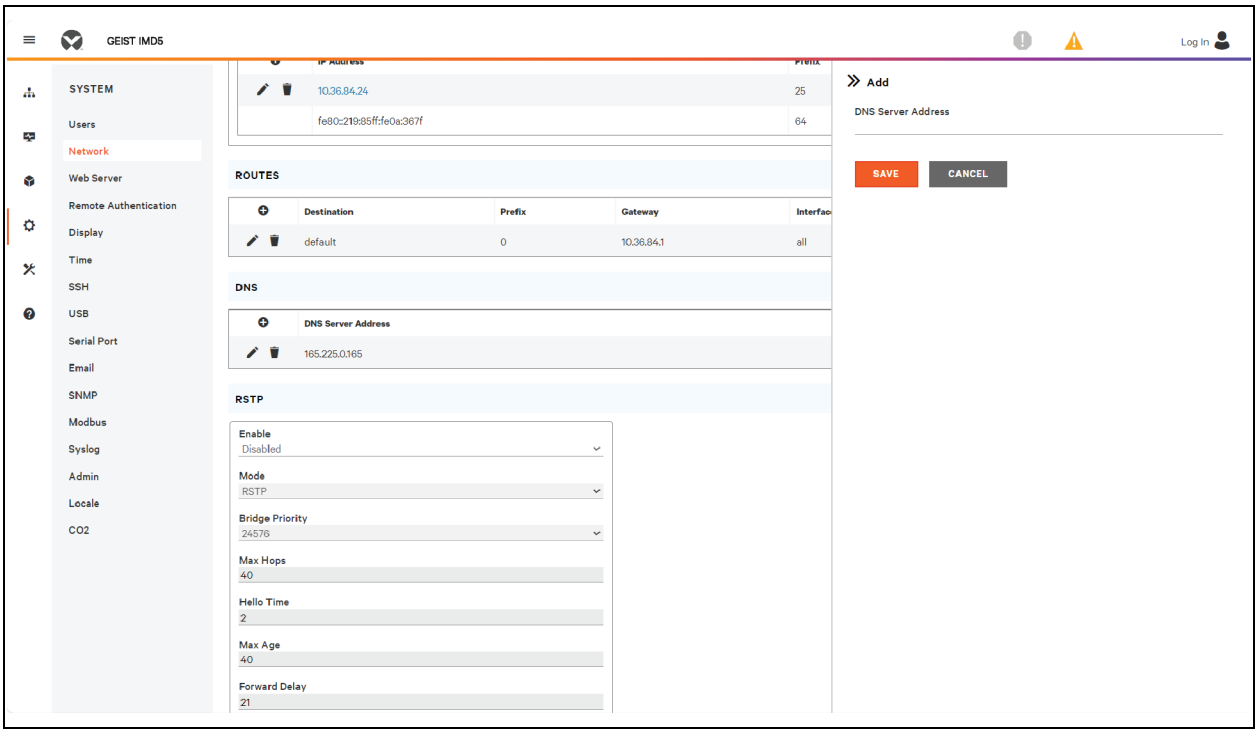
Figura 5.39 Modificar rota



Para adicionar um novo endereço de servidor DNS:

1. Clique no ícone Add.
2. Insira o IP do servidor DNS desejado. É possível adicionar até dois servidores DNS.
3. Clique em *SAVE*.

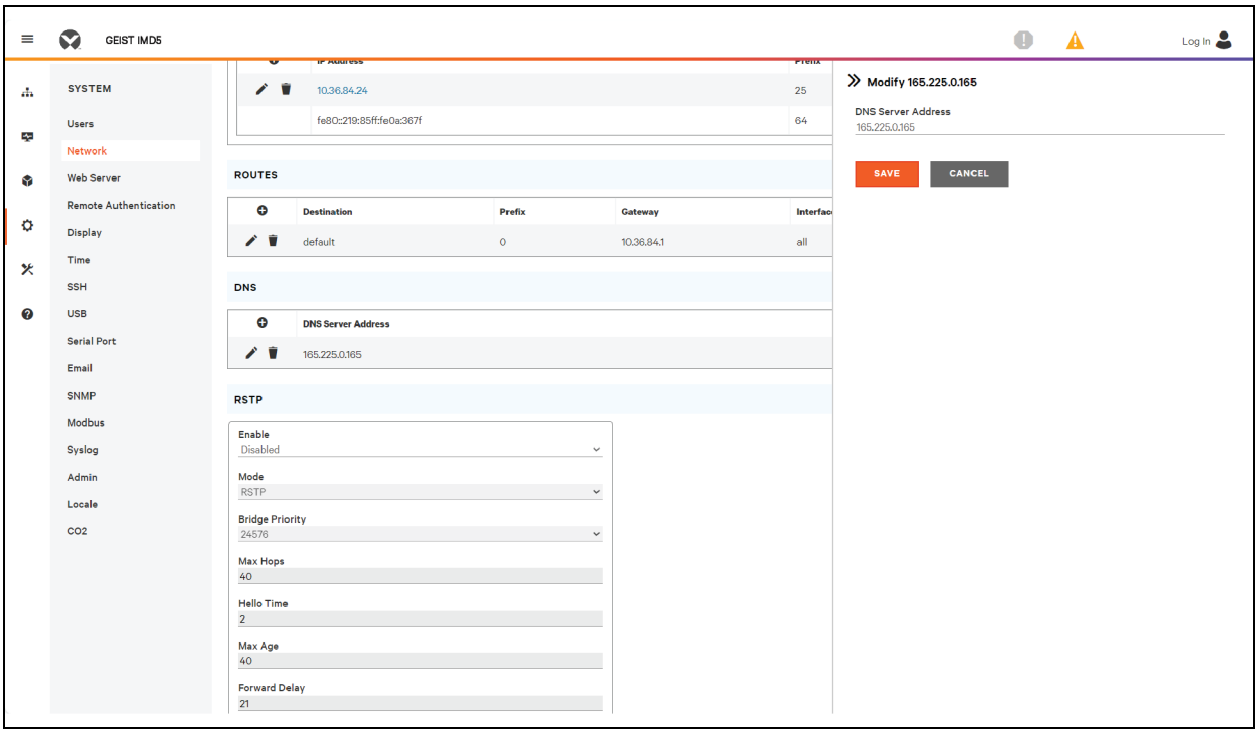
Figura 5.40 Adicionar um endereço de servidor DNS



Para modificar um endereço de servidor DNS existente:

1. Clique no ícone Modify.
2. Edite o campo DNS Server Address conforme necessário.
3. Clique em *SAVE*.

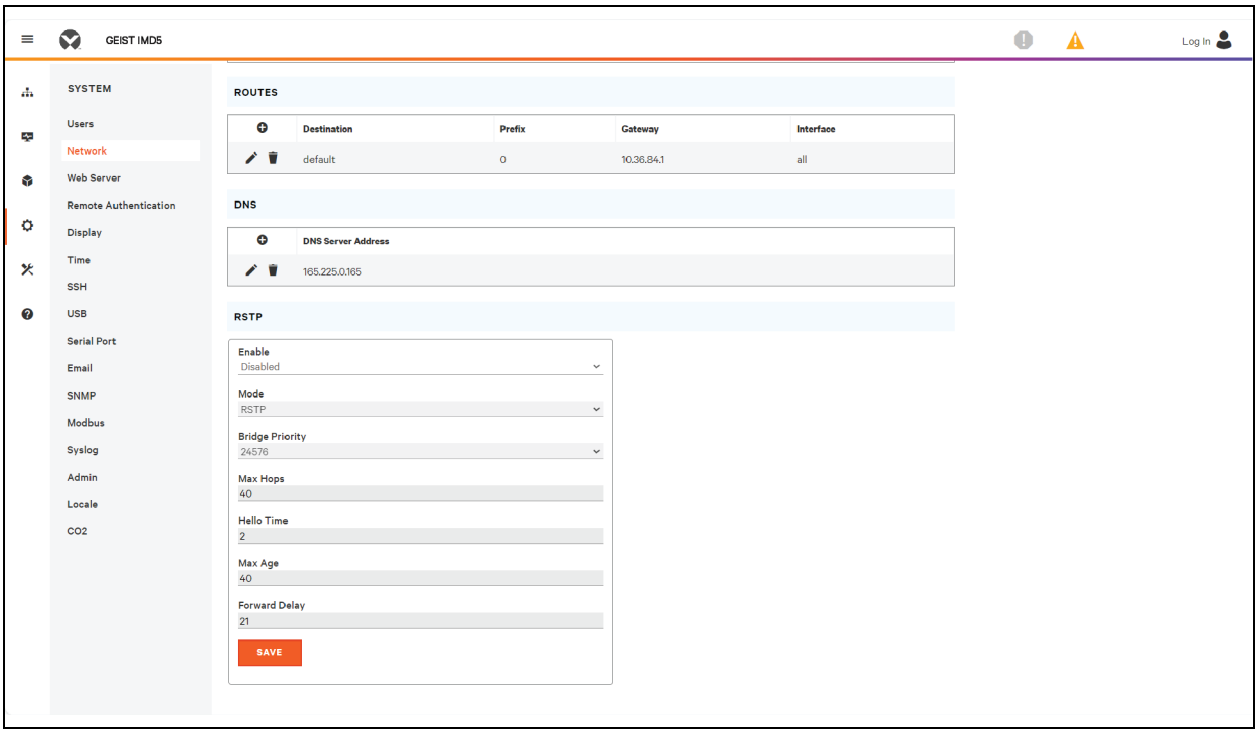
Figura 5.41 Modificar um endereço de servidor DNS



Para alterar as configurações de RSTP:

1. Altere as configurações, conforme desejado.
   a. **Enable:** ativar ou desativar o protocolo RSTP.
   b. **Mode:** o modo RSTP aceita fallback para STP, quando necessário.
   c. **Bridge Priority:** clique no menu suspenso, selecione o valor adequado e clique em *Save*.
   d. **Max Hops:** usada quando o modo está com RSTP ativado.
   e. **Hello Time:** o intervalo, em segundos, entre as transmissões periódicas das mensagens de configuração pelas portas designadas.
   f. **Max Age:** a duração máxima, em segundos, das informações transmitidas por esta interface, quando ela funciona como ponte raiz. Definida como 2 segundos.
   g. **Forward Delay:** o atraso, em segundos, usado pelas pontes para transição da ponte raiz e das portas designadas para o modo de encaminhamento. Definida como 21 segundos.
2. Clique em *SAVE*.

Figura 5.42 Alterar as configurações de RSTP



5.6.3 Servidor Web

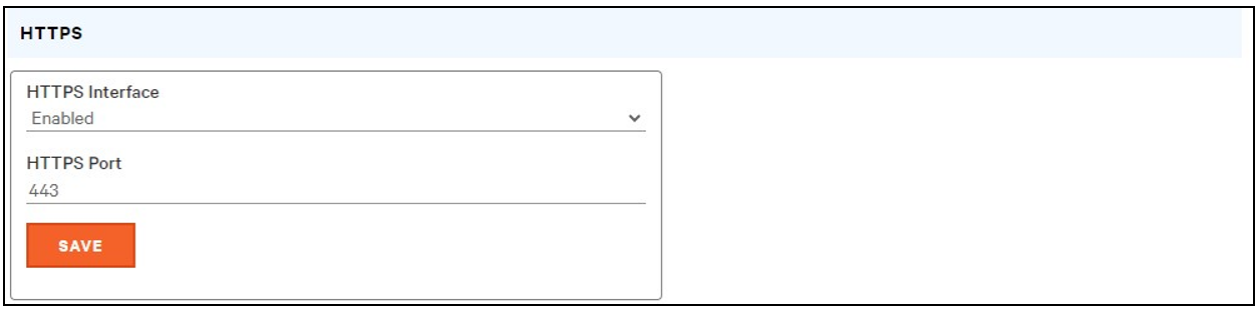
É possível atualizar a configuração do servidor Web da unidade na guia Web Server do menu System.

- HTTP Interface: ativada ou redirecionada para HTTPS, enquanto a interface do HTTPS pode ser ativada ou desativada. Quando a interface do HTTP for redirecionada para HTTPS e a interface do HTTPS for desativada, a interface do HTTP também será desativada.

NOTA: Não é possível desativar os protocolos HTTP, HTTPS e SSH ao mesmo tempo.

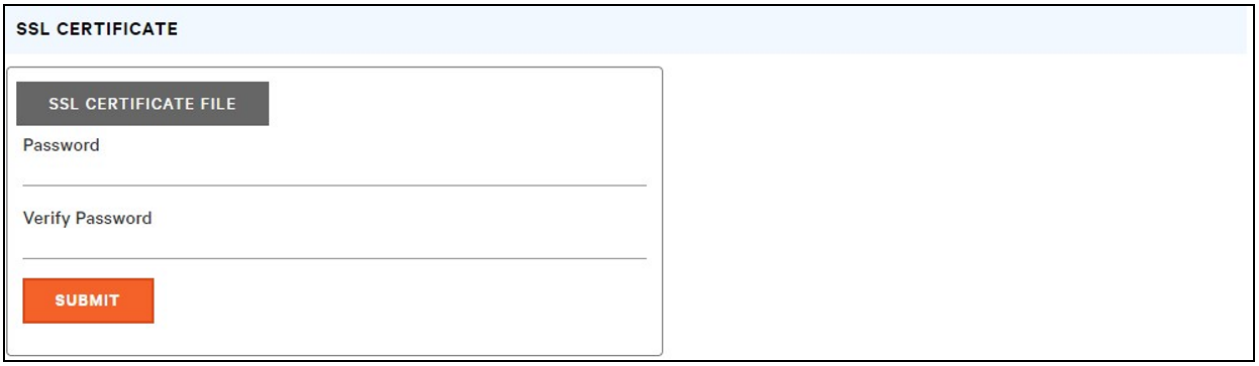
- Porta do servidor HTTP/HTTPS: permite alterar as portas TCP em que os serviços HTTP e HTTPS escutam as conexões de entrada. Os padrões são a porta 80 para HTTP e a porta 443 para HTTPS.

Figura 5.43 Página de configuração de HTTP



- SSL Certificate: permite carregar seu próprio arquivo de certificado SSL assinado para substituir o padrão. O certificado pode ser autoassinado ou assinado por uma autoridade de certificação. O certificado SSL deve estar no formato *PEM* ou *PFX* (PKCS12)

Figura 5.44 Certificado SSL



- Formato *PEM*:
  - O certificado público e a chave privada devem estar no mesmo arquivo.
  - O certificado deve seguir o padrão x.509.
  - A chave privada deve ser gerada com o algoritmo RSA ou ECDSA. Deve estar no formato *PEM*.
    - 2048-bit RSA ou inferior não são aceitos.
    - P-384 é o tamanho aceito da chave para ECDSA.
  - A chave privada *PEM RSA* deve ser protegida por senha.
- Formato *PFX*: o suporte também está disponível para o padrão PKCS12 (*.pfx*), que é uma combinação binária criptografada de um certificado público *PEM* e a respectiva chave privada *PEM*. Ao gerar um certificado *PFX*, você terá que inserir uma senha opcional.

5.6.4 Remote Authentication

A página Remote Authentication permite designar um dos três protocolos de autenticação para acesso remoto ao dispositivo. Por padrão, o dispositivo usa o banco de dados local para autenticar usuários. A autenticação remota permite que o dispositivo autentique um usuário com um servidor remoto. Em caso de falha na autenticação remota, ela será revertida para a autenticação local.

Para alterar as configurações de autenticação remota:

1. Selecione o modo necessário no menu suspenso.
   - Disabled: autenticação local.
   - LDAP: Lightweight Directory Access Protocol.
   - TACACS+: Terminal Access Controller Access Control System Plus.
   - RADIUS: Remote Authentication Dial-In User Service.
2. Clique em *SAVE*.

LDAP

É possível configurar o Lightweight Directory Access Protocol (LDAP) nesse menu.

NOTA: É necessário saber as configurações do seu servidor LDAP para configurar o dispositivo rPDU Geist™ Vertiv™ com esse protocolo de autenticação remota. Se você não está familiarizado com essas configurações, consulte o administrador do servidor LDAP.

Configuração para autenticação remota por meio de LDAP.

- LDAP Server Address: especifique o endereço de host do LDAP. O *HOST* pode ser um endereço IPv4, um endereço IPv6 entre colchetes (ex. *[2001:0DB8:AC10:FE01::]*) ou um nome de host.
- LDAP Server Port: usada para definir o número da porta LDAP. A porta padrão para LDAP é *389* - use-a para Security Type *None* ou *StartTLS*. Use *636* para o Security Type *SSL*.
- LDAP Mode: no menu suspenso, selecione *Active Directory* ou OpenLDAP. Consulte Exemplo de configuração de LDAP para credenciais do Active Directory na página 153.
- Security Type: no menu suspenso, selecione *None*, *SSL* ou *StartTLS*.
- Bind DN: nome exclusivo usado para vinculação com o servidor de diretório. Bind DN e Password vazios indicam uma vinculação anônima.
- Bind Password: senha usada para vinculação com o servidor de diretório.
- Base DN: DN que será usado como base da pesquisa.

Os campos restantes são provenientes do esquema NIS, definido no RFC2307. Eles são usados para autenticar usuários no LDAP. Se você deixá-los em branco, o valor padrão será preenchido.

- User Filter: filtro LDAP para seleção de usuários.
- "uid" Mapping: nome do atributo de servidor que corresponde ao atributo *uid* no esquema.
- "uidNumber"Mapping: nome do atributo de servidor que corresponde ao atributo *uidNumber* no esquema.
- Group Filter: filtro LDAP para seleção de grupos.
- "gid" Mapping: nome do atributo de servidor que corresponde ao atributo *gid* no esquema.
- "memberUid" Mapping: nome do atributo de servidor que corresponde ao atributo *memberUid* no esquema.

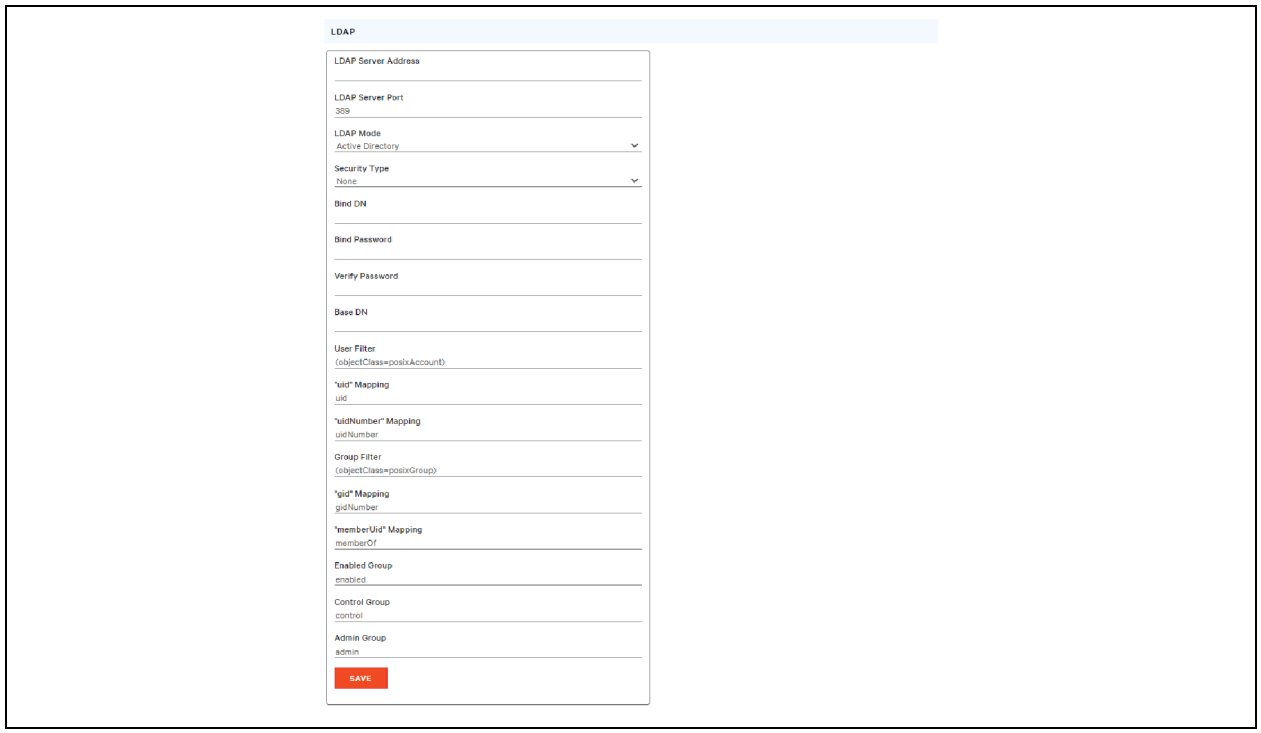
NOTA: Os usuários *devem* preencher o uidNumber. Um valor nulo ou ausente provocará falha em um login válido. O uidNumber do usuário *deve* ser no mínimo 1000. Um valor inferior a 1000 provocará falha em um login válido.

- Enabled Group: os usuários nesse grupo têm privilégios somente visualização, conforme descrito na seção Usuários deste manual.
- Control Group: os usuários nesse grupo têm privilégios de controle, conforme descrito na seção Usuários deste manual.
- Admin Group: os usuários nesse grupo têm privilégios administrativos, conforme descrito na seção Usuários deste manual. Os usuários de LDAP não são incluídos no número mínimo de usuários admin necessários.

Clique em *SAVE*.

Os campos Enabled Group, Control Group e Admin Group mostram como mapear os grupos às permissões de usuário. Um usuário deve pertencer a um desses grupos para acessar o dispositivo. Se um usuário pertencer a mais de um grupo, o grupo com a permissão mais alta será usado.

Figura 5.45 Menu LDAP



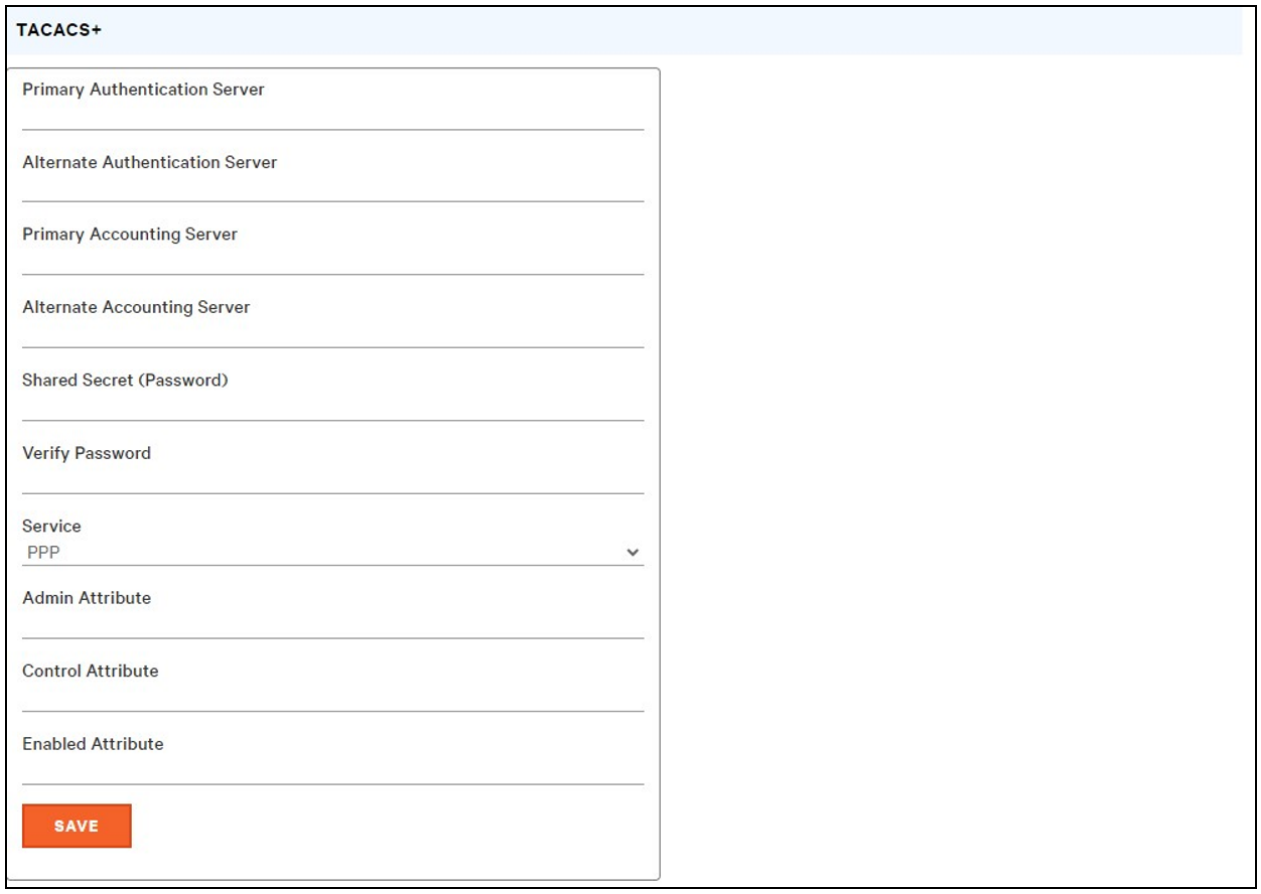
TACACS+

É possível configurar o protocolo Terminal Access Controller Access-Control Plus (TACACS+) nesse menu.

NOTA: É necessário saber as configurações do seu servidor TACACS+ para configurar o dispositivo rPDU Geist™ Vertiv™ com esse protocolo de autenticação remota. Se você não está familiarizado com essas configurações, consulte o administrador do servidor TACACS+.

Configuração para autenticação remota por meio de TACACS+.

Figura 5.46 Menu TACACS+



- Primary Authentication Server: o servidor de autenticação/autorização principal, que pode ser um endereço IPv4, um endereço IPv6 entre colchetes (ex. *[2001:0DB8:AC10:FE01::]*) ou um nome de host. O servidor de autenticação principal é usado para autenticação e autorização. O endereço/nome de host do servidor AA é obrigatório.
- Alternate Authentication Server: o servidor de autenticação/autorização alternativo, que pode ser um endereço IPv4, um endereço IPv6 entre colchetes ou um nome de host. O servidor de autenticação secundário é usado para autenticação e autorização.
- Primary Accounting Server: o servidor de contabilidade principal, que pode ser um endereço IPv4, um endereço IPv6 entre colchetes ou um nome de host. O servidor de contabilidade principal é opcional. Se configurado, o servidor será notificado quando um usuário for autorizado.
- Alternate Accounting Server: o servidor de contabilidade alternativo, que pode ser um endereço IPv4, um endereço IPv6 entre colchetes ou um nome de host. O servidor de contabilidade secundário é opcional. Se configurado, o servidor será notificado quando um usuário for autorizado.
- Shared Secret (Password): insira uma palavra ou frase secreta no campo Shared Secret (aplicável aos servidores de autenticação principais, secundários e de contabilidade).
- Service: o valor que será usado no campo de serviço nas solicitações TACACS+. As opções válidas são *PPP* e *raccess*.

- Admin Attribute: um usuário com esse atributo terá privilégios de *administrador*, conforme descrito na seção Usuários deste manual. Os usuários de TACACS+ não são incluídos no número mínimo de usuários admin necessários.
- Control Attribute: os usuários com esse atributo terão privilégios de controle, conforme descrito na seção Usuários deste manual.
- Enabled Attribute: os usuários com esse atributo terão privilégios somente visualização, conforme descrito na seção Usuários deste manual.

Clique em *SAVE*.

NOTA: Os pares atributo-valor (AVPs) retornados pelo servidor durante a autenticação/autorização determinam as permissões do usuário. O campo Group Attribute mostra para o sistema o AVP que contém o grupo de acesso do usuário. Se o valor do AVP corresponder ao campo Admin Group, o usuário terá acesso de Administrador (completo). Se o valor do AVP corresponder ao campo Control Group, o usuário terá acesso de Controle. Se o AVP corresponder ao campo Enabled Group, o usuário terá acesso somente visualização. Se nenhum resultado for encontrado, o usuário não terá acesso à unidade. Um campo Group em branco não encontrará nenhum AVP.

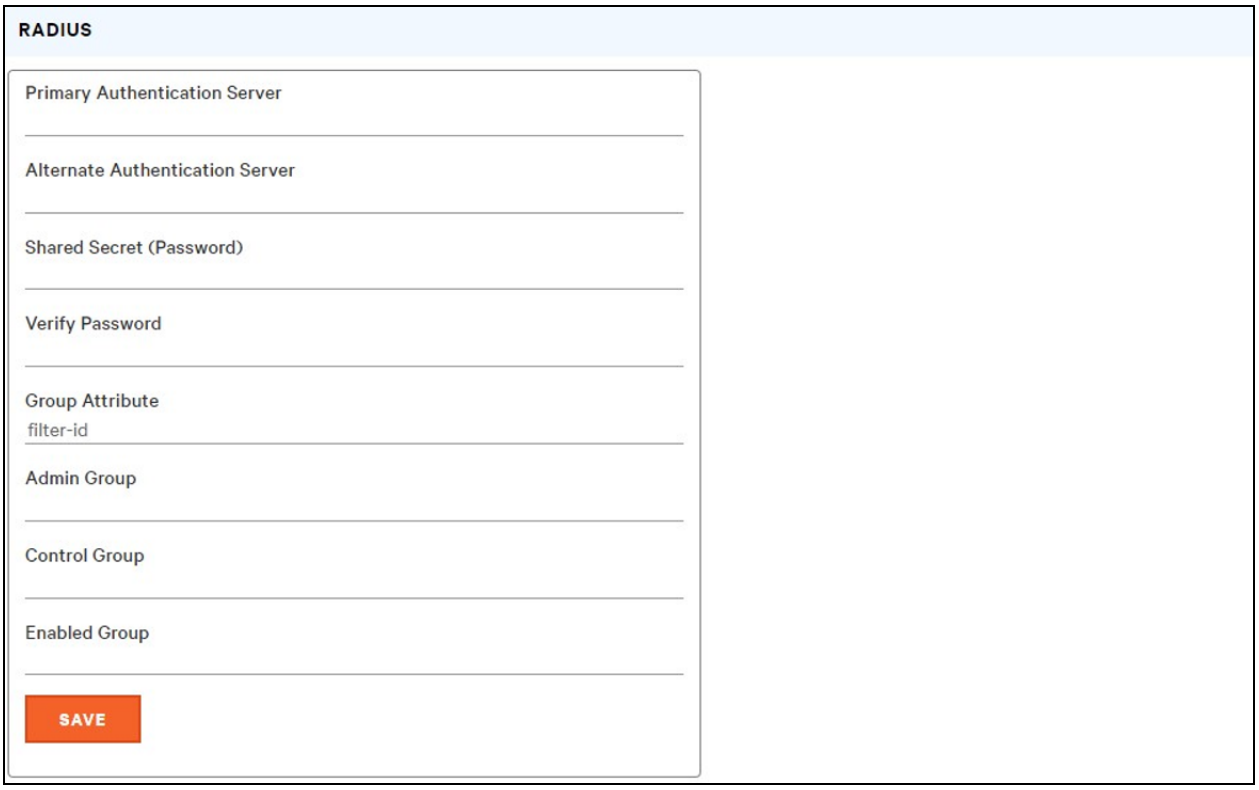
RADIUS

É possível configurar o protocolo Remote Authentication Dial-In User Service (RADIUS) nesse menu.

NOTA: É necessário saber as configurações do seu servidor RADIUS para configurar o dispositivo rPDU Geist™ Vertiv™ com esse protocolo de autenticação remota. Se você não está familiarizado com essas configurações, consulte o administrador do servidor RADIUS.

Configuração para autenticação remota por meio de RADIUS.

Figura 5.47 Menu RADIUS



- Primary Authentication Server: insira o endereço IP do servidor principal de autenticação/autorização/contabilidade. O servidor de autenticação principal pode ser um endereço IPv4, um endereço IPv6 entre colchetes (ex. *[2001:0DB8:AC10:FE01::]*) ou um nome de host. O servidor de autenticação principal é usado para autenticação, autorização e contabilidade. Este servidor AA é obrigatório.
- Alternate Authentication Server: se aplicável, insira o endereço IP do servidor de contabilidade/autorização/autenticação alternativo. O servidor de autenticação alternativo pode ser um endereço IPv4, um endereço IPv6 entre colchetes ou um nome de host. O servidor de autenticação secundário é usado para autenticação, autorização e contabilidade.
- Shared Secret (Password): insira uma palavra ou frase secreta no campo Shared Secret (aplicável aos servidores de autenticação principais, secundários e de contabilidade).
- Group Attribute: identifica o par atributo-valor (AVP) que indica o grupo de acesso a que o usuário pertence. Os valores válidos são *filter-id* e *management-privilege-level*.
- Admin Group: um usuário que pertence a esse grupo tem privilégios de administrador, conforme descrito na seção Usuários do manual.
- Control Group: um usuário que pertence a esse grupo tem privilégios de controle, conforme descrito na seção Usuários do manual.
- Enabled Group: um usuário que pertence a esse grupo tem privilégios somente visualização **ativados**, conforme descrito na seção Usuários do manual.

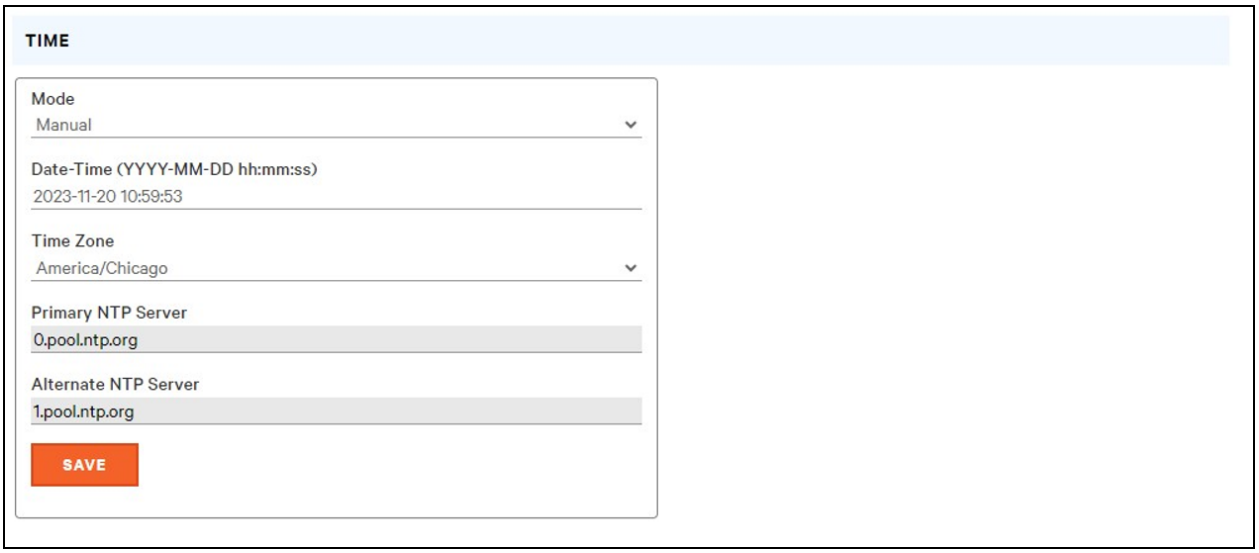
Clique em *SAVE*.

NOTA: Os pares atributo-valor (AVPs) retornados pelo servidor durante a autenticação/autorização determinam as permissões do usuário. O campo Group Attribute mostra para o sistema o AVP que contém o grupo de acesso do usuário. Se o valor do AVP corresponder ao campo Admin Group, o usuário terá acesso de Administrador (completo). Se o valor do AVP corresponder ao campo Control Group, o usuário terá acesso de Controle. Se o AVP corresponder ao campo Enabled Group, o usuário terá acesso somente visualização. Se nenhum resultado for encontrado, o usuário não terá acesso à unidade. Um campo Group em branco não encontrará nenhum AVP.

5.6.5 Time

A hora e a data da unidade são definidas nesta página.

Figura 5.48 Página de configuração de tempo



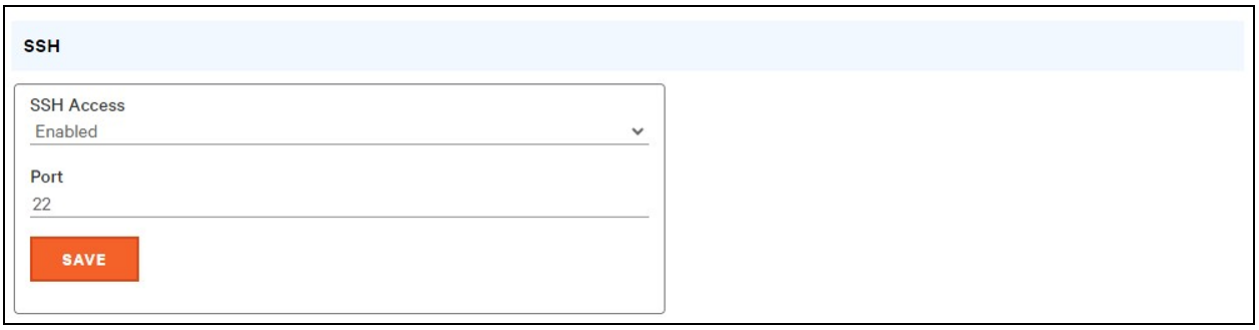
Há dois modos disponíveis:

- Network Time Protocol (NTP): sincroniza a data e hora da unidade de acordo com o fuso horário especificado usando os servidores NTP listados. É possível reconfigurar os servidores NTP.
- Manual: nesse modo, a data e hora devem ser digitadas conforme indicado à esquerda do campo.

5.6.6 SSH

No menu SSH, é possível definir as configurações de acesso SSH ao dispositivo.

Figura 5.49 Página de configuração de SSH



- SSH Access: ativa ou desativa o acesso por SSH.
- SSH Port: permite alterar a porta em que o serviço SSH escuta as conexões de entrada. O padrão é a porta 22.

NOTA: O usuário de SSH será automaticamente desconectado após 10 minutos de inatividade.

5.6.7 USB

Para ativar ou desativar a porta USB:

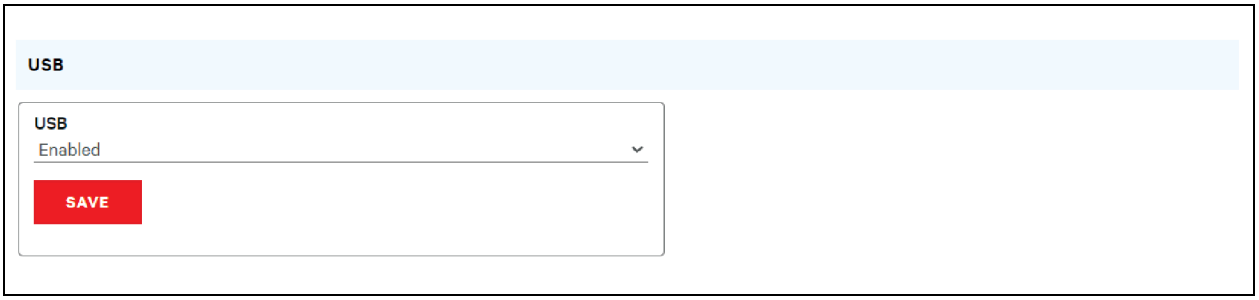
1. Selecione Enable ou Disable no menu suspenso.
2. Clique no botão *SAVE*.

Quando a porta USB está ativada, os dispositivos USB conectados aparecem na interface da Web.

NOTA: O dispositivo USB deve ser formatado como FAT32.

Se um dispositivo de armazenamento USB válido for detectado e os dados históricos estiverem sendo gravados, esses dados também serão armazenados em um arquivo na unidade de armazenamento USB. Se ainda não existir, será criado um arquivo chamado log-1.csv no diretório log na parte superior do sistema de arquivos. Se já houver arquivos de log, aquele com o identificador de número mais alto no título será usado como ponto de partida. A cada período de log, novos dados são anexados a esse arquivo no mesmo formato que a recuperação CSV. Se forem criados ou removidos pontos de dados referentes ao que consta na lista no cabeçalho CSV, um novo arquivo será criado com o próximo número sequencial no nome. Se o sistema de arquivos ficar cheio, esta gravação de logs será interrompida.

Figura 5.50 USB



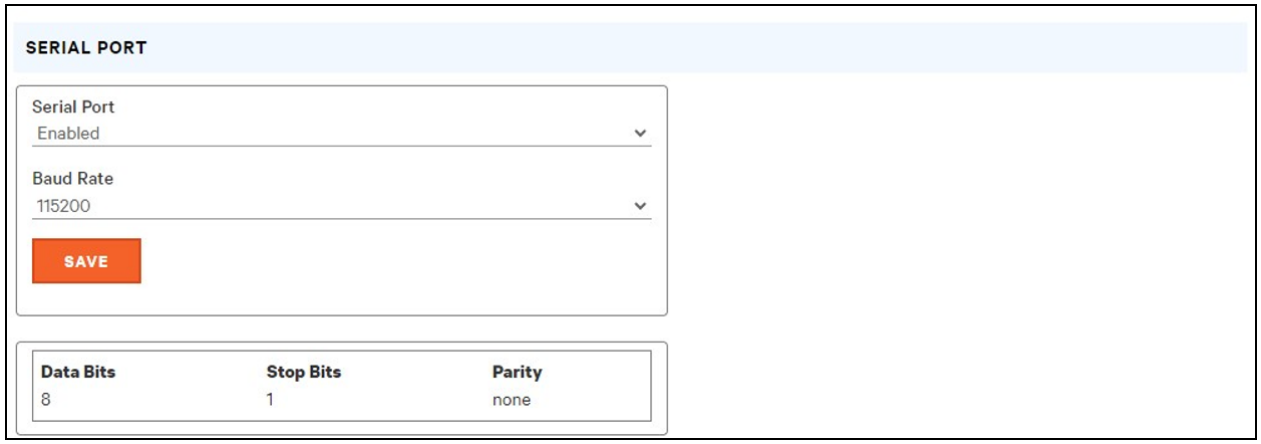
5.6.8 Serial Port

NOTA: A conexão serial não permite controle de fluxo.

O menu Serial Port permite definir as configurações da porta serial, ativando ou desativando a porta e configurando a taxa de transferência.

1. Clique no menu suspenso Serial Port, selecione *Enabled/Disabled*.
2. Clique no menu suspenso Baud Rate, selecione o valor *Baud Rate*.
3. Clique em *SAVE*.

Figura 5.51 Menu suspenso System – Serial Port



5.6.9 Email

A unidade pode enviar notificações por e-mail para até 10 endereços em caso de evento de alarme ou de advertência.

Figura 5.52 Página de configuração de e-mail

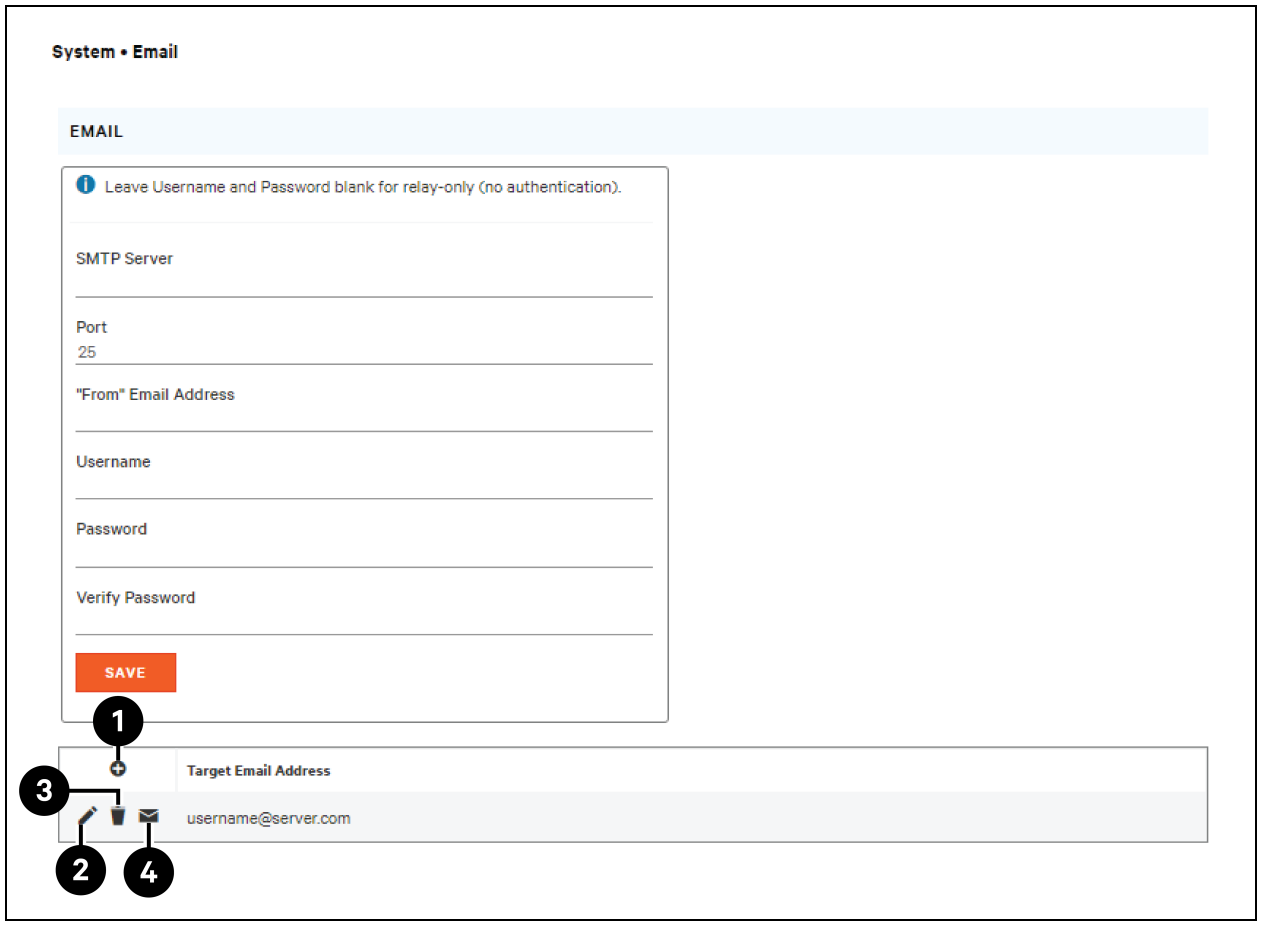


Tabela 5.12 Descrições da página de configuração de e-mail

Item	Descrição
1	Adicionar novo endereço de e-mail de destino.
2	Modificar um endereço de e-mail de destino existente.
3	Excluir um endereço de e-mail de destino existente.
4	Enviar e-mail de teste.

Para enviar e-mails, é necessário configurar a unidade para acessar o servidor de e-mail da seguinte maneira:

- SMTP Server: o nome ou endereço IP de um servidor SMTP ou ESMTP adequado.
- Port: a porta TCP que o servidor SMTP usa para fornecer os serviços de e-mail. Normalmente, os valores são a porta 25 para uma conexão não criptografada, ou 465 e 587 para uma conexão criptografada com TLS/SSL, mas isso pode variar de acordo com a configuração do servidor de e-mail.
- From Email Address: o endereço de onde os e-mail da unidade são enviados. Muitos serviços de e-mail hospedados, como o Gmail, exigem que seja a conta de e-mail de um usuário válido.
- Username e Password: as credenciais de login do servidor de e-mail. Se seu servidor não exige autenticação (retransmissão aberta), esses valores podem ficar em branco.

É necessário configurar os servidores Microsoft Exchange para permitir a retransmissão SMTP do endereço IP da unidade. É necessário também definir o servidor Exchange como Autenticação Básica para que a unidade possa fazer login com o método AUTH LOGIN de envio das credenciais de login. Outros métodos, como AUTH PLAIN e AUTH MD5, não são compatíveis.

Para adicionar ou modificar um endereço de e-mail de destino:

1. Clique no ícone Add ou Modify.
2. Insira o endereço de e-mail e clique em *Save*.

Para excluir um endereço de e-mail de destino:

1. Clique no ícone Delete ao lado do endereço que deseja excluir.
2. Clique em *Delete* na janela pop-up para confirmar.

Para enviar um e-mail de teste:

1. Clique no ícone Testar e-mail ao lado do endereço que deseja testar.
2. Uma janela pop-up indica que o e-mail de teste será enviado. Clique em *OK* para ignorá-la.

5.6.10 SNMP

É possível usar o Simple Network Management Protocol (SNMP) para monitorar as medições e o status da unidade. SNMP V1, V2c e V3 são compatíveis. É possível também enviar as interceptações de alarme para até dez endereços IP.

Clique em *ZIP* para fazer download do arquivo *mib.zip* que contém o arquivo MIB e a planilha formatada como CSV.

É possível ativar ou desativar os serviços SNMP-V1/V2c e SNMP-V3 de maneira independente. O serviço escuta as solicitações de leitura de dados na porta 161, que é o padrão para serviços SNMP. Isso também pode ser alterado.

É possível fazer download do Management Information Base (MIB) da unidade pelo link ZIP na parte superior da página da Web. Clique neste link para fazer download de um arquivo .Zip, que contém o arquivo MIB e uma planilha no formato CSV com a descrição dos OIDs disponíveis em formato legível que ajudam você na configuração do gerenciador SNMP para leitura dos dados da unidade.

Figura 5.53 Página de configuração de SNMP

Figura 5.54 Página de configuração de usuários de SNMP

A seção Users permite configurar as diversas comunidades Read, Write e Trap para os serviços SNMP. Você também pode configurar os tipos de autenticação e os métodos de criptografia usados para o SNMP V3, se desejado. Clique no ícone Modify para alterar as configurações.

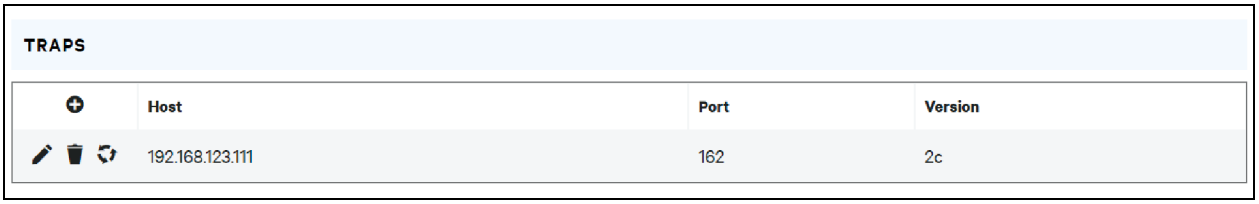
As interceptações permitem definir os tipos SNMP que você deseja que sejam enviados e os endereços IP dos destinatários.

Para configurar o destino de uma interceptação:

1. Encontre a seção *Traps* da página SNMP e clique no ícone Add.
2. Insira o endereço IP para o qual a interceptação deve ser enviada no campo Host.
3. Se necessário, altere o número da porta.
4. Selecione a versão de interceptação que será usada (V1, V2c ou V3) e clique em *SAVE*.

É possível enviar uma interceptação de teste clicando no ícone Testar ao lado do endereço IP do host. Você também pode atualizar/alterar as configurações de interceptação. Clique no ícone Modify ao lado do endereço IP do host.

Figura 5.55 Interceptação



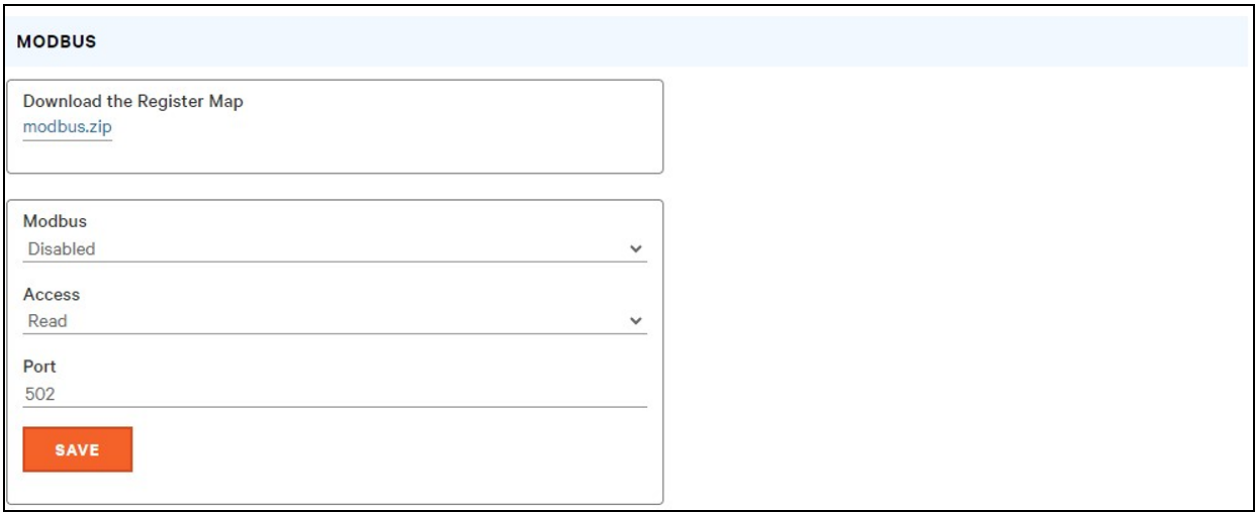
5.6.11 Modbus

É possível usar o protocolo de comunicação TCP Modbus para monitorar as medições e o status da unidade. Ele também permite que os usuários ajustem as configurações da unidade.

É possível fazer download do mapa de registro da unidade pelo link ZIP na parte superior da página da Web. Clique neste link para fazer download de um arquivo .zip, que contém uma planilha no formato CSV com a descrição do mapeamento Modbus em um formato legível que ajuda você na configuração do gerenciador Modbus para leitura/gravação dos dados na unidade.

É possível ativar ou desativar o protocolo de comunicação Modbus. O acesso do Modbus à unidade pode ser *Read* ou *Read/Write*. As solicitações de leitura ou de gravação de dados são feitas na porta 502, que é o padrão do protocolo Modbus. Essa porta também pode ser alterada.

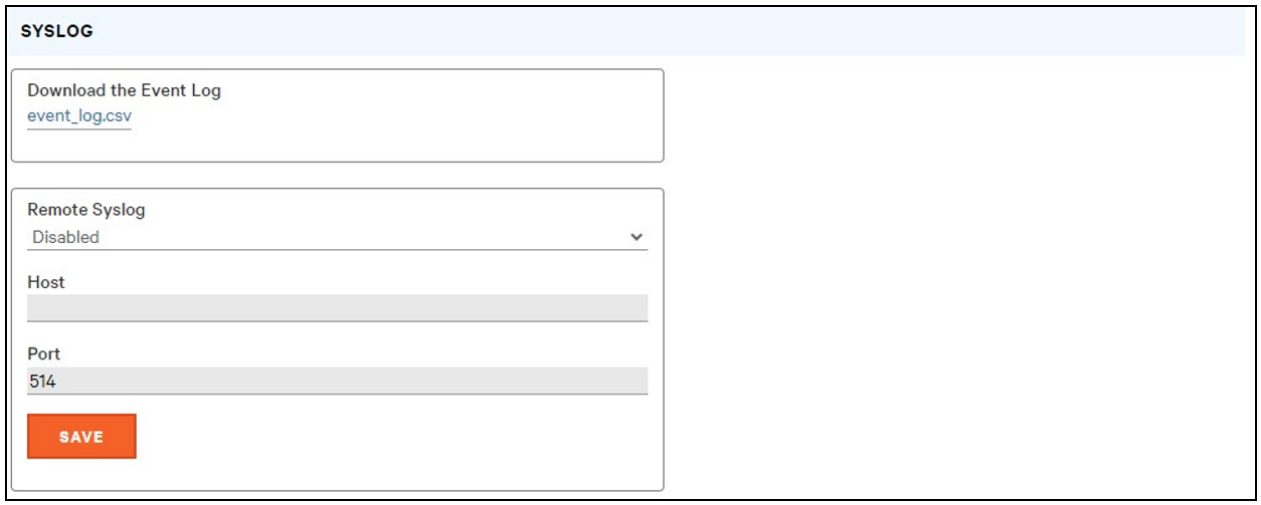
Figura 5.56 Modbus



5.6.12 SYSLOG

É possível capturar os dados de Syslog remotamente, mas primeiro é necessário configurá-los e ativá-los na página SYSLOG.

Figura 5.57 SYSLOG



NOTA: Esta função é útil, principalmente, para fins de diagnóstico e deve ser deixada desativada, exceto quando orientado a ativá-la pelo suporte técnico da Vertiv™ para solução de um problema específico.

O usuário deve ter acesso de administrador para usar o botão Download the Event Log CSV.

5.6.13 Admin

Na página Admin, o administrador do dispositivo pode salvar as informações de contato dele com a descrição e o local do dispositivo. Quando um administrador salva as informações, outros usuários (não administradores) podem visualizá-las. É possível também modificar o rótulo do sistema nesta página. Este rótulo costuma aparecer na barra de título da janela do navegador da Web e/ou na aba do navegador que está exibindo o dispositivo.

5.6.14 Locale

A página Locale define o idioma padrão e as unidades de temperatura do dispositivo. Essas configurações serão as opções de visualização padrão do dispositivo, embora cada usuário possa alterá-las em suas próprias contas. A conta de convidado somente poderá visualizar o dispositivo com as opções definidas aqui.

5.7 Submenu Utilities

O submenu Utilities no menu System permite restaurar padrões, reinicializar o sistema de comunicação e executar atualizações de firmware.

5.7.1 Configuration Backup and Restore

Salve as definições de configuração padrão e restaure as anteriores, conforme necessário.

Tabela 5.13 Opções de backup e restauração

Opção	Descrição
Download Configuration Backup File	Não é necessária a autenticação do usuário para fazer downloads. O nome do arquivo baixado é **backup_XXX.bin**, em que XXX representa a string do endereço MAC da interface **ETHERNET** da unidade sem os caracteres :.
Backup File	Carrega o arquivo de backup da configuração. Essa opção requer autenticação do usuário, e o usuário deve ter privilégios de administrador. É possível usar um arquivo de backup apenas para carregar a configuração em unidades com o mesmo número de modelo.

Para salvar as definições de configuração atuais:

1. Selecione *Download Configuration Backup File*.
2. Clique em *BIN*.

NOTA: Não é necessária a autenticação do usuário para salvar a configuração.

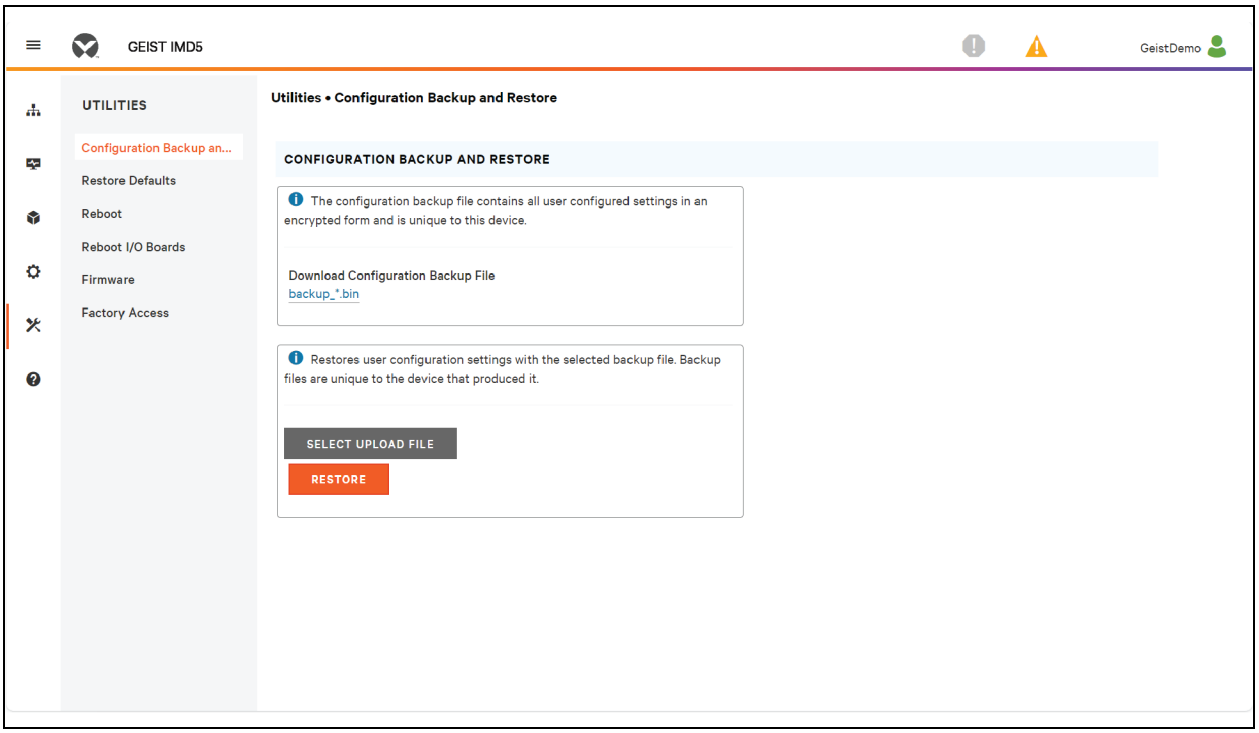
Para restaurar uma definição de configuração anterior:

1. Clique em *Backup File*.
2. Clique em *SELECT UPLOAD FILE*.
3. Selecione o arquivo de backup.
4. Clique em *RESTORE*.

NOTA: A restauração das configurações requer autenticação do usuário, e o usuário deve ter privilégios de administrador.

NOTA: É possível usar um arquivo de backup apenas para carregar a configuração em unidades com o mesmo número de modelo.

Figura 5.58 Visão geral de Configuration Backup and Restore



5.7.2 Restaurar padrões

Restaure as configurações padrão.

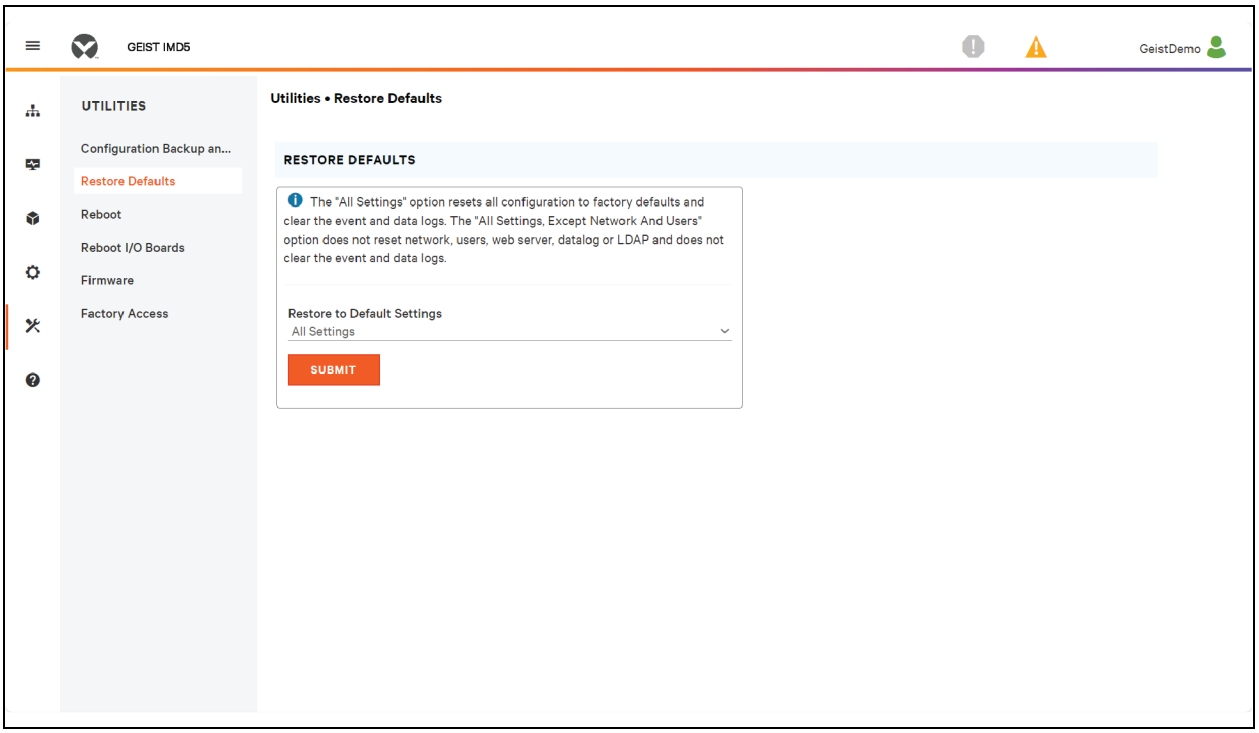
Tabela 5.14 Opções para restaurar padrões

Opção	Descrição
All Settings	Redefine todas as configurações em /conf, /alarm e /dev aos padrões de fábrica. Apaga também o log de eventos, o log de dados e executa o comando de exclusão em qualquer dispositivo com o estado **unavailable**. Isso faz com que partes do sistema sejam reinicializadas. Ela retornará uma resposta de êxito, seguida de um breve período em que o acesso ao sistema estará indisponível.
All Settings, Except Networks And Users	Igual à opção **padrão** acima, mas não redefine /conf/network, /conf/http, /conf/datalog, /auth ou /conf/ldap nem apaga o log de eventos ou de dados. Isso faz com que partes do sistema sejam reinicializadas. Ela retornará uma resposta de êxito, seguida de um breve período em que o acesso ao sistema estará indisponível.

Para restaurar as configurações padrão:

1. Selecione *All Settings* ou *All Settings, Except Networks And Users* no menu suspenso.
2. Clique em *SUBMIT*.

Figura 5.59 Visão geral de Restore Defaults



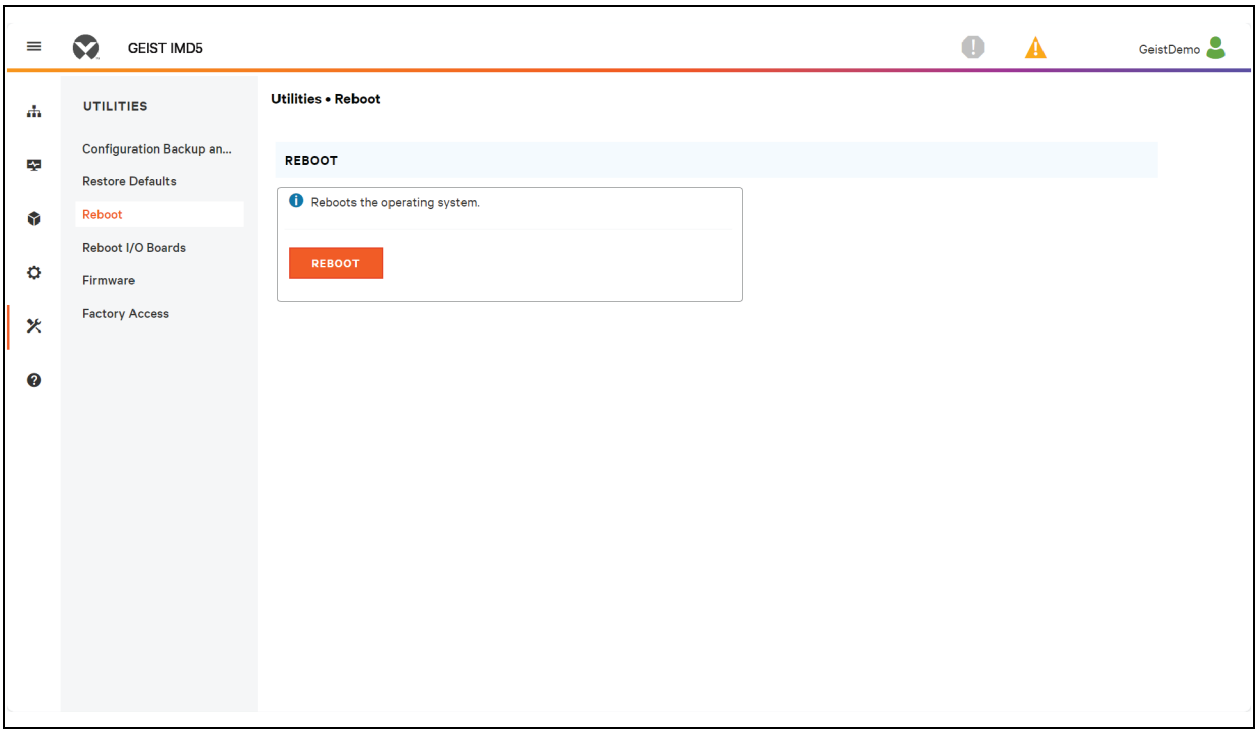
5.7.3 Reboot

Reinicializa o sistema operacional. Redefine o processador do IMD que está provocando a reinicialização do IMD.

Clique em *REBOOT* para reinicializar o sistema operacional:

NOTA: A potência nos dispositivos conectados não é afetada.

Figura 5.60 Visão geral de Reboot



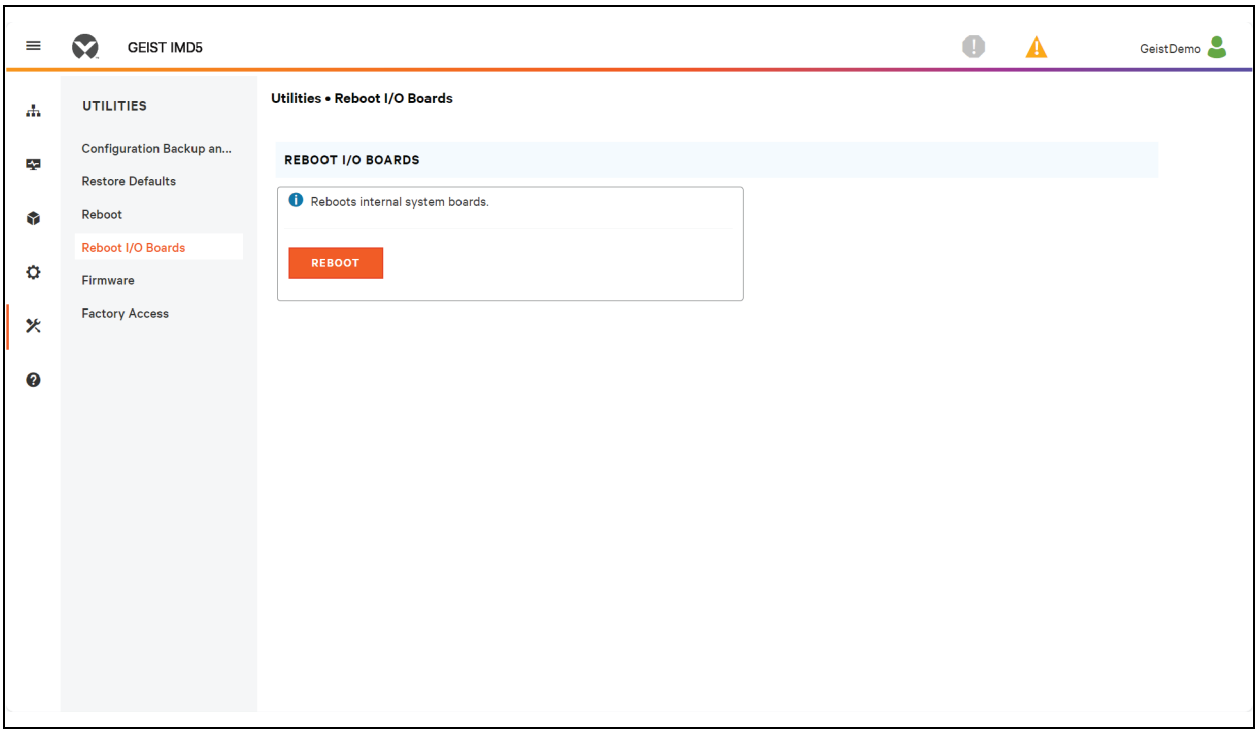
5.7.4 Reboot I/O Boards

Se a rPDU Geist™ Vertiv™ não responde ou não exibe todos os valores, reinicialize as placas internas para reinicializar o sistema. Isso redefinirá os processadores na placa de entrada interna e nas placas da tomada, fazendo com que elas sejam reiniciadas.

Clique em *REBOOT* para reinicializar as placas internas do sistema.

NOTA: A potência nos dispositivos conectados não é afetada.

Figura 5.61 Visão geral de Reboot I/O Boards Overview



5.7.5 Atualizações do firmware

Carrega um arquivo de firmware que atualiza o sistema. Esta ação requer autenticação do usuário, e o usuário deve ter privilégios de administrador. Normalmente, as atualizações de firmware estão incluídas em um arquivo .zip com vários arquivos que contêm o próprio pacote do firmware, uma cópia do MIB de SNMP, um arquivo de texto readme explicando como instalar o firmware e muitos outros arquivos de suporte, conforme necessário. Certifique-se de descompactar o arquivo e seguir as instruções incluídas.

Para atualizar o firmware por meio do arquivo de pacote do firmware:

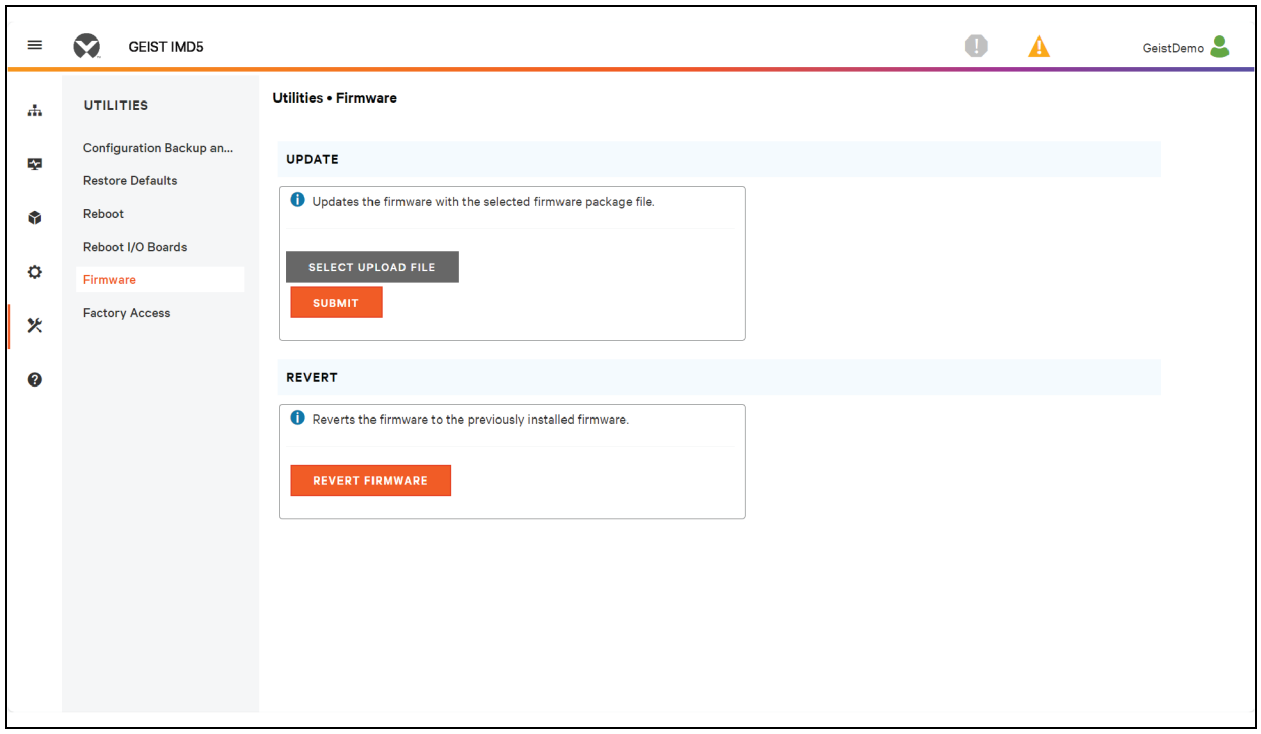
1. Clique em *SELECT UPLOAD FILE* e selecione o arquivo .*firmware* na janela *Open*.
2. Clique em *SUBMIT*.
3. Se algum problema for detectado (a unidade não está funcionando corretamente) após o firmware ter sido instalado, clique em *REVERT FIRMWARE*.

Para atualizar o Firmware por uma unidade flash USB:

1. Faça download do firmware mais recente em *https://www.vertiv.com/en-us/support/software-download/power-distribution/geist-upgradeable-series-v5-firmware/* e descompacte a pasta.
2. Consiga uma unidade flash USB e formate-a como FAT32.
3. Crie um diretório na unidade flash USB denominado *FIRMWARE* (as letras não precisam ser maiúsculas).
4. Abra a pasta do firmware descompactada e copie o arquivo .firmware.
5. Cole este arquivo na pasta *FIRMWARE* da unidade flash.
6. Conecte a unidade flash USB à PDU.

Durante a atualização, o IMD para a rolagem de dados. Após a conclusão da atualização, uma mensagem de inicialização aparecerá na tela. Após o término da reinicialização, o IMD retomará a rolagem de dados na tela.

Figura 5.62 Visão geral do firmware



5.7.6 Factory Access

O acesso de fábrica fornece as informações para suporte técnico.

Tabela 5.15 Opções do acesso de fábrica

Opção	Descrição
Download Factory Support Package	Faz download de um pacote de diagnóstico criptografado que pode ser enviado à equipe de suporte técnico.
Factory Access	Permitir acesso de fábrica à unidade por SSH (para fins de depuração).

Para fazer download de um support pack de fábrica:

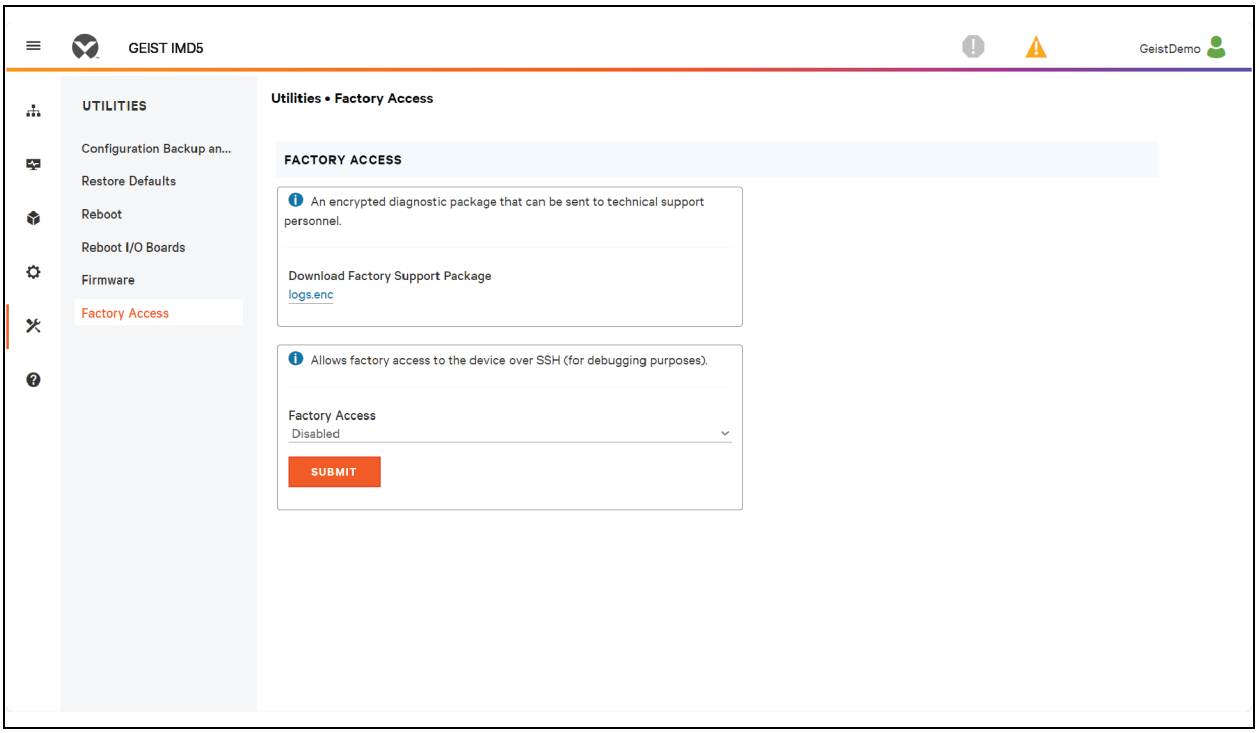
1. Clique em *Download Factory Support Package*.
2. Clique em *ENC*.

Para ativar/desativar o acesso de fábrica:

1. Selecione *Enable* ou *Disable* no menu suspenso.
2. Clique em *SUBMIT*.

NOTA: Essa opção requer autenticação do usuário, e o usuário deve ter privilégios de administrador.

Figura 5.63 Visão geral de Factory Access

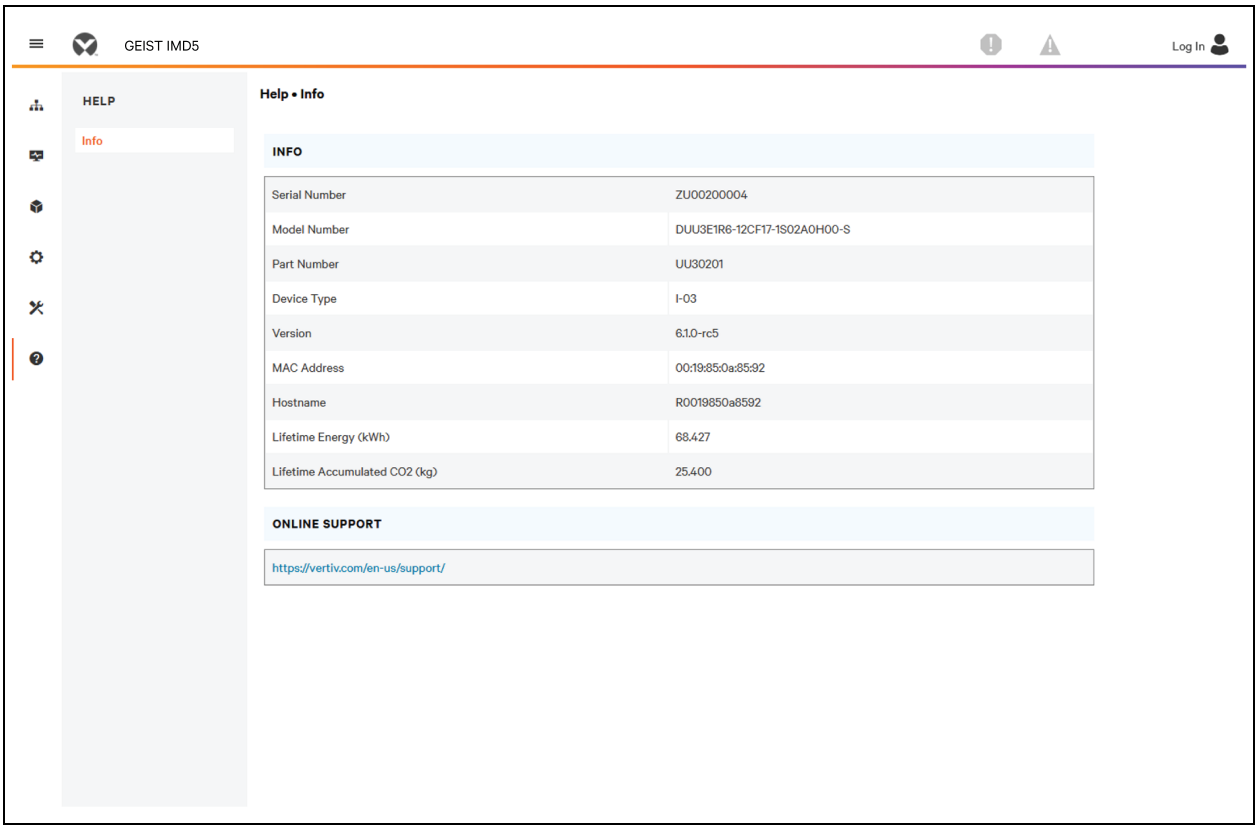


5.8 Submenu Help

Página Info

A página Info exibe as informações de configuração atuais da unidade, incluindo nome e ID do dispositivo, tipo de IMD instalado, versões de firmware atuais da unidade e dados sobre rede. As informações de suporte do fabricante também são exibidas aqui.

Figura 5.64 Página Info



Esta página foi deixada intencionalmente em branco

6 Vertiv™ Intelligence Director

O Vertiv Intelligence Director oferece uma camada de visualização unificada para implementações pequenas de rPDUs Geist™ Vertiv™, UPSs Vertiv™, sensores ambientais e tomadas da rPDU Geist™. Quando implantado, o Vertiv Intelligence Director oferece funcionalidades avançadas usando a rPDU Geist™ não como um dispositivo independente, mas como um gateway para reconhecer o ecossistema mais amplo do dispositivo no qual está instalada.

6.1 Agregação

O elemento inicial do Vertiv Intelligence Director, disponível com as rPDUs Geist™ com firmware 5.3.0, ou versão mais recente, é chamado Agregação. Esse único elemento permite que você:

- Use a agregação para reduzir a quantidade de endereços IP, agregar dados de várias PDUs de rack e ativar o gerenciamento de grupos de tomadas da PDU de rack.
- As PDUs de rack são conectadas por cadeia ETHERNET, conforme mostrado no exemplo de encadeamento acima.
- A frente da PDU de rack em cadeia é configurada como o gerenciamento matricial.
- A rede de portas matriz pode incluir switches de rede.
- É possível usar um único endereço IP atribuído ao gerenciamento matricial para acessar até 50 dispositivos (o gerenciamento matricial e 49 portas matriz).
- As configurações de rede das portas matriz são definidas automaticamente.
- As portas matriz são acessadas por meio do endereço IP e do número da porta do gerenciamento matricial. É possível saber o número da porta acessando *Device>List page* e passando o cursor do mouse sobre o dispositivo.
- Os usuários podem definir grupos de dispositivos, por exemplo, que representam racks.
- O gerenciamento matricial gera medições agregadas, como potência total do grupo e potência total, incluindo médias, mínimos e máximos.
- O encadeamento tolerante a falhas não é permitido com o uso do Vertiv Intelligence Director.

Figura 6.1 Aba Aggregation

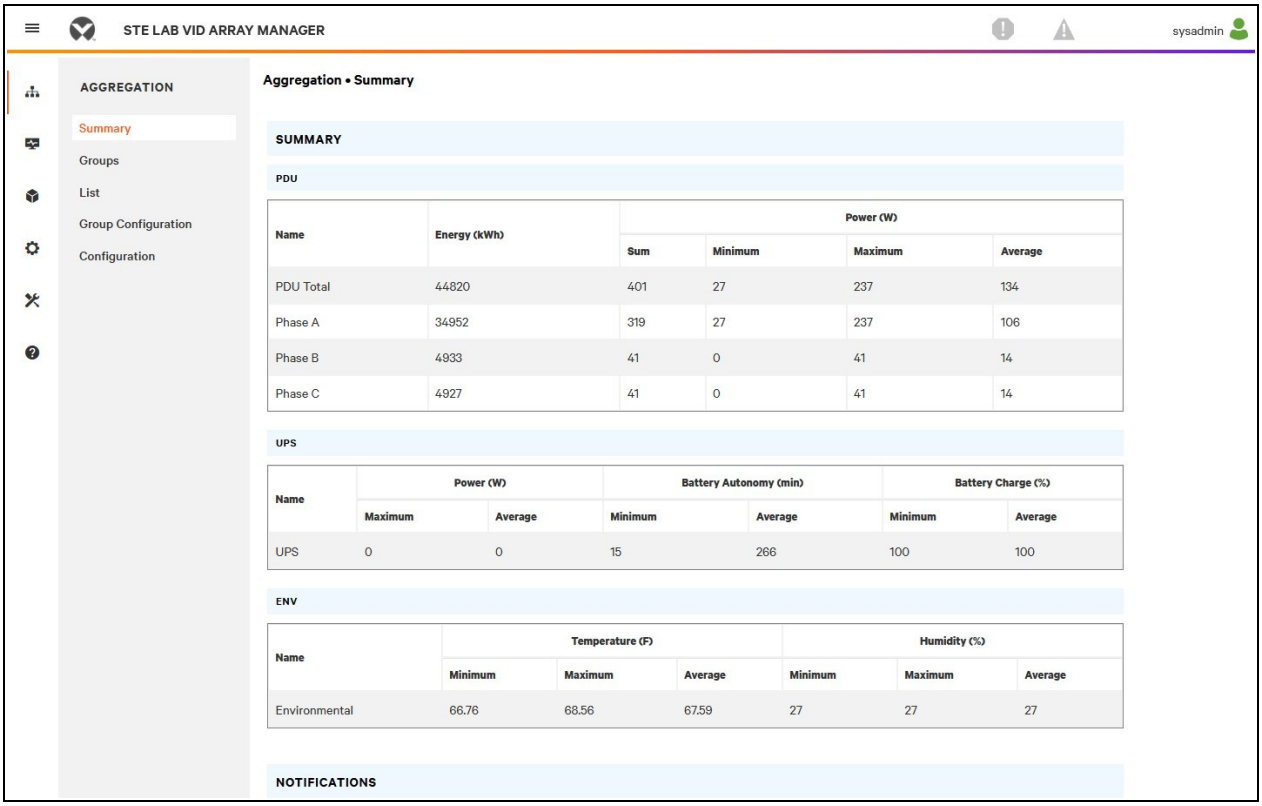
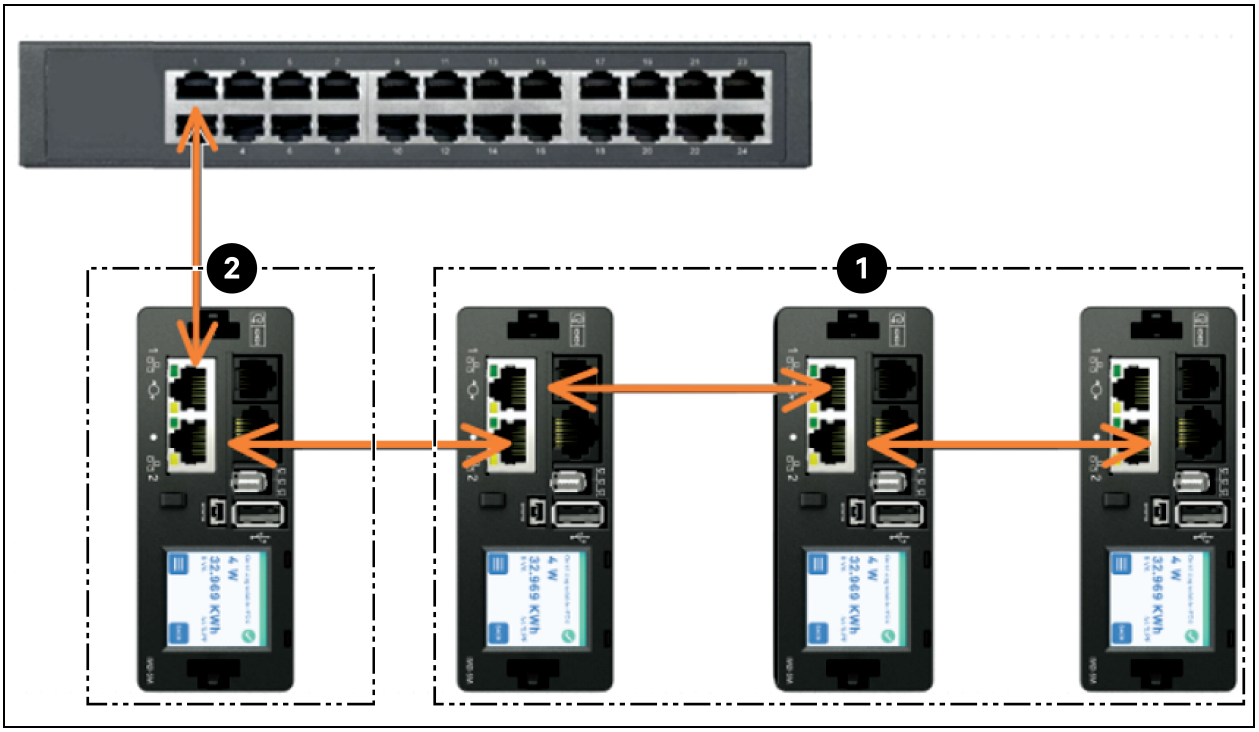


Figura 6.2 Agregação



Item	Descrição
1	Porta matriz
2	Gerenciamento matricial

Um elemento adicional do Vertiv Intelligence Director, disponível com as rPDUs Geist™ Vertiv™ com firmware 5.7.0 ou versão mais recente, é o agrupamento de tomadas da PDU de rack. Esse elemento permite que você:

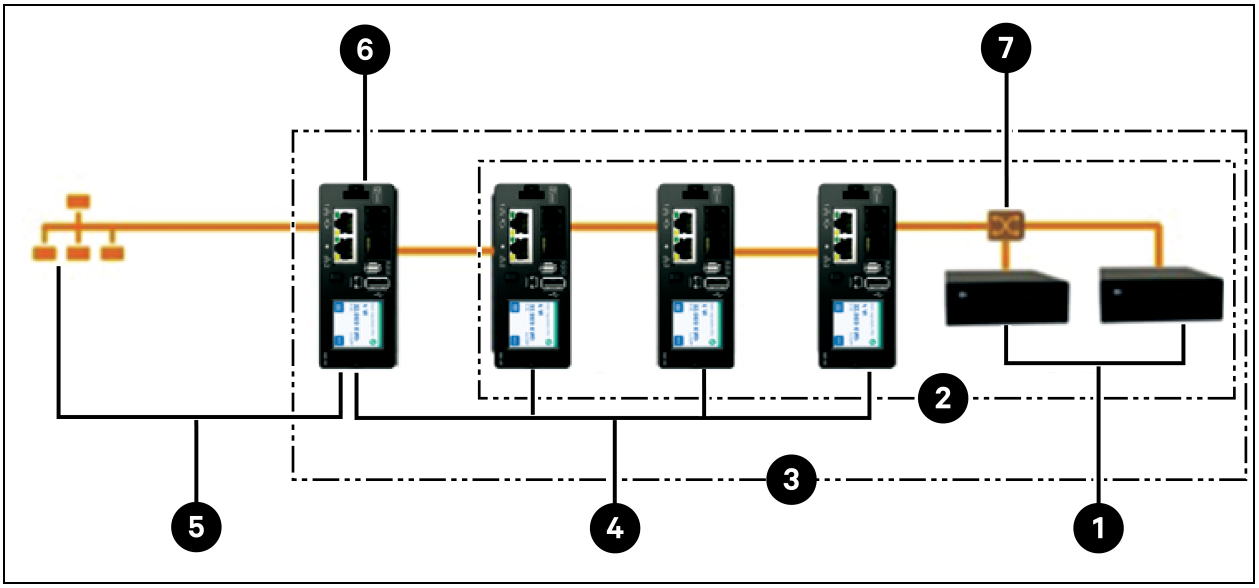
- Crie grupos de tomadas da rPDU Geist™ que incluam uma ou mais rPDUs Geist™.
- Gere um relatório da potência e energia totais do grupo de tomadas (com relatório das rPDUs Geist™ das medições por tomada).
- Desligue, ligue ou defina um ciclo de liga/desliga no grupo de tomadas com um único comando (com as rPDUs Geist™ que permitem chaveamento de tomada).

Com o firmware 5.10.1, ou versão mais recente, a visibilidade total dos dispositivos do Vertiv Intelligence Director (agregado) está disponível por CLIs de porta serial e SSH.

6.2 Gerenciamento matricial

A agregação exige a designação de um gerenciamento matricial implementado com PDUs de rack Geist™ equipadas com os modelos de IMD 5M que tenham a versão 6.1.0 do firmware ou mais recente ou modelos 3E, 03E, 3E (-S ou -G) ou 03E (-S ou -G), que tenham a versão 5.3.0 do firmware ou mais recente (embora a versão mais recente do firmware seja altamente recomendada). O IMD do gerenciamento matricial facilita e configura a rede de dispositivos, a matriz interconectada de rPDUs Geist™, UPSs Vertiv™, sensores de resfriamento e ambientais Vertiv™, e tomadas da rPDU Geist™, além de agregar determinados pontos de dados desses dispositivos. Ele também interage com a rede de gerenciamento para monitorar e gerenciar ele próprio e as portas matriz.

Figura 6.3 Exemplo de configuração



Item	Descrição
1	Vertiv™ Liebert® GXT4
2	Dispositivos posteriores
3	Rede do dispositivo
4	GU
5	Rede de gerenciamento
6	Dispositivo mestre (GU2)
7	Comutador ETHERNET

Não é mais possível integrar novas PDUs de rack IMD-02x ao usar um gerenciamento matricial com firmware 6.1.0 ou mais recente.

6.3 Configuração de rede

Na versão inicial da agregação, as portas matriz são definidas como rPDUS Geist™ Vertiv™ nas plataformas de produtos GU2 Geist™ Vertiv™, bem como rPDUs de rack MPH2™ Vertiv™ e MPX™ Vertiv™, UPS GXT4 Vertiv™ Liebert®, GXT5 Vertiv™ Liebert®, PSI5 Vertiv™ Liebert®, EXM Vertiv™ Liebert®, APM Vertiv™ Liebert® e ITA2 Vertiv™ Liebert®, resfriamento de linha CRV Liebert® Vertiv™ e resfriamento VRC Liebert® Vertiv™ conectado por USB. Cada gerenciamento matricial permite até 49 portas matriz, portanto, o número de gerenciadores depende do tamanho geral da instalação e da arquitetura de rede preferida.

O gerenciamento matricial deve ser comissionado antes de ser conectado à rede de gerenciamento principal ou à rede de portas matriz. Normalmente, esse comissionamento é feito em um laptop ou uma máquina local conectada diretamente à porta 1 no IMD.

Depois que a conectividade local for estabelecida, você poderá comissionar o gerenciamento matricial.

Para comissionar o gerenciamento matricial:

1. Navegue até *System>Locale*. Selecione o idioma padrão e as unidades de temperatura adequados nos menus suspensos. Essas configurações são enviadas às portas matriz na respectiva rede.
2. Navegue até *System>Network*. Em Protocol IPv6, escolha *Enabled* no menu suspenso.
3. Navegue até *Aggregation>Configuration* e altere as configurações conforme desejar.
    a. Aggregation: escolha *Enabled* no menu suspenso.
    b. Array device Username: define o nome de usuário configurado em todas as portas matriz.
    c. Array device Password: define a senha configurada em todas as portas matriz.
    - Insira a nova senha, confirme-a e clique em *Submit*. Ao configurar a agregação, verifique se a senha do dispositivo gerenciado atende a todas as regras de complexidade da senha das portas matriz. Exceto se alterado pelo usuário, o requisito é uma senha de no mínimo 8 caracteres em rPDUs com firmware 5.9.0 ou versão mais recente.
4. Clique em *Submit*.

Depois de ativar Aggregation no gerenciamento matricial, defina as demais configurações dele. Conecte o gerenciamento matricial à rede de gerenciamento (porta 1) no IMD e à rede do dispositivo (porta 2).

NOTA: O gerenciamento matricial tem uma rede DHCP integrada para atribuir endereços às portas matriz. Essa rede DHCP usa os endereços *192.168.123/192.168.124*, que não podem ser usados para a rede de gerenciamento.

Equipamentos conectados

Na versão inicial da agregação, as portas matriz são definidas como rPDUS Geist™ Vertiv™ nas plataformas de produtos GU2 Geist™ Vertiv™, bem como rPDUs de rack MPH2™ Vertiv™ e MPX™Vertiv™, UPS GXT4 Vertiv™ Liebert®, GXT5 Vertiv™ Liebert®, PSI5 Vertiv™ Liebert®, EXM Vertiv™ Liebert®, APM Vertiv™ Liebert® e ITA2 Vertiv™ Liebert®, resfriamento de linha CRV Liebert® Vertiv™ e resfriamento VRC Liebert® Vertiv™ conectado por USB. Todas as rPDUs Geist™ GU1 devem ter o firmware versão 3.4 ou mais recente. As rPDUs Geist™ GU2 devem ter o firmware versão 5.3.0, ou mais recente. As portas matriz GU1 não podem ser integradas aos controladores matriz com firmware 6.1.0 ou mais recente. Em todos os casos, é altamente recomendado atualizar todas as rPDUs para a versão mais recente do firmware disponível. Se as rPDUs Geist™ são recém-compradas e nunca foram configuradas, elas estão com a agregação pronta para uso. Se as rPDUs Geist™ foram implantadas em um ambiente de computação e comissionadas com as configurações de LAN do local e as contas de usuário, cada rPDU Geist™ deve ser redefinida aos padrões de fábrica por meio de *Utilities>Restore Defaults*. Selecione *All Settings* e clique em *Submit*. O gerenciamento matricial envia os dados de configuração às portas matriz.

Para configurar uma nova instalação com um gerenciamento matricial:

1. Instale os equipamentos conectados nos racks e ligue os racks.
2. Faça o cascateamento dos equipamentos conectados quando apropriado usando as portas rotuladas 1 e 2 no IMD.
    - No caso de conexões da rPDU em cadeia, verifique se o encadeamento não tem mais de 20 rPDUs.
    - É possível conectar os equipamentos em rede usando cascateamento, conexão em estrela ou uma combinação dos dois.
3. Instale o gerenciamento matricial em um rack. Em um laptop ou uma máquina local, conecte-se à porta 1 para configurar a Aggregation.
4. Conecte o gerenciamento matricial à rede de gerenciamento por meio da porta 1.
5. Conecte o gerenciamento matricial à rede das portas matriz por meio da porta 2.

Para configurar uma instalação existente com um gerenciamento matricial:

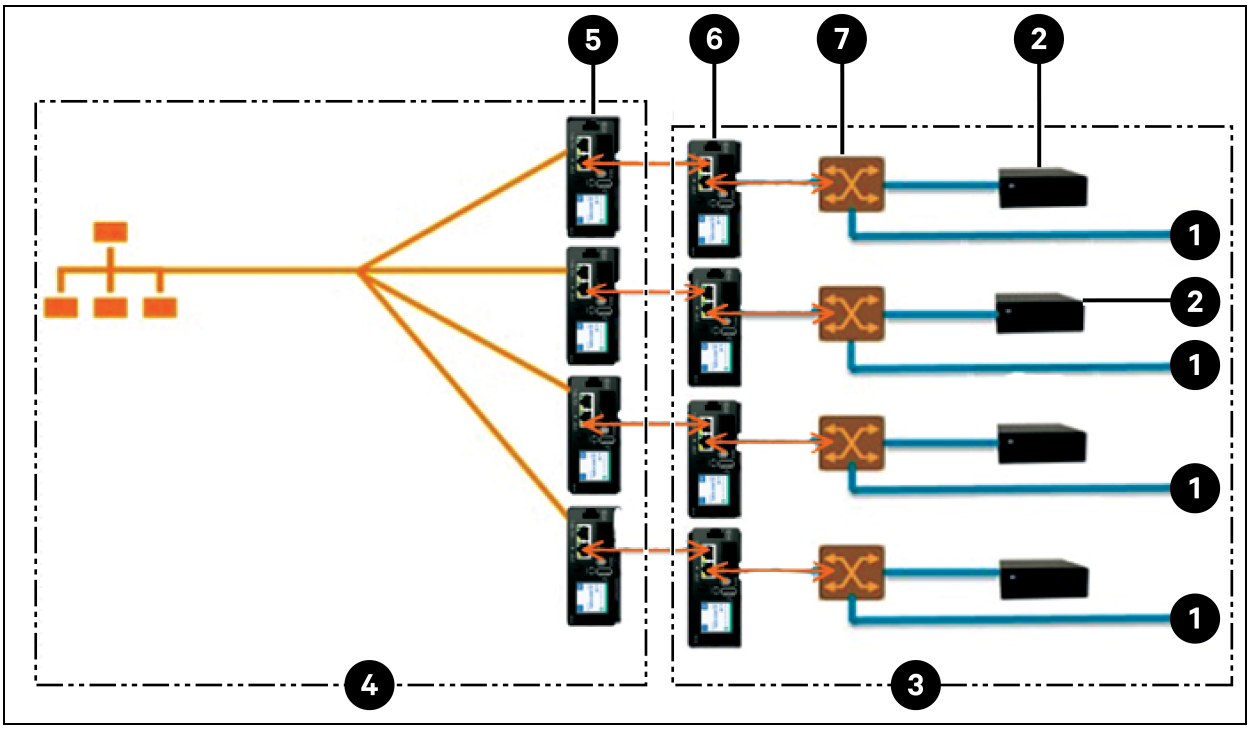
NOTA: Siga as instruções abaixo se houver rPDUs Geist™ conectadas em cadeia.

1. Determine um gerenciamento matricial e desconecte-o da rede de gerenciamento.
2. Redefina todas as portas matriz conectadas às configurações padrão de fábrica. As conexões físicas ETHERNET em cadeia podem continuar as mesmas; no entanto, se estavam conectadas em uma configuração de loop, a rPDU Geist™ final na cadeia deve ser desconectada do comutador de rede.
3. Ative a agregação no gerenciamento matricial.
4. Conecte o gerenciamento matricial à rede de gerenciamento por meio da porta 1.
5. Conecte o gerenciamento matricial à rede matricial por meio da porta 2.

Vários gerenciadores

Para instalações com vários gerenciadores, lembre-se de que a rede de cada dispositivo deve operar como uma rede independente e isolada. Considere uma rPDU 200 representada na Figura 6.4 abaixo. Para esta instalação, é necessário um mínimo de quatro gerenciadores, cada um operando sua própria rede de dispositivo independente. Cada gerenciamento matricial está visível na rede de gerenciamento e funciona como um servidor DHCP para suas portas matriz. Um usuário na rede de gerenciamento pode navegar por cada gerenciamento matricial para acessar a interface de uma porta matriz. Outras considerações podem afetar a quantidade de gerenciamentos matriciais. Se você tem uma arquitetura de rede de linha, talvez prefira um gerenciamento matricial no início de cada linha, em vez de um gerenciamento matricial que passe por várias linhas. Dependendo de como esses 200 gabinetes estiverem divididos em linhas, você poderá ter mais de quatro gerenciamentos matriciais. Depois de definir a configuração, siga o processo adequado de agregação.

Figura 6.4 Exemplo de configuração de rede



Item	Descrição
1	Outros dispositivos
2	UPS
3	Rede do dispositivo
4	Rede de gerenciamento
5	Dispositivo mestre (GU2)
6	rPDU posterior
7	Comutador ETHERNET

NOTA: Um comutador ETHERNET na rede do dispositivo será necessário apenas na conexão de mais de um dispositivo de porta de rede com a extremidade de uma cadeia da rPDU ou quando não forem usadas conexões com encadeamento.

6.4 Telas

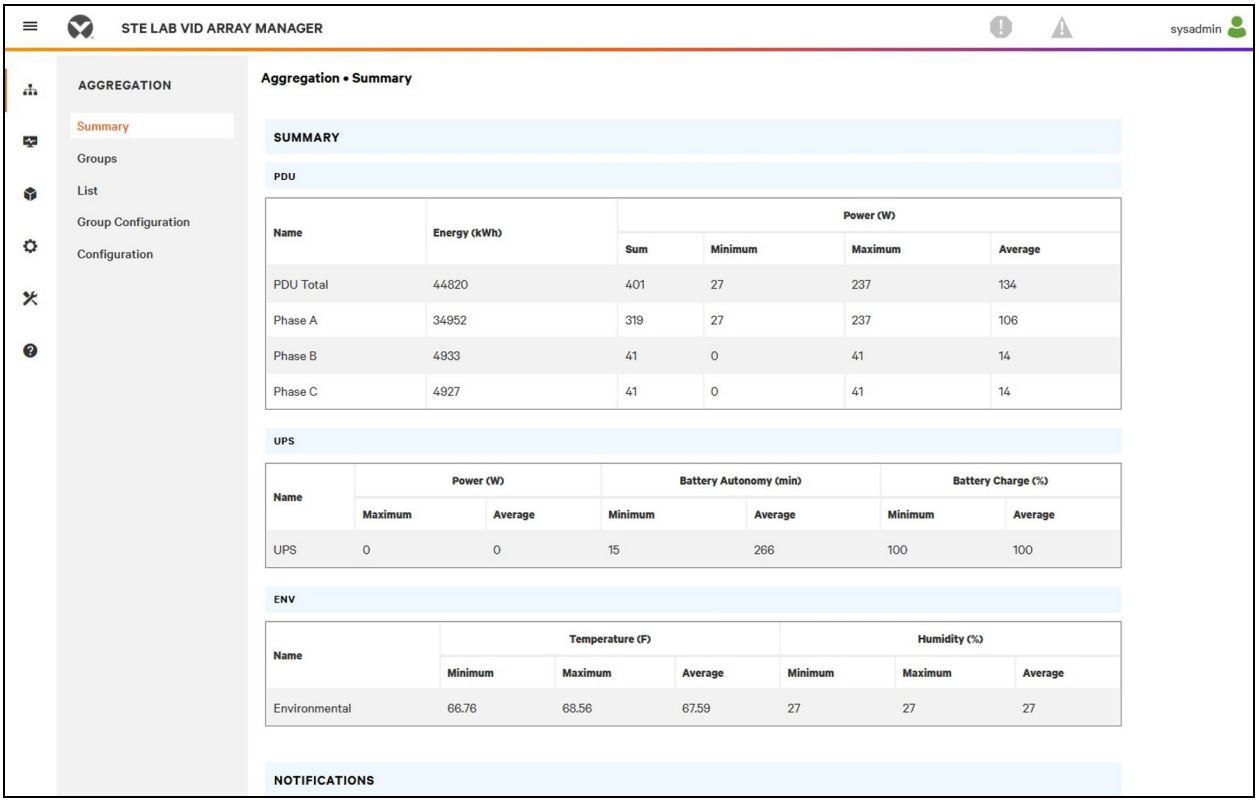
Quando a comunicação é estabelecida entre o gerenciamento matricial e as portas matriz, diversas telas são automaticamente preenchidas na interface de usuário. As novas telas na guia Device na barra de navegação superior são:

- Summary
- Groups
- List
- Group Configuration
- Configuration

6.4.1 Summary

A tela Summary agrega os dados de todas as portas matriz conectadas, apresentando uma descrição concisa dos detalhes relevantes de energia, ambiente e alarme.

Figura 6.5 Aba Summary



PDUs de rack

A rede da rPDU Geist™ Vertiv™ é resumida nos seguintes pontos de dados:

- **Energy (kWh):** a energia total da rPDU Geist™ na rede do dispositivo.
- **Power (W) Sum:** a carga de energia total da rPDU Geist™ na rede do dispositivo.
- **Power (W) Minimum:** a carga de energia mais baixa da rPDU Geist™ de grupo na rede do dispositivo.
- **Power (W) Maximum:** a carga de energia mais alta da rPDU Geist™ de grupo na rede do dispositivo.
- **Power (W) Average:** a carga de energia média da rPDU Geist™ de grupo na rede do dispositivo.

NOTA: Essas leituras são repetidas por fase (mostradas quando há rPDUs Geist™ trifásicas).

UPS

A rede do UPS é resumida nos seguintes pontos de dados:

- **Power (W) Maximum:** a carga de energia mais alta do UPS de grupo na rede de dispositivos.
- **Power (W) Average:** a carga de energia média do UPS de grupo na rede de dispositivos.
- **Battery Autonomy (min) Minimum:** a autonomia mais baixa da bateria do UPS na rede de dispositivos.
- **Battery Autonomy (min) Average:** a autonomia média da bateria do UPS na rede de dispositivos.
- **Battery Charge (%) Minimum:** a carga de bateria mais baixa do UPS na rede de dispositivos.
- **Battery Charge (%) Average:** a carga de bateria média do UPS na rede de dispositivos.

Sensores ambientais (ENV)

A categoria Environmental é resumida nos seguintes pontos de dados:

NOTA: Os valores de umidade estarão em branco quando os sensores somente de temperatura forem usados.

- **Temperature (F) Minimum:** a temperatura mais baixa na rede de dispositivos.
- **Temperature (F) Maximum:** a temperatura mais alta na rede de dispositivos.
- **Temperature (F) Average:** a temperatura média na rede de dispositivos.
- **Humidity (%) Minimum:** a umidade mais baixa na rede de dispositivos.
- **Humidity (%) Maximum:** a umidade mais alta na rede de dispositivos.
- **Humidity (%) Average:** a umidade média na rede de dispositivos.

Resfriamento térmico

- **Fan Speed (%) Minimum:** a velocidade mais baixa da ventoinha térmica do dispositivo na rede de dispositivos.
- **Fan Speed (%) Maximum:** a velocidade mais alta da ventoinha térmica do dispositivo na rede de dispositivos.
- **Fan Speed (%) Average:** a velocidade média da ventoinha térmica do dispositivo na rede de dispositivos.
- **Temperature (F) Minimum:** a temperatura térmica mais baixa do dispositivo na rede de dispositivos.
- **Temperature (F) Maximum:** a temperatura térmica mais alta do dispositivo na rede de dispositivos.

- **Temperature (F) Average:** a temperatura térmica média do dispositivo na rede de dispositivos.
- **Capacity (%) Minimum:** a capacidade térmica mais baixa do dispositivo na rede de dispositivos.
- **Capacity (%) Maximum:** a capacidade térmica mais alta do dispositivo na rede de dispositivos.
- **Capacity (%) Average:** a capacidade térmica média do dispositivo na rede de dispositivos.

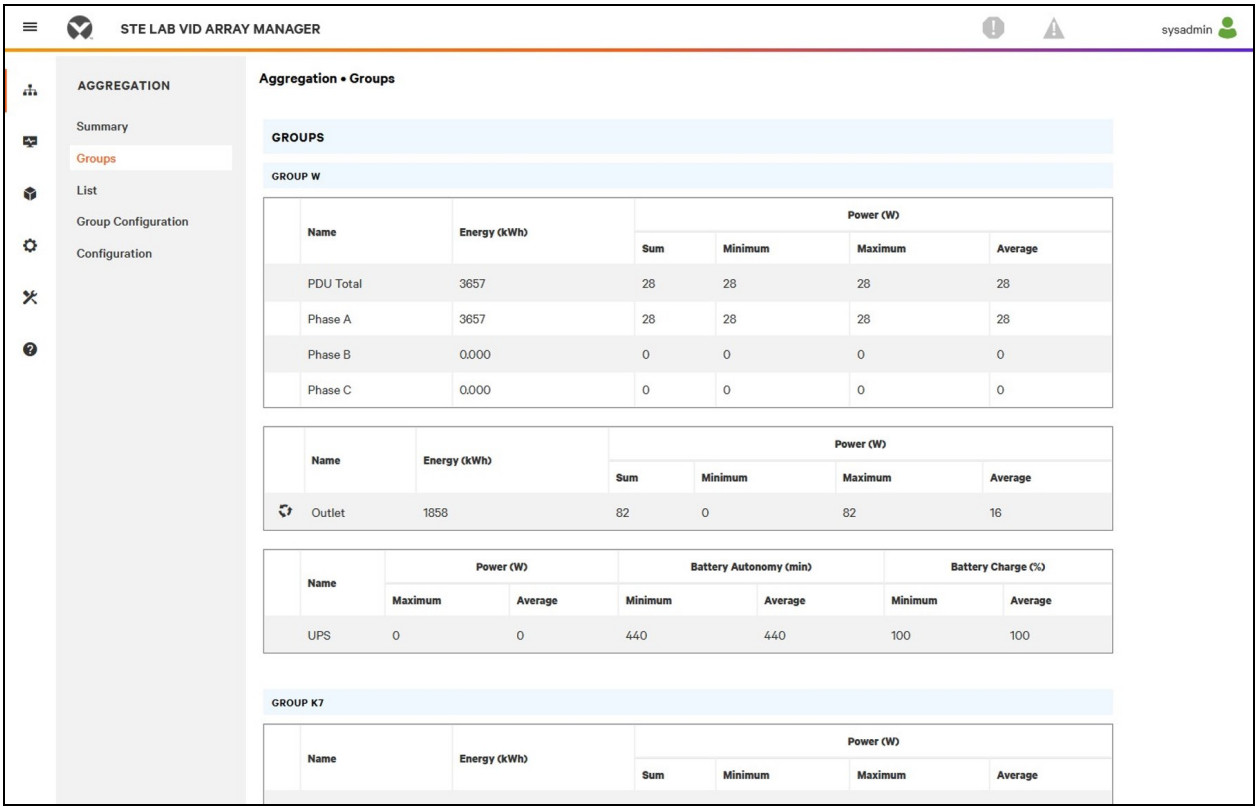
Notificações

As notificações mostram os alarmes pendentes dos dispositivos na rede dos dispositivos.

6.4.2 Groups

Depois que os grupos forem estabelecidos na configuração de grupo, a tela Groups mostrará um resumo dos dados ambientais e de potência.

Figura 6.6 Aba Groups



Os pontos de dados disponíveis são:

rPDU de grupo

- **Energy (kWh):** a energia total da rPDU Geist™ Vertiv™ no grupo.
- **Power (W) Sum:** a carga de energia total da rPDU rPDU Geist™ no grupo.
- **Power (W) Minimum:** a carga de energia mais baixa da rPDU Geist™ no grupo.
- **Power (W) Maximum:** a carga de energia mais alta da rPDU Geist™ no grupo.
- **Power (W) Average:** a carga de energia média da rPDU Geist™ no grupo.

NOTA: Essas leituras são repetidas por fase (mostradas quando há rPDUs trifásicas).

Tomada da rPDU de grupo

- Energy (kWh): a energia total da tomada da rPDU Geist™ no grupo.
- Power (W) Sum: a carga de energia total da tomada da rPDU Geist™ no grupo.
- Power (W) Minimum: a carga de energia mais baixa da tomada da rPDU Geist™ no grupo.
- Power (W) Maximum: a carga de energia mais alta da tomada da rPDU Geist™ no grupo.
- Power (W) Average: a carga de energia média da tomada da rPDU Geist™ no grupo.

Essas leituras se repetem para cada grupo de tomadas da rPDU Geist™ Vertiv™ presentes no grupo quando há pelo menos uma tomada monitorada. Se houver uma combinação de PDUs de rack de tomada monitorada e sem tomada no grupo, as leituras retornarão somente o total de PDUs de rack de tomada monitorada.

Essas leituras são repetidas por fase (mostradas quando há PDUs trifásicas).

NOTA: As leituras de energia refletem a soma das leituras de energia da tomada. A redefinição de cada leitura de energia da tomada também redefinirá a energia total do grupo de tomadas.

O ícone de operação aparece para cada grupo com pelo menos uma tomada da PDU de rack com capacidade de comutação.

Para alterar a operação do grupo de tomadas:

1. Clique no ícone de operação.
2. Selecione a operação que será executada (válido apenas para tomadas da PDU de rack com capacidade de comutação atribuídas ao grupo):
   - On/Off: liga ou desliga todas as tomadas.
   - Reboot: para tomadas ligadas, a reinicialização desliga e depois liga as tomadas após o atraso durante a reinicialização.

     Para as tomadas que estão desligadas, a reinicialização as liga.
   - Cancel: cancela a operação atual se ainda não foi concluída.
3. Para operações que envolvem o estado das tomadas, a definição de Delay (Atraso) como True (Verdadeiro) usa a configuração de atraso atual de cada tomada.
4. Selecione *Submit* para emitir a ação.

UPS de grupo

- Power (W) Maximum: a carga de energia mais alta do UPS no grupo.
- Power (W) Average: a carga de energia média do UPS no grupo.
- Battery Autonomy (min) Minimum: a autonomia mais baixa da bateria do UPS no grupo.
- Battery Autonomy (min) Average: a autonomia média da bateria do UPS no grupo.
- Battery Charge (%) Minimum: a carga mais baixa da bateria do UPS no grupo.
- Battery Charge (%) Average: a carga de bateria média do UPS para o grupo.

Ambiente do grupo

- Temperature (F) Minimum: a temperatura mais baixa no grupo.

- **Temperature (F) Maximum:** a temperatura mais alta no grupo.
- **Temperature (F) Average:** a temperatura média no grupo.
- **Humidity (%) Minimum:** a umidade mais baixa no grupo.
- **Humidity (%) Maximum:** a umidade mais alta no grupo.
- **Humidity (%) Average:** a umidade média no grupo.

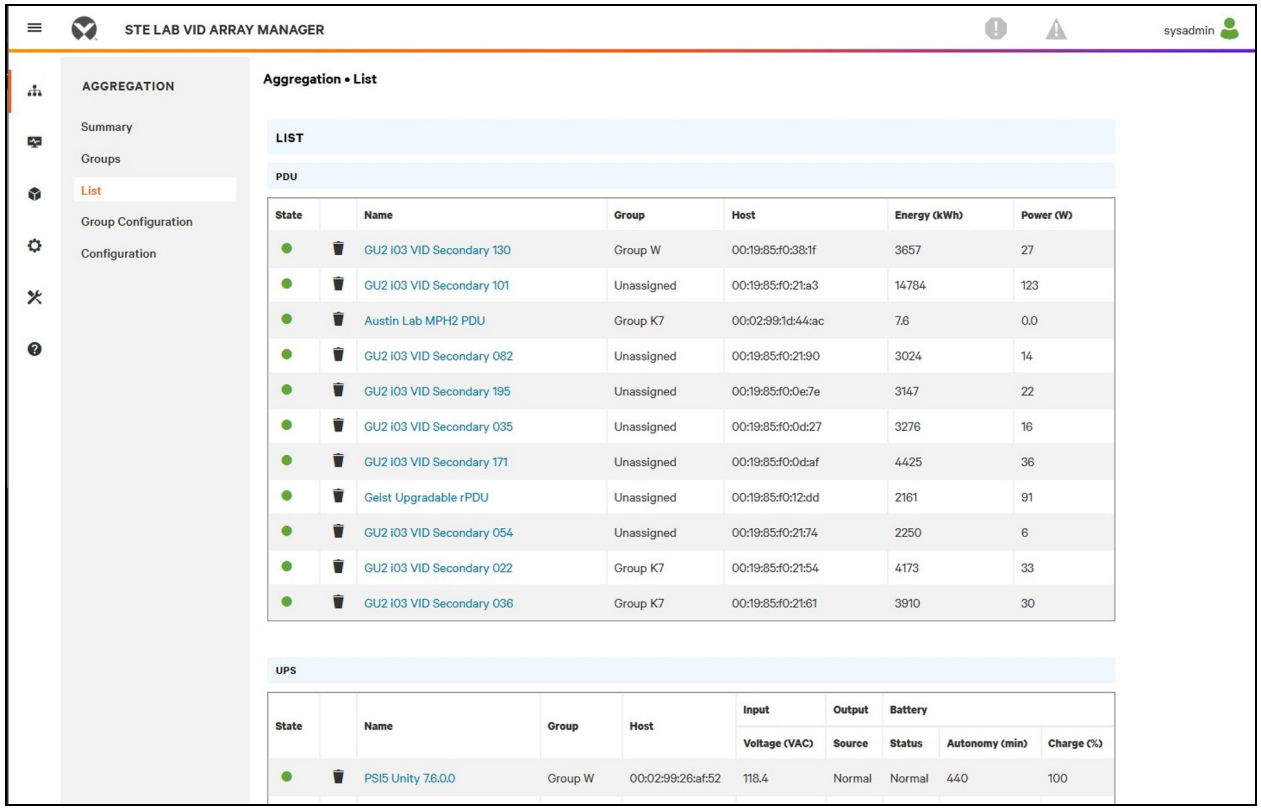
Resfriamento térmico de grupo

- **Fan Speed (%) Minimum:** a velocidade mais baixa da ventoinha térmica do dispositivo no grupo.
- **Fan Speed (%) Maximum:** a velocidade mais alta da ventoinha térmica do dispositivo no grupo.
- **Fan Speed (%) Average:** a velocidade média da ventoinha térmica do dispositivo no grupo.
- **Temperature (F) Minimum:** a temperatura térmica mais baixa do dispositivo no grupo.
- **Temperature (F) Maximum:** a temperatura térmica mais alta do dispositivo no grupo.
- **Temperature (F) Average:** a temperatura térmica média do dispositivo no grupo.
- **Capacity (%) Minimum:** a capacidade térmica mais baixa do dispositivo no grupo.
- **Capacity (%) Maximum:** a capacidade térmica mais alta do dispositivo no grupo.
- **Capacity (%) Average:** a capacidade térmica média do dispositivo no grupo.

6.4.3 List

A visualização List apresenta um inventário de todos os dispositivos na rede de dispositivos do gerenciamento matricial.

Figura 6.7 Aba List (Lista)



O inventário está subdivido nas seguintes categorias:

PDUs de rack

Todas as rPDUs Geist™ Vertiv™ na rede do dispositivo se enquadram nesta categoria e apresentam os seguintes pontos de dados:

- State: o status da rPDU Geist™. O status é Normal ou Unavailable (perda de conectividade).
- Name: Geist™ rótulo da rPDU . Clique no nome para abrir uma guia do navegador e acessar o dispositivo.
- Group: o nome do grupo. Se não houver um grupo criado pelo usuário, o nome do grupo será Unassigned.
- Energy: Geist™ energia da rPDU .
- Power: a carga de energia total da rPDU Geist™.

UPS

Todos os dispositivos UPS na rede do dispositivo se enquadram nesta categoria e apresentam os seguintes pontos de dados:

- State: o status do UPS. O status é Normal ou Unavailable (perda de conectividade).
- Name: rótulo do UPS. Clique no nome para abrir uma guia do navegador e acessar o dispositivo.
- Group: o nome do grupo. Se não houver um grupo criado pelo usuário, o nome do grupo será Unassigned.
- Input Voltage: tensão de entrada do UPS.
- Output Source: o modo de operação do UPS, que pode ser: Normal, Bypass, Battery, Booster, Reducer, Off ou Other.
- Status: o status da bateria, que pode ser: Normal, Low, Depleted ou Unknown.
- Battery Autonomy: autonomia da bateria do UPS.
- Charge: carga da bateria do UPS.

Sensores ambientais (ENV)

Todos os sensores ambientais na rede do dispositivo se enquadram nesta categoria e apresentam os seguintes pontos de dados:

- State: o status do sensor. O status é Normal ou Unavailable (perda de conectividade).
- Name: rótulo do sensor. Clique no nome para abrir uma guia do navegador e acessar o dispositivo.
- Group: o nome do grupo. Se não houver um grupo criado pelo usuário, o nome do grupo será Unassigned.
- Device: exibe o rótulo e o endereço MAC da rPDU Geist™ Vertiv™ principal do sensor.
- Temperature (F): leitura da temperatura (temperatura principal somente com sensores GT3HD).
- Humidity (%): leitura da umidade. Esse campo ficará em branco se forem implantados somente sensores de temperatura SRT.

Os sensores ambientais relatam seus valores no MIB das rPDUs Geist™ às quais estão conectados. Eles não são sensores independentes com seus próprios endereços IP. Nesta versão, os únicos sensores válidos são os SRT, GTHD ou GTHD3 Geist™ conectados por rPDU Geist™.

NOTA: Para personalizar o rótulo de qualquer dispositivo, faça login nele e edite-o usando o ícone Configuração.

NOTA: Para excluir um dispositivo que foi removido da rede, selecione o ícone de Lixeira ao lado do dispositivo. Se você selecionar o ícone Delete, o dispositivo e todos os sensores ambientais conectados a ele serão excluídos.

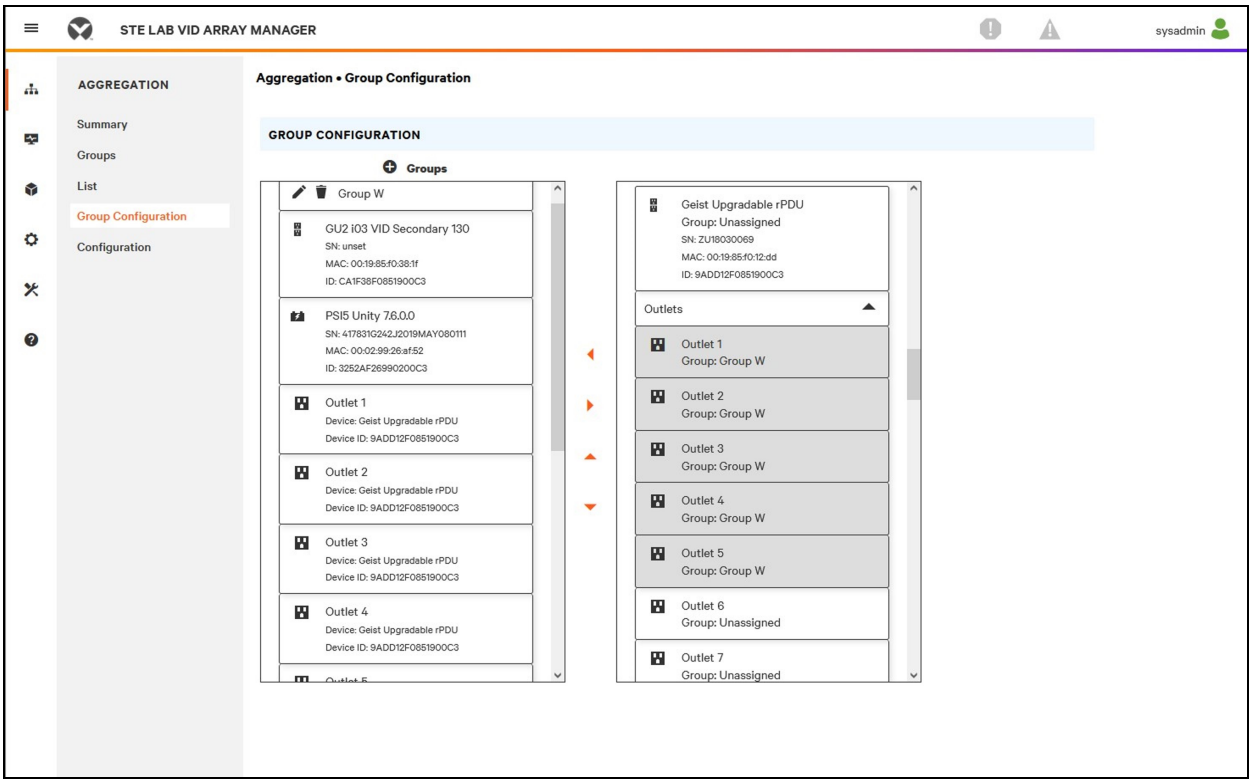
Resfriamento térmico

- State: o status do resfriamento. O status é Normal ou Unavailable (perda de conectividade).
- Name: rótulo do dispositivo de resfriamento térmico. Clique no nome para abrir uma guia do navegador e acessar o dispositivo.
- Group: o nome do grupo. Se não houver um grupo criado pelo usuário, o grupo será Unassigned.
- Host: endereço MAC.
- Fan Speed (%): velocidade da ventoinha térmica do dispositivo.
- Temperature (F): temperatura térmica do dispositivo.
- Capacity (%): capacidade térmica do dispositivo.

6.4.4 Group Configuration

Na página Group Configuration, é possível definir grupos de dispositivos para fins de agregação e análise de dados. Geralmente, um grupo refere-se a uma unidade de medida no ambiente de computação que inclui várias portas matriz, como um rack com duas rPDUs Geist™, dispositivos UPS e sensores ambientais, ou uma linha com vários racks.

Figura 6.8 Configuração de grupo



A página Group Configuration lista os dispositivos detectados automaticamente na coluna *Unassigned* e mostra:

- Um ou mais ícones que definem o tipo de dispositivo, como rPDU Geist™ Vertiv™, sensor ambiental, UPS ou tomada da rPDU Geist™.
- Rótulo do dispositivo
- Número de série
- Endereço MAC
- ID

Os grupos de dispositivos configurados (costumam representar racks) são exibidos à esquerda.

Para criar um novo grupo:

1. Clique no *sinal de mais (+)* à esquerda de Groups para adicionar um novo grupo abaixo de Groups.
2. Clique no ícone de Configuração para alterar o rótulo do nome do grupo.
3. Edite o rótulo, se desejado, e clique em *Save*.
4. Para atribuir dispositivos ao grupo, destaque o grupo desejado (na categoria Groups) e destaque os dispositivos desejados na categoria Unassigned.

NOTA: Você deve clicar na seta para baixo localizada sob a PDU para ver a lista de tomadas.

5. Clique na *Seta para a direita* para atribuir os dispositivos ao grupo.
6. Repita o processo para outros grupos, conforme necessário.

NOTA: É possível reordenar os grupos clicando nas setas para cima ou para baixo.

Para remover dispositivos de um grupo:

Destaque os dispositivos e clique na *Seta para a direita*.

Para excluir um grupo:

Clique no ícone de Lixeira ao lado do nome do grupo.

NOTA: A exclusão de um grupo retorna todos os seus dispositivos ao grupo Unassigned.

6.5 Interfaces

As portas matriz são combinadas para formar grupos; cada dispositivo mantém a própria interface de usuário independente e os dados SNMP.

Para acessar a interface de usuário da porta matriz:

1. Na visualização List, passe o cursor do mouse sobre as entradas na tabela. Um destaque amarelo e uma caixa de texto aparecem quando você pausa nos dispositivos. A caixa de texto exibe o endereço IP e o número da porta do dispositivo.
2. Navegue até um endereço IP e número da porta para acessar a interface do servidor Web do dispositivo.

   - ou -

3. Clique no nome do dispositivo para acessar o hiperlink para a interface Web do dispositivo.

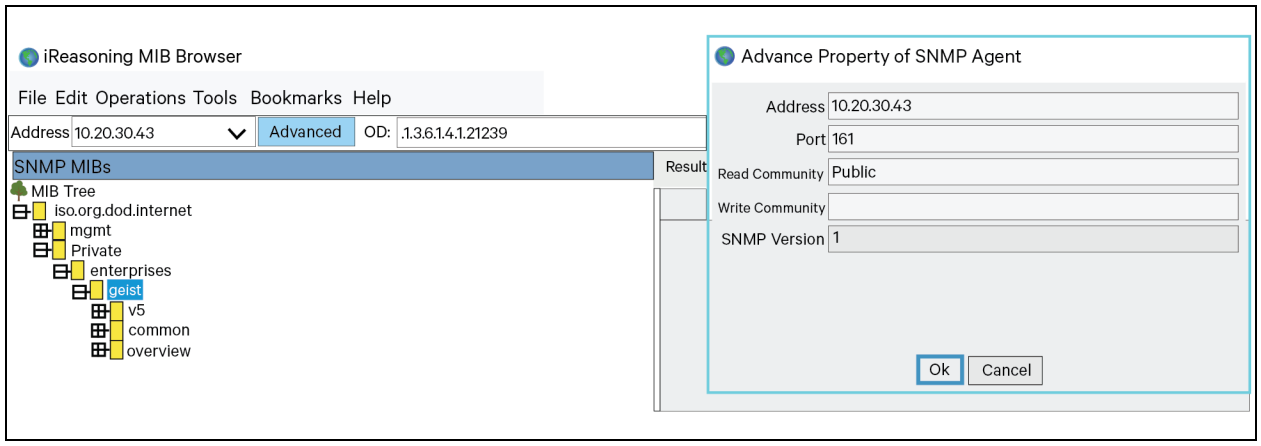
Para acessar os dados SNMP da porta matriz:

Os dados SNMP da PDU de rack Geist estão disponíveis por meio do acesso com mapeamento de porta pelo endereço IP do dispositivo de gerenciamento matricial com MIB v5 Geist™. O arquivo MIB pode ser baixado na página de SNMP do gerenciamento matricial.

1. Na visualização em lista, passe o cursor do mouse sobre as entradas na tabela. Quando você pausa sobre um dispositivo, um destaque amarelo e uma caixa de texto aparecem com a porta SNMP do dispositivo.
2. No navegador do MIB, insira a porta SNMP listada.

NOTA: O software que monitora os portas matriz individuais devem aceitar um número de porta SNMP exclusivo por dispositivo monitorado.

Figura 6.9 Navegador do MIB



6.5.1 Dados SNMP de grupo

Dados agregados, tanto de resumo (como kWH total e kW máximo) quanto de grupo, estão disponíveis pelo endereço IP da rPDU Geist™ Vertiv™ mestre e porta SNMP 161 padrão. Dois MIBS estão disponíveis para a PDU de rack Array Controller Geist.

- v5: contém pontos de dados para a rPDU Geist™ mestre individual.
- Oneview: contém pontos de dados agregados em todas as portas matriz.

6.5.2 Dicas e solução de problemas

- É recomendável atualizar todos os dispositivos para a versão mais recente do firmware antes de configurar a agregação.
- Verifique se a PDU de rack indicada como gerenciamento matricial está totalmente configurada e se a agregação está ativada antes de conectar quaisquer portas matriz.
- Verifique se todas as portas matriz foram redefinidas aos padrões de fábrica antes de conectá-las ao gerenciamento matricial. Se as configurações já foram alteradas ou se foram definidos usuários em um dispositivo, o dispositivo deve ser restaurado aos padrões de fábrica antes de ser conectado ao gerenciamento matricial.
- Se você for restaurar a PDU de rack às configurações padrão de fábrica, use a função *Utilities>Restore defaults>All Settings*. O uso do botão para centralizar do IMD ou do comutador de redefinição (furo) abaixo da porta de rede 2 para restaurar as configurações não restaura todas as configurações e pode fazer com que as portas matriz não sejam identificadas corretamente.
- Depois de restaurar uma PDU de rack às configurações padrão de fábrica e antes de ligá-la à porta matriz, desconecte-a da rede e reinicie-a usando o botão abaixo da porta de rede 1. Esse procedimento garante que qualquer endereço DHCP alocado durante a restauração dos padrões de fábrica seja liberado.
- As portas matriz podem levar até 20 minutos para serem reconhecidas após uma configuração inicial.
- Não é possível ativar alarmes com base em dados agregados de resumo e de grupo.

- É possível usar a ferramenta Provisioner (*Provisioner>Discovery and Provisioner>File Management*) para atualizar facilmente o firmware da PDU de rack do gerenciamento matricial e da porta matriz.
- Não é possível usar os dados agregados de resumo e de grupo para gerar interceptações SNMP.
- Os nomes das comunidades de SNMP são configurados em cada dispositivo. Siga os links dos dispositivos exibidos na página List no menu Devices e faça login em cada dispositivo para configurar o SNMP.
- Não altere o número da porta SNMP padrão, as configurações de rede e as configurações do servidor Web enquanto estiver conectado a uma porta matriz.
- As intercepções SNMP e os alarmes são roteados de um dispositivo para a rede de gerenciamento pelo dispositivo mestre.

Esta página foi deixada intencionalmente em branco

Apêndices

Apêndice A: Suporte técnico

A.1 Redefinir uma rPDU Geist™ Vertiv™

Se uma rPDU Geist™ ficar sem comunicação, o processador poderá ser reinicializado manualmente sem afetar a alimentação das tomadas. Se você pressionar o botão de reinicialização na frente do IMD, o processador será reinicializado. A interface da Web continuará offline durante a inicialização. Para obter mais informações, consulte Dispositivo de monitoramento intercambiável na página 27.

A.2 Serviço e manutenção

Não é necessário serviço ou manutenção. Se a rPDU Geist™ for aberta, a garantia poderá ser invalidada. Não há peças no interior da rPDU Geist™ que possam ser reparadas pelo usuário além do Dispositivo de monitoramento intercambiável (IMD) que pode ser substituído em campo. Geist™ recomenda desligar a alimentação de energia da unidade antes de instalar ou remover qualquer equipamento.

O IMD foi projetado para ser substituído em campo somente por pessoal de manutenção devidamente treinado e qualificado. O IMD foi desenvolvido para ser substituído com a rPDU Geist™ ainda conectada à rede elétrica. Consulte o Guia de substituição dos módulos IMD da rPDU Geist™ para obter mais informações.

A.3 Mais suporte técnico

Acesse o suporte técnico pelo site *www.Vertiv.com/support*.

Américas

- Site: *www.Vertiv.com/geist*
- E-mail: geistsupport@vertiv.com
- Telefone: 1-888-630-4445

Europa e Oriente Médio

- Suporte técnico: *www.Vertiv.com/en-emea/support*
- E-mail: eoc@Vertiv.com
- Telefone: 44 1823 275100

Ásia

- Telefone (inglês): 1-888-630-4445 (número dos EUA)
- Telefone (chinês): +86 755 23546462

A.4 Uso do Microsoft Exchange como servidor SMTP

Se sua instalação usa o servidor de e-mail Microsoft Exchange, a rPDU Geist™ do IMD poderá usá-lo para enviar e-mails de notificação de alarmes e advertências. No entanto, o servidor Exchange talvez tenha que ser configurado para permitir conexões SMTP da unidade primeiro, já que, por padrão, os serviços SMTP ou a autenticação básica estão desativados nas versões mais recentes do servidor Exchange. Se você tiver dificuldades para fazer com que a rPDU Geist™ do IMD envie e-mails pelo servidor Exchange, as notas a seguir poderão ajudar.

NOTA: Estas sugestões serão aplicadas somente se você usar um servidor Exchange físico próprio. O serviço hospedado Office 365 da Microsoft não é compatível com a rPDU Geist™ Vertiv™ do IMD que tem versões do firmware anteriores à v3.0.0, já que o Office 365 requer uma conexão StartTLS. As versões 3.0.0 e mais recentes do firmware são compatíveis com StartTLS e Office 365.

Primeiramente, como a rPDU Geist™ do IMD não pode usar IMAP nem protocolos MAPI/RPC do Exchange/Outlook de propriedade da Microsoft para enviar mensagens, você deve ativar o SMTP configurando um Conector de Envio SMTP no servidor Exchange. Há mais informações sobre como configurar o Conector de Envio SMTP no Exchange disponíveis no artigo do Microsoft TechNet: *http://technet.microsoft.com/en-us/library/aa997285.aspx*

Segundo, talvez você tenha que configurar o servidor Exchange para permitir a retransmissão de mensagens da unidade de monitoramento. Normalmente, isso envolve ativar a opção *Redirecionar e-mails SMTP recebidos* nas propriedades de redirecionamento do servidor Exchange e adicionar o endereço IP da rPDU Geist™ do IMD como um domínio com permissão para retransmitir e-mails por meio do servidor Exchange. Há mais informações sobre como ativar e configurar a retransmissão SMTP no Exchange disponíveis no artigo do Microsoft TechNet: *http://technet.microsoft.com/en- us/library/dd277329.aspx*

Normalmente, os métodos de autenticação SMTP AUTH PLAIN e AUTH LOGIN para login no servidor não estão mais ativados por padrão no Exchange Server; somente o método de autenticação NTLM proprietário da Microsoft está ativado.

Para reativar o método AUTH LOGIN:

1. No console do Exchange, selecione *Server Configuration - Hub Transport*.
2. Clique com o botão direito em *Client Server* e selecione *Propriedades*.
3. Selecione a guia *Authentication* e clique na caixa de seleção *Basic Authentication*.
4. Desmarque a caixa de seleção *Offer Basic only after TLS*.
5. Clique em *Apply* ou *Save* e em *Exit*.

NOTA: Talvez seja necessário reiniciar o serviço Exchange depois de fazer essas alterações.

Por fim, depois que você ativou o SMTP, a retransmissão e o método de autenticação básica AUTH LOGIN, talvez seja necessário criar uma conta do usuário especificamente para login da rPDU Geist™ do IMD. Se você criou uma conta antes de ativar o Conector de Envio SMTP ou se está tentando usar uma conta criada para outro usuário, e a rPDU Geist™ do IMD ainda não pode se conectar ao servidor Exchange, a conta provavelmente não herdou as novas permissões quando você as ativou conforme descrito acima. Isso costuma acontecer com mais frequência nos servidores Exchange que foram atualizados desde a criação da conta que você está tentando usar, mas às vezes pode acontecer em contas com novos conectores e plug-ins adicionados, seja qual for a versão do Exchange. Exclua a conta do usuário, depois crie uma nova para a unidade de monitoramento usar, e a nova conta deve herdar a autenticação SMTP e as permissões de retransmissão de e-mail corretamente.

Se nenhuma das sugestões acima funcionar para fazer com que a rPDU Geist™ do IMD envie e-mails pelo servidor Exchange, talvez seja necessário entrar em contato com o suporte técnico da Microsoft para obter ajuda na configuração do servidor Exchange e permitir o envio de e-mails por SMTP de qualquer dispositivo de terceiros (não Windows) por sua rede.

Esta página foi deixada intencionalmente em branco

Apêndice B: Sensores disponíveis

B.1 Sensores remotos

- SRT: temperatura remota inoxidável.
- GTHD: temperatura/umidade/ponto de condensação.
- GT3HD: temperatura/umidade/ponto de condensação com dois sensores SRT.
- RTAFHD3: temperatura/fluxo de ar/umidade/ponto de condensação.
- A2D: converte sensores de E/S analógicos em sensores digitais remotos.

B.2 Sensores analógicos de E/S

- FS-15: sensor de inundação (água).
- PFS-100 US/PFS-100 UN: sensor de falha de energia.
- RPDS: kit de comutadores de porta.

B.3 Sensores integrados e modulares Liebert®

NOTA: É necessário um adaptador para usar qualquer um dos sensores a seguir.

- SN-T: uma sonda de temperatura.
- SN-TH: uma sonda de temperatura e uma sonda de umidade.
- SN-Z01: cabo integrado com uma sonda de temperatura.
- SN-Z02: cabo integrado com três sondas de temperatura.
- SN-Z03: cabo integrado com quatro sondas (três de temperatura e uma de umidade).
- SN-2D: sensor do monitor do comutador de duas portas.

B.4 Conexão de sensores remotos

É possível conectar até 16 sensores remotos plug-and-play à unidade, a qualquer momento, por meio dos conectores RJ-12 na parte frontal da unidade. Em alguns casos, talvez sejam necessários separadores para adicionar sensores. Cada sensor tem um número de série exclusivo e é detectado e adicionado automaticamente à página da Web. O número de série do sensor determina a ordem de exibição na Web. É possível personalizar os nomes dos sensores na página Sensors Overview.

NOTA: Os sensores usam Cat 5, fio CMP e conectores RJ-12. A fiação deve ser direta. A reversão da polaridade desativa temporariamente todos os sensores até a correção. Os sensores usam um protocolo de comunicação serial e estão sujeitos às restrições de sinal de rede, dependendo da blindagem, do ruído ambiental e do comprimento do fio. As instalações comuns permitem distâncias de até 600 pés (180 m) do fio do sensor.

Apêndice C: Adaptadores USB sem fio de TP-Link

- Archer T2U Nano (adaptador nano USB sem fio AC600)
- Archer T2U Plus (adaptador USB Dual Band de alto ganho sem fio AC600)
- Archer T2U v3 (adaptador USB Dual Band sem fio AC600)
- Archer T3U (adaptador mini USB MU-MIMO sem fio AC1300)
- Archer T3U Plus (adaptador USB Dual Band de alto ganho sem fio AC1300)
- Archer T4U v3 (adaptador USB Dual Band sem fio AC1300)

NOTA: Esses dispositivos são detectados automaticamente quando conectados e podem ser configurados como interface de rede adicional.

Esta página foi deixada intencionalmente em branco

Apêndice D: LEDs da tomada

NOTA: Este apêndice refere-se apenas a rPDUs Geist™ Vertiv™ de tomada monitorada/comutada.

Os LEDs da tomada indicam visualmente o status de alimentação da tomada (On, Off ou Error). Os LEDs são numerados sequencialmente com números brancos fáceis de ler sobre um fundo preto. Dependendo do status da alimentação da tomada, os LEDs acenderão em cores sólidas ou intermitentes.

Tabela D.1 Tomadas LED

LED	Descrição
Verde	Tensão da tomada presente e acima do limite mínimo
Vermelho	Tensão da tomada não está presente
Âmbar	Condição de erro da tomada de alimentação detectada

Tabela D.2 Descrição dos status de LED

Tensão medida	Estado do relé	Estado	LED	
Ligado	Ligado ou desconhecido	Sólido	Verde	
Desligado	Desligado ou desconhecido	Sólido	Vermelho	
Desligado	Ligado	Piscando [1]	Âmbar	Vermelho
Ligado	Desligado	Piscando [2]	Âmbar	Verde

[1] Tomada indicada como Desligada, mas deveria ser Ligada.

[2] Tomada indicada como Ligada, mas deveria ser Desligada.

Código do erro

Os LEDs acendem na cor sólida âmbar quando:

- Falha de energia (todos os relés são abertos à força em caso de falha de energia para permitir o sequenciamento de ativação)
- Disjuntor aberto
- Nenhuma tensão de entrada detectada

Apêndice E: Códigos de tela do IMD

Tabela E.1 Códigos de tela do IMD

Tela	Tipo de IMD	Explicação
Err1	IMD-01 (apenas com medição)	O IMD não detectou nenhuma ou mais de uma placa de entrada. Isso pode ser causado por problemas de cabeamento interno ou por uma placa de entrada que não responde. Ele também é exibido quando há um erro de medição relatado pela placa de entrada.
8888	IMD-02, IMD-03, IMD-3	O IMD está sendo inicializado e ainda precisa detectar a tela simples e exibir *boot* nela. Se ele aparecer por mais do que alguns segundos, a placa da tela ou o cabeamento interno estará com algum problema.
-- (dois traços na posição da tela mais à direita)	IMD-02, IMD-03, IMD-3	O IMD não pode se comunicar com a placa de entrada. Ele também pode aparecer de modo intermitente para medições individuais. Há um problema com a placa de entrada ou com o cabeamento interno.
boot	IMD-01	O IMD está sendo inicializado e detectando a placa de entrada.
boot	IMD-02, IMD-03, IMD-3	O firmware está sendo inicializado. Isso aparece durante a atualização do firmware nas placas internas.
updt	IMD-02, IMD-03, IMD-3	Atualização do firmware em andamento.
rset dflt	IMD-02, IMD-03, IMD-3	Após a ação do usuário, *rset* (redefinir) aparecerá durante uma sequência de redefinições de parâmetros. Durante a redefinição de parâmetros, *dflt* (padrão) aparece rapidamente.
bcup	IMD-02, IMD-03, IMD-3	*bcup* (backup) aparecerá durante um backup de configuração.
rest conf	IMD-02, IMD-03, IMD-3	*rest* (restaurar) e *Conf* (configuração) aparecem durante uma restauração de configuração.
____ (quatro sublinhados na parte inferior da tela)	IMD-03 IMD-3	A tela do IMD foi configurada com Total Power, Voltage e Current desativados.

NOTA: O IMD-5M não tem códigos de exibição; a tela sensível ao toque exibe as informações do status.

Esta página foi deixada intencionalmente em branco

Apêndice F: Provisioner: formato do arquivo de configurações

NOTA: Veja a seguir a descrição do formato do arquivo de configurações usado pelo Provisioner. Os exemplos seguem amplamente as configurações disponíveis na interface de usuário da Web da rPDU Geist™ Vertiv™.

1. Nos exemplos a seguir, é possível copiar o texto em azul em um arquivo de texto e atualizá-lo conforme necessário. Depois disso, o arquivo de texto poderá ser carregado na ferramenta de instalação.
2. Ao editar arquivos de configuração, use um editor de texto, como o Bloco de notas, que pode salvar arquivos no formato .txt.
3. Os recuos mostrados nos exemplos podem ser omitidos.
4. Verifique se foram usadas as aspas duplas corretas ao editar a configuração.
5. Se uma configuração não constar no arquivo de configurações, o valor dela permanecerá inalterado.
6. Ao configurar uma rPDU Geist™ já configurada (ou seja, original de fábrica), a primeira configuração deve ser a definição de um usuário admin. Consulte Local Users abaixo.
7. Para combinar várias configurações (além dos usuários locais) em um arquivo (consulte também o Example 1 na página 141 no fim deste documento):
   - Anexe as configurações obrigatórias juntas em um arquivo.
   - Exclua todas as ocorrências de {"conf":{, exceto a primeira linha do arquivo.
   - Substitua todas as linhas que têm apenas }} por , (vírgula), exceto a última linha do arquivo.
8. Se houver configurações de usuário local combinadas com outras configurações em um arquivo, consulte o Example 2 na página 142 no fim deste documento.
9. Depois de selecionar *Provisioner>Discovery>Update*, insira o nome de usuário e a senha apenas para configurar as rPDUs Geist™ já configuradas (use o mesmo nome de usuário e a mesma senha de quando as rPDUs Geist™ foram instaladas). Não insira um usuário e uma senha ao configurar unidades originais de fábrica (identificadas pelo atributo Provisioned igual a False).

Local Users

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

username	O nome do usuário que será criado (entre aspas)
password	Senha (entre aspas)
enabled	As opções são true ou false para determinar se o usuário está ativado
control	As opções são true ou false para determinar se o usuário terá privilégios de controle
admin	As opções são true ou false para determinar se o usuário terá privilégios de admin
language	Substitui o idioma padrão deste usuário. As opções válidas são "de", "en", "es", "fr", "ja", "ko", "pt", "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 LDAP (ref. RFC4516 > RFC2255) (entre aspas) necessário se LDAP estiver ativado.
port	Porta para comunicação por protocolo
mode	Determina a compatibilidade padrão entre os tipos diferentes de LDAP. As opções são “openLdap ou activeDirectory”
securityType	Criptografia que será usada para conexão com o servidor LDAP. As opções são “ssl” e “starttls”
bindDn	Nome exclusivo (entre aspas) (ref. RFC4514 > RFC2253), usado para vinculação com o servidor de diretório. Uma string em branco significa vinculação anônima
password	Senha (entre aspas) usada para vinculação com o servidor de diretório
baseDn	Nome exclusivo (entre aspas) (ref. RFC4514 > RFC2253) que será usado como base da pesquisa
userFilter	Filtro de pesquisa LDAP (entre aspas) (ref. RFC4515 > RFC2254), objectClass equivalente a posixAccount (ref. RFC2307)
userId	Equivalente ao atributo "uid" (entre aspas) (ref. RFC2307)
userIdNum	Equivalente ao atributo "uidNumber" (entre aspas) (ref. RFC2307)
groupFilter	Filtro de pesquisa LDAP (entre aspas) (ref. RFC4515 > RFC2254), objectClass equivalente a posixGroup (RFC2307)
groupId	Equivalente ao atributo "gidNumber" (ref. RFC2307) (entre aspas)
groupMemberUid	Equivalente ao atributo "memberUid" (ref. RFC2307) (entre aspas)
enabledGroup	O usuário (entre aspas) neste grupo terá o privilégio "enabled"
controlGroup	O usuário (entre aspas) neste grupo terá o privilégio "control"
adminGroup	O usuário (entre aspas) neste grupo terá o privilégio "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 autenticação/autorização principal (entre aspas)
authenticationServer2	Servidor de autenticação/autorização alternativo (entre aspas)
accountingServer1	Servidor de contabilidade principal (entre aspas)
accountingServer2	Servidor de contabilidade alternativo (entre aspas)
sharedSecret	Segredo (entre aspas) compartilhado pelo cliente e servidor (null exclui o segredo)
service	O valor que será usado no campo de serviço nas solicitações TACACS. As opções são "ppp" e "raccess"
adminAttribute	O usuário (entre aspas) com este par atributo-valor terá o privilégio "admin"
controlAttribute	O usuário (entre aspas) com este par atributo-valor terá o privilégio "control"
enabledAttribute	O usuário (entre aspas) com este par atributo-valor terá o privilégio "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 autenticação principal (entre aspas)
authenticationServer2	Servidor de autenticação alternativo (entre aspas)
accountingServer1	Servidor de contabilidade principal (entre aspas)
accountingServer2	Servidor de contabilidade alternativo (entre aspas)
sharedSecret	Segredo compartilhado pelo cliente e servidor (entre aspas)
groupAttribute	Identifica o AVP que informa o grupo de acesso ao qual o usuário pertence. Os valores válidos são "filter-id" e "management-privilege-level".
adminGroup	O usuário (entre aspas) pertencente a este grupo tem o privilégio "admin"
controlGroup	O usuário (entre aspas) pertencente a este grupo tem o privilégio "control"
enabledGroup	O usuário (entre aspas) pertencente a este grupo terá o privilégio "enabled"

Network Hostname and IP Addresses

```
{"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	Nome (entre aspas) para identificar a unidade em uma rede
ip6Enabled	As opções são true ou false para ativar ou desativar suporte a IPV6
label	Rótulo da ponte (entre aspas)
enabled	As opções são true ou false para ativar ou desativar a ponte de rede
dhcpOn	As opções são true ou false para ativar ou desativar DHCP
address	Endereço IP (entre aspas) da interface
prefix	Prefixo do endereço IP da interface

Network Ports

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

label	Rótulo da porta (entre aspas)
enabled	As opções são true ou false para determinar se a porta está ativada
cost	Custo do protocolo Spanning Tree desta porta

Network Routes

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

gateway	Endereço gateway (entre aspas) da rota
prefixDestination	Prefixo de rede. 0 para gateway padrão
destination	Endereço da rede de destino (entre aspas): “0.0.0.0” para rede padrão

Network DNS

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

address	O endereço do servidor DNS (entre aspas). A segunda ocorrência é para o servidor DNS alternativo.

Network RSTP

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

enabled	As opções são true ou false para determinar se o Spanning Tree Protocol está ativado
mode	As opções são "stp" ou "rstp". O modo RSTP aceita fallback para STP, quando necessário
bridgePriority	A prioridade da ponte do protocolo Spanning Tree desta interface
helloTime	O intervalo, em segundos, entre as transmissões periódicas das mensagens de configuração
maxAge	A duração máxima das informações transmitidas por esta interface, quando ela funciona como ponte raiz. Usada quando "mode" está definido como "stp". Deve ser no mínimo 2 * (helloTime + 1)
maxHops	O número máximo de travessias de ponte das informações transmitidas por esta interface, quando ela funciona como ponte raiz, usado quando "mode" está definido como "rstp"
forwardDelay	O atraso usado pelas pontes para transição da ponte raiz e das portas designadas para o modo de encaminhamento deve ser no mínimo (maxAge / 2) + 1

Web Server


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


httpEnabled	As opções são true ou false para permitir comunicações não criptografadas
httpPort	Número da porta para comunicação HTTP
httpsPort	Número da porta para comunicação HTTPS

Reports


```
{"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 do dia em que o intervalo é aplicado. O formato é “(00-23):(00-59)” configurável em incrementos de 15 minutos
days	Primeira letra dos dias selecionados (entre aspas) na ordem de segunda-feira a domingo. Um '-' é usado para representar destinos em dias não selecionados
	Lista de chaves que fazem referência a destinos de e-mail (entre aspas)
interval	Número de horas entre os relatórios. As opções permitidas são 1, 2, 3, 4, 6, 8, 12 e 24

Display

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

mode	Seleciona um conjunto de dados para mostrar na tela. As opções são “current”, “totalPower” e “currentAndTotalPower”
inverted	As opções são true ou false para descrever a orientação atual da tela
enabled	As opções são true ou false para determinar o modo da tela VLC da rPDU

Time

```
{"conf":{
"time": {
"mode": "ntp",
"datetime": "2021-03-09 12:05:36",
"zone": "UTC",
"ntpServer1": "0.pool.ntp.org",
"ntpServer2": "1.pool.ntp.org"}
}}
```

mode	Modo. As opções válidas são "ntp" e "manual"
datetime	Data e hora no formato "YYYY-MM-DD HH:MM:SS", com o intervalo de horas de 0-23 (este campo é exibido no horário local), somente devem ser usadas com o modo = ”manual”
Zone	Deve ser um nome válido (entre aspas) do banco de dados tz
ntpServer1	O endereço do servidor NTP principal (entre aspas) apenas deve ser usado com o modo = ”ntp”
ntpServer2	O endereço do servidor NTP de backup (entre aspas) apenas deve ser usado com o modo = ”ntp”

SSH

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

enabled	As opções são true ou false para ativar ou desativar SSH
port	Número da porta para comunicação SSH

USB

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

enabled	As opções são true ou false: ativa ou desativa a porta USB

Serial Port

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

baudRate	Taxa de transferência. Os valores são 1200, 2400, 4800, 9600, 19200, 38400, 57600 e 115200
dataBits	Número de bits de dados em uma estrutura. As opções são 7 e 8
enabled	As opções são true ou false: ativa ou desativa a CLI serial no dispositivo
parity	Tipo de bit de paridade usado na estrutura. As opções são “none”, “even” e “odd”
stopBits	Número de bits de parada usados para encerrar cada estrutura. As opções são 1 e 2

Email

```
{"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	Endereço do servidor SMTP (entre aspas)
port	Número da porta SMTP
sender	Endereço de e-mail dos remetentes (entre aspas)
username	Nome de usuário SMTP (entre aspas)
password	Senha SMTP (entre aspas)
name	Endereço de e-mail de destino (entre aspas)

SNMP v1 ou 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	As opções são true ou false: ativa ou desativa o SNMP versão 1 e 2c
port	Número da porta para comunicação SNMP
readCommunity	O nome da comunidade de leitura (entre aspas) deve ser diferente de writeCommunity
writeCommunity	O nome da comunidade de gravação (entre aspas) deve ser diferente de readCommunity
trapCommunity	Nome da comunidade de interceptação (entre aspas)
port	Número da porta para interceptações SNMP
name	Endereço (entre aspas) do destino da interceptação SNMP
trapVersion	Versão da interceptação SNMP: "1" ou "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	As opções são true ou false: ativar ou desativar o SNMP versão 1 e 2c
port	Número da porta para comunicação SNMP
type	Tipo de permissão. Os valores possíveis são "read", "write" ou "trap"
username	Nome de usuário SNMPv3 (entre aspas)
privPassword	Senha de privacidade (entre aspas)
privType	Tipo de criptografia de privacidade. Os valores são "aes", “des” ou "none"
authPassword	Senha de autenticação (entre aspas)
authType	Tipo de autenticação. Os valores são "sha1", “md5” ou "none"

Syslog

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

enabled	As opções são true ou false: ativar a transmissão de mensagens syslog para um destino remoto
target	Endereço (entre aspas) do destino remoto das mensagens syslog
port	Número da porta de destino para mensagens

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	Descrição da unidade (entre aspas)
location	Local da unidade (entre aspas)
contactName	Nome de contato da unidade (entre aspas)
contactEmail	E-mail de contato da unidade (entre aspas)
contactPhone	Número de telefone de contato da unidade (entre aspas)
label	Rótulo do sistema da unidade (entre aspas)

Locale

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

defaultLang	Idioma. As opções válidas são "de", "en", "es", "fr", "ja", "ko", "pt", "zh"
units	Unidades. As opções válidas são "metric" e "imperial"

Data Logging Interval

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

interval	O intervalo de gravação de logs de dados em minutos

Aggregation

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

enabled	As opções são true ou false para determinar se a agregação está ativada
username	O nome de usuário (entre aspas) que será definido nos equipamentos conectados
password	A senha (entre aspas) que será definida para os equipamentos conectados (null exclui a senha)

Example 1

Arquivo para configurar nome de host, endereço IP, gateway, nomes e localidade da comunidade SNMP v1:

```
{"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"}
}}
```

Example 2

Arquivo para configurar usuário admin, desativar HTTP e configurar 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"} }}
```

Configurações e alarmes do 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	O device-id que será configurado (disponível na página sensors>overview) da rPDU. Se este device-id não corresponder a nenhum dos dispositivos selecionados que foram provisionados, todos os dispositivos selecionados serão provisionados. Configure o device-id como 0000000000000000 para garantir que todos os dispositivos selecionados sejam configurados.
label	O rótulo da rPDU (exibido na página sensors>overview)
type	Para a configuração de alarmes nas medições da PDU interna, o "type" deve corresponder ao IMD usado na PDU, portanto, deve ser "i03" para PDUs que usam qualquer IMD-03x ou IMD-3x e "i05" para PDUs que usam o IMD-5M. Para a configuração de alarmes nos sensores externos, o "type" deve ser o tipo do sensor externo. Valores válidos: "remotetemp", "afht3", "thd", "t3hd", "a2d", "snt", "snh", "snd". Se omitido, impede a configuração de qualquer rPDU selecionada quando o device-id não corresponde a nenhuma rPDU.
outletControlEnabled	Aplica-se apenas às rPDUs com chaveamento de tomada e determina se é possível controlar tomadas em uma rPDU com chaveamento de tomada. O valor "true" permite que as tomadas sejam controladas e o valor "false" evita que as tomadas sejam controladas.
outlet	A seção de tomada é relevante apenas às rPDUs com chaveamento de tomada e define as configurações de cada tomada da rPDU. A numeração de tomadas começa em 0 (a tomada número 1 da rPDU). Se essas configurações não exigirem alteração, será possível omitir as tomadas individuais (ou a seção Outlet na íntegra).
poaAction	Define o estado inicial da tomada quando ela é ligada ("on", "off" ou "last").
rebootHoldDelay	Tempo, em segundos, que a unidade aguarda depois que desliga a tomada e antes de ligá-la novamente durante uma reinicialização. É possível especificar qualquer número inteiro entre 0 e 14400.
rebootDelay	Tempo, em segundos, que a unidade aguarda para reinicializar uma tomada. É possível especificar qualquer número inteiro entre 0 e 14400.
poaDelay	Tempo, em segundos, que a unidade aguarda depois de ser ligada e antes de ligar a tomada. É possível especificar qualquer número inteiro entre 0 e 14400.
onDelay	Quanto tempo, em segundos, a unidade aguarda para ligar uma tomada. É possível especificar qualquer número inteiro entre 0 e 14400.
mode	Deve ter o valor "manual" para tomadas controladas pelo usuário.
offDelay	Quanto tempo, em segundos, a unidade aguarda para desligar uma tomada. É possível especificar qualquer número inteiro entre 0 e 14400.
label	O rótulo da tomada.
entity	A seção da entidade é usada para identificar medições não relacionadas à tomada na página sensors>overview.
total0 label	Rótulo do total da rPDU na página sensors>overview

breaker0 label	Rótulo do primeiro circuito (se houver). É possível identificar outros circuitos, se houver, como breaker1, breaker2 e assim por diante.
phase0 label	Rótulo da primeira fase. É possível identificar outras fases, se houver, usando phase1 e phase2.
line3 label	Rótulo da linha neutra.
alarm	A seção de alarme define os métodos que podem ser usados para enviar alarmes. Cada método é numerado a partir de 0 e define:
target	Para o envio de alarmes por trap SNMP, o destino pode ter os valores "trap0", "trap1" etc., o que indica os traps SNMP definidos como primeiro, segundo e assim por diante, na página System>SNMP. Para o envio de alarmes por e-mail, o destino pode ter os valores "email0", "email1" etc., o que indica o e-mail de destino definido como primeiro, segundo, e assim por diante, na página System>Email. O destino não deve especificar detecções de SNMP ou destinos de e-mail que não foram configurados.
delay	Determina por quanto tempo este evento deve permanecer ativado antes de enviar a primeira notificação desta ação.
repeat	Determina se várias notificações serão enviadas para esta ação de evento.
trigger	Essa seção define os alarmes que devem ser configurados, começando pelo primeiro, que é indicado com o número 0.
Path	Define a medição que ativará o alarme. O formato deste campo é: "0000000000000000/entity/phase0/measurement/0" define alarmes para medições de fase de entrada da rPDU, em que phase0 indica a primeira fase de entrada da rPDU, phase1 indica a segunda fase (se houver) e assim por diante. O número logo depois da medição indica o tipo de medição para acionar o alarme, conforme definido abaixo: 0: Tensão 4: Corrente 8: Potência real 9: Potência aparente 10: Fator de potência 11: Energia 14: Fator de pico da corrente "0000000000000000/outlet/0/measurement/0" define alarmes por tomada das rPDUs com monitoramento de tomada, em que o número logo depois da tomada especifica o número da tomada (começa em zero). O número logo depois da medição indica o tipo de medição para acionar o alarme, conforme definido abaixo:

	0: Tensão 4: Corrente 8: Potência real 9: Potência aparente 10: Fator de potência 11: Energia 12: Equilíbrio 14: Fator de pico da corrente "0000000000000000/entity/total0/measurement/0" define alarmes para medições totais de entrada da fase da rPDU. O número logo depois da medição indica o tipo de medição para acionar o alarme, conforme definido abaixo: 0: Potência real 1: Potência aparente 2: Fator de potência 3: Energia "0000000000000000/entity/breaker0/measurement/4" define alarmes para alarmes do circuito da rPDU, em que o primeiro circuito é indicado por breaker0, o segundo por breaker1 e assim por diante. O número logo depois da medição indica o tipo de medição para acionar o alarme, conforme definido abaixo: 4: Corrente "0000000000000000/entity/line3/measurement/4" define os alarmes de corrente neutra da rPDU. O número logo depois da medição indica o tipo de medição para acionar o alarme, conforme definido abaixo: 0: Corrente
severity	Pode ser "warning" ou "alarm", o que descreve a gravidade do alarme gerado.
type	Pode ser "high" ou "low", o que define se este limite é alto ou baixo.
threshold	O valor de limite pode ser qualquer número entre -999,0 e 999,0. É possível especificar a corrente de linha neutra com até duas casas decimais.
tripDelay	A medição deve exceder o limite por esse número de segundos para que o evento seja ativado. É possível especificar qualquer número inteiro entre 0 e 14400.

clearDelay	A medição deverá voltar ao normal por esse número de segundos para que o evento seja apagado e redefinido. É possível especificar qualquer número inteiro entre 0 e 14400.
latching	Pode ser verdadeiro ou falso. Se verdadeiro, o evento e suas ações associadas continuarão ativos até a confirmação do evento, mesmo que a medição seguinte volte ao normal.
selectedActions	Determina quais ações definidas acima serão usadas para enviar o alarme. ["0","1"] define as ações 0 e 1, que estão definidas como ações quem usam trap0 e email0 no exemplo anterior.

Apêndice G: Códigos de erro da API/CLI

G.1 Success

Código	Explicação
Success	Operação bem-sucedida

Erros de autenticação

Código	Explicação
No Admin user configured	No mínimo, um usuário Admin deve ser configurado no sistema
Not Authorized	O usuário atual não tem autorização
Not Authorized: Session expired	O token usado não é mais válido
Not Authorized: Not enough permissions	O usuário atual não tem permissões suficientes para executar a operação
Invalid credential combination	Tanto o nome de usuário/senha quanto o token foram inseridos, ou somente o nome de usuário ou a senha foi inserida
Must have at least one admin user	No mínimo, um usuário Admin deve ser configurado no sistema

Erros de formato JSON

Código	Explicação
Malformed JSON	O JSON recebido não é válido ou está incorreto
Missing field	Um arquivo esperado não foi encontrado na estrutura JSON
Duplicate fields	O mesmo campo foi definido várias vezes, por exemplo, no corpo HTTP e na string de consulta

Erros de caminho

Código	Explicação
Invalid path	O caminho inserido não segue os requisitos do sistema
Path not found	O caminho inserido não foi encontrado
Identifier not found	Um dos campos na estrutura JSON recebida não existe
Field not applicable	Existe um campo na estrutura JSON que não deve ter sido enviado

Erros de validação de dados

Código	Explicação
Invalid input	Um campo de entrada é inválido, mas não se enquadra em outras categorias de validação de dados
Input too long	Um campo de entrada excede o tamanho máximo permitido
Invalid characters	Um campo de entrada contém caracteres inválidos
Invalid serial	Um campo de entrada tem um número de série inválido
Invalid Boolean	Um campo de entrada é um valor booliano inválido
Out of range	Um campo de entrada está fora do intervalo válido
Invalid integer	Um campo de entrada não é um número inteiro, quando número inteiro era esperado
Invalid number	Um campo de entrada não é um número, quando um número era esperado
Invalid URL	Um campo de entrada não é um URL válido, quando URL era esperado
Invalid IP	Um campo de entrada não é um endereço IP válido, quando endereço IP era esperado
Paths not allowed	Um campo de entrada contém um caminho, mas isso não era esperado
Invalid username	Um campo de entrada é um nome de usuário não permitido
Invalid email address	Um campo de entrada não é um endereço de e-mail válido, quando endereço de e-mail era esperado
Invalid option	Um campo de entrada contém uma seleção de opção inválida
Invalid datetime	Um campo de entrada não é uma data ou hora válida, quando data/hora era esperada
Out of bounds	Um campo de entrada está fora dos limites permitidos
Invalid week	Um campo de entrada representa uma seleção inválida de dias da semana
Duplicate entry	Um campo de entrada criará uma duplicata, o que não é permitido
Invalid Route	Uma rota de rede estava configurada incorretamente

Outros erros

Código	Explicação
Unknown error	Houve um erro no sistema para o qual nenhum outro código de erro se aplica
Command not allowed	O comando recebido não é permitido no caminho especificado
System busy	Não é possível executar a tentativa de ação no momento. Tente novamente

Erros de consistência de dados

Código	Explicação
Inconsistent state	O comando fará com que o sistema fique inconsistente, portanto, ele será rejeitado
Syslog enabled requires target	Para ativar o syslog remoto, é necessário especificar um host de destino
NTP mode requires servers	Para ativar o NTP, é necessário ter servidores para consulta
Start time must come before end time	O horário está com o fim antes do início
Invalid SNMPv3 auth/priv combination	Não é possível usar a privacidade do SNMPv3 sem autenticação
Port not available	Houve uma tentativa de definir o número da porta como um número já em uso
Vertiv Intelligence Director missing credentials	A ativação do Vertiv Intelligence Director exige a definição de um nome de usuário e senha
Time not settable	Para configurar a data/hora, é necessário o modo de horário manual

Erros de carregamento

Código	Explicação
Invalid firmware package	O pacote está formatado incorretamente ou corrompido
Invalid file key	O pacote especifica uma chave OEM incorreta e não pode ser usado com esta unidade
Invalid version	A versão é muito antiga ou incompatível
Invalid product	O pacote foi criado para uma arquitetura de hardware diferente
Invalid certificate file	Não foi possível analisar o certificado SSL inserido
Invalid certificate password	A senha foi inválida com o certificado SSL fornecido

Esta página foi deixada intencionalmente em branco

Apêndice H: Exemplo de configuração de LDAP para credenciais do Active Directory

H.1 Visão geral

A integração do Active Directory com o Dispositivo de monitoramento intercambiável (IMD) das marcas Vertiv e Geist permite que os usuários façam a autenticação e a autorização na página da Web do IMD e na interface CLI usando as credenciais corporativas do Active Directory deles. O usuário também será autorizado em uma das três funções do IMD com base no grupo de segurança do Active Directory do qual ele for membro. As funções são estas:

- Admin: direitos completos de configuração, incluindo as permissões da função Control.
- Control: capacidade de controlar o estado da tomada, se aplicável, e de alterar nomes de dispositivos e configurações de alarmes/eventos.
- Enabled: somente leitura das configurações e nenhum direito de controle da tomada.

H.2 Requisitos e observações gerais

- É possível usar o IMD v5.3.3 ou um novo firmware neste procedimento.
- Os exemplos estão representados em verde.

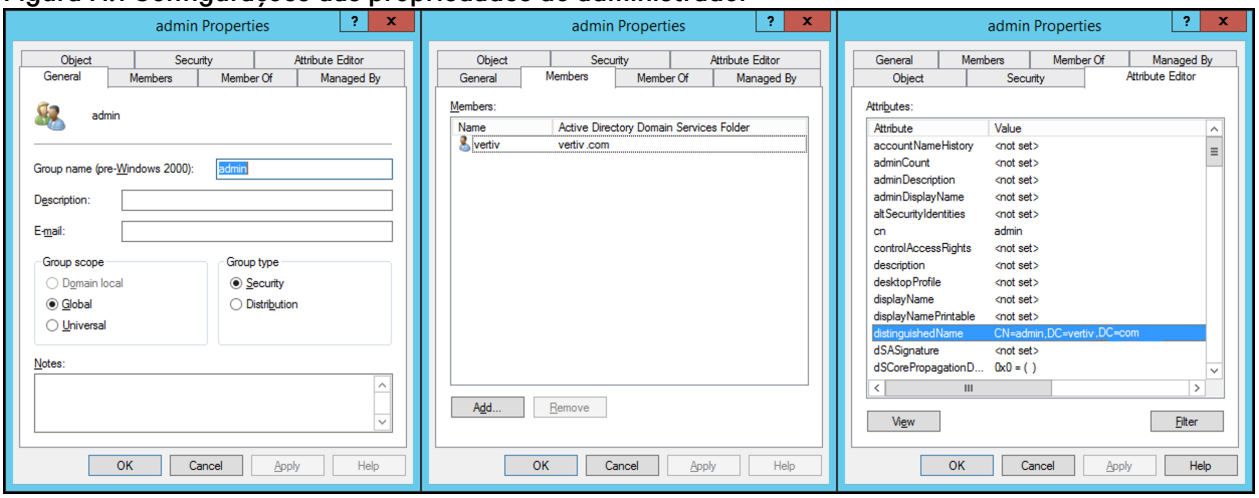
H.3 Procedimento de configuração do Active Directory

- Crie ou utilize uma conta de vinculação do AD existente para o IMD. O IMD usará essa conta para pesquisar o domínio do AD e autenticar usuários. A senha desta conta deve ser definida para nunca expirar.
- Crie um ou mais grupos de segurança do AD para representar as funções Admin, Control e Enabled do IMD.
- Torne o usuário do AD um membro do grupo de segurança relevante.
    - A conta do AD “vertiv” atribuiu um membro do grupo de segurança “admin” no exemplo mostrado abaixo. Como resultado, a conta de usuário “vertiv” do AD assumirá a função Admin do IMD após o login.

NOTA: A nomenclatura do grupo de segurança fica a seu critério. O nome e o DN do grupo de segurança devem corresponder aos que foram definidos na seção “Group” do LDAP do IMD.

NOTA: Um usuário do AD que pertencer a mais de um desses grupos de segurança mapeados por função do IMD herdará os privilégios da função mais alta.

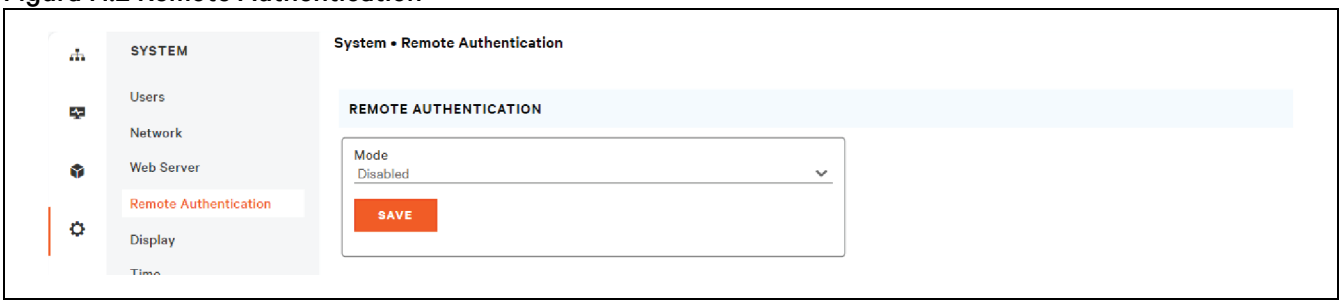
Figura H.1 Configurações das propriedades do administrador



H.4 Procedimento de configuração do IMD (interface da Web)

- Abra um navegador da Web com o IP ou o nome DNS do IMD e faça login usando a conta de administrador local.
- Navegue até *System > Remote Authentication*.
- Defina o modo de autenticação remota como LDAP e salve.

Figura H.2 Remote Authentication



- Consulte a ilustração abaixo para ver as descrições das configurações da seção LDAP.

Figura H.3 Configuração de LDAP

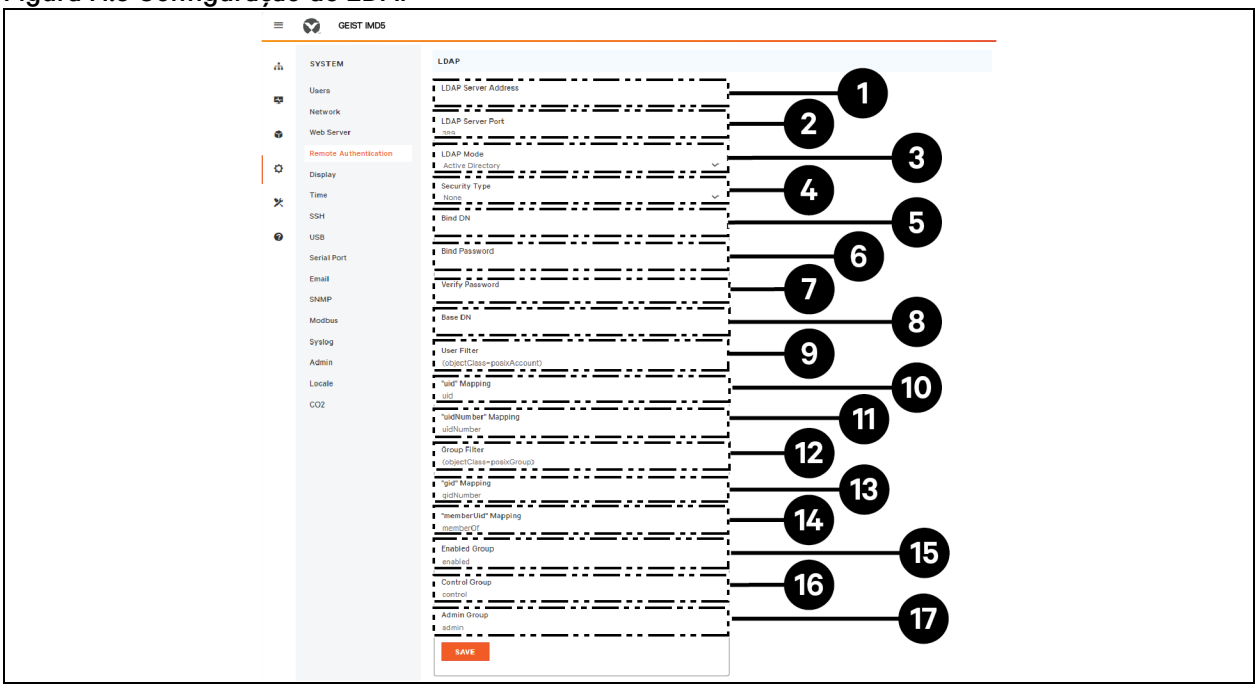


Tabela H.1 Configuração de LDAP

Item	Descrição
1	Endereço IP do servidor Active Directory
2	Porta TCP do Active Directory[2] 389 - Não SSL 636 - SSL
3	Modo LADAP OpenLDAP - Active Directory
4	Segurança do Active Directory[2] None - SSL - StartTLS
5	Conta do AD usada para vinculação com o servidor AD Deve ser representado como notação de caminho completo do DN CN=adbindacct,CN=Users,DC=vertiv,DC=com A senha da conta não deve expirar
6	Definir senha da conta de vinculação do AD
7	Verificar senha
8	Caminho do domínio de base para pesquisar usuários do AD[1] Deve ser representado como notação de caminho completo do DN DC=vertiv, DC=com
9	Filtro do atributo ObjectClass do usuário do AD (objectClass=user)

Tabela H.1 Configuração de LDAP (continuação)

Item	Descrição
10	Filtro de nome da conta do usuário do AD samaccountname
11	Mapeamento "uidNumber" uidNumber
12	Filtro do atributo ObjectClass do grupo do AD (objectClass=group)
13	Mapeamento "gid" gidNumber
14	Configuração obrigatória memberOf
15	Mapear grupo de segurança do AD para a função Enabled Deve ser representado como notação de caminho completo do DN CN=enabled, DC=vertiv, DC=com
16	Mapear grupo de segurança do AD para a função Control Deve ser representado como notação de caminho completo do DN CN=control, DC=vertiv, DC=com
17	Mapear grupo de segurança do AD para a função Admin Deve ser representado como notação de caminho completo do DN CN=admin, DC=vertiv, DC=com
NOTA: [1]A prática recomendada é reduzir o escopo da passagem do domínio do AD para procurar usuários autenticados. Evite especificar apenas o domínio de base quando houver uma esquema do AD grande e aninhado. • Ideal: OU=Enabled Users, OU=User Accounts, DC=vertiv, DC=com • Não é ideal: DC=vertiv, DC=com	
NOTA: [2]StartTLS usa a porta TCP 389. Inicialmente, isso estabelece a sessão sem criptografia, mas ela será criptografada a partir deste ponto se a solicitação LDAP_START_TLS_OID for aceita pelo servidor do Active Directory.	

Siga a Vertiv nas redes sociais

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

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

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

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

Vertiv.com | Sede da Vertiv, 505 N Cleveland Ave, Westerville, OH, 43082, USA

SL-71211_REVA_04-24