

Guia do usuário

Placa de gerenciamento de rede do no-break

AP9630, AP9631



This manual is available in English on the APC Web site (www.apc.com).

Dieses Handbuch ist in Deutsch auf der APC Webseite (www.apc.com) verfügbar.

Este manual está disponible en español en la página web de APC (www.apc.com).

Ce manuel est disponible en français sur le site internet d'APC (www.apc.com).

Questo manuale è disponibile in italiano sul sito web di APC (www.apc.com).

Este manual está disponível em português no site da APC (www.apc.com).

Данное руководство на русском языке доступно на сайте APC (www.apc.com)

本マニュアルの日本語版は APC ウェブサイト (www.apc.com) からダウンロードできます。

在 APC 公司的网站上 (www.apc.com) 有本手册的中文版。

APC 웹사이트 (www.apc.com) 에 한국어 매뉴얼 있습니다 .

This manual is available in English on the enclosed CD.

Dieses Handbuch ist in Deutsch auf der beiliegenden CD-ROM verfügbar.

Este manual está disponible en español en el CD-ROM adjunto.

Ce manuel est disponible en français sur le CD-ROM ci-inclus.

Questo manuale è disponibile in italiano nel CD-ROM allegato.

Este manual está disponível em português no CD fornecido.

Данное руководство на русском языке имеется на прилагаемом компакт-диске.

本マニュアルの日本語版は同梱の CD-ROM からご覧になれます。

동봉된 CD 안에 한국어 매뉴얼이 있습니다 .

您可以从包含的 CD 上获得本手册的中文版本。

Introdução

Descrição do Produto

Recursos

As duas placas de gerenciamento de rede (NMC) de no-break da Schneider Electric mencionadas abaixo são produtos baseados na Web e prontos para IPv6. Elas podem gerenciar dispositivos compatíveis usando vários padrões abertos tais como:



HTTP (Hypertext Transfer Protocol)
SNMPv1, SNMPv3 (Simple Network Management Protocol) versões 1 e 3
FTP (File Transfer Protocol)
Telnet
RADIUS

SSH (Secure SHell)
HTTPS - HTTP (Hypertext Transfer Protocol) em conjunto com SSL (Secure Sockets Layer)
SCP (Secure Copy)
Syslog

A placa de gerenciamento de rede **AP9630 2**:

- Fornece recursos de agendamento de autoteste e controle do no-break.
- Fornece logs de dados e eventos.
- Possibilita que você configure notificações por meio de logs de eventos, e-mail e traps de SNMP.
- Fornece suporte ao Desligamento de rede do PowerChute®.
- É compatível com o uso de um servidor com protocolo de configuração de host dinâmico (DHCP, Dynamic Host Configuration Protocol) ou protocolo BOOTstrap (BOOTP) para fornecer os valores de rede (TCP/IP) da NMC.
- Permite utilizar o serviço de monitoração remota (RMS, Remote Monitoring Service).
- Permite exportar um arquivo de configuração do usuário (.ini) a partir de uma placa configurada para uma ou mais placas não configuradas sem converter o arquivo em binário.
- Fornece uma seleção de protocolos de segurança para autenticação e criptografia.
- Comunica-se com o StruxureWare Central ou com o InfraStruXure Manager.

A placa de gerenciamento de rede **AP9631** inclui todos os recursos da placa de gerenciamento de rede AP9630 e também os seguintes:

- Fornece duas portas USB, que dão suporte ao upgrade do firmware.
- Dá suporte a duas portas universais de entrada/saída às quais você pode conectar:
 - Sensores de temperatura (AP9335T) ou de temperatura/umidade (AP9335TH)
 - Conectores de entrada/saída de relés que dão suporte a dois contatos de entrada e um relé de saída (usando o acessório de E/S de contato seco AP9810, que é um complemento opcional)

Dispositivos nos quais é possível instalar a placa de gerenciamento de rede 2. A NMC pode ser instalada em:

- Qualquer modelo Smart-UPS® que tenha um slot de expansão interno, ou qualquer no-break Symmetra® exceto os no-breaks Symmetra PX 250 e Symmetra PX 500
- MGE® Galaxy® 300, 3500 ou 7000
- Chassi de expansão (AP9600)
- Triplo chassi de expansão (AP9604)

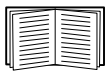
Configuração inicial de IPv4

Você deve definir duas configurações de TCP/IP para a NMC antes que ela possa ficar em operação na rede:

- O endereço IP da NMC
- O endereço IP do gateway padrão (necessário apenas se você vai sair do segmento)



Cuidado: Não use o endereço de auto-retorno (127.0.0.1) como gateway padrão. Isso desativará a placa. Em seguida, você deve fazer logon utilizando uma conexão serial e redefinir as configurações de TCP/IP aos seus padrões.



Para fazer as configurações de TCP/IP, consulte o *Manual de Instalação* da placa de gerenciamento de rede, disponível no CD de *utilitários* da placa de gerenciamento de rede, no [site da APC](#) e na forma impressa.

Para obter informações detalhadas sobre a utilização de um servidor DHCP para fazer as configurações de TCP/IP em uma NMC, consulte “Opções de resposta do DHCP”.

Configuração inicial de IPv6

A configuração de rede IPv6 dá flexibilidade para acomodar suas necessidades. O IPv6 pode ser usado em qualquer local em que for inserido um endereço IP nesta interface. Você pode configurar de modo manual, automático ou com DHCP, consulte “Tela Configurações de TCP/IP para IPv6”.

Gerenciamento de rede com outros aplicativos

Esses aplicativos e utilitários funcionam com um no-break conectado à rede por meio da NMC.

- Desligamento de rede com o PowerChute — Proporciona um desligamento remoto normal, sem necessidade de monitoramento, dos computadores conectados a dispositivos de no-break
- PowerNet® Management Information Base (MIB) com um navegador MIB padrão — Realiza SETs e GETs de SNMP e usa traps de SNMP.
- StruxureWare Central — Fornece gerenciamento de energia de nível corporativo e gerenciamento de agentes, dispositivos de no-break e monitores ambientais.
- Utilitário de configuração do IP do dispositivo — Faz as configurações básicas de uma ou mais NMCs via rede, consulte “Utilitário de Configuração do IP do Dispositivo”.
- Assistente de segurança — Cria os componentes necessários para auxiliar com a segurança da NMC quando estiver utilizando SSL (Secure Sockets Layer, camada de soquetes seguros), protocolos relacionados e rotinas de criptografia.

Recursos de gerenciamento interno

Visão geral

Use a interface de usuário (UI) da Web ou a interface de linha de comando (CLI) para exibir o status do no-break e gerenciar o no-break e a NMC. Você pode também usar o SNMP para monitorar o status do no-break.



Para obter mais informações sobre UIs, consulte “Interface do usuário da Web” e o guia da interface da linha de comando (CLI) no CD de *Utilitários* da placa de gerenciamento de rede e no [site da APC](#). Consulte “Telas SNMP” para obter informações sobre o controle de acesso do SNMP à NMC.

Prioridade de acesso para fazer logon

Você pode ativar mais de um usuário para fazer logon ao mesmo tempo, onde cada usuário tenha acesso igual. Consulte “Tela Gerenciamento de sessão”.

Tipos de contas de usuário

A NMC tem vários níveis de acesso — Administrador, Usuário de dispositivos, Usuário somente leitura e Usuário somente rede — que são protegidos pelos requisitos de nome de usuário e senha.

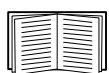
- Um **Administrador** ou superusuário pode utilizar todos os menus na UI e todos os comandos na interface de linha de comando. O padrão para nome de usuário e senha é `apc`.
- Um **Usuário de dispositivos** tem acesso de leitura e gravação às telas relacionadas com o dispositivo. As funções administrativas, como o gerenciamento de sessões, no menu Segurança e no Firewall em Logs ficam desativadas (em cinza).

O nome de usuário padrão é `device` e a senha padrão é `apc`.

- Um **Usuário somente leitura** tem o seguinte acesso restrito:
 - Acesso somente por meio da UI.
 - Acesso aos mesmos menus que o Usuário de dispositivos acima, mas sem poder alterar configurações, controlar dispositivos, excluir dados nem usar opções de transferência de arquivos. Os links para as opções de configuração ficam visíveis, mas desativados. (Os Logs de dados e eventos não exibem nenhum botão para que esse usuário possa apagar o log.)

O nome de usuário padrão é `readonly` e a senha padrão é `apc`.

- Um **Usuário somente rede** só pode fazer logon usando a interface de usuário (UI) da Web e a CLI (telnet não serial). Não há nome e senha padrão.



Para configurar os valores de **Nome de usuário** e **Senha** para os três tipos de conta, consulte “Usuários locais”.

Como recuperar após perder uma senha

Você pode usar um computador local que se conecta à NMC pela porta serial para acessar a interface da linha de comando.

1. Selecione uma porta serial no computador local e desative todos os serviços que usam essa porta.
2. Conecte o cabo serial fornecido (número de peça 940-0299) à porta selecionada no computador e à porta de configuração na NMC.
3. Execute um programa do tipo terminal (por exemplo, o Hyperterminal[®]) e configure a porta selecionada para 9600 bps, 8 bits de dados, sem paridade, 1 bit de parada e sem controle de fluxo.
4. Pressione ENTER (várias vezes, se necessário) para exibir o prompt **User Name** (Nome de usuário). Se não for possível exibir o prompt **User Name**, verifique o seguinte:
 - Se a porta serial não está sendo utilizada por outro aplicativo.
 - Se as configurações do terminal estão corretas, conforme especificado na etapa 3.
 - Se está sendo utilizado o cabo correto, conforme especificado na etapa 2.
5. Pressione o botão **Reset** (Redefinir). O LED de Status piscará alternadamente com as cores laranja e verde. Pressione o botão **Reset** uma segunda vez, enquanto o LED estiver piscando, para redefinir temporariamente o nome de usuário e a senha aos seus padrões.
6. Pressione ENTER (várias vezes se necessário) para voltar a exibir o prompt **User Name**. Em seguida, utilize o padrão, **apc**, para nome de usuário e senha. (Se você demorar mais de 30 segundos para fazer logon, depois que o prompt **User Name** for exibido novamente, será necessário repetir a etapa 5 e fazer logon outra vez).
7. Na interface de linha de comando, use os seguintes comandos para alterar a configuração de **Password** (Senha), que neste estágio está configurada como **apc**:

```
user -n <nome do usuário> -pw <senha do usuário>
```

Por exemplo, para alterar a senha para **XYZ**, digite:

```
user -n apc -pw XYZ
```

No caso de superusuário, deve-se especificar também a senha atual; para isso, digite:

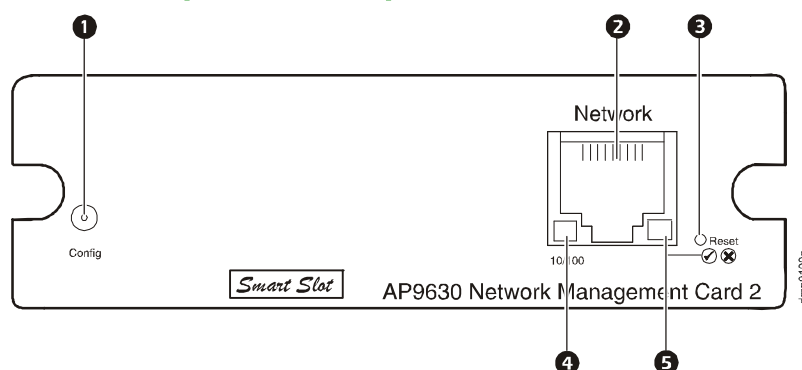
```
user -n <nome do usuário> -cp <senha atual> -pw <senha do usuário>
```

Por exemplo, para alterar a senha de um superusuário para **XYZ** (do nome de usuário e senha padrão **apc**), digite:

```
user -n apc -cp apc -pw XYZ
```

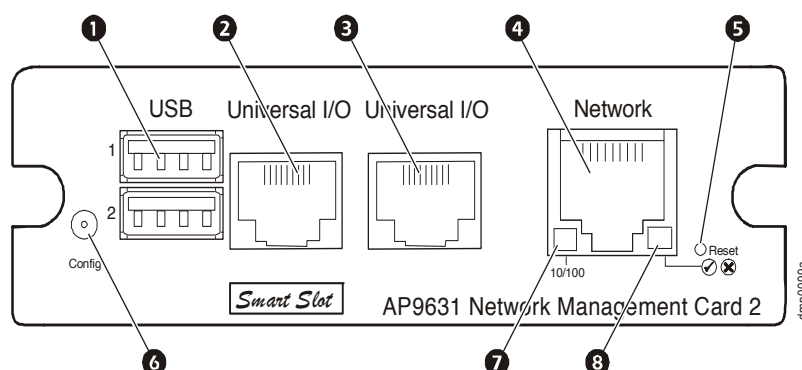
8. Digite **quit** ou **exit** para fazer logoff, conecte novamente os cabos seriais que foram desconectados e reinicie os serviços desativados.

Painel dianteiro (AP9630)



	Item	Descrição
1	Porta serial para configuração	Conecta a NMC a um computador local para ajustar as configurações iniciais da rede ou acessar a interface de linha de comando (CLI).
2	Conector 10/100 Base T	Conecta a NMC à rede Ethernet.
3	Botão Redefinir	Redefine a NMC enquanto mantém o fornecimento de energia.
4	LED Link–RX/TX (10/100)	Consulte “LED Link–RX/TX (10/100)”.
5	LED de status	Consulte “LED Status”.

Painel dianteiro (AP9631)



	Item	Descrição
1	Portas USB	Dá suporte a upgrades de firmware da NMC, consulte “Transferências de arquivos”.
2	Portas dos sensores	Conectar sensores de temperatura, sensores de temperatura/umidade ou conectores de entrada/saída de relés que suportem dois contatos de entrada e um relé de saída.
3		
4	Conector 10/100 Base T	Conecta a NMC à rede Ethernet.
5	Botão Reinicializar	Reinicializa (redefine) a NMC mantendo a alimentação de energia.
6	Porta serial para configuração	Conecta a NMC a um computador local para ajustar as configurações iniciais da rede ou acessar a interface de linha de comando (CLI).
7	LED Link–RX/TX (10/100)	Consulte “LED Link–RX/TX (10/100)”.
8	LED de status	Um LED (diodo emissor de luz) é uma fonte de luz. Consulte “LED Status”.

Descrições dos LEDs

LED Status

Esse LED (diodo emissor de luz) indica o status da NMC.

Condição	Descrição
Apagado	Ocorre uma das seguintes situações: <ul style="list-style-type: none">• A NMC não está recebendo potência de entrada.• A NMC não está funcionando corretamente. Poderá ser necessário repará-la ou substituí-la. Entre em contato com o Serviço de Atendimento ao Cliente. Consulte “Atendimento mundial ao cliente da APC”.
Verde aceso	A NMC possui configurações de TCP/IP válidas.
Laranja aceso	O hardware da NMC não está funcionando como esperado. Entre em contato com o Serviço de Atendimento ao Cliente. Consulte “Atendimento mundial ao cliente da APC”.
Verde piscando	A NMC não possui configurações de TCP/IP válidas. ¹
Laranja piscando	A NMC está fazendo solicitações de BOOTP. ¹
Piscando alternadamente em verde e laranja	Se o LED estiver piscando lentamente, a NMC está fazendo solicitações de DHCP ^{2, 1} . Se o LED estiver piscando rapidamente, a NMC está inicializando.
<p>1. Se você não usa um servidor BOOTP ou DHCP, consulte o Manual de instalação da placa de gerenciamento de rede, fornecido em formato impresso e no CD de <i>Utilitários</i> da placa de gerenciamento de rede em PDF, para fazer as configurações de TCP/IP da NMC.</p> <p>2. Para usar um servidor DHCP, consulte “Opções de resposta do DHCP”.</p>	

LED Link–RX/TX (10/100)

Este LED indica o status de rede da NMC.

Condição	Descrição
Desativado	Ocorrem uma ou mais das seguintes situações: <ul style="list-style-type: none">• A NMC não está recebendo potência de entrada.• O cabo que conecta a NMC à rede está desconectado ou defeituoso.• O dispositivo que conecta a NMC à rede está desligado ou não está funcionando corretamente.• A NMC não está funcionando corretamente. Poderá ser necessário repará-la ou substituí-la. Entre em contato com o Serviço de Atendimento ao Cliente. Consulte “Atendimento mundial ao cliente da APC”.
Verde aceso	A NMC está conectada a uma rede operando a 10 Megabits por segundo (Mbps).
Laranja aceso	A NMC está conectada a uma rede operando a 100 Mbps.
Verde piscando	A NMC está recebendo ou transmitindo pacotes de dados a 10 Mbps.
Laranja piscando	A NMC está recebendo ou transmitindo pacotes de dados a 100 Mbps.

Recursos de monitoramento

Visão geral

Para detectar problemas internos e se recuperar de entradas não esperadas, a NMC usa mecanismos internos de monitoramento em todo o sistema. Quando ela reinicia para recuperar-se de um problema interno, um evento **Sistema: interface de rede reiniciada** é registrado no log de eventos.

Mecanismo de monitoramento da interface de rede

A NMC implementa mecanismos internos de monitoramento para se proteger de modo a não ficar inacessível pela rede. Por exemplo, se a NMC não receber nenhum tráfego de rede durante 9,5 minutos (tanto tráfego direto, como SNMP, ou tráfego de radiodifusão, como uma solicitação do protocolo de resolução de endereços (ARP, [Address Resolution Protocol])), ela considerará que existe um problema na interface de rede e reinicializará.

Redefinição do temporizador de rede

Para assegurar que a NMC não se reinicialize se a rede ficar inativa durante 9,5 minutos, a NMC tenta entrar em contato com o gateway padrão a cada 4,5 minutos. Se o gateway estiver presente, ele responderá à NMC e essa resposta reiniciará o temporizador de 9,5 minutos. Se o seu aplicativo não requer ou não tem um gateway, especifique o endereço IP de um computador que esteja em execução na rede e esteja na mesma sub-rede. O tráfego de rede desse computador reiniciará o temporizador de 9,5 minutos com frequência suficiente para evitar a reinicialização da NMC.

Interface do usuário da Web

Introdução

Visão geral

A interface do usuário (UI) da Web oferece opções de gerenciamento do no-break e da placa de gerenciamento de rede 2 (NMC) do no-break e de visualização de status do no-break.



Consulte “Tela Acesso à Web” para obter informações sobre como selecionar, ativar e desativar os protocolos que controlam o acesso à UI e definir as portas do servidor da Web para os protocolos.

Navegadores da Web compatíveis

Você pode usar o Microsoft® Internet Explorer® (IE) 7.x ou superior (somente nos sistemas operacionais Windows®) ou Mozilla® Firefox® 3.0.6 ou superior (em todos os sistemas operacionais) para acessar a NMC por sua UI. Outros navegadores comumente disponíveis talvez funcionem, mas eles não foram totalmente testados.

A NMC não funciona com um servidor proxy. Para que você possa usar um navegador para acessar a UI da NMC, deve fazer o seguinte:

- Configurar o navegador para desativar o uso de um servidor proxy para a NMC.
- Configurar o servidor proxy de modo que ele não substitua o endereço IP específico da NMC.

Como fazer login

Visão geral

Você pode usar o nome DNS ou o endereço IP do sistema da NMC como endereço URL da UI. Ao fazer login diferencie maiúsculas de minúsculas no nome de usuário e na senha. O nome de usuário padrão varia dependendo do tipo da conta:

- `apc` para administrador
- `device` para um usuário de dispositivos
- `readonly` para um usuário somente leitura

A senha padrão é `apc` para todos esses três tipos de conta. Não há padrão para um tipo de conta Somente rede. Veja também “Tipos de contas de usuário”.

Você pode configurar o idioma de sua UI ao fazer login selecionando um idioma na caixa suspensa **Idioma**. Consulte “Adição e alteração de pacotes de idiomas”.



Quando HTTPS estiver ativado, a NMC gera seu próprio certificado. Esse certificado negocia métodos de criptografia com seu navegador. Consulte o Guia de segurança no CD ou no site www.apc.com para obter mais detalhes.

Formatos de endereços URL

Digite o nome DNS ou o endereço IP da NMC no campo do endereço URL do navegador da Web e pressione ENTER. Quando você especifica no Internet Explorer uma porta não padrão do servidor da Web, deve incluir `http://` ou `https://` na URL.

Mensagens de erro comuns do navegador ao fazer login.

Mensagem de erro	Navegador	Causa do erro
“Esta página não pode ser exibida.”	Internet Explorer	O acesso à Web está desativado ou a URL não estava correta.
“Não é possível conectar-se.”	Firefox	

Exemplos de formato de URL. Veja também “Tela Configurações de TCP/IP para IPv6”.

Exemplo e modo de acesso	Formato URL
Nome DNS de Web1	
HTTP	http://Web1
HTTPS	https://Web1
Endereço IP do sistema de 139.225.6.133 e um padrão Porta do servidor da Web (80)	
HTTP	http://139.225.6.133
HTTPS	https://139.225.6.133
Endereço IP do sistema de 139.225.6.133 e um não padrão Porta do servidor da Web (5000)	
HTTP	http://139.225.6.133:5000
HTTPS	https://139.225.6.133:5000
Endereço IPv6 do sistema de 2001:db8:1::2c0:b7ff:fe00:1100 e uma porta não padrão do servidor da Web (5000)	
HTTP	http:// [2001:db8:1::2c0:b7ff:fe00: 1100]:5000




Tela Início

Visão geral

Caminho: Início

Na tela **Início** da interface, você pode exibir alarmes ativos e os eventos mais recentes, registrados no Log de eventos.


Um ou mais ícones e o texto que os acompanha indicam o status de operação atual do no-break:


Símbolo	Descrição
	Sem alarmes: Não existe nenhum alarme e o no-break e a NMC estão funcionando normalmente.
	Aviso: uma condição de alarme requer atenção e poderá comprometer os dados ou equipamentos se sua causa não for tratada.
	Crítico: existe um alarme crítico que exige ação imediata.

No canto superior direito de cada tela, os mesmos ícones relatam o status do no-break. Se existir algum alarme **Crítico** ou **Aviso**, o número de alarmes ativos também é exibido.

Para exibir todo o Log de eventos, clique em **Mais eventos**.

Ícones e links

Para transformar qualquer tela em tela de “Início” (isto é, a tela exibida em primeiro lugar quando você faz logon), acesse essa tela e clique no ícone  localizado acima, à direita.

Clique em  para inverter e exibir a tela Início quando você faz logon.

No canto inferior esquerdo de cada tela da interface, existem três links configuráveis para sites úteis. Por padrão, os links acessam as URLs para estas páginas da Web:

- Link 1: a página **Base de conhecimento** de www.apc.com com informações úteis de solução de problemas.
- Link 2: a página **Informações do produto** de www.apc.com com informações secundárias sobre seu hardware
- Link 3: a página **downloads** de www.apc.com com firmware e software úteis.



Para reconfigurar os links, consulte “Tela Configurar links”.

Monitoramento do no-break: Menu Status

As opções do menu Status relatam o estado atual do seu no-break e da rede.



Você pode configurar seu no-break e a rede usando as opções do menu Configuração. Consulte “Ajuste das configurações: 1” e “Ajuste das configurações: 2”.

Consulte as seguintes seções:

- “No-break no menu Status”
- “Grupos de tomadas no menu Status”
- “Sistema de bateria no menu de Status”
- “E/S Universal no menu Status”
- “Rede no menu Status”

No-break no menu Status

Caminho: Status > No-break

Apresenta a carga do no-break, a carga da bateria, a tensão e outras informações úteis.

Campo	Descrição
Última transferência de bateria	A causa da última mudança para operação no modo de bateria.
Temperatura interna	A temperatura dentro do no-break
Tempo de funcionamento restante	Quanto tempo o no-break pode usar a energia da bateria para alimentar sua carga atual.
Entrada do no-break	
Tensão de entrada	A tensão de corrente alternada (VCA) que está sendo recebida pelo no-break.
Tensão de entrada de bypass	A tensão de corrente alternada (VCA) usada quando o no-break estiver no modo de bypass. Esta opção não está disponível para todos os dispositivos de no-break.
Saída do no-break	
Tensão de saída	A tensão de corrente alternada (VCA) que o no-break está fornecendo a sua carga.
Corrente da carga	A corrente, em Amps, fornecida pela tensão de entrada.
Carga de saída	A carga colocada em cada fase pelo equipamento conectado, em kVA.
Carga percentual de saída	A carga colocada em cada fase pelo equipamento conectado, na forma de percentual dos kVA disponíveis sem redundância.
Potência percentual de saída	A carga colocada em cada fase pelo equipamento conectado, na forma de percentual dos kVA disponíveis.
Watts de saída	A carga do no-break na forma de percentual de Watts disponíveis.
VA de saída	A carga do no-break na forma de percentual de VA disponíveis.
Eficiência de saída	O percentual de alimentação de entrada que vai diretamente para fora da carga. A alimentação de entrada que não vai para a carga é consumida pelo no-break.

Campo	Descrição
Uso da energia de saída	A energia usada pela carga, iniciando no momento em que o no-break foi redefinido pela última vez para os padrões.
Status da bateria	
Capacidade da bateria	O percentual de capacidade de bateria do no-break disponível para dar suporte ao equipamento conectado.
Tensão da bateria	A tensão CC das baterias.
Baterias externas	O número de baterias conectado ao no-break, excluindo qualquer bateria interna.



As opções abaixo não estão disponíveis para todos os dispositivos de no-break.

Campo	Descrição
Tensão nominal da bateria	A capacidade nominal de tensão das baterias do no-break; a tensão CC que as baterias têm capacidade nominal para fornecer quando o no-break utiliza sua bateria para alimentação de saída.
Tensão real do barramento da bateria	A alimentação CC disponível.
Classificação do gabinete de bateria externo	A corrente nominal em ampère-hora do gabinete de bateria de uma fonte de bateria externa.
Baterias	O número total de baterias (internas e externas) do no-break
Baterias com falhas	O número de baterias “defeituosas” (baterias que precisam ser trocadas).
Corrente da bateria	A corrente de saída da bateria.
Data da próxima substituição da bateria	Dentre os cartuchos de bateria do no-break instalados, esta é a primeira data recomendada para substituir as baterias.
Módulo de inteligência	Informações sobre o Módulo de inteligência. Talvez lhe solicitem essas informações (Revisão de firmware, Data de fabricação, Número de série e Revisão de hardware) quando você procurar assistência do Serviço de Atendimento ao Cliente da APC.
Tensão de entrada	A tensão de corrente alternada (VCA) que está sendo recebida pelo no-break.
Tensão de entrada de bypass	A tensão de corrente alternada (VCA) usada quando o no-break estiver no modo de bypass.
Frequência de entrada	A frequência em Hertz (Hz) da tensão que está sendo recebida pelo no-break.
Frequência	A frequência em Hertz (Hz) compartilhada pela tensão de entrada e pela tensão de saída.
Frequência de bypass	A frequência em Hertz (Hz) da tensão usada quando o no-break estiver no modo de bypass.
Corrente de saída	A corrente, em Amps, aplicada à carga.
Frequência de saída	A frequência em Hertz (Hz) da tensão de saída.
Potência da carga	A carga do no-break na forma de percentual de Watts disponíveis.
Potência da carga aparente	A carga do no-break na forma de percentual de VA disponíveis.
Módulos	Informações sobre os módulos instalados no no-break. Talvez lhe solicitem essas informações (Revisão de firmware, Data de fabricação, Número de série e Revisão de hardware) quando você procurar assistência do Serviço de Atendimento ao Cliente da APC.

Campo	Descrição
Módulo de potência	Informações sobre o módulo de alimentação instalado no no-break. Talvez lhe solicitem essas informações quando você procurar assistência do Serviço de Atendimento ao Cliente da APC.

Grupos de tomadas no menu Status

Caminho: Status > Grupos de tomadas

Esta opção não está disponível para todos os dispositivos de no-break. Ela exibe detalhes de status de todos os grupos de tomadas em seu no-break. Consulte também “Grupos de tomadas no menu Controle” e “Grupos de tomadas no menu Configuração”

Sistema de bateria no menu de Status

Caminho: Status > Sistema de bateria



Esta opção não está disponível para todos os dispositivos de no-break

Campo	Descrição
Status do sistema de bateria	
Estado da carga	O percentual de capacidade de bateria do no-break disponível para dar suporte ao equipamento conectado.
Tempo de funcionamento restante	Quanto tempo o no-break pode usar a energia da bateria para alimentar sua carga atual.
Tensão do barramento positivo/Tensão do barramento negativo:	O dispositivo de no-break tem suporte para ambas as tensões da bateria, positiva e negativa.
SKU do cartucho da bateria de reposição	O número da peça que deve ser fornecido para um cartucho de bateria de reposição.
Status do battery pack	
Battery Pack 1, 2...	O número do Battery pack proveniente do método de numeração interno.
Número de série	O número de série do Battery pack.
Integridade	Contém todos os erros do sistema do Battery pack, inclusive os erros dos cartuchos individuais. Os erros são registrados como eventos.
Status	O status do Battery pack, inclusive o status dos cartuchos individuais. Além de OK, este valor pode estar sinalizando que a bateria está próxima ao fim da vida útil ou que a vida útil da bateria foi excedida para o conjunto. Os erros são registrados como eventos.

Clique em Battery pack 1,2... para acessar a página da tela **Battery Pack n**.

Campo	Descrição
Battery Pack 1, 2... ou pack interno	

Campo	Descrição
Número de série (se existir)	O número de série do Battery pack.
Revisão do firmware	O número da revisão do Battery pack.
Temperatura	A temperatura, conforme relatada pelo sensor no compartimento da bateria.
Status do pacote	Somente erros do battery pack, não incluindo os erros dos cartuchos individuais. Os erros são registrados como eventos e podem ser: <ul style="list-style-type: none"> • temperatura fora do intervalo • erros gerais • erros de comunicação • uma estrutura de pacote desconectado • o firmware é incompatível com o hardware
Cartucho de bateria 1 e Cartucho de bateria 2 (caso esteja presente)	
Integridade	Pode ser OK, bateria próxima ao fim da vida útil, vida útil da bateria excedida, ou vida útil da bateria medida excedida para o cartucho. Os erros são registrados como eventos.
Data da instalação	A data em que os cartuchos individuais foram instalados. Esta data pode ser editada.
Data de reposição prevista	O no-break calcula quando a bateria deverá ser substituída. O campo Integridade acima provém desta data.
Status	Específico para o cartucho. Consulte “Status do pacote” acima para obter os erros gerais do pacote. Os erros são registrados como eventos e podem ser: <ul style="list-style-type: none"> • cartucho desconectado • o cartucho precisa de substituição • temperatura do cartucho muito alta: crítico • temperatura do cartucho muito alta: aviso. Esse aviso geralmente é exibido antes do aviso crítico acima, mas nem sempre.

E/S Universal no menu Status

Caminho: Status > E/S Universal

Esta opção não está disponível para todos os dispositivos de no-break.

Temperatura e Umidade exibe o nome, status do alarme, temperatura e a umidade (se houver suporte) para cada sensor. Clique no nome de um sensor para editar o nome e a localização e configurar seus limites e sua histerese. Consulte “Tela Temperatura e umidade” para obter mais detalhes.

Contatos de entrada exibe o nome, o status do alarme e o estado (aberto ou fechado) de cada contato. Eles serão automaticamente encontrados e exibidos aqui quando o acessório ambiental estiver instalado. Clique o nome de um contato de entrada para ver o status detalhado ou configurar seus valores. Se os contatos estiverem configurados e desativados, eles não são exibidos aqui. Consulte “Tela Temperatura e umidade” para obter mais detalhes.

Relé de saída exibe o nome e o estado (aberto ou fechado) de cada relé. Eles serão automaticamente encontrados e exibidos aqui quando o acessório ambiental estiver instalado. Clique o nome de um contato de entrada para ver o status ou configurar seus valores. Consulte “Tela Relé de saída” para obter mais detalhes.

Eventos ambientais recentes exibe eventos relacionados ao seu monitoramento ambiental, por exemplo uma violação de limite de temperatura ou uma advertência sobre um contato de entrada do monitor ambiental. Clique no link Mais eventos para ver uma lista completa de eventos recentes.

Rede no menu Status

Caminho: Status > Rede

A tela Rede apresenta seu IP, nome de domínio e configurações da porta ethernet. Consulte “Rede no menu Configuração” para obter detalhes secundários sobre os campos.

Controle do no-break e a segurança

As opções do menu Controle permitem executar ações imediatas que afetem o no-break e as tomadas e também têm algumas funções de segurança e de rede. Estas opções podem ser aplicadas a dispositivos de no-break individuais e a um grupo de controle sincronizado (SCG), se ativado. Consulte “Controle sincronizado dos dispositivos de no-break”.



Esta opção não está disponível para todos os dispositivos de no-break.

Consulte as seguintes seções:

- “No-break no menu Controle”
- “Grupos de tomadas no menu Controle”
- “Segurança no menu Controle”
- “Rede no menu Controle”

No-break no menu Controle

Caminho: Controle > No-break

Esta opção se aplica a dispositivos de no-break individuais e, apenas nos Smart-UPS, a um grupo de controle sincronizado (SCG). Consulte “Controle sincronizado dos dispositivos de no-break”.

Ao escolher uma opção do botão e clicar em Avançar, outra tela resume a ação a ser executada; clique em Aplicar para continuar com a ação.

As ações variam conforme você tenha um dispositivo de no-break com grupos de tomadas ou não. As duas tabelas abaixo mostram-nas separadamente.

- “Ações na tela do no-break para dispositivos COM Grupos de tomadas”.
 - “Ações na tela do no-break para dispositivos SEM Grupos de tomadas”.
- Esta tem informações sobre as opções da CLI (Interface da linha de comando).

Estas opções da caixa de seleção da tela diretamente abaixo se aplicam a ambas as tabelas.

Caixa de seleção	Descrição
Sinalizar clientes de desligamento de rede do PowerChute	<p>Esta opção estará acinzentada se não existirem clientes do PowerChute (consulte “Clientes de desligamento de rede do PowerChute”).</p> <p>Selecione esta opção para notificar todos os servidores configurados como Clientes de desligamento de rede do PowerChute que estiverem em comunicação com este no-break para desligar de acordo com os valores configurados para os Parâmetros de desligamento de rede do PowerChute (consulte “Desligamento no menu Configuração”).</p> <p>No entanto, esta opção não notificará os servidores ao executar qualquer ação de controle de Bypass.</p>
Ignorar atrasos de desligamento de tomadas	<p>Desliga as tomadas imediatamente, ignorando os atrasos configurados do grupo de tomadas.</p> <p>Você pode necessitar disso em uma emergência ou para economizar tempo de funcionamento.</p> <p>Ou talvez os dispositivos de carga já tenham sido desligados manualmente.</p>
Aplicar ao grupo de sincronização	<p>Este exibe apenas se o controle sincronizado estiver ativado. Consulte “Controle sincronizado dos dispositivos de no-break”.</p> <p>Consulte as descrições individuais dos campos nas duas tabelas abaixo.</p>



Para obter mais informações sobre atrasos e configurações, consulte “Desligamento no menu Configuração”, “Controle sincronizado dos dispositivos de no-break” e “Grupos de tomadas no menu Controle”.

Ações na tela do no-break para dispositivos **COM** Grupos de tomadas

Ação	Descrição
Reinicializar grupos de tomadas do no-break	<p>Aplica um comando Desligar imediatamente, reiniciar CA para todos os grupos de tomadas (consulte “Grupos de tomadas no menu Controle”). Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos.</p> <p>Desliga a potência de saída dos grupos de tomadas comutados e depois, se houver, o Grupo principal de tomadas. Qualquer grupo de tomadas no qual a ação for aplicada esperará o número de segundos configurado para sua “Duração da reinicialização” e “Atraso ao ligar”. (depois, os grupos de tomadas serão ligados se a rede de energia elétrica estiver disponível, ou esperarão para ser ligados até que a alimentação da rede de energia elétrica esteja disponível. Consulte “O que são grupos de tomadas?”).</p> <p>Se o no-break estiver em um Grupo de controle sincronizado (SCG), selecione Sim ou Não para Aplicar ao grupo de sincronização para escolher se deseja reinicializar todos os membros ativados do grupo. O no-break esperará o número de segundos configurado para Atraso do desligamento e Atraso do retorno, depois será ligado se a alimentação da rede de energia elétrica estiver disponível ou esperará para ligar até que a alimentação da rede de energia elétrica esteja disponível.</p>
Ligar grupos de tomadas do no-break	<p>Liga o grupo de tomadas principal, se houver, e depois todos os grupos de tomada comutados. Esta opção só é exibida se o no-break estiver desligado no momento. Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos.</p> <p>Se o no-break estiver em um Grupo de controle sincronizado, selecione Sim ou Não para Aplicar ao grupo de sincronização para escolher se deseja ligar todos os membros ativados do grupo. O no-break e os grupos de tomadas esperarão o tempo configurado para “Atraso do retorno” e depois serão ligados.</p>
Desligar os grupos de tomadas do no-break	<p>Desliga a potência de saída dos grupos de tomadas comutados e depois, se houver, o Grupo principal de tomadas. Qualquer grupo de tomadas no qual a ação for aplicada permanece desligado até que você ligue a potência novamente. Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos.</p> <p>Se o no-break estiver em um Grupo de controle sincronizado, selecione Sim ou Não para Aplicar ao grupo de sincronização para escolher se deseja desligar todos os membros ativados do grupo.</p>
Suspender grupos de tomadas do no-break	<p>Coloca os grupos de tomadas do no-break no modo de suspensão, desligando a potência de saída do no-break por um período de tempo definido pelos parâmetros a seguir. Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos</p> <ul style="list-style-type: none">• Os grupos de tomadas esperam o tempo configurado como seu “Atraso ao desligar” antes de desligar a alimentação.• Quando a potência de entrada retornar, o no-break ativará a potência de saída após transcorrerem dois períodos de tempo configurados: “Tempo de suspensão” e “Duração da reinicialização”. <p>Se o no-break estiver em um Grupo de controle sincronizado, selecione Sim ou Não para Aplicar ao grupo de sincronização para escolher se deseja colocar todos os membros ativados do grupo no modo de suspensão. A NMC do no-break que inicia a ação espera até o número de segundos configurados como “Atraso sincronizado de energia” para que os membros ativados do grupo obtenham novamente a potência de entrada antes de começar o “Atraso do retorno”. O no-break esperará o número de segundos configurado para seu “Atraso do desligamento” e depois será desligado. Transcorridas as horas configuradas como “Tempo de suspensão”, o no-break esperará o número de segundos configurado para seu “Atraso do retorno”, depois será ligado se a alimentação da rede de energia elétrica estiver disponível ou esperará para ligar até que a alimentação da rede de energia elétrica esteja disponível.</p>



Para obter mais informações sobre atrasos e configurações, consulte “Desligamento no menu Configuração”, “Controle sincronizado dos dispositivos de no-break” e “Grupos de tomadas no menu Controle”.

Ações na tela do no-break para dispositivos **SEM** Grupos de tomadas

Ação	Descrição
Reinicializar no-break (interface do usuário) <code>ups -c Reboot</code> (interface da linha de comando, CLI)	<p>Reinicializa os equipamentos conectados fazendo o seguinte. (Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos.)</p> <ul style="list-style-type: none">• Desliga a potência no no-break após o Atraso do desligamento (em Configuração - Desligamento).• Liga a alimentação no no-break depois que a capacidade da bateria do no-break retornar para, no mínimo, a porcentagem configurada para Capacidade mínima da bateria (Configuração - Desligamento - Término do desligamento), consulte “Atrasos no desligamento e forçar negociações”. Em seguida, o no-break aguarda o tempo especificado em Atraso do retorno (em Configuração - Desligamento). <p>Para uma ação do Grupo de controle sincronizado (SCG):</p> <ol style="list-style-type: none">1. Esta opção desliga a potência dos dispositivos de no-break que sejam membros ativados do grupo depois de aguardar o tempo configurado como “Atraso do desligamento” para os dispositivos de no-break em inicialização. <p>Os no-breaks em inicialização aguardam até o número de segundos especificado em “Atraso sincronizado de energia” para dar tempo aos membros do grupo até que voltem a receber a potência de entrada. Se todos os membros do grupo já tiverem obtido novamente a potência de entrada, esse atraso será omitido. Se todos os membros do grupo obtiverem novamente a potência de entrada durante o atraso, o restante do atraso será cancelado.</p> <ol style="list-style-type: none">2. “Atraso do retorno” é inicializado quando o no-break em inicialização estiver em Capacidade mínima de bateria configurada (Configuração - Desligamento - Término do desligamento), consulte “Atrasos no desligamento e forçar negociações”. <p>A Capacidade mínima da bateria do no-break em Inicialização do no-break também é exigida dos membros do SCG. No entanto, é possível reduzir os requisitos de um membro do grupo configurando o “Desvio da duração do tempo de funcionamento de retorno” desse membro. Por exemplo, se a Capacidade mínima da bateria do iniciador for de 50%, e o desvio da Capacidade mínima da bateria de um membro (Configuração - Controle sincronizado) for de 5%, esse membro precisará de 45% de capacidade da bateria para reiniciar.</p>
Ligar no-break (interface do usuário) <code>ups -c On</code> (CLI)	<p>Liga a potência no no-break. A opção mostra apenas quando o no-break está desligado. Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos.</p> <p>Para um Grupo de controle sincronizado, após um atraso de alguns segundos, a ação liga todos os membros ativados do grupo que tenham potência de entrada.</p>
Desligar no-break (interface do usuário) <code>ups -c Off</code> (CLI)	<p>Desliga a potência de saída do no-break imediatamente, sem um atraso de desligamento. O no-break permanece desligado até você ligá-lo novamente.</p> <p>Para um Grupo de controle sincronizado, esta ação desliga a potência em todos os membros ativados do grupo. Nenhum valor de “Atraso do desligamento” é usado. Os no-breaks desligam após alguns segundos e permanecem desligados até você ligar a potência.</p> <p>Observação: Para uma ação de desligamento sincronizada que utilize o valor do “Atraso do desligamento” do no-break em inicialização, utilize o SNMP (para o upsAdvControlUpsOff OID, defina o valor em turnUpsSyncGroupOffAfterDelay (5)).</p>
<code>ups -c GraceOff</code> (CLI)	<p>Desliga a potência da tomada do no-break após o “Atraso máximo necessário” e o “Atraso do desligamento” configurado.</p>

Ações na tela do no-break para dispositivos **SEM** Grupos de tomadas

Ação	Descrição
Suspender no-break ups -c GraceReboot (CLI)	<p>Esta ação é semelhante a Reinicializar no-break apresentada acima, mas com um atraso adicional antes do desligamento.</p> <p>Os equipamentos conectados desligam somente depois que o no-break (ou o no-break em inicialização, para uma ação do grupo de controle sincronizado) aguarde o “Atraso máximo necessário”, que é calculado conforme descrito em “Atrasos no desligamento e forçar negociações”.</p> <p>Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos.</p>
Suspender no-break (interface do usuário) ups -c Sleep (CLI)	<p>Coloca o no-break no modo de suspensão desligando sua potência de saída por um período de tempo definido. Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos.</p> <ul style="list-style-type: none"> • O no-break desliga a potência de saída depois de aguardar o tempo configurado em “Atraso do desligamento”. • Quando a potência de entrada retornar, o no-break ativar a potência de saída após dois períodos de tempo configurados: “Tempo de suspensão” e “Atraso do retorno”. • Para uma ação do Grupo de controle sincronizado (SCG), a NMC do no-break em inicialização aguarda o número de segundos configurado em “Atraso sincronizado de energia” para que os membros ativados do grupo obtenham novamente a potência de entrada antes de iniciar o “Atraso do retorno”. Se todos os membros do grupo já tiverem obtido novamente a potência de entrada, o “Atraso sincronizado de energia” será omitido. Se todos os membros do grupo obtiverem novamente a potência de entrada durante o atraso, o restante do atraso será cancelado.
ups -c GraceSleep (CLI)	<p>Coloca o no-break no modo de suspensão (desligando a potência por um período de tempo definido):</p> <ul style="list-style-type: none"> • O no-break desliga a potência de saída depois de aguardar o “Atraso máximo necessário” para dar tempo para que o Desligamento de rede do PowerChute desligue seu servidor com proteção e para aguardar seu “Atraso do desligamento”. • Quando a potência de entrada retornar, o no-break ativar a potência de saída após dois períodos de tempo configurados: seu “Tempo de suspensão” e “Atraso do retorno”. • Sobre o Grupo de controle sincronizado (SCG), consulte o último marcador na linha diretamente acima.
Colocar no-break em bypass e Retirar no-break de bypass (interface do usuário) ups -b Enter ups -b Exit (CLI)	<p>Estas ações têm suporte:</p> <ul style="list-style-type: none"> • Somente para no-breaks individuais, NÃO para Grupos de controle sincronizados • Somente para no-break Symmetra e alguns dispositivos Smart-UPS <p>Controlam o uso do modo de derivação, que permite que a manutenção seja executada em um no-break Symmetra e em alguns dispositivos de Smart-UPS sem desligar a potência no no-break.</p> <p>Clique em Avançar para consultar detalhes específicos sobre ajuste e atrasos.</p>

Grupos de tomadas no menu Controle

Caminho: Controle > Grupos de tomadas



Esta opção não está disponível para todos os dispositivos de no-break.

Use esta opção para ligar, desligar ou reinicializar grupos de tomadas individuais de maneira independente do dispositivo de no-break. Esta opção pode ser aplicada a dispositivos de no-break individuais e a um grupo de controle sincronizado (se ativado, consulte “Controle sincronizado dos dispositivos de no-break”).

(Essa tela relacionará por nome e estado cada grupo de tomadas do no-break que esteja configurado pela opção **Configuração - Grupos de tomadas**, consulte “Grupos de tomadas no menu Configuração”).

Você pode selecionar qualquer uma das seguintes ações (ou nenhuma ação) para cada grupo de tomadas. Estas são ações únicas.

- Quando o estado do grupo de tomadas for **desligado**:
 - **Ligar imediatamente**
 - **Ligar com atraso**: Liga o grupo de tomadas após o número de segundos configurados em **Atraso ao ligar**. (consulte “Desligamento no menu Configuração”).

- Quando o estado do grupo de tomadas for **ligado**:
 - **Desligar imediatamente**
 - **Desligar com atraso**: Desliga o grupo após o número de segundos configurados em **Atraso ao desligar** (consulte “Desligamento no menu Configuração”).
 - **Reinicializar imediatamente**: Desliga o grupo imediatamente e, em seguida, liga o grupo após o número de segundos configurado em **Duração da reinicialização** (consulte “Desligamento no menu Configuração”) e **Atraso ao ligar**.
 - **Reinicializar com atraso**: Desliga o grupo de tomadas após o número de segundos configurado em **Atraso ao desligar** e, em seguida, liga o grupo após o número de segundos configurado em **Duração da reinicialização** e **Atraso ao ligar**.
- Para alguns dispositivos de no-break, quando o estado do grupo de tomadas for **ligado** e o no-break estiver no modo de bateria:
 - **Desligar imediatamente, reiniciar CA**: Desliga o grupo imediatamente. Após o número de segundos configurado em **Duração da reinicialização** e **Atraso ao ligar**, verifique se a energia da rede elétrica retornou e se o no-break pode suportar a demanda do tempo mínimo de funcionamento de retorno e, em seguida, ligue o grupo.
 - **Desligar com atraso, reiniciar CA**: Desliga o grupo após o número de segundos configurado em **Atraso ao desligar**. Após o número de segundos configurado em **Duração da reinicialização** e **Atraso ao ligar**, verifique se a energia da rede elétrica retornou e se o no-break pode suportar a demanda do tempo mínimo de funcionamento de retorno e, em seguida, ligue o grupo.

Depois de selecionar uma ação, clique em Avançar para exibir uma descrição detalhada da ação, inclusive a duração de qualquer atraso. Clique em Aplicar para confirmar a ação.

Segurança no menu Controle

Caminho: Controle > Segurança > Gerenciamento de sessão

As telas oferecem detalhes sobre os usuários que estão conectados, a interface que estão usando (por exemplo, a interface de usuário da Web, a CLI), seu endereço IP e há quanto tempo estão conectados.

Se você tiver direitos suficientes, clique no nome para ver quais meios de autenticação foram usados para validar o usuário. Portanto você pode usar o botão **Encerrar sessão** para desconectar um usuário.

Rede no menu Controle

Caminho: Controle > Rede > Redefinir/Reinicializar

Use estas opções para redefinir várias opções da placa de gerenciamento de rede e a interface de usuário.

Ação	Descrição
Reinicializar interface de gerenciamento	Reinicializa a interface de gerenciamento (por exemplo, a interface do usuário da Web, a CLI) quando você se desconecta. O no-break e os dispositivos da NMC não são reiniciados.
Redefinir tudo ¹	Cuidado: Redefine todos os valores configurados na interface de gerenciamento que você está usando, por exemplo, a interface de usuário da Web. Desmarque a caixa de seleção Excluir TCP/IP para redefinir TODOS os valores de configuração no padrão. Selecione a caixa de seleção Excluir TCP/IP para redefinir todos os valores exceto como este dispositivo obtém seus valores de configuração de TCP/IP (o padrão é DHCP).
Redefinir somente ¹	TCP/IP: Redefina como este dispositivo obtém seus valores de configuração de TCP/IP no padrão DHCP.
	Configuração do evento: Cancelar todas as alterações de configuração de evento, por evento e por grupo, restaurando as configurações padrão. Consulte “Menu Notificação”.
	No-break para padrões: Restaurar os padrões somente das configurações do no-break, e não das configurações de rede.
	Esta opção estará disponível apenas quando um monitor ambiental estiver conectado. Perda de alarmes de comunicação ambiental: Cancelar quaisquer alarmes ambientais que são causados por perda de comunicação com um sensor externo. Por exemplo, se um sensor de temperatura for desconectado e causar um alarme, o cancelamento dos alarmes ambientais perdidos fará o status de alarme deste sensor retornar para Normal. Observação: para cancelar alarmes de um sensor que esteja conectado à porta de sensor universal de uma NMC AP9631, conecte novamente o sensor ou reinicie a NMC.
	Diretiva de controle: Redefinir as configurações que definem como a NMC responderá a alarmes que sejam detectados no acessório de E/S de contato seco.
¹ A redefinição pode levar até um minuto. O nome do no-break que você configurou não será redefinido (consulte “Tela No-break - Geral”).	

Ajuste das configurações: 1

Com as opções do menu Configuração, é possível definir valores operacionais fundamentais para o no-break e a NMC.

Consulte as seções abaixo e também “Ajuste das configurações: 2”.

- “Grupos de tomadas no menu Configuração”
- “Configurações de potência no menu Configuração”
- “Desligamento no menu Configuração”
- “Tela No-break - Geral”
- “Tela Agendamento de autoteste”
- “Programação do desligamento”
- “Tela Atualização de firmware”
- “Clientes de desligamento de rede do PowerChute”
- “Controle sincronizado dos dispositivos de no-break”
- “Tela Suporte de terceiros”
- “Tela E/S universal”
- “Menu Segurança”

Grupos de tomadas no menu Configuração

Caminho: Configuração > Grupos de tomadas

Com esta opção você pode exibir e configurar os atrasos de sequenciamento e tomadas.

Consulte também “Grupos de tomadas no menu Status”, “Grupos de tomadas no menu Controle” e “Desligamento no menu Configuração”.

O que são grupos de tomadas?



O agrupamento das tomadas está disponível somente em alguns dispositivos de no-break. Para determinar se o seu dispositivo de no-break tem suporte para grupos de tomadas, consulte a documentação do no-break.

As configurações disponíveis variam dependendo do dispositivo no-break.

Principais grupos de tomadas . Alguns dispositivos de no-break fornecem energia da rede elétrica a um grupo de tomadas principal. O grupo de tomadas principal controla a distribuição de energia a todos os grupos de tomadas comutadas (se houver) para o no-break.

- Se o grupo de tomadas principal estiver desligado, os grupos de tomadas comutadas não poderão ser ligados.
- Se você desligar o grupo de tomadas principal, o no-break desligará os grupos de tomadas comutadas antes de desligar o grupo de tomadas principal
- Para ligar um grupo de tomadas comutadas, o no-break deverá ligar antes o grupo de tomadas principal.

Grupos de tomadas comutadas . Cada tomada comutada pode realizar ações independentemente. Você pode iniciar ou interromper essas tomadas em sequência e também reiniciar os dispositivos conectados a essas tomadas.

O modo como os grupos de tomadas são ligados e desligados dependerá de sua configuração e de como você liga ou desliga o no-break:

- Até que você configure os atrasos para as ações quando ligar a saída do no-break (descritos em “No-break no menu Controle” e “Configurações de sequenciamento”, qualquer grupo de tomadas que esteja desligado ficará ligado por padrão. Quando uma tomada for ligada, ela aplicará energia a todos os dispositivos conectados.
- Após configurar as ações e atrasos, eles controlarão quando os grupos de tomadas serão ligados e desligados após você ligar ou desligar o no-break. (Este é o caso de você desligar usando a UI da Web da NMC ou a interface de exibição no no-break).

Configuração dos Grupos de tomadas

Nome e tipo do grupo de tomadas. Exiba o nome, tipo e atrasos das tomadas do no-break na tela

Configuração - Grupos de tomadas. Clique no nome de um grupo de tomadas em **Grupo** para alterar suas configurações inclusive as opções de redução de carga e atrasos de sequenciamento.

Configurações de sequenciamento. As configurações variam conforme o dispositivo de no-break. Use as opções de sequenciamento para definir como o no-break responderá aos comandos emitidos pelo usuário.

Campo	Descrição
Atraso ao desligar	Quando este grupo de tomadas está ligado, ele espera este atraso em segundos antes de desligar. Configurando diversos horários aqui para as tomadas, você pode sequenciar seus desligamentos, ou seja, pode especificar a ordem na qual eles serão desligados.
Duração da reinicialização	A tomada espera este tempo antes de reinicializar.
Atraso ao ligar	Quando este grupo de tomadas está desligado e recebe um sinal para ligar, ele espera este atraso em segundos antes de ligar. Configurando diferentes horários aqui para as tomadas, você pode sequenciar as ações de ligar.
Tempo de funcionamento de retorno mínimo	É o tempo mínimo em que o no-break deve dar suporte à carga antes que possa ser ligado novamente.

Opções de redução de carga. A redução de carga permite especificar as condições que causam a perda de potência dos grupos de tomadas comutadas individuais. Não está disponível para Grupos principais de tomadas.

Um exemplo do uso da redução de carga seria para desligar cargas não críticas como monitores quando o no-break está funcionando na bateria ou está sobrecarregado. Isto economizaria a carga da bateria e o tempo de execução para cargas essenciais. Outro exemplo seria desativar uma reinicialização automática após uma sobrecarga para investigar a causa da sobrecarga antes de ligar o grupo de tomadas novamente.

As opções permitem desligar um grupo de tomadas quando ocorrer QUALQUER UMA das condições que você especificar:

- Quando o tempo em modo de bateria exceder um número pré-definido de minutos.
- Quando o tempo restante de autonomia do no-break for menor que um número pré-definido de minutos. (o Tempo de funcionamento é quanto tempo o no-break pode usar a energia da bateria para suportar sua carga presente).
- O no-break está sobrecarregado (a demanda de potência dos dispositivos conectados ao no-break excede a quantidade de potência que o no-break pode fornecer).

Você também pode ativar estas ações:

- **Ignorar atraso de desligamento de tomada.** (Desliga o grupo de tomadas imediatamente, sem aguardar o número de segundos configurado em **Atraso ao desligar**. Por padrão, esta opção fica desativada.)
- **Permanecer desligado após o retorno da energia.** (Permanecer desligado quando a energia da rede elétrica retornar. Por padrão, esta opção fica desativada e o no-break aguarda o número de segundos configurado em **Atraso ao ligar**, em seguida liga os grupos de tomadas).

Eventos do grupo de tomadas e traps. Uma alteração no estado de um grupo de tomadas gera o evento **No-break: Grupos de tomadas ligado** com severidade Informativo ou **No-break: Grupo de tomadas desligado** com uma severidade Aviso. O formato das mensagens de evento é "No-break: Grupo de tomadas *group_number*, *group_name*, *action* devida a *reason*". Por exemplo:

UPS: Outlet Group 1, Web Server, turned on.

UPS: Outlet Group 3, Printer, turned off.

Por padrão, o evento gera uma entrada no log de eventos, um e-mail e uma mensagem do Syslog.

Se você configurar receptores de traps para os eventos, o trap 298 será gerado quando um grupo de tomadas ligar e o trap 299 será gerado quando um grupo de tomadas desligar. A mensagem do evento é o argumento do trap. O nível de severidade padrão é o mesmo do evento.

Configurações de potência no menu Configuração

Caminho: Configuração > Configurações de potência



configurações disponíveis variam dependendo do dispositivo no-break.

A **Tensão de saída nominal** é a tensão de CA que o no-break fornece à carga. Você pode configurar os seguintes tipos de itens específicos do dispositivo:

- As configurações de **Tensão** superior e inferior determinam as faixas nas quais o no-break automaticamente regula a saída da bateria para a carga. Isto protege a carga.
Quando a tensão superior for interrompida, o no-break usará o recurso de ajuste do AVR (regulador automático de tensão); quando a tensão inferior for interrompida, o no-break usará o recurso de impulso do AVR (ou ele alternará para a operação da bateria se o no-break não tiver o recurso de impulso do AVR).
- Ao ativar o **Modo ecológico** o no-break é executado em bypass, o que usa a potência com mais eficiência. No entanto, no modo ecológico, a velocidade de transferência de potência da bateria do no-break, quando necessária, é mais lenta. Se o seu ambiente precisar de comutação rápida, você pode desativar o modo ecológico.
- O ruído elétrico é energia eletromagnética indesejada que diminui a qualidade dos sinais e dados. Quando há muito ruído, seu no-break começa a fornecer energia da bateria. Você pode especificar a resposta ao ruído através de **Sensibilidade**. Use as opções **Reduzido** e **Baixa** na caixa suspensa Sensibilidade quando houver muito ruído.
- Valor nominal da saída em watts:** o máximo valor nominal de potência para atender os requisitos dos seus dispositivos de carga.
- As configurações de **Bypass** definem as condições sob as quais o no-break pode passar para o modo de bypass.
- Os **Limites de alarme** baseiam-se no tempo de funcionamento disponível, na energia redundante e na carga do no-break.

Desligamento no menu Configuração

Caminho: Configuração > Desligamento

Use esta opção para configurar seus desligamentos especificando as durações na bateria, atrasos antes de desligar e reiniciar, tempo mínimo de execução e carga necessária antes de reiniciar etc. Estas opções de desligamento ajudam a garantir desligamentos com proteção.

Consulte a tabela abaixo e também “Desligamento precoce controlado e final do desligamento”.

Para os Grupos de tomadas, esta tela é executada em conjunto com o “Grupos de tomadas no menu Configuração”.

Campo	Descrição
Duração da bateria baixa	Quando o no-break passa para o modo bateria, espera este tempo antes de desligar. Consulte “Atrasos no desligamento e forçar negociações”.
Atraso máximo necessário	Em um desligamento, o no-break espera este tempo antes de desligar. Consulte “Atrasos no desligamento e forçar negociações”.
Sinalização básica de desligamento	A sinalização básica fornece notificação e desligamento protegido do sistema, mas não fornece os recursos avançados de monitoramento contínuo disponíveis na sinalização avançada ou inteligente. Ative-a se o no-break tiver um cabo de sinalização básica, não tiver suporte para sinalização avançada ou estiver configurado para comunicar-se em sinalização básica.
Duração de bateria baixa básica	Define o tempo de execução disponível da bateria no qual o no-break sinaliza uma condição de bateria baixa.
Tempo de suspensão	Define quanto tempo o no-break mantém a potência de saída desligada quando você usa os campos de suspensão do “No-break no menu Controle”.
Campos Controle sincronizado (consulte “Controle sincronizado dos dispositivos de no-break”)	
Atraso do desligamento	Define quanto tempo o no-break aguarda antes de ser desligado em resposta a um comando de desligar do controle sincronizado.
Atraso do retorno	Define quanto tempo o no-break aguarda antes de ser ligado após um desligamento iniciado por um comando do controle sincronizado. Se a bateria estiver abaixo da capacidade para fornecer o tempo de execução configurado em “Tempo de funcionamento de retorno mínimo”, o no-break primeiro esperará até que a bateria esteja recarregada para fornecer esse tempo de execução.
Desligamento de rede do PowerChute	
Atraso máximo necessário	Calcula o atraso necessário para garantir que cada cliente do PowerChute tenha tempo suficiente para desligar de forma protegida. Este é o atraso de desligamento mais longo necessário para qualquer servidor relacionado como um dos “Tela Suporte de terceiros”. Consulte “Atrasos no desligamento e forçar negociações”.
Comportamento de desligamento em modo de bateria	Depois que os clientes do PowerChute desligarem seus sistemas de computador, este parâmetro determinará se o no-break ligará automática ou manualmente quando a potência de entrada for restabelecida.
Frase de autenticação	Define a frase de 15 a 32 caracteres ASCII que diferencia maiúsculas de minúsculas e que deverá ser usada durante a autenticação MD5 (decriptação) para comunicação do PowerChute. A configuração padrão do Administrador é “admin user phrase”.

Desligamento precoce controlado e final do desligamento. Estas opções NÃO estão disponíveis para todos os dispositivos de no-break. As opções de Desligamento precoce controlado permitem que você desligue um dispositivo de no-break que esteja usando energia da bateria, quando ocorrer QUALQUER UMA das condições que você especificar:

- Quando o tempo em modo de bateria exceder um número pré-definido de minutos.
- Quando o tempo restante de autonomia do no-break for menor que um número pré-definido de minutos (o Tempo de funcionamento é quanto tempo o no-break pode usar a energia da bateria para suportar sua carga presente).
- Quando a carga da bateria é menor que uma porcentagem pré-definida de sua capacidade total.
- Quando a carga na saída do no-break for menor que uma porcentagem pré-definida.

Com **Permanecer desligado após o retorno da energia**, você também pode decidir se o no-break será religado ou não, quando a energia da rede elétrica for restaurada.

As opções de **Término do desligamento** permitem definir uma condição e um tempo de atraso para quando um no-break puder ser ligado novamente quando a energia da rede elétrica for restaurada. Você pode especificar uma **Capacidade mínima da bateria** antes de ligar novamente o no-break. Defina outra pausa, se necessário, antes de ligar com **Atraso do retorno**.

Atrasos no desligamento e forçar negociações. Uma hora de desligamento para o no-break é calculada de forma diferente para um no-break *SEM* grupos de tomadas, em comparação com um no-break *com* grupos de tomadas.

1. Para um no-break SEM grupos de tomadas, a hora do desligamento é o valor do **Atraso máximo necessário** na tela **Desligamento** da placa de gerenciamento de rede, *mais* 2 minutos, e *mais* o atraso no desligamento para o no-break.

No-break SEM grupos de tomadas: hora do desligamento



2. Para um no-break COM grupos de tomadas, a hora de desligamento é o valor do **Atraso ao desligar** na tela **Grupos de tomadas** da NMC, consulte “Grupos de tomadas no menu Configuração”. (Não disponível para todos os dispositivos de no-break).

No-break COM grupos de tomadas: hora do desligamento



Observe que os dispositivos com o prefixo SOMA comportam-se como no item 1 acima e não como no item 2.

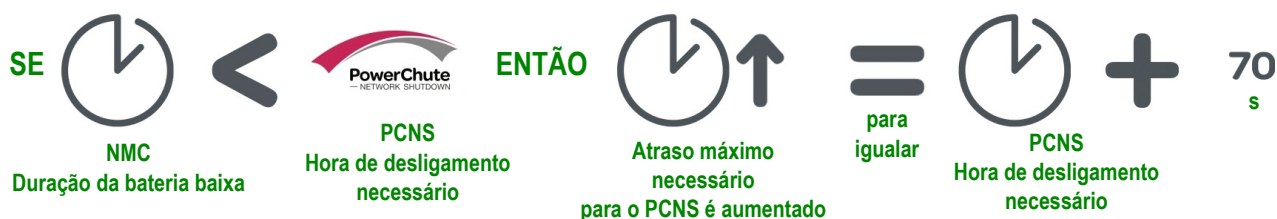
Para ambos os tipos de no-break, a hora de desligamento é negociado pela placa de gerenciamento de rede interagindo com o PCNS (Desligamento de rede do PowerChute).

Use a opção **Forçar negociação** (Configuração - Desligamento) para recalibrar o tempo quando você alterar ou acrescentar um cliente PCNS. Ao forçar uma negociação, o procedimento é automático; os detalhes são discutidos a seguir.

O PCNS inicia com o valor de **Duração da bateria baixa**, compara esse valor com sua própria hora de desligamento e, se o tempo de duração da bateria for muito baixo, avisa a placa de gerenciamento de rede para que ela aumente os valores nos itens 1 e 2 abaixo para o valor da HORA DE DESLIGAMENTO NECESSÁRIO DO PCNS* *mais* 70 segundos.

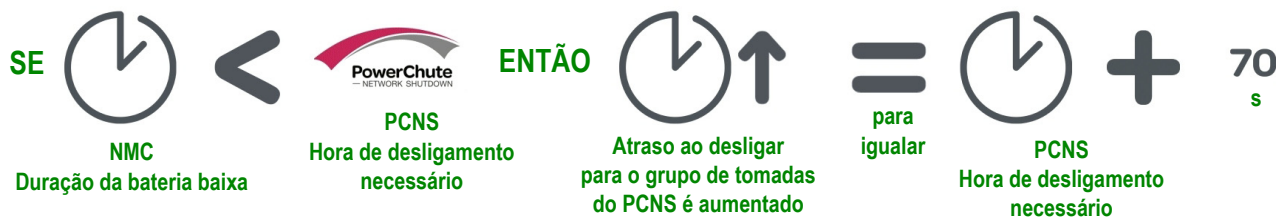
1. SEM grupos de tomadas, o **Atraso máximo necessário**.

Forçar negociação: No-break SEM grupos de tomadas



2. Com grupos de tomadas, o **Atraso ao desligar** para o grupo de tomadas que fornece alimentação ao cliente PCNS.

Forçar negociação: No-break COM grupos de tomadas



*A HORA DE DESLIGAMENTO NECESSÁRIO DO PCNS = o atraso no desligamento + a duração do comando de desligamento. Quando o valor padrão de 70 segundos é adicionado, o tempo é sempre arredondado para o minuto mais próximo. Por exemplo, um total de 3 min 50 s é arredondado para 4 minutos. Um total de 2 min ainda é arredondado para 3 min.



Obs.:

Os 70 segundos mencionados são o tempo padrão de desligamento do sistema operacional para o PCNS.

O PCNS nunca altera o valor do campo **Duração da bateria baixa** da placa de gerenciamento de rede.

No caso do PCNS v3.x, o valor do **Atraso máximo necessário** nunca é usado pela placa de gerenciamento de rede para um no-break com grupos de tomadas.

Tela No-break - Geral

Caminho: Configuração > No-break - Geral



Esta tela não está disponível para todos os dispositivos de no-break.

Algumas das opções explicadas a seguir talvez NÃO sejam exibidas para alguns dispositivos de no-break.

Campo	Descrição
Nome do no-break	Um nome que identifique o no-break.
Posição do no-break	A orientação física do no-break, rack ou torre.
Alarme sonoro	Ativar ou desativar o alarme sonoro do no-break e, para alguns dispositivos de no-break, definir a condição que fará o alarme tocar.
Preferência de idioma do LCD	Especifique o idioma que deseja usar no mostrador de seu no-break.
Exibir	Ativa ou desativa o acesso de gravação à interface do mostrador do no-break. Quando estiver desativado, o usuário mantém o acesso de leitura à maioria das telas, mas não às subtelas nos menus Controle e Configuração.
Última substituição de bateria	Insira o mês e ano da mais recente substituição de bateria do no-break.
Número de baterias ou Baterias externas	O número de baterias, excluindo as baterias internas do no-break. Alguns dispositivos com mais de 16 baterias devem adicionar baterias em múltiplos de 16 (por exemplo, 16, 32, 48 etc.), mas depois podem ser ajustadas para o valor correto.
Gabinete de bateria externo	A corrente nominal em ampère-hora do gabinete de bateria de uma fonte de bateria externa.

Campo	Descrição
Taxa do carregador de bateria	Com esse campo, é possível alterar a taxa de carga do no-break em termos percentuais. Aqui, 100% representa a taxa recomendada pelo fabricante. Por exemplo, para dobrar a taxa de carga, configure para 200%. A taxa inclui baterias internas e externas. Este número não se altera quando pacotes externos são adicionados ou removidos. Entretanto, remover um pacote de bateria externo aumenta efetivamente a taxa de carregamento. Da mesma forma, adicionar um pacote de bateria externo diminui a taxa de carregamento. Cuidado: Carregar a uma taxa muito elevada pode fazer com que os eletrólitos alcancem ponto de ebulição e/ou vazem, e causar ainda um aumento da pressão do gás. Não altere essa configuração a não ser que tenha um sólido conhecimento dessa área.
Tipo de bateria	Indica o tipo de bateria, onde VRLA é uma bateria chumbo-ácida regulada por válvula e Célula ventilada é um tipo de bateria de célula molhada (como as utilizadas em automóveis).

Tela Agendamento de autoteste

Caminho: No-break > Configuração > Agendamento de autoteste

Use essa opção para definir quando o no-break iniciará um autoteste.

Programação do desligamento

Caminho: Configuração > Agendamento



Esta opção não está disponível para todos os dispositivos de no-break.

Para as opções no-break e grupo de tomadas.

Você pode agendar um desligamento de um dispositivo de no-break em **No-break** ou de um grupo individual de tomadas comutadas (se aplicável) em **Grupos de tomadas**.

Os agendamentos de desligamento configurados são exibidos ao longo da parte superior da tela quando você selecionar **No-break** ou **Grupos de tomadas**, com detalhes relevantes, inclusive se estiverem atualmente ativados ou desativados.

Editar, ativar, desativar ou excluir um desligamento agendado. Clique no nome do agendamento na lista de agendamentos ao longo da parte superior da tela **No-break** ou **Grupos de tomadas**. Isso exibe os detalhes completos onde você pode editar os parâmetros. Também pode desativá-lo temporariamente limpando a caixa de seleção **Ativar** ou excluindo-o permanentemente.

Criação de um agendamento de desligamento de no-break ou de grupo de tomadas comutadas.

1. Em **Agendamento**, selecione **No-break** ou **Grupos de tomadas**.
2. Use os botões de opção para selecionar o tipo de desligamento para agendar, **Desligamento uma vez**, **Desligamento diário** ou **Desligamento semanal** e clique no botão **Avançar**.
3. Para desativar um agendamento temporariamente, desmarque o botão **Ativar**.
4. Especifique um nome e uma data e hora de agendamento.
Para um desligamento semanal, especifique a frequência usando a caixa suspensa.
5. Especifique se o dispositivo ou grupo de tomadas deve voltar a ligar depois do desligamento:

Ligar novamente: Especifique se o no-break será ligado em um dia e hora específicos, **Nunca** (o no-break deverá ser ligado manualmente), ou **Imediatamente** (o no-break será ligado após aguardar 6 minutos e o tempo especificado em **Atraso do retorno**, consulte “Atraso do retorno”).

Para apenas um grupo de tomadas, especifique o grupo para desligar selecionando o botão apropriado.

Sinalizar clientes de desligamento de rede do PowerChute: Especifique se os clientes PowerChute serão notificados, consulte “Clientes de desligamento de rede do PowerChute”.

Apenas para a opção no-break: desligamentos sincronizados

Agendar um desligamento sincronizado. Quando o no-break que inicia o desligamento é um membro ativado de um Grupo de controle sincronizado (SCG), todos os membros do SCG são desligados.

Sempre agende os desligamentos por meio do mesmo membro do SCG. Cada no-break do SCG deve ter uma conexão de rede na hora do desligamento. Consulte “Controle sincronizado dos dispositivos de no-break”.



Cuidado: NÃO agende desligamentos *por meio de mais de um membro do grupo*. Agendamentos desse tipo poderão causar resultados imprevisíveis.



Esta opção permite que você use o utilitário de Desligamento de rede do PowerChute para desligar no máximo 50 servidores na rede que usem uma versão cliente do utilitário.

Tela Atualização de firmware

Caminho: No-break > Configuração > Atualização de firmware

Esta opção não está disponível para todos os dispositivos de no-break.



Esta atualização refere-se *ao firmware do no-break*. Não confunda isto com a atualização de firmware da NMC (consulte “Transferências de arquivos”).



A saída do no-break deve ser desligada antes de ser realizada a atualização do firmware.

Siga estes passos para atualizar o firmware. (Consulte “Uso do FTP para atualizar o firmware do no-break” para obter uma forma alternativa.)

1. Consulte os IDs [FA164737](#) e [FA170679](#) de artigos da Base de conhecimento no [site da APC](#) para obter informações sobre uma atualização de firmware e mais instruções.
2. Selecione **Configuração - Atualização do firmware**.
3. Clique no botão e localize o arquivo de atualização baixado em seu computador.
4. Clique no botão **Atualizar no-break** para atualizar o firmware do no-break.
5. Quando a atualização terminar, verifique o status em **Resultado da última atualização** ou no Log de eventos.

Como usar o FTP para atualizar o firmware do no-break

Se você tiver atualizações para muitos dispositivos de no-break, pode ser mais rápido usar o FTP. Os passos a seguir mostram um exemplo de como fazer isso. Esta é uma **alternativa** para a atualização a partir da “Tela de atualização do firmware”.

1. Consulte os IDs [FA164737](#) e [FA170679](#) de artigos da Base de conhecimento no [site da APC](#) para obter informações sobre uma atualização de firmware e mais instruções.
2. Inicie o FTP na placa e insira o arquivo de atualização no diretório `upsfw` para iniciar o processo de atualização do firmware. A NMC pode cancelar a transferência do firmware do FTP se detectar que o arquivo de atualização está corrompido ou se não for aplicável ao no-break.

A seguir, mostra-se um exemplo de carregamento de um arquivo de atualização usando o comando DOS FTP:

```
$ ftp <NMC Network Address Here>
Connected to <NMC Network Address>.
220 AP9631 Network Management Card AOS vX.Y.Z FTP server ready.
User (<NMC Network Address>:(none)): apc
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> cd upsfw
250 CWD requested file action okay, completed.
ftp> put "<Path to UPS Firmware File>"
200 PORT Command okay.
150 File status okay; about to open data connection.
226 Closing data connection.
ftp: 121984 bytes sent in 1.39Seconds 87.70Kbytes/sec.
ftp> quit
221 Goodbye.
```

3. Quando a atualização terminar, verifique o status em **Resultado da última atualização** na página de atualização do firmware da interface web ou no Log de eventos.

Clientes de desligamento de rede do PowerChute

Caminho: No-break > Configuração > PowerChute

O desligamento de rede do PowerChute pode desligar os dispositivos de no-break remotamente.

Ao instalar um cliente de Desligamento de rede do PowerChute em sua rede, ele é adicionado a esta lista automaticamente. Ao desinstalar um cliente de Desligamento de rede do PowerChute, ele é removido automaticamente.

Clique em **Adicionar cliente** para inserir o endereço IP de um novo cliente de Desligamento de rede do PowerChute. Para excluir um cliente, clique no endereço IP desse cliente na lista e, em seguida, clique em **Excluir cliente**. A lista pode conter os endereços IP de até 50 clientes.

Com grupos de tomadas, você também deve especificar o grupo de tomadas que está fornecendo potência ao cliente PowerChute.

Controle sincronizado dos dispositivos de no-break

Caminho: No-break > Configuração > Controle de sincronização

Esta opção não está disponível para todos os dispositivos de no-break.

O que é um grupo de controle sincronizado (SCG)? Com um SCG você pode aplicar ações simultaneamente a cada no-break do grupo. Se você aplicar uma ação a um SCG, os membros ativados do grupo terão o seguinte comportamento:

- Cada no-break recebe o comando independentemente do status de saída (por exemplo, mesmo com bateria baixa).
- A ação usa os períodos de atraso [como o **Atraso do desligamento** e **Atraso do retorno**, configurados *para o no-break em inicialização*. (Consulte “Desligamento no menu Configuração”).
- Quando a ação inicia, um no-break que não possa participar retém seu status de saída atual enquanto os outros dispositivos de no-break executarão a ação. Portanto, se um no-break já estiver em um estado de saída exigido pela ação (por exemplo, um no-break já está desligado quando é iniciada a ação Reinicializar no-break), esse no-break registrará um evento e executará o resto da ação, se for o caso.
- Todos os no-breaks participantes sincronizam seu desempenho da ação (dentro de um período de tempo de um -segundo em condições ideais para o Smart-UPS), mas às vezes durante um período mais longo.
- Em ações de reinicialização e suspensão:
 - Imediatamente antes da inicialização do no-break, começa o tempo especificado como **Atraso do retorno**, por padrão ele aguarda até 120 segundos (**seu Atraso sincronizado de energia configurável**) para qualquer no-break que não tenha potência de entrada até que obtenha novamente essa potência.
Qualquer no-break que não obtiver novamente a potência de entrada durante esse atraso não participará da reinicialização sincronizada, mas aguardará o retorno de sua própria potência de entrada antes de reinicializar.
 - Os LEDs na frente do no-break não sequenciam suas luzes como fazem para uma ação normal (não sincronizada), de reinicialização ou de suspensão.
- Os eventos e status do no-break são relatados para ações sincronizadas do mesmo modo que para ações em dispositivos de no-break individuais.

Orientações para Grupos de controle sincronizado. Antes de configurar este no-break como um membro do grupo de controle sincronizado (SCG), releia essas orientações:

- Todos os dispositivos de no-break de um SCG devem ser dispositivos iguais.
- Os SCGs dão suporte para qualquer no-break Smart-UPS que tenha um slot que aceite a placa de gerenciamento de rede.
- Quando sua associação em um grupo de controle sincronizado estiver ativada, a NMC bloqueará as comunicações do no-break a partir de um dispositivo de gerenciamento conectado na porta de

comunicação serial. No entanto, a NMC ainda permitirá acesso à interface da linha de comando na porta de comunicação serial.

- Consulte também os artigos da Base de Conhecimentos FA156114 e 11135, no site de suporte www.apc.com.

Exibir o status de um membro em um Grupo de controle sincronizado. Quando o SCG estiver ativado, serão exibidas as informações adicionais a seguir sobre a associação ao SCG deste membro do grupo: Seu **Endereço IP**, **Status de entrada** (Bom é aceitável; Ruim não é aceitável); e seu **Status de saída** (Ligado ou Desligado).

Campo	Descrição
Associação a grupos	Quando você ativar ou desativar a associação ao grupo de controle sincronizado (SCG), a alteração fará com que a interface de gerenciamento reinicialize na próxima vez que fizer logoff e será implementada naquele momento. A opção Controle de sincronização usa SNMPv3 para a comunicação do grupo. Ao ativar a associação ao grupo, o SNMPv3 será ativado automaticamente.
Número do grupo de controle	O identificador único do SCG. Este valor deverá ser um número de 1 a 65534. Um no-break pode ser um membro de apenas um SCG. Todos os membros de um SCG deverão ter o mesmo número de grupo de controle.
Endereço IP de multicast	Especifique o endereço IP usado para comunicação entre os membros de um SCG. A faixa permitida é de 224.0.0.3 a 224.0.0.254. Todos os membros deverão ter o mesmo Endereço IP de multicast.
Atraso sincronizado de energia	Quando o no-break em inicialização do SCG estiver pronto para ligar, este valor será o tempo máximo que o no-break em inicialização esperará, se necessário, para que outros membros do grupo obtenham novamente a potência de entrada. (O valor padrão é 120 segundos). Quando esse atraso expirar, o no-break em inicialização aguardará a recarga de sua bateria até o tempo de funcionamento especificado como Desvio da duração do tempo de funcionamento de retorno (abaixo), se necessário, e aguardará o tempo especificado em “Atraso do retorno” e, em seguida, ele ligará.
Desvio da duração do tempo de funcionamento de retorno	Especifique o número de segundos do tempo de funcionamento que será subtraído do “Tempo de funcionamento de retorno mínimo” do no-break em inicialização. Isto determinará o tempo de funcionamento disponível necessário para ligar este membro do grupo em particular. Você pode configurar este valor de forma diferente para cada membro do SCG.
Frase de autenticação	A frase (15 a 32 caracteres ASCII), que diferencia maiúsculas de minúsculas, usada para autenticar membros de um SCG. Todos os membros de um SCG deverão ter a mesma frase de autenticação. O padrão é “APC ASI auth phrase”.
Frase de criptografia	A chave de criptografia para o protocolo que garante a comunicação segura entre os membros de um SCG. Todos os membros de um SCG deverão ter a mesma frase de criptografia. O padrão é “APC ASI crypt phrase”.
Porta de controle sincronizada	A porta de rede que os SCGs usam para se comunicar. Você pode usar qualquer porta não padrão, de 5000 a 32768.

A opção de unidades paralelas (dispositivos de no-break Smart-UPS VT)

Esta opção é exibida apenas com dispositivos Smart-UPS VT quando estiver definida uma configuração paralela. Relaciona todas as unidades paralelas (dispositivos de no-break que compartilham uma carga e continuam a fornecer potência à carga se uma unidade paralela não estiver funcionando). O no-break ao qual você está conectado é relacionado em primeiro lugar. Use **Adicionar unidade** para adicionar um no-break paralelo e especifique seu nome e endereço IP.

Tela Suporte de terceiros

Caminho: Configuração > Suporte de terceiros > EnergyWise

O Cisco® EnergyWise™ permite a medição e o gerenciamento do consumo de energia dos dispositivos de rede. Ele pode ser utilizado para reduzir o consumo, e os custos associados, do no-break e seus dispositivos conectados.

A tela **EnergyWise** na interface de usuário dessa NMC facilita o uso de um interruptor Cisco EnergyWise para monitorar e controlar o no-break e seus dispositivos. Isso inclui o desligamento do no-break e as tomadas comutadas individuais (se existirem).

O recurso EnergyWise na NMC SÓ pode ser usado em conjunto com um interruptor Cisco EnergyWise. Use esta tela de NMC EnergyWise para configurar as comunicações entre os dispositivos (inclusive o no-break) e o interruptor Cisco EnergyWise.

Qualquer geração de relatórios, análise e controle (como o desligamento de uma tomada) é feito usando o interruptor Cisco.

Selecione EnergyWise nas opções do menu Configuração da NMC. Use a tela inicial **Configuração EnergyWise** para definir os parâmetros de comunicação com o interruptor Cisco. O nome de domínio e a senha secreta compartilhada (se utilizada) devem ser iguais aos utilizados no interruptor.

Campo	Descrição
Versão	A versão atual do conjunto de ferramentas do EnergyWise na NMC. Esta deve ser igual à versão do interruptor Cisco EnergyWise.
EnergyWise	Essa opção fica desativada por padrão. Selecione-a para ativar a comunicação do EnergyWise.
Porta	Especificar a porta de rede que a NMC usará para comunicar-se com o EnergyWise (por padrão, 43440). Os valores variam entre 0 e -65535.
Nome do domínio	Especifique o nome do domínio compartilhado entre a NMC e o interruptor Cisco EnergyWise.
Modo seguro	Selecione esta caixa de seleção para ativar o modo seguro para a comunicação entre a NMC e o interruptor. Isto é opcional.
Segredo compartilhado	Se você marcar a caixa de seleção do modo Seguro, deve inserir a senha secreta compartilhada usada entre seus dispositivos e o interruptor.

Uma vez definidos os parâmetros, clique em Aplicar e o interruptor Cisco consultará o domínio e encontrará o no-break e qualquer dispositivo conectado, inclusive aqueles conectados que usam Grupos de tomadas comutadas.

A metade inferior desta tela mostra seus dispositivos e os classifica em **Pai** e **Filho** (se for o caso).

O Pai é sempre seu no-break. Se houver dispositivos conectados aos Grupos de tomadas comutadas, eles serão exibidos no cabeçalho Configuração de filho.

Os campos associados, **Nome**, **Função**, **Palavras-chave** e **Importância** podem ser editados clicando no link Nome ou você pode aceitar os padrões. É obrigatório ter valores em Nome e Importância.



Os valores de **Função**, **Palavras-chave**, **Importância** devem ser valores de especificação padrão do Cisco EnergyWise. Eles permitem a consulta do estado de seus dispositivos.

Campo	Descrição
Nome	O Nome usado para identificar o pai e os filhos associados do no-break.
Função	Esta é uma categoria de pesquisa disponível para o interruptor Cisco. A função define o trabalho ou função do dispositivo dentro da rede. O valor padrão da função do pai é “Uninterruptible Power Supply”. O valor padrão da função do filho é “Grupos de tomadas”, se houver suporte.

Campo	Descrição
Palavras-chave	<p>Esta é uma categoria de pesquisa disponível para o interruptor Cisco.</p> <p>As palavras-chave são uma forma de agrupar o pai e os dispositivos filhos associados. Isto permite filtrar os resultados da pesquisa e gerar relatórios.</p> <p>O valor padrão de um pai é “apc,ups,smartups”. O padrão de cada filho é “apc,ups,smartups,outlet”.</p>
Importância	<p>Use o campo Importância para classificar ou priorizar um dispositivo.</p> <p>O valor pode ser um número inteiro de 1 a 100 onde 1 é o menos importante e 100 é o mais importante. O valor padrão do pai e cada filho é 1.</p>

Tela E/S universal



O menu **E/S universal** é importante quando estiverem instalados os sensores de temperatura e umidade (AP9335T/TH) ou o Acessório de E/S de contato seco (AP9810). O uso destes normalmente é chamado de monitoramento ambiental.

Tela Temperatura e umidade

E/S Universal > Temp e Umidade

Exibe o nome, o status do alarme, a temperatura e a umidade (se houver suporte) de cada sensor. Clique no nome de um sensor para editar o nome e a localização e para configurar seus limites e histerese.

Limites. Para cada sensor, são configurados os limites de temperatura e (se houver suporte) umidade, medidas no sensor. Quando o limite for ultrapassado, o alarme sinalizará.

Alta e **Baixa** são mensagens de advertência. **Máximo** e **Mínima** são críticos e devem ser tratados.

Histerese. Use o valor da histerese para evitar que o alarme seja acionado repetidamente para a mesma violação do limite de temperatura ou umidade.

Quando a temperatura ou umidade que causa uma violação tende a oscilar levemente para cima e para baixo, pode disparar o alarme repetidamente. Um valor de histerese maior pode evitar isso.

Se o valor da histerese não for alto o suficiente, a oscilação pode causar primeiro uma violação de limite e depois cancelá-lo, o que significa que o alarme pode ser disparado várias vezes. Consulte os exemplos abaixo, após observar o seguinte.

- Para as violações dos limites máximo e alto, o ponto de cancelamento para o alarme é o limite *menos* o valor da histerese inserido por você.
- Para as violações dos limites baixo e mínimo, o ponto de cancelamento é o limite *mais* o valor da histerese.

Exemplo de temperatura em aumento, mas oscilante: Digamos que o limite *máximo* de umidade é 65% e a histerese da umidade é 10%. Em seguida, a umidade sobe acima de 65%, disparando o alarme. Depois ela oscila para baixo até 60% e para cima até 70% repetidamente, mas — por causa do valor da histerese de 10% — o alarme não é cancelado e portanto não ocorre um novo alarme. Para cancelar o alarme existente, a umidade teria que cair abaixo de 55% (que é 65% *menos* 10%).

Exemplo de temperatura em queda, mas oscilante: Digamos que o limite *mínimo* da temperatura é de 12 °C, e a histerese da temperatura é 2 °C. Em seguida, a temperatura cai abaixo de 12 °C, causando um alarme. Em seguida, ela oscila novamente até 13 ° e para baixo até 11 ° repetidamente, mas — por causa do valor da histerese de 2 ° — o alarme não é cancelado e portanto não ocorre um novo alarme. Para cancelar o alarme existente, a temperatura teria que subir acima de 14 ° (que é 12 ° *mais* 2 °).

Tela Contatos de entrada

Caminho: E/S universal > Contatos de entrada

Contatos de entrada exibe o nome, o status do alarme e o estado (aberto ou fechado) de cada contato. Estes são automaticamente encontrados e exibidos aqui quando você instala o acessório ambiental.

Clique no nome de um contato de entrada para ver o status detalhado ou para configurar seus valores. Quando estiver desativado, o contato não gera alarmes, mesmo quando estiver em posição anormal. Outros campos são discutidos a seguir:

Campo	Descrição
Status do alarme	Normal se este contato de entrada não estiver relatando um alarme, ou a severidade do alarme, se este contato de entrada estiver relatando um alarme. Se não estiver ativado para um contato, será exibido Desativado .
Estado	O estado atual desse contato de entrada: Fechado ou Aberto .
Estado normal	O estado normal (sem alarme) desse contato de entrada: Fechado ou Aberto .
Severidade	A severidade do alarme que o estado anormal desse contato de entrada gera: Aviso ou Crítico .

Tela Relé de saída

Caminho: E/S Universal > Relé de saída

Relé de saída exibe o nome e o estado (aberto ou fechado) de cada relé. Estes são automaticamente encontrados e exibidos aqui quando você instala o acessório ambiental.

Clique no nome de um contato de entrada para ver o status detalhado ou para configurar seus valores. Os campos são discutidos a seguir:

Campo	Descrição
Estado	O estado atual deste relé de saída: Fechado ou Aberto .
Estado normal	O estado normal (sem alarme) deste relé de saída: Fechado ou Aberto .
Controle	Para alterar o estado atual deste relé de saída, selecione esta caixa de seleção e clique em Aplicar.
Atraso	O número de segundos que uma condição de alarme selecionada deverá existir antes que o relé de saída seja ativado. Use esta configuração para evitar ativar um alarme para condições transientes breves. Se ocorrerem alarmes adicionais mapeados após o início do atraso, este não será reiniciado mas continuará a contagem regressiva até que o relé de saída seja ativado.
Permanência	O número mínimo de segundos que o relé de saída permanece ativado após a ocorrência do alarme. Mesmo que a condição que ativa o alarme seja corrigida, o relé de saída permanecerá ativado até que este período de tempo expire.

Configuração da Diretiva de controle

Caminho: E/S Universal > Diretiva de controle

Em uma NMC AP9631 com até dois acessórios de E/S de contato seco conectados (AP9810), você pode:

- configurar relés de saída para abrir ou fechar contatos de entrada e eventos com base no no-break, consulte “Configuração de uma saída para responder a um evento”
- configurar o no-break para executar uma ação com base em contatos de entrada, consulte “Configuração do no-break ou da saída para responder a um alarme de entrada”



Nem todos os dispositivos de no-break podem ser configurados para responder aos contatos de entrada.

Configuração de uma saída para responder a um evento.

1. No menu **Configuração**, selecione **E/S universal** e **Diretiva de controle**.
2. Clique no botão **Adicionar diretiva**.
3. Clique no nome de uma categoria ou subcategoria para ver os eventos correspondentes.
4. Para configurar, clique no nome de um evento, selecione a caixa de seleção do relé de saída que mudará de estado quando este evento ocorrer, e clique em **Salvar diretiva**.

Configuração do no-break ou da saída para responder a um alarme de entrada.

1. No menu **Configuração**, selecione **E/S universal** e **Diretiva de controle**.
2. Clique no botão **Adicionar diretiva**.
3. Clique na subcategoria **Contato de E/S**.
4. Escolha o evento com a mesma severidade que o contato de entrada. Por exemplo, se a severidade do contato de entrada for crítica, escolha o evento crítico.

A NMC tem suporte para até quatro entradas. Deve-se especificar a entrada que será associada a este evento.

5. Na lista suspensa **Porta**, selecione o número da **Porta** universal do sensor (1 ou 2) para o qual o acessório de E/S de contato seco foi instalado.
6. Na lista suspensa **Zona**, selecione a letra da zona (A ou B) do contato para o qual a entrada foi instalada.
7. Defina a ação que o no-break realizará (se for o caso) quando a entrada mudar de estado.
8. Selecione a saída que abrirá ou fechará (se houver).
9. Clique em **Salvar diretiva**.



A ação que você configurar ocorrerá uma vez.

Se você restaurar a saída para o estado normal antes que a condição de alarme seja cancelada, ela não abrirá nem fechará novamente, a menos que a condição de alarme seja cancelada e, em seguida, ocorra novamente.

Menu Segurança

Tela Gerenciamento de sessão

Caminho: Configuração > Segurança > Gerenciamento de sessão

Ao ativar **Permitir logins simultâneos**, dois ou mais usuários poderão efetuar login ao mesmo tempo. Cada usuário tem acesso igual e cada interface (HTTP, FTP, console telnet, console serial (CLI) etc.) conta como um usuário que fez login.

Substituição de autenticação remota: A NMC tem suporte para armazenamento de senhas do Radius em um servidor. No entanto, se você ativar este cancelamento, a NMC permitirá que um usuário local efetue login usando a senha para a NMC que está armazenada localmente na NMC. Consulte também “Usuários locais” e “Autenticação de Usuários remotos”.

Resposta de ping

Caminho: Configuração > Segurança > Resposta de ping

Ative a caixa de seleção **Resposta de ping IPv4** para permitir que a placa de gerenciamento de rede 2 responda aos pings da rede. Isso não se aplica ao IPv6.

Usuários locais

Use estas opções do menu para exibir e para configurar o acesso e as preferências individuais (como o formato de exibição da data), para as interfaces de usuário da NMC. Isto se aplica aos usuários conforme definido por seu nome de login.

Caminho: Configuração > Segurança > Usuários Locais > Gerenciamento

Configuração do acesso de usuário. Com esta opção, um administrador ou superusuário pode relacionar e configurar o acesso dos usuários autorizados à UI. Clique no link do nome para exibir os detalhes e para editar ou excluir um usuário.

Clique em **Adicionar usuário** para adicionar um usuário. Na tela resultante **Configuração de usuário**, você pode adicionar um usuário e impedir o acesso limpando a caixa de seleção **Acesso**. O tamanho máximo tanto para o nome quanto para a senha é de 64 bytes, menos para os caracteres multibyte. Você deve inserir uma senha.



Os valores que ultrapassem os 64 bytes no Nome e na Senha podem ficar truncados!

Para alterar a configuração de um administrador ou superusuário, você deve preencher todos os três campos de senha.

Use **Tempo limite da sessão expirado** para configurar o tempo que esta UI espera antes de desconectar este

usuário (por padrão, 3 minutos). Se você alterar este valor, deve-se fazer o logout para que a alteração entre em vigor.

Substituição de autenticação remota serial: Ao selecionar esta opção, você pode ignorar o RADIUS usando a conexão da console serial (CLI). Esta tela a ativa para o usuário selecionado, mas também deve ser ativada globalmente para funcionar por meio da “Tela Gerenciamento de sessão”.

Veja também “Configuração > Segurança > Usuários Locais > Configurações padrão” abaixo. Para obter informações secundárias sobre contas, consulte “Tipos de contas de usuário”.

Opções do usuário. Marque a caixa de seleção **Código de cores do log de eventos** para ativar a codificação de cores do texto de alarme registrado no log de eventos. (As entradas de eventos do sistema e as entradas de alterações de configuração não mudam de cor).

Cor do texto	Severidade do alarme
Vermelho	Crítico: existe um alarme crítico que exige ação imediata.
Laranja	Aviso: uma condição de alarme requer atenção e poderá comprometer os dados ou equipamentos se sua causa não for tratada.
Verde	Alarme cancelado: as condições que causaram o alarme melhoraram.
Preto	Normal: não existem alarmes. A placa de gerenciamento de rede e todos os dispositivos conectados estão funcionando normalmente.

Formato de exportação do log: Os arquivos de log exportados podem ser formatados usando CSV (valores separados por vírgulas) ou tabulações. Consulte “Para exibir o Log de eventos”.

Selecione a escala de temperatura para medições nesta UI. **Padrão dos EUA** corresponde a Fahrenheit e **Métrico** corresponde a Celsius.

É possível especificar o idioma padrão para a interface do usuário no campo **Idioma**. Isso pode ser configurado também quando você fizer o login.



É possível também especificar idiomas diferentes para os destinatários de e-mail e receptores de traps SNMP. Consulte “Destinatários de email” e “Receptores de traps”.

Caminho: Configuração > Segurança > Usuários Locais > Configurações padrão

Com as configurações padrão é possível adicionar usuários de forma mais rápida. Use esta opção para definir os padrões para as múltiplas opções na tela Gerenciamento, consulte “Configuração > Segurança > Usuários Locais > Gerenciamento” acima.

Autenticação de Usuários remotos

Caminho: Configuração > Segurança > Usuários remotos > autenticação

Autenticação. Especifique como deseja que os usuários sejam autenticados no login.



Para obter informações sobre a autenticação local (não usando a autenticação centralizada de um servidor RADIUS), consulte o *Manual de segurança*, disponível no CD de *Utilitários* e no site www.apc.com.

As seguintes funções de autorização e autenticação do RADIUS (Remote Authentication Dial-In User Service, serviço de usuário de discagem de autenticação remota) são compatíveis:

- Quando um usuário acessa a NMC ou outro dispositivo ativado por rede que tenha o RADIUS ativado, uma solicitação de autenticação é enviada ao servidor RADIUS para determinar o nível de permissão do usuário.
- Os nomes de usuário do RADIUS são limitados a 32 caracteres com a NMC.

Selecione uma das opções:

- **Somente autenticação local:** o RADIUS fica desativado. Consulte “Usuários locais”.
- **RADIUS e, depois, Autenticação local:** Ambos estão ativados. A autenticação é solicitada primeiro do servidor RADIUS. Se o servidor RADIUS não responder, será utilizada a autenticação local.
- **Somente RADIUS:** Não há autenticação local.



Se **Somente RADIUS** for a opção selecionada e o servidor RADIUS estiver indisponível, estiver incorretamente identificado ou incorretamente configurado, o acesso remoto ficará indisponível para todos os usuários. Para obter acesso novamente, deve-se utilizar uma conexão serial para a interface da linha de comando e alterar a configuração de **Acesso para Local** ou **radiusLocal**.

Por exemplo, o comando para alterar a configuração de acesso para **local** seria:
`radius -a local`



Veja também “Tela RADIUS” abaixo e “Configuração do servidor RADIUS”.

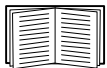
Tela RADIUS

Caminho: Configuração > Segurança > Usuários remotos > RADIUS

É possível utilizar um servidor RADIUS para autenticar os usuários remotos. Use esta opção para fazer o seguinte:

- Relacionar os servidores RADIUS (no máximo dois) disponíveis para a NMC e o tempo limite para cada um.
- Configure os parâmetros de autenticação para um servidor RADIUS novo ou existente clicando em um link do **Servidor RADIUS**.

Configuração do RADIUS	Descrição
Servidor RADIUS	O nome do servidor ou o endereço IP (IPv4 ou IPv6). Observação: os servidores RADIUS usam a porta 1812 para autenticar usuários e isto não pode ser alterado.
Segredo	O segredo compartilhado entre o servidor RADIUS e a NMC.
Tempo limite de resposta esgotado	O tempo em segundos durante o qual a NMC aguarda uma resposta do servidor RADIUS.
Testar configurações	Digite o nome de usuário e a senha do administrador para testar o caminho do servidor RADIUS que você configurou.
Ignorar teste e aplicar	Não testar o caminho do servidor RADIUS.



Veja também “Autenticação de Usuários remotos” acima e “Configuração do servidor RADIUS” abaixo.

Configuração do servidor RADIUS

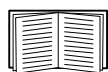
Resumo do procedimento de configuração.

Deve-se configurar o servidor RADIUS para que este funcione com a NMC. Veja os passos abaixo.



Para obter exemplos do arquivo de usuários do RADIUS com atributos específicos do fornecedor (VSAs) e um exemplo de uma entrada no arquivo de dicionário no servidor RADIUS, consulte o *Manual de segurança*, disponível no CD de *Utilitários* e no site www.apc.com.

1. Adicione o endereço IP da NMC à lista de clientes do servidor RADIUS (arquivo).
2. Os usuários deverão ser configurados com os atributos do tipo de serviço a menos que sejam definidos os atributos específicos do fornecedor (VSAs). Se não houver atributo de tipo de serviço configurado, os usuários terão acesso somente leitura (somente na interface do usuário).



Consulte a documentação do servidor RADIUS para obter informações sobre o arquivo de usuários RADIUS e consulte o *Manual de segurança* para obter um exemplo.

3. Os atributos específicos do fornecedor podem ser utilizados no lugar dos atributos de tipo de serviço fornecidos pelo servidor RADIUS. Os atributos específicos do fornecedor requerem uma entrada de dicionário e um arquivo de usuários do RADIUS. No arquivo do dicionário, defina os nomes para as palavras-chave ATTRIBUTE e VALUE, mas não para os valores numéricos. Se os valores numéricos forem alterados, a autenticação e a autorização do RADIUS não funcionarão. Os atributos específicos do fornecedor têm preferência sobre os atributos padrão do RADIUS.

Configuração de um servidor RADIUS no UNIX® com senhas duplicadas.

Se forem utilizados arquivos UNIX com senhas duplicadas (/etc/passwd) com os arquivos de dicionário do RADIUS, os dois métodos a seguir poderão ser utilizados para autenticar os usuários:

- Se todos os usuários UNIX tiverem privilégios administrativos, adicione o item a seguir ao arquivo "user" do RADIUS. Para permitir somente usuários de dispositivos, altere APC-Service-Type para Device.

```
DEFAULT Auth-Type = System
APC-Service-Type = Admin
```

- Adicione nomes de usuário e atributos ao arquivo "user" do RADIUS e verifique a senha comparando com /etc/senha. O exemplo a seguir é para os usuários bconners e thawk:

```
bconners Auth-Type = System
APC-Service-Type = Admin
thawk Auth-Type = System
APC-Service-Type = Device
```

Servidores RADIUS compatíveis.

FreeRADIUS e Microsoft IAS 2003 são compatíveis. Outros aplicativos RADIUS normalmente disponíveis poderão funcionar, mas ainda não foram totalmente testados.

Tela Firewall

Caminho: Configuração > Segurança > Firewall

Opção do menu	Descrição de uso
Configuração	Ativar ou desativar o recurso de firewall geral. Qualquer diretiva configurada também será relacionada, mesmo se que o firewall esteja desativado.
Diretiva ativa	Selecione uma diretiva ativa entre as diretivas de firewall disponíveis. A validade da diretiva também é relacionada aqui.
Regras ativas	Quando um Firewall está ativado (consulte Configuração acima, nesta tabela), este relaciona as regras individuais impostas por uma diretiva ativa atual. Você pode editar regras existentes e adicionar ou excluir novas regras aqui.
Criar/Editar diretiva	Criar uma nova diretiva ou editar uma existente.
Carregar diretiva	Carregar um arquivo de diretiva (com um sufixo .fwl) de uma fonte externa para este dispositivo.
Teste	Temporariamente imponha as regras de uma diretiva escolhida, para uma hora especificada por você.

Ajuste das configurações: 2

Com as opções do menu Configuração, é possível definir valores operacionais fundamentais para o no-break e a NMC.

Consulte as seções abaixo e também “Ajuste das configurações: 1”.

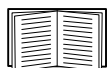
- “Rede no menu Configuração”
- “Menu Notificação”
- “Menu Geral”
- “Logs no menu Configuração”

Rede no menu Configuração

Tela Configurações de TCP/IP para IPv4

Caminho: Configuração > Rede > TCP/IP > Configurações IPv4

Esta opção mostra qualquer endereço de IPv4 atual, máscara de sub-rede, gateway padrão, endereço MAC e o modo de inicialização da Placa de gerenciamento de rede 2 do no-break (NMC). Use a parte inferior da tela para definir essas configurações, inclusive desativar o IPv4.



Para obter informações sobre o DHCP e opções do DHCP, consulte [RFC2131](#) e [RFC2132](#).

Opções	Descrição
Manual	Especifique o endereço IPv4, máscara de sub-rede, gateway padrão aqui.
BOOTP*	A cada 32 segundos o dispositivo solicita uma atribuição de rede de qualquer servidor BOOTP: <ul style="list-style-type: none">• Se ele receber uma resposta válida, iniciará os serviços de rede.• Se houver alguma configuração anterior de rede e ele não receber uma resposta válida de cinco solicitações (a original mais quatro tentativas), por padrão ele usará as configurações anteriores. Isto garante que ele permaneça acessível se já não houver um servidor de BOOTP acessível.• Se ele encontrar um servidor BOOTP, mas uma solicitação para esse servidor não funcionar ou tiver seu tempo limite esgotado, o dispositivo interromperá a solicitação das configurações de rede até que seja reiniciado.
DHCP*	A cada 32 segundos o dispositivo solicita uma atribuição de rede de qualquer servidor DHCP: <ul style="list-style-type: none">• Se um servidor DHCP for encontrado, mas uma solicitação para esse servidor não funcionar ou tiver seu tempo limite esgotado, o dispositivo interromperá a solicitação das configurações de rede até que seja reiniciado.• Opcionalmente, você pode configurar o dispositivo com Requer cookie específico do fornecedor para aceitar endereço DHCP para aceitar a concessão e iniciar os serviços de rede. Consulte “Opções de resposta do DHCP”.

*

Classe do fornecedor: APC

ID do cliente: o endereço MAC do dispositivo. Se alterar este valor, o novo valor deve ser único na LAN.

Classe de usuários: o nome do módulo de firmware do aplicativo, consulte “Transferências de arquivos”.

Tela Configurações de TCP/IP para IPv6

Caminho: Configuração > Rede > TCP/IP > Configurações IPv6

Esta opção mostra qualquer configuração de IPv6 atual da placa de gerenciamento de rede 2 do no-break (NMC). Use a parte inferior da tela para definir essas configurações, inclusive desativar o IPv6.

Você pode escolher o uso do endereçamento IP manual ou automático. Também é possível utilizar ambos simultaneamente. Para a opção **Manual**, marque a caixa de seleção e insira o endereço v6 **IP do sistema** e o **Gateway padrão**.

Marque a caixa de seleção **Configuração automática** para permitir que o sistema obtenha os prefixos de endereçamento do roteador (se disponíveis). Ele usará esses prefixos para configurar automaticamente os endereços IPv6.

Formatos possíveis do IPv6	Descrição
fe80:0000:0000:0000:0204:61ff:fe9d:f156	Forma completa do IPv6
fe80:0:0:0:204:61ff:fe9d:f156	excluindo zeros iniciais
fe80::204:61ff:fe9d:f156	substituindo os zeros múltiplos por:: no endereço IPv6
fe80:0000:0000:0000:0204:61ff:254.157.241.86	IPv4 quatro dígitos no final
fe80:0:0:0:0204:61ff:254.157.241.86	excluindo zeros iniciais, IPv4 quatro dígitos no final
fe80::204:61ff:254.157.241.86	quatro dígitos no final, substituindo os zeros múltiplos
::1	localhost
fe80::	prefixo de link local
2001::	prefixo unicast global

Para **Modo DHCPv6**, consulte a tabela abaixo.

Modo DHCPv6 para configuração de IPv6	
Opções	Descrição
Roteador controlado	<p>Quando esta caixa de opção é selecionada, o DHCPv6 é controlado pelos sinalizadores gerenciados M (sinalizador de configuração de endereço gerenciado) e O (outro sinalizador de configuração de stateful) recebidos nos anúncios do roteador IPv6.</p> <p>Quando um anúncio de roteador for recebido, a NMC verificará o sinalizador que está configurado, M ou O. A NMC os interpreta como segue:</p> <ul style="list-style-type: none">• Nenhum está configurado: Indica que a rede local não tem uma infraestrutura DHCPv6. A NMC usa anúncios do roteador e configuração manual para obter endereços que não sejam links locais e outras configurações.• M, ou M e O estão configurados: Nesta situação, ocorre a configuração total do endereço DHCPv6. O DHCPv6 é utilizado para obter endereços E outros ajustes de configuração. Isso é conhecido como “DHCPv6 stateful”. Assim que o sinalizador M for recebido, a configuração de endereço DHCPv6 permanecerá em vigor até que a interface em questão seja fechada, mesmo que sejam recebidos pacotes subsequentes de anúncios do roteador nos quais o sinalizador M não esteja definido. Se um sinalizador O for recebido em primeiro lugar e, em seguida, for recebido um sinalizador M subsequentemente, a NMC executará a configuração total do endereço ao receber o sinalizador M.• Somente O está configurado: Nesta situação a NMC envia um pacote de solicitação de informações do DHCPv6. O DHCPv6 é utilizado para ajustar "outras" configurações (como o local dos servidores DNS), mas NÃO para fornecer endereços. Isso é conhecido como “DHCPv6 stateless”.

Modo DHCPv6 para configuração de IPv6	
Opções	Descrição
Endereço e outras informações	O DHCPv6 é utilizado para obter endereços E outros ajustes de configuração. Isso é conhecido como “DHCPv6 stateful”.
Somente informações diferentes de endereço	O DHCPv6 é utilizado para ajustar "outras" configurações (como o local dos servidores DNS), mas NÃO para fornecer endereços. Isso é conhecido como “DHCPv6 stateless”.
Nunca	O DHCPv6 NÃO é utilizado para nenhum ajuste de configuração.

Opções de resposta do DHCP

Cada resposta válida do DHCP contém opções que fornecem as configurações de TCP/IP que a NMC necessita para operar em uma rede. Cada resposta também tem outras informações que afetam a operação da NMC. Consulte também o ID FA156110 em <http://www.apc.com/site/support/index.cfm/faq/index.cfm>.

Informações específicas do fornecedor (opção 43) A NMC utiliza esta opção em uma resposta do DHCP para determinar se a resposta do DHCP é válida. Essa opção contém uma opção em um formato TAG/LEN/DATA, denominado Cookie da APC. Por padrão ela fica desativada.

- **Cookie da APC. Tag 1, Len 4, Data “1APC”**

A opção 43 comunica à NMC que um servidor DHCP está configurado para os dispositivos de serviço.

Abaixo, em formato hexadecimal, apresentamos um exemplo da opção de informação específica do fornecedor que contém o cookie da APC:

Opção 43 = 0x01 0x04 0x31 0x41 0x50 0x43

Opções de TCP/IP. A NMC utiliza as seguintes opções em uma resposta válida do DHCP para definir suas configurações de TCP/IP. Todas essas opções exceto a primeira estão descritas na [RFC2132](#).

- **Endereço IP** (no campo `yiaddr` da resposta do DHCP, descrito na [RFC2131](#)): O endereço IP que o servidor DHCP está concedendo à NMC.
- **Máscara de sub-rede** (opção 1): O valor da máscara de sub-rede que a NMC necessita para operar na rede.
- **Roteador**, isso é, Gateway padrão (opção 3): O endereço do gateway padrão que a NMC necessita para operar na rede.
- **Tempo de concessão do endereço IP** (opção 51): O período de duração da concessão do endereço IP para a NMC.
- **Tempo para renovar, T1** (opção 58): O tempo que a NMC deve aguardar depois que uma concessão de endereço IP for atribuída, antes que ela possa solicitar uma renovação dessa concessão.
- **Tempo para revalidar, T2** (opção 59): O tempo que a NMC deverá aguardar depois que uma concessão de endereço IP for atribuída, antes que ela possa procurar revalidar essa concessão.

Outras opções. A NMC também utiliza essas opções em uma resposta válida do DHCP. Todas essas opções exceto a primeira estão descritas na [RFC2132](#).

- **Servidores do protocolo de horário da rede (NTP, Network Time Protocol)** (opção 42): Até dois servidores NTP (primário e secundário) que a NMC pode utilizar.
- **Diferença de horário** (opção 2): A diferença da sub-rede da NMC, em segundos, em relação à hora universal coordenada (UTC).
- **Servidor de nomes de domínio** (opção 6): Até dois servidores (primário e secundário) de nomes de domínio (DNS, Domain Name System) que a NMC pode utilizar.
- **Nome do host** (opção 12): O nome do host que a NMC utilizará (no máximo 32 caracteres).

- **Nome de domínio** (opção 15): O nome do domínio que a NMC utilizará (no máximo 64 caracteres).
- **Nome do arquivo de inicialização** (do campo **arquivo** da resposta do DHCP, descrito na RFC2131): O caminho do diretório totalmente qualificado para fazer download de um arquivo de configuração do usuário (.ini). O campo **siaddr** da resposta do DHCP especifica o endereço IP do servidor a partir do qual a NMC fará o download do arquivo .ini. Após o download, a NMC usa o arquivo .ini como arquivo de inicialização (boot) para reajustar as suas configurações.

Tela Velocidade da porta

Caminho: Configuração > Rede > Velocidade da porta

A configuração Velocidade da porta define a velocidade de comunicação da porta da rede Ethernet. Sua configuração atual é exibida em **Velocidade atual**.

Você pode alterar a configuração escolhendo um botão de opção em **Velocidade da porta**:

- Para **Autonegociação** (o padrão), os dispositivos de rede negociam para transmitir na velocidade mais alta possível, mas se as velocidades às quais os dois dispositivos têm suporte forem incompatíveis, será adotada a velocidade mais baixa.
- Opcionalmente, você pode selecionar **10 Mbps** ou **100 Mbps**, cada um com a opção de:
 - **semi-duplex** (comunicação em uma só direção ao mesmo tempo) ou
 - **bidirecional** (comunicação em ambas as direções no mesmo canal simultaneamente).

Tela DNS

Caminho: Configuração > Rede > DNS > Configuração

Os valores em **Status do Sistema de Nomes de Domínio** relacionam o status e a configuração atuais.

Use as opções em **Configurações manuais do Sistema de Nomes de Domínio** para configurar o sistema de nomes de domínio (DNS):

- Ativar **Substituir configurações manuais de DNS** significa que os dados de configuração de outras fontes como DHCP têm preferência sobre as configurações manuais aqui.
- Especifique o **Servidor DNS primário** e, opcionalmente, o **Servidor DNS secundário** com endereços IPv4 ou IPv6. Para que a NMC envie e-mail, você deve definir pelo menos o endereço IP do servidor DNS primário.
 - A NMC aguarda até 15 segundos pela resposta do servidor DNS primário ou do servidor DNS secundário. Se a NMC não receber uma resposta dentro desse tempo, o e-mail não poderá ser enviado. Use os servidores DNS no mesmo segmento da NMC ou em um segmento próximo, mas não em uma rede de longa distância (WAN).
 - Após definir os endereços IP dos servidores DNS, faça um teste, consulte “Tela Testando o DNS”.
- **Sincronização de nomes do sistema**: A ativação deste sincroniza o nome de host DNS com o nome do sistema da NMC. Clique no link Nome do sistema para defini-lo.
- **Nome do host**: Depois de configurar aqui um nome de host e um nome de domínio no campo **Nome do domínio**, os usuários poderão digitar um nome de host em qualquer campo da interface da NMC (exceto endereços de e-mail) que aceite um nome de domínio.

- **Nome do domínio (IPv4/IPv6):** Para a interface da NMC, é necessário configurar apenas o nome de domínio aqui. Em todos os outros campos nesta UI — exceto endereços de e-mail — que aceitam nomes de domínio, a NMC adiciona por padrão este nome de domínio quando for digitado apenas um nome do host.
 - Para cancelar a expansão de um determinado nome de host pela adição de um nome de domínio, configure este campo do nome de domínio com seu padrão, `somedomain.com`, ou com `0.0.0.0`.
 - Para cancelar a expansão de uma entrada *específica* de nome de host (por exemplo, ao definir um receptor de trap), inclua um ponto no final do nome de host. A NMC reconhece um nome de host com um ponto no final (como `mySnmpServer.`) como se fosse um nome de domínio totalmente qualificado e não acrescenta o nome de domínio.
- **Nome do domínio (IPv6):** Especificar aqui o nome de domínio IPv6.

Tela Testando o DNS

Caminho: Configuração > Rede > DNS > Teste

Use esta opção para enviar uma consulta DNS que teste a configuração dos servidores DNS pesquisando o endereço IP. Consulte a “Tela DNS” acima sobre como configurar seus servidores.

Exibir o resultado de um teste no campo **Resposta da última consulta**.

- Em **Tipo de consulta**, selecione o método para usar na consulta DNS. Consulte a tabela abaixo.
- Em **Pergunta da consulta**, especifique o valor a ser utilizado no tipo de consulta selecionado, conforme explicado na tabela.

Tipo de consulta selecionado	Pergunta da consulta a ser utilizada
por host	O nome do host, a URL
por FQDN	O nome de domínio totalmente qualificado, <code>my_server.my_domain.com</code>
por IP	O endereço IP do servidor.
por MX	O endereço de troca de e-mails.

Tela Acesso à Web

Caminho: Configuração > Rede > Web > Acesso

Use esta opção para configurar o método de acesso para a interface da Web. (Para ativar qualquer alteração aqui, você deve desconectar-se da interface de usuário da NMC).

Você pode ativar o acesso a esta UI por meio de **HTTP** ou **HTTPS** ou por meio de ambos, usando as caixas de seleção Ativar. O HTTPS criptografa nomes de usuário, senhas e dados durante a transmissão; o HTTP não.

O HTTPS também autentica a NMC por certificado digital. Consulte "Criação e instalação de certificados digitais" no *Manual de Segurança* no CD de *Utilitários* da NMC para ver como usar certificados digitais.

Para as **portas**, você pode alterar a configuração em qualquer porta não usada para obter segurança adicional; a faixa é de 5000 a 32768. Você deve usar dois pontos (:) no campo de endereço do navegador para especificar o número da porta. Por exemplo, para um número de porta 5000 e um endereço IP 152.214.12.114:

```
http(s)://152.214.12.114:5000
```

Tela Certificado SSL da Web

Caminho: Configuração > Rede > Web > Certificado SSL

Adicionar, substituir ou remover um certificado de segurança. O SSL (Secure Socket Layer) é um protocolo utilizado para criptografar dados entre seu navegador e o servidor da Web.

O **Status** pode ser:

- **Certificado válido:** Um certificado válido foi instalado ou foi gerado pela NMC. Clique neste link para exibir o conteúdo do certificado.
- **Certificado não instalado:** Não há um certificado instalado, ou então foi instalado por FTP ou SCP em um local incorreto. Usando **Adicionar ou substituir arquivo de certificado** é possível instalar o certificado no local correto: `/ssl` na NMC.
- **Gerando:** A NMC está gerando um certificado porque não foi encontrado um certificado válido.
- **Carregando:** Um certificado está sendo ativado na NMC.



Se instalar um certificado inválido, ou se nenhum certificado for carregado ao ativar o SSL, a NMC gerará um certificado padrão, um processo que atrasa o acesso à interface em até um minuto. É possível utilizar o certificado padrão para obter a segurança básica com base em criptografia, mas será exibida uma mensagem de alerta de segurança sempre que fizer o login.

Adicionar ou substituir arquivo de certificado: Procure o arquivo de certificado criado com o Assistente de segurança. Consulte "Criação e instalação de certificados digitais" no *Manual sobre Segurança* no CD de *Utilitários* da placa de gerenciamento de rede para ver como utilizar certificados digitais criados pelo Assistente de segurança ou gerados pela NMC.

Remover: Excluir o certificado. Ver também o texto na tela.

Tela Console

Caminho: Configuração > Rede > Console > Acesso

Caminho: Configuração > Rede > Console > Chave do host SSL

Acesso ao console. É necessário ativar o acesso ao console para atualizar o firmware do no-break, consulte "Tela Atualização de firmware". O acesso ao console ativa o uso da interface da linha de comando (CLI).

Você pode ativar o acesso à CLI através do **Telnet** ou **SSH** ou através de ambos, usando as caixas de seleção Ativar. O Telnet não criptografa nomes de usuário, senhas e dados durante a transmissão, enquanto o SSH 2 o faz.

Para as **portas** a serem utilizadas para comunicação com a NMC, é possível alterar a configuração para qualquer porta não utilizada, de 5000 a 32768, para obter segurança adicional.

- **Porta Telnet:** Esta é 23 por padrão. Os usuários deverão utilizar os dois pontos (:) ou um espaço para especificar a porta não padrão, conforme exigido pelo seu programa cliente Telnet.
Por exemplo, para a porta 5000 e um endereço IP de 152.214.12.114, o cliente Telnet requer um desses comandos:
`telnet 152.214.12.114:5000` ou `telnet 152.214.12.114 5000`
- **Porta SSH:** Esta é 22 por padrão. Consulte a documentação de seu cliente SSH para obter o formato da linha de comando exigido para especificar uma porta não padrão. Consulte também "Chave do host SSH" abaixo.

Chave do host SSH. Se estiver utilizando o SSH (Secure Shell Protocol) para o acesso ao console (CLI), você pode adicionar, substituir ou remover a chave de host na tela Chave do host SSL.

Status indica se a chave de host (chave privada) é válida. O Status pode ser:

- **SSH desativado:** Nenhuma chave de host em uso.

- **Gerando:** A NMC está criando uma chave de host porque nenhuma chave de host válida foi encontrada.
- **Carregando:** Uma chave de host está sendo ativada na NMC.
- **Válida:** Uma das seguintes chaves de host válidas está no diretório `/ssh` (o local exigido na placa de gerenciamento da rede):
 - Uma chave de host de 1024 ou 2048 bits criada pelo Assistente de segurança
 - Uma chave de host RSA de 2048 bits gerada pela placa de gerenciamento da rede

Adicionar ou substituir a chave de host: Faça upload de um arquivo de chaves de host criado pelo Assistente de segurança. Para utilizar o Assistente de segurança, consulte o Manual de segurança no CD de *Utilitários* da placa de gerenciamento de rede. Para usar uma chave de host criada externamente, carregue a chave de host antes de ativar o SSH (com o “Acesso ao console” acima).

Observação: para reduzir o tempo necessário para ativar o SSH, crie e faça upload de uma chave de host antecipadamente. *Se você ativar o SSH sem ter carregado uma chave de host, a NMC levará até um minuto para criar uma chave de host e o servidor SSH ficará inacessível durante esse tempo.*

Remover: Excluir a chave de host. Ver também o texto na tela.



Para utilizar o SSH, você deverá ter um cliente SSH instalado. A maioria das plataformas Linux e outras plataformas UNIX incluem um cliente SSH, mas os sistemas operacionais Windows da Microsoft não fazem isso. Os clientes estão disponíveis a partir de vários fornecedores.

Telas SNMP

Todos os nomes de usuários, senhas e nomes de comunidades para o SNMP são transferidos pela rede como texto sem formatação. Se a rede requer a alta segurança da criptografia, desative o acesso ao SNMP ou configure o acesso para cada comunidade como de leitura. (Uma comunidade com acesso de leitura pode receber as informações de status e utilizar traps SNMP.)

Ao utilizar o **StruxureWare Central** para gerenciar um no-break na rede pública de um sistema StruxureWare, você *deve* ter o SNMP v1 ou SNMP v3 ativado na interface da NMC. O acesso de leitura permitirá que o dispositivo do StruxureWare receba traps da NMC, mas o acesso de gravação é necessário enquanto você usar a interface de usuário da NMC para configurar o dispositivo do StruxureWare como um receptor de traps.



Para obter informações detalhadas sobre como melhorar e gerenciar a segurança do sistema, consulte o *Manual de segurança*, disponível no CD *Utilitários* da placa de gerenciamento de rede ou no site www.apc.com.

SNMPv1.

Caminho: Configuração > Rede > SNMPv1 > Acesso e Controle de acesso

Use **acesso** para ativar ou desativar o SNMP versão 1 como um método de comunicação com a NMC.

Controle de acesso. É possível configurar até quatro entradas de controle de acesso para especificar os sistemas de gerenciamento de rede (NMSs) que têm acesso à NMC. Para editar, clique no nome de uma comunidade.

Por padrão uma entrada é atribuída a cada uma das quatro comunidades SNMPv1 disponíveis. Você pode editar estas configurações para aplicar *mais de uma entrada a qualquer comunidade* para oferecer acesso por vários endereços IPv4 e IPv6 específicos, nomes de host ou máscaras de endereço IP.

- Por padrão, uma comunidade tem acesso à NMC de qualquer local na rede.
- Se configurar várias entradas de controle de acesso para qualquer nome de comunidade, isso significa que uma ou mais comunidades não têm acesso ao dispositivo.

Nome da comunidade: O nome que um NMS deve utilizar para acessar a comunidade. O tamanho máximo é de 15 caracteres ASCII, e os nomes padrão são `public`, `private`, `public2` e `private2`.

IP do NMS/Nome do host: Os endereços IPv4 e IPv6, a máscara do endereço IP ou o nome de host que controla o acesso por NMSs. Um nome de host ou um endereço IP específico (por exemplo, 149.225.12.1) permite acesso somente pelo NMS nesse local. Endereços IP que contêm 255 restringem o acesso como descrito a seguir:

- 149.225.12.**255**: Acesso somente por um NMS no segmento 149.225.12.
- 149.225.**255.255**: Acesso somente por um NMS no segmento 149.225.
- 149.**255.255.255**: Acesso somente por um NMS no segmento 149.
- 0.0.0.0 (a configuração padrão) que também pode ser expressa como 255.255.255.255: Acesso por qualquer NMS em qualquer segmento.

Tipo de acesso: As ações que um NMS pode executar por meio da comunidade.

- **Ler:** GETS somente, a qualquer momento
- **Gravar:** GETS a qualquer momento e SETS quando nenhum usuário estiver conectado à interface de usuário ou à interface da linha de comando.
- **Gravar+:** GETS e SETS a qualquer momento.
- **Desativar:** Nenhum GETS ou SETS em nenhum momento.

SNMPv3.

Caminho: Configuração > Rede > SNMPv3 > Acesso, Perfis de usuário e Controle de acesso

Para GETs, SETs e receptores de traps, o SNMPv3 usa um sistema de perfis de usuário para identificar os usuários. Um usuário do SNMPv3 deve ter um perfil atribuído no programa do software MIB para executar GETs e SETs, navegar no MIB e receber traps.



Para usar o SNMPv3, você precisa ter um programa de MIB que dê suporte a SNMPv3.

A NMC tem suporte para autenticação SHA ou MD5 e criptografia AES ou DES.

A ativação do acesso ao SNMPv3 no acesso ativa este método de comunicação com este dispositivo.

Perfis de usuário. Por padrão, relaciona as configurações de quatro perfis de usuário, configurados com os nomes de usuário **apc snmp profile1** a **apc snmp profile4** e sem autenticação e sem privacidade (sem criptografia). Para editar as configurações a seguir para um perfil de usuário, clique em um nome de usuário na lista.

- **Nome do usuário:** O identificador do perfil do usuário. O SNMP versão 3 mapeia GETs, SETs e traps para um perfil de usuário fazendo o nome de usuário do perfil corresponder ao nome de usuário no pacote de dados que está sendo transmitido. Um nome de usuário pode ter até 32 caracteres ASCII.
- **Senha de autenticação:** Uma senha de 15 a 32 caracteres ASCII (`apc auth passphrase`, por padrão) que verifica se o NMS que se comunica com este dispositivo por meio do SNMPv3 é o NMS que afirma ser.

Também verifica se a mensagem não foi alterada durante a transmissão e se a mensagem foi comunicada pontualmente. Isso indica que não foi adiado e que não foi copiado e enviado novamente mais tarde em uma hora inapropriada.

- **Senha de privacidade:** Uma senha de 15 a 32 caracteres ASCII (`apc crypt passphrase`, por padrão) que garante a privacidade dos dados que um NMS está enviando a esse dispositivo ou recebendo desse dispositivo por meio do SNMPv3, usando criptografia.
- **Protocolo de autenticação:** A implementação do SNMPv3 dá suporte a autenticação SHA e MD5. Uma dessas opções deve ser selecionada:
- **Protocolo de privacidade:** A implementação do SNMPv3 dá suporte a AES e DES como protocolos para criptografar e descriptografar dados. Você deve usar tanto um protocolo de privacidade como uma senha de privacidade, caso contrário a solicitação do SNMP não será criptografada.

Na sequência, não é possível selecionar o protocolo de privacidade se não houver protocolo de autenticação selecionado.

Controle de acesso. É possível configurar até quatro entradas de controle de acesso para especificar os sistemas de gerenciamento de rede (NMSs) que têm acesso à NMC. Para editar, clique no nome de um usuário.

Por padrão uma entrada é atribuída a cada um dos quatro perfis de usuário. Você pode editar estas configurações para aplicar *mais de uma entrada a qualquer perfil de usuário* para oferecer acesso por vários endereços IP específicos, nomes de host ou máscaras de endereço IP.

- Por padrão, todos os NMSs que usam esse perfil têm acesso a este dispositivo.
- Se configurar várias entradas de controle de acesso para um perfil de usuário, significa que um ou mais dos outros perfis de usuário não devem ter acesso a este dispositivo.

Nome do usuário: Na lista suspensa, selecione o perfil de usuário para o qual essa entrada de controle de acesso será aplicada. As escolhas disponíveis são os quatro nomes de usuário configurados por meio da opção “Perfis de usuário”.

IP do NMS/Nome do host: O endereço IP, máscara do endereço IP ou nome do host que controla o acesso pelo NMS. Um nome de host ou um endereço IP específico (por exemplo, 149.225.12.1) permite acesso somente pelo NMS nesse local. Uma máscara de endereço IP que contém 255 restringe o acesso conforme descrito a seguir:

- 149.225.12.**255**: Acesso somente por um NMS no segmento 149.225.12.
- 149.225.**255.255**: Acesso somente por um NMS no segmento 149.225.
- 149.**255.255.255**: Acesso somente por um NMS no segmento 149.
- 0.0.0.0 (a configuração padrão) que também pode ser expressa como 255.255.255.255: Acesso por qualquer NMS em qualquer segmento.

Tela Servidor FTP

Caminho: Configuração > Rede > Servidor FTP

Use esta tela para ativar o acesso a um servidor FTP e especificar uma porta.

Opções	Descrição
Acesso	<p>O FTP transmite arquivos sem criptografá-los.</p> <p>Para transferência de arquivos criptografados, use Secure CoPy (SCP). O SCP é ativado automaticamente quando o SSH for ativado, mas deve-se desativar o Servidor FTP nesse caso, para reforçar uma transferência de arquivos altamente segura.</p> <p>Observação: Quando quiser que um dispositivo fique acessível para gerenciamento pelo InfraStruXure Central ou Manager, o Servidor FTP deve ser ativado na interface da placa de gerenciamento de rede daquele no-break. Para obter informações detalhadas sobre como melhorar e gerenciar a segurança do seu sistema, consulte o <i>Manual de segurança</i> disponível no CD de utilitários ou no site da APC.</p>
Porta	<p>A porta TCP/IP do servidor FTP (21 por padrão).</p> <p>O servidor FTP usa tanto a porta especificada quanto a porta um número abaixo da porta especificada. Os números de porta diferentes do padrão permitidos são indicados na tela: 21 e 5001–32768.</p> <p>Observação: Configurar o servidor FTP para utilizar uma porta não padrão melhora a segurança ao exigir que os usuários adicionem o nome da porta ao endereço IP na linha de comando FTP. O nome da porta adicionado deve ser precedido de um espaço ou dois pontos, dependendo do cliente FTP utilizado.</p>

Menu Notificação

Consulte estas seções:

- “Tipos de notificação”
- “Configuração de ações de eventos”
- “Telas de notificação por e-mail”
- “Tela de teste de traps de SNMP”
- “Tela de receptores de traps de SNMP”
- “Serviço de Monitoração Remota”

Tipos de notificação

É possível configurar ações de notificação para ocorrerem em resposta a um evento. Você pode notificar os usuários sobre o evento por qualquer um de vários métodos:

- Ativo, notificação automática. Os usuários ou dispositivos de monitoramento especificados são contatados diretamente.
 - Notificação por e-mail
 - Traps do SNMP
 - Serviço de monitoração remota
 - Notificação do syslog
- Notificação indireta
 - Log de eventos. Se não houver uma notificação direta configurada, os usuários deverão verificar o log para determinar quais eventos ocorreram



Você pode também registrar os dados de desempenho do sistema para usar na monitoração de dispositivos. Consulte “Log de dados” para obter informações sobre como configurar e usar esta opção de registro de dados.

- Consultas (GETs do SNMP)



Para obter mais informações, consulte “Tela de receptores de traps de SNMP” e “Tela de teste de traps de SNMP”. O SNMP possibilita que uma NMS realize consultas informativas. Para o SNMPv1, que não criptografa os dados antes da transmissão, configurar o tipo de acesso SNMP mais restritivo (LEITURA) ativa as consultas informativas sem o risco de permitir alterações remotas de configuração.

A placa de gerenciamento de rede suporta o uso da **MIB RFC1628** (Management Information Base, Base de Informações de Gerenciamento). Consulte “Tela de receptores de traps de SNMP” para obter informações sobre como configurar um receptor de traps. O grupo de três eventos da **1628 MIB** funciona somente com aquela MIB, e não com a MIB alternativa da Powernet. Eles podem ser configurados com qualquer evento (consulte “Configuração de ações de eventos” abaixo).

Configuração de ações de eventos

Configuração por evento.

Caminho: Configuração > Notificação > Ações de eventos > Por evento

Por padrão, a ação de registrar um evento está selecionada para todos os eventos. Para definir ações de eventos para um evento individual:

1. Selecione o menu **Configuração**, em seguida **Notificação**, **Ações de eventos** e **Por evento**.

2. Para achar um evento, clique no cabeçalho de uma coluna para ver as listas nas categorias **Eventos de energia**, **Eventos de ambiente** ou **Eventos de sistema**.

Ou você pode clicar em uma sub-categoria nesses cabeçalhos como **Status da linha de entrada** ou **Temperatura**.

3. Clique no nome do evento, para visualizar ou alterar a configuração atual como, por exemplo, os destinatários a serem notificados por e-mail, ou os sistemas de gerenciamento de rede (NMSs) a serem notificados pelos traps do SNMP. Consulte “Parâmetros de notificação por e-mail”.



Se não houver um servidor do Syslog configurado, os itens relacionados à configuração do Syslog não serão exibidos.



Ao exibir detalhes da configuração de um evento, você pode ativar ou desativar o registro dos eventos ou o Syslog ou desativar a notificação para determinados destinatários de e-mail ou receptores de traps, mas você não pode adicionar nem remover destinatários ou receptores. Para adicionar ou remover destinatários ou receptores, consulte:

- “Identificação dos servidores do Syslog”
- “Destinatários de email”
- “Receptores de traps”

Configuração por grupos de eventos.

Caminho: Configuração > Notificação > Ações de eventos > Por grupo

Para configurar um grupo de eventos simultaneamente:

1. Selecione o menu **Configuração**, em seguida **Notificação**, **Ações de eventos** e **Por grupo**.
2. Escolha como agrupar eventos para configuração:
 - Selecione **Agrupados por severidade** e, em seguida, selecione um ou mais níveis de severidade. Não é possível alterar a severidade de um evento.
 - Selecione **Agrupados por categoria** e, em seguida, selecione todos os eventos em uma ou mais categorias predefinidas.
3. Clique em Avançar para passar de uma tela para outra para fazer o seguinte:
 - a. Selecionar ações de eventos para o grupo de eventos.
 - Para selecionar qualquer ação exceto **Registro** (padrão), deve-se antes ter pelo menos um receptor ou destinatário pertinente configurado.
 - Se você selecionar **Registrando** e tiver configurado um servidor do Syslog, selecione **Log de eventos** ou Syslog (ou ambos) na próxima tela (consulte “Logs no menu Configuração”).
 - b. Selecione deixar a ação de evento recém-configurada ativada para esse grupo de eventos ou selecione desativar a ação.

Consulte “Parâmetros de notificação por e-mail” diretamente abaixo.

Parâmetros de notificação por e-mail. Estes campos de configuração definem parâmetros de e-mail para enviar notificações de eventos. Consulte “Configuração por evento” e “Configuração por grupos de eventos”.

Normalmente são acessados clicando-se no nome do destinatário ou receptor.

Campo	Descrição
Atraso <i>n</i> tempo antes de enviar	Se o evento persistir pelo tempo especificado, uma notificação será enviada. Se a condição for cancelada antes do tempo expirar, nenhuma notificação será enviada.

Campo	Descrição
Repetir em um intervalo de <i>n</i>	A notificação é enviada repetidamente no intervalo especificado (o padrão é a cada 2 minutos até que a condição seja cancelada).
Até <i>n</i> vezes	Durante um evento ativo, a notificação é repetida este número de vezes.
ou	
Até que a condição seja cancelada	A notificação é enviada repetidamente até que a condição seja cancelada ou resolvida.

Para eventos que têm um evento de cancelamento associado, você também pode definir estes parâmetros. (Um exemplo de um evento com este evento de cancelamento é UPS: Lost communication with the battery packs e UPS: Restored communication with the battery packs) (No break: Perda de comunicação com módulos de bateria; No-break: Comunicação com módulos de bateria restaurada.)

Telas de notificação por e-mail

Visão geral das configurações. Use o SMTP (Simple Mail Transfer Protocol) para enviar e-mails para até quatro destinatários quando ocorrer um evento.

Para usar o recurso de email, você deve definir as seguintes configurações:

- Os endereços IP dos servidores do sistema de nomes de domínio (DNS, Domain Name System) primários e, opcionalmente, secundários. (Consulte “Tela DNS”)
- O endereço IP ou nome de DNS para o **Servidor SMTP** e o **Endereço De**. (Consulte “Servidor SMTP” abaixo)
- Os endereços de e-mail para um máximo de quatro destinatários. (Consulte “Destinatários de email”)



Você pode usar a configuração de **Endereço Para** da opção **destinatários** para enviar o e-mail a uma tela com base em texto.

Servidor SMTP.

Caminho: Configuração > Notificação > E-mail > Servidor

Esta tela relaciona o servidor DNS primário e secundário (consulte “Tela DNS”) e em seguida estes campos:

Campo	Descrição
Configuração de saída de e-mails	
Endereço De	<p>O conteúdo do campo De nas mensagens de e-mail enviadas pela NMC:</p> <ul style="list-style-type: none"> • No formato <i>usuário@[endereço_IP]</i> (se um endereço IP estiver especificado como Servidor SMTP local) • No formato <i>usuário@domínio</i> (se o DNS estiver configurado e o nome DNS estiver especificado como Servidor SMTP local) nas mensagens de e-mail. <p>Observação: O servidor SMTP local pode exigir a utilização de uma conta de usuário válida no servidor para essa configuração. Consulte a documentação do servidor.</p>
Servidor SMTP	<p>O endereço IPv4/ IPv6 ou nome DNS do servidor SMTP local.</p> <p>Observação: Esta definição é necessária somente quando o Servidor SMTP está configurado como Local. Consulte “Destinatários de email”.</p>
Autenticação	Ative isto se o servidor SMTP exigir autenticação.
Porta	O número da porta do SMTP, com um padrão de 25. A faixa é de 1 a 65535.
Nome de usuário/Senha/ Confirmar senha	Se o seu servidor de e-mail requer autenticação, digite o seu nome de usuário e senha aqui. Isso irá realizar uma autenticação simples, não uma SSI.

Campo	Descrição
Avançado	
Usar SSL/TLS	<ul style="list-style-type: none"> • Nunca: O servidor SMTP não exige nem tem suporte para criptografia. • Se compatível: O servidor SMTP anuncia suporte para STARTTLS, mas <i>não</i> requer que a conexão seja criptografada. O comando STARTTLS é enviado após o anúncio. • Sempre: O servidor SMTP requer que o comando STARTTLS seja enviado na conexão a este. • Implicitamente: O servidor SMTP só aceita conexões que comecem criptografadas. Nenhuma mensagem do STARTTLS é enviada ao servidor.
Exigir certificado raiz da autoridade de certificação	Isto deve estar ativado apenas se a diretiva de segurança de sua organização não permitir confiança implícita das conexões SSL. Se esta opção estiver ativada, deve ser carregado um certificado raiz de autoridade de certificação válido na NMC para que os e-mails criptografados sejam enviados.
Nome do arquivo	Este campo depende dos certificados raiz de autoridade de certificação instalados na NMC e se um certificado é necessário ou não.

Destinatários de email.

Caminho: Configuração > Notificação > E-mail > Destinatários

Especificar até quatro destinatários de e-mail. Clique em um nome para definir as configurações. Consulte também “Servidor SMTP” acima.

Campo	Descrição
Geração de e-mail	Ativa (por padrão) ou desativa o envio de e-mail ao destinatário.
Endereço Para	<p>Os nomes de usuário e domínio do destinatário. Para usar e-mail para paging, use o endereço de e-mail para a conta de gateway do pager do destinatário (por exemplo, myacct100@skytel.com). O gateway do pager irá gerar a página.</p> <p>Para ignorar a pesquisa de DNS do endereço IP do servidor de e-mail, use o endereço IP entre colchetes em vez do nome de domínio do e-mail, por exemplo, use jsmith@[xxx.xxx.x.xxx] em vez de jsmith@company.com. Isto é útil quando as pesquisas de DNS não estiverem funcionando corretamente.</p> <p>Observação: O pager do destinatário deverá ser capaz de usar o recurso de mensagens com base em texto.</p>
Formato	O formato longo contém nome, local, contato, endereço IP, número de série do dispositivo, data e hora, código do evento e descrição do evento. O formato curto fornece apenas a descrição do evento.
Idioma	Selecione um idioma na lista suspensa e todos os e-mails serão enviados nesse idioma. É possível usar idiomas diferentes para usuários diferentes. Consulte “Adição e alteração de pacotes de idiomas”.
Servidor	<p>Selecione um dos seguintes métodos para roteamento de e-mails:</p> <ul style="list-style-type: none"> • Local: Por meio do servidor SMTP do site local. Esta configuração recomendada garante que o e-mail seja enviado usando o servidor SMTP do site local. A escolha desta configuração limita os atrasos e paralisações da rede e tenta novamente enviar o e-mail por muitas horas. Ao escolher a configuração Local você também deve ativar o encaminhamento no servidor SMTP do dispositivo e configurar uma conta de e-mail externa especial para receber o e-mail encaminhado. Verifique com o administrador do servidor SMTP antes de fazer estas alterações. • Destinatário: Por meio do servidor SMTP do destinatário. A NMC executa uma procura de registro de MX no endereço de e-mail dos destinatários e utiliza este como seu servidor SMTP. O e-mail é enviado apenas uma vez portanto poderia se perder facilmente. • Personalizado: Esta configuração ativa cada destinatário de e-mail para ter suas próprias configurações de servidor. Estas configurações são independentes das configurações dadas em “Servidor SMTP” acima.

Certificados SSL de email.

Caminho: Configuração > Notificação > E-mail > Certificados SSL

Carregue um certificado SSL de e-mail na NMC para obter maior segurança. O arquivo deve ter uma extensão .crt ou .cer. Até cinco arquivos podem ser carregados a qualquer momento.

Quando instalado, os detalhes do certificado também são exibidos aqui. Um certificado inválido exibirá “n/a” para todos os campos exceto o Nome do arquivo.

Os certificados podem ser excluídos desta tela. Qualquer destinatário de e-mail que usar o certificado deve ser modificado manualmente para remover a referência a este certificado.

Enviar email de teste.

Caminho: Configuração > Notificação > E-mail > Teste

Envia uma mensagem de teste a um destinatário configurado.

Tela de receptores de traps de SNMP

Receptores de traps.

Caminho: Configuração > Notificação > Traps do SNMP > receptores de traps

Com os traps do protocolo simples de gerenciamento de rede (SNMP), você pode ser notificado automaticamente de eventos significativos do no-break. Eles são uma ferramenta útil para monitorar dispositivos na rede.

Os receptores de trap são exibidos por **Nome do host/IP do NMS**, onde NMS significa Sistema de gerenciamento de redes. É possível configurar até seis receptores de traps.

Para configurar um novo receptor de traps, clique em **Adicionar receptor de traps**. Para editar (ou excluir), clique no endereço IP/nome do host.

Se você excluir um receptor de traps, todas as configurações de notificações ajustadas em “Configuração de ações de eventos” para o receptor de traps excluído serão retornadas aos seus valores padrão.

Selecione o botão de opção **SNMPv1** ou **SNMPv3** para especificar o tipo de trap. Para um NMS receber *ambos* os tipos de traps deve-se configurar dois receptores de traps separadamente para esse NMS, um para cada tipo de trap.

Campo	Descrição
Geração de traps	Ativar (padrão) ou desativar a geração de traps para esse receptor de traps.
Geração de traps Powernet MIB/ RFC1628	Escolha entre estes dois tipos de geração de traps para MIB para cada trap criado. A opção da Powernet é personalizada para a Schneider Electric e contém muitas variáveis adicionais relevantes aos produtos da empresa. A MIB RFC1628 é a MIB (Management Information Base, Base de Informações de Gerenciamento) genérica padrão para dispositivos de no-break. Se você utilizar a MIB RFC1628, também poderá usar as três notificações de eventos da RFC1628 (consulte “Configuração de ações de eventos”). Elas podem ser usadas para evitar configurar eventos de notificação fora do ambiente da NMC, consulte RFC1628 MIB .
Nome do host/IP do NMS	O endereço IPv4/ IPv6 ou o nome do host desse receptor de traps. O padrão, 0.0.0.0, deixa o receptor de traps indefinido.
Idioma	Selecione um idioma na lista suspensa. Ele pode ser diferente da interface de usuário e de outros receptores de traps.

Campo	Descrição
SNMPv1	Nome da comunidade: O nome (“public” por padrão) utilizado como um identificador quando os traps de SNMPv1 forem enviados para esse receptor de traps. Traps de autenticação: Quando essa opção estiver ativada (padrão), o NMS identificado pela configuração de Nome do host/IP do NMS receberá traps de autenticação (traps gerados por tentativas inválidas de fazer login nesse dispositivo).
SNMPv3	Nome do usuário: Selecione o identificador do perfil de usuário para esse receptor de traps. Consulte também “Perfis de usuário” em “Telas SNMP”.

Tela de teste de traps de SNMP

Caminho: Configuração > Notificação > Traps do SNMP > Teste

Resultado do último teste: O resultado do teste mais recente de trap do SNMP. Um teste de trap do SNMP bem-sucedido verifica somente se um trap foi enviado; ele não verifica se o trap foi recebido pelo receptor de traps selecionado. Um teste de trap será bem-sucedido se:

- A versão do SNMP (SNMPv1 ou SNMPv3) configurada para o receptor de traps selecionado estiver ativada nesse dispositivo.
- O próprio receptor de traps estiver ativado.
- O nome do host estiver selecionado no endereço **Para**, de modo que o nome do host possa ser mapeado para um endereço IP válido.

Para: Selecione o endereço IP ou o nome do host para o qual um trap de SNMP de teste será enviado. Se não houver receptor de traps configurado, um link para a tela de configuração do **Receptor de traps** será exibido. Consulte “Tela de receptores de traps de SNMP” acima.

Serviço de Monitoração Remota

Caminho: Configuração > Notificação > Monitoração remota

O serviço de monitoração remota (RMS, Remote Monitoring Service) é um serviço opcional da Schneider Electric que monitora seu sistema a partir de um centro de operação remoto 24 horas por dia, 7 dias na semana, e notifica os eventos do sistema e dos dispositivos.



Para adquirir o serviço RMS, entre em contato com seu fornecedor ou clique no link na parte superior desta tela: **Site do RMS da APC na Web**.

Registro. Uma vez adquirido o serviço, você deve ativar o RMS para a NMC. Selecione **Ativar Serviço de Monitoração Remota da APC**, escolha entre **Registrar empresa e dispositivo** e **Registrar somente dispositivo**, preencha o formulário e clique no botão Aplicar.

Use a caixa de seleção **Redefinir Registro do Serviço de Monitoração Remota da APC** para cancelar o serviço, de modo permanente ou temporário (por exemplo, se estiver movendo uma NMC).

Menu Geral

Este menu tem diversos itens de configuração inclusive a identificação do dispositivo, data e hora, exportação e importação das opções de configuração da NMC, os três links na área inferior esquerda da tela e consolidação de dados para solução de problemas.

Tela Identificação

Caminho: Configuração > Geral > Identificação

Defina o **Nome** (o nome do dispositivo, consulte “Tela DNS”), o **Local** (o local físico), e o **Contato** (a pessoa responsável pelo dispositivo) usados para:

- o agente SNMP da NMC
- StruxureWare Central
- Gerenciador InfraStruxure



Especificamente, o campo nome é utilizado pelos identificadores de objetos (OIDs) **sysName**, **sysContact** e **sysLocation** no agente SNMP da NMC. Para obter mais informações sobre os OIDs do MIB-II, consulte o Guia de referência *PowerNet[®] SNMP Management Information Base (MIB)*, disponível no CD de *Utilitários* da placa de gerenciamento de rede e no site www.apc.com.

Os campos **Nome** e **Local** também identificam o dispositivo ao ser feito o registro no Serviço de Monitoração Remota. Consulte “Serviço de Monitoração Remota” para obter mais informações.

Tela Data/Hora

Modo.

Caminho: Configuração > Geral > Data/hora > Modo

Defina a data e hora utilizadas pela NMC. Você pode alterar as configurações atuais manualmente ou pelo servidor NTP (Network Time Protocol):

De ambas as maneiras, você pode selecionar o **Fuso horário**. Esta é a diferença de sua hora local em relação à hora universal coordenada (UTC), também conhecido como Horário do Meridiano de Greenwich (GMT).

- **Modo manual:** Realize um dos seguintes procedimentos:
 - Digite data e hora para a NMC ou
 - marque a caixa de seleção **Aplicar hora do computador local** para ler as configurações de data e hora do computador que você está utilizando e aplicá-las aqui.
- **Sincronizar com servidor NTP:** Deixar um servidor NTP (Network Time Protocol) definir data e hora para a NMC.



Por padrão, qualquer NMC no lado privado de um StruxureWare Central obtém suas configurações de hora utilizando a StruxureWare Central como um servidor NTP.

Campo	Descrição
Substituir configurações manuais de NTP	Se você selecionar esta opção, os dados de outras fontes (normalmente o DHCP) têm preferência sobre as configurações do NTP que você define aqui.
Servidor NTP primário	Digitar o endereço IP ou nome de domínio do servidor NTP primário.

Campo	Descrição
Servidor NTP secundário	Digitar o endereço IP ou nome de domínio do servidor NTP secundário, quando houver um servidor secundário disponível.
Intervalo de atualização	Defina, em horas, com que frequência a NMC acessa o servidor NTP para uma atualização. <i>Mínimo: 1; Máximo: 8760 (1 ano).</i>
Atualizar usando NTP agora.	Iniciar uma atualização imediata da data e hora pelo servidor NTP.

Horário de verão.

Caminho: Configuração > Geral > Data/Hora > Horário de verão

Por padrão, o horário de verão (DST) fica desativado. É possível ativar o horário de verão tradicional dos EUA ou ativar e configurar um horário de verão personalizado para coincidir com o implementado em sua região.

Ao personalizar o DST, o sistema adiantará o relógio em uma hora quando chegar a data e a hora especificada em **Início** e atrasará uma hora novamente quando chegar a data e a hora especificada em **Término**.

- Se o horário de verão local iniciar ou terminar na *quarta* ocorrência de um determinado dia da semana de um mês (por exemplo, no quarto domingo), selecione **Quarto/Último**. Se um quinto domingo ocorrer naquele mês, ainda deve ser selecionado **Quarto/Último**.
- Se o horário de verão local iniciar ou terminar na *última* ocorrência de um determinado dia da semana de um mês, quer seja a quarta ou a quinta ocorrência, selecione **Quinto/Último**.

Criação e importação de configurações com o arquivo de configuração

Caminho: Configuração > Geral > Arquivo de configuração de usuário

Você pode acelerar e simplificar a configuração de novos dispositivos reutilizando as definições de configuração existentes com esta opção. Use **Carregar** para transferir dados de configuração para esta interface e **Fazer download** para transferir a partir desta interface (e em seguida use o arquivo para configurar outra interface). O nome padrão do arquivo é **config.ini**.



Para recuperar e personalizar o arquivo de uma NMC, configurada, consulte “Como exportar os valores das configurações”.

Tela Configurar links

Caminho: Configuração > Geral > Links rápidos

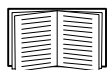
Use esta opção para visualizar e alterar os links da URL exibidos na parte inferior esquerda de cada tela da interface.

Para reconfigurar um link, clique no nome do link na coluna **Nome**. Você pode redefinir os links nos padrões a qualquer momento clicando em **Redefinição de padrões** ali.

Logs no menu Configuração

Caminho: Configuração > Logs > Syslog > opções

A NMC pode enviar mensagens para até quatro servidores do Syslog quando ocorrer um evento. Os servidores do Syslog registram eventos que ocorrem nos dispositivos da rede em um log que fornece um registro centralizado dos eventos.



Este guia do usuário não descreve o Syslog ou seus valores de configuração em detalhes. Consulte a RFC3164 para obter mais informações sobre o Syslog.

Identificação dos servidores do Syslog

Caminho: Configuração > Logs > Syslog > Servidores

Campo	Descrição
Servidor do Syslog	Usa endereços IPv4/IPv6 ou nomes de host para identificar de um a quatro servidores para receber mensagens do Syslog enviadas pela NMC.
Porta	A porta do protocolo de datagrama do usuário (UDP, User Datagram Protocol) que a NMC usará para enviar mensagens do Syslog. O padrão é 514, a porta UDP atribuída ao Syslog.
Idioma	Selecionar o idioma para qualquer mensagem do Syslog.
Protocolo	Selecionar entre UDP e TCP.

Configurações do Syslog

Caminho: Configuração > Logs > Syslog > Configurações

Campo	Descrição
Geração de mensagens	Ativa a geração e o registro das mensagens do Syslog para eventos que possuem o Syslog configurado como método de notificação. Consulte “Configuração de ações de eventos”.
Código da instalação	Seleciona o código da instalação atribuído às mensagens do Syslog da NMC (Usuário , por padrão). Observação: Usuário define melhor as mensagens do Syslog enviadas pela NMC. Não altere essa seleção a menos que seja aconselhado pelo administrador do sistema ou pela rede do Syslog.

Campo	Descrição
Mapeamento de severidade	<p>Mapeia cada nível de severidade da NMC ou dos eventos de ambiente para as prioridades disponíveis do Syslog. As opções locais são Crítico, Aviso, e Informativo. Não deve ser necessário alterar os mapeamentos.</p> <p>As seguintes definições são da RFC3164:</p> <ul style="list-style-type: none"> • Emergência: O sistema não está utilizável • Alerta: Uma ação deverá ser tomada imediatamente • Crítico: Condições críticas • Erro: Condições de erro • Aviso: Condições de aviso • Alerta: Condições normais, mas significativas • Informativo: Mensagens informativas • Depuração: Mensagens do nível de depuração <p>A seguir estão as configurações padrão para as configurações de Prioridade local:</p> <ul style="list-style-type: none"> • Severo é mapeado para Crítico • Aviso é mapeado para Aviso • Informativo é mapeado para Info <p>Observação: Para desativar as mensagens do Syslog, consulte “Configuração de ações de eventos”.</p>

Teste do Syslog e exemplo de formato

Caminho: Logs > Syslog > Teste

Enviar uma mensagem de teste aos servidores do Syslog (configurados por meio da opção “Identificação dos servidores do Syslog” acima). O resultado será enviado a todos os servidores do Syslog configurados.

Selecione uma severidade para atribuir à mensagem de teste e em seguida defina a mensagem de teste. Formate a mensagem para incluir o tipo de evento (APC, sistema ou dispositivo, por exemplo) seguido por dois pontos, um espaço e o texto do evento. A mensagem pode conter no máximo 50 caracteres.

- A prioridade (PRI): a prioridade do Syslog atribuída ao evento da mensagem e o código de facilidade das mensagens enviadas pela NMC.
- O título: um carimbo de data e hora e o endereço IP da NMC.
- A parte da mensagem (MSG):
 - Um campo TAG, seguido por dois pontos [:] e um espaço, identifica o tipo de evento.
 - O campo CONTENT é o texto do evento, seguido (opcionalmente) por um espaço e o código do evento.

Exemplo: APC: Test Syslog é válido.

Menu Testes

Teste e calibração

Caminho: Testes > No-break



Esta opção não está disponível para todos os dispositivos de no-break.

Com alguns dispositivos de no-break, você pode executar um autoteste, um teste de alarme, ou uma calibração do tempo de funcionamento para o no-break. Os campos **Autoteste** e **Calibração** exibem os resultados do teste e calibração mais recente.

A calibração do tempo de funcionamento faz o no-break recalcular sua capacidade de tempo de funcionamento disponível com base em sua carga atual. Isso garante que o tempo de funcionamento relatado seja mais preciso. Como a calibração exaure temporariamente as baterias do no-break, você somente poderá executá-la se a capacidade das baterias for 100%. A carga do no-break deve ser pelo menos 15% sem flutuação para garantir que uma calibração será aceita.



Cuidado - As calibrações do tempo de funcionamento descarregam rapidamente as baterias do no-break, o que pode levar o no-break a ficar temporariamente impossibilitado de dar suporte a seus equipamentos, se ocorrer falta de energia.

Frequentes calibrações reduzem a vida das baterias. Execute uma calibração sempre que aumentar significativamente a carga que o no-break está suportando.

O teste de alarme do no-break é específico para cada dispositivo e talvez não esteja disponível para o seu no-break. Para ativar o alarme, consulte “Tela No-break - Geral”.

- Ao selecionar o **Teste de alarme do no-break**, ele emitirá um bipe por quatro segundos e os LEDs acenderão.
- Ao selecionar o **Teste de alarme do no-break - Contínuo**, ele emitirá um bipe e acenderá os LEDs até você cancelar o teste. Um aviso separado será exibido nesta tela, **Cancelar teste de alarme contínuo**. Para cancelar o teste, selecione esta opção e clique em Aplicar. Opcionalmente pressione qualquer tecla na interface do mostrador LED do no-break. Este teste é útil para localizar um no-break.

Configuração das luzes do LED da NMC para intermitência do led

Caminho: Testes > Rede > Intermitência do Led

Se tiver problemas para encontrar seu dispositivo de no-break, insira um número de minutos no campo **Duração da intermitência do Led**, clique em Aplicar e as luzes do LED da NMC começarão a piscar. Isso pode ajudar na localização do dispositivo físico.

Menus Logs e Sobre

Usar os logs de dados e eventos

O Log de eventos registra ocorrências individuais. O Log de dados, ao contrário, fornece um instantâneo de seu sistema registrando valores a intervalos regulares de tempo.

Log de eventos

Caminho: Logs > Eventos > *opções disponíveis*

Por padrão, o log exibe todos os eventos registrados durante os últimos dois dias, começando pelos eventos mais recentes. Consulte “Configuração por evento”.


Além disso, o log registra: i) Todo evento que envia um trap de SNMP, com exceção de falhas de autenticação de SNMP. ii) Eventos anormais do sistema interno.

Você pode ativar a codificação em cores dos eventos por meio de “Usuários locais” no menu Configuração.

Para exibir o Log de eventos.

Caminho: Logs > Eventos > Log

Por padrão, o Log de eventos exibe os eventos mais recentes em primeiro lugar. Para ver os eventos relacionados em uma página da Web, clique no botão **Iniciar log em nova janela**. O JavaScript deve estar ativado em seu navegador para fazer isso.

Para abrir o log em um arquivo de texto ou salvar o log em disco, clique no ícone de disquete, , na mesma linha que o cabeçalho **Log de eventos**.



Você também pode usar FTP ou Secure CoPy (SCP) para exibir o Event Log. Consulte “Como usar FTP ou SCP para recuperar os arquivos de log”.

Para filtrar o Log de eventos. Use o filtro para omitir informações que não deseja exibir.

Como filtrar o log por data ou hora	Use os botões de opção Último ou De . (A configuração do filtro fica salva até que a NMC reinicie.)
Filtrar o log por severidade ou categoria do evento	Clique em Filtrar log . Limpe uma caixa de seleção para removê-la da visualização. Depois que você clicar em Aplicar , o texto no canto superior direito da página do log de eventos indica que existe um filtro ativo. O filtro estará ativo até que você o limpe ou até que a NMC seja reiniciada. Para remover um filtro ativo, clique em Filtrar log e, em seguida, em Limpar filtro (Mostrar tudo) . Como Administrador, clique em Salvar como padrão para salvar este filtro como a nova exibição padrão do log para todos os usuários.

Observação importante sobre filtros:

- os eventos são processados pelo filtro usando a lógica OU. Se você aplicar um filtro, ele funciona independentemente dos outros filtros.
- Os eventos que você limpou na lista **Filtrar por severidade** nunca são exibidos no log de eventos filtrado, mesmo se forem selecionados na lista **Filtrar por categoria**.
- Da mesma forma, os eventos que você limpar na lista **Filtrar por categoria** nunca são exibidos no log de eventos filtrados.

Para excluir o log de eventos. Para excluir todos os eventos, clique em **Limpar log**. Os eventos excluídos não podem ser recuperados.



Para desativar o log de eventos com base na atribuição de nível de severidade ou categoria do evento, consulte “Configuração por grupos de eventos”.

Para configurar a pesquisa inversa:

Caminho: Logs > Eventos > Pesquisa inversa

Com a pesquisa inversa ativada, quando ocorrer um evento relacionado à rede, tanto o endereço IP *quanto* o nome de domínio do dispositivo em rede associado ao evento serão registrados no log de eventos. Se não houver entrada de nome de domínio para o dispositivo, somente seu endereço IP será registrado com o evento.

Como os nomes de domínio geralmente mudam com menos frequência do que os endereços IP, a ativação da pesquisa inversa pode aumentar a capacidade de identificar os endereços dos dispositivos em rede que estejam causando os eventos.

A pesquisa inversa fica desativada por padrão. Você não precisará ativá-la se não tiver nenhum servidor DNS configurado ou um fraco desempenho na rede devido ao tráfego pesado.

Para redimensionar o Log de eventos.

Caminho: Logs > Eventos > Tamanho

Use o Tamanho do log de eventos para especificar a quantidade máxima de entradas do log.



Cuidado: ao redimensionar o log de eventos para especificar um tamanho máximo, *todas as entradas de log existentes serão excluídas*. Para evitar a perda de dados de log, use o FTP ou o SCP para recuperar o log primeiro. Consulte “Como usar FTP ou SCP para recuperar os arquivos de log”. Quando o log chegar ao tamanho máximo, as entradas mais antigas serão excluídas.

Log de dados

Caminho: Logs > Dados > opções

Use um log de dados para exibir medições sobre o no-break, a entrada de alimentação para o no-break e a temperatura ambiente do no-break e das baterias.

Os passos para exibir e redimensionar o log de dados são as mesmas do log de eventos, exceto que você usa opções de menu em **Dados** em vez de **Eventos**. Consulte “Para exibir o Log de eventos” e “Para redimensionar o Log de eventos”.

Para filtrar o log de dados por data ou hora, use os botões de opção **Último** ou **De**. (A configuração do filtro é salva até que a NMC seja reiniciada.) Para excluir todos os dados registrados no log de dados, clique em **Limpar log de dados**. Os dados excluídos não poderão ser recuperados.

Para configurar o intervalo de coleta dos dados (Logs > Dados > Intervalo): Defina, na configuração **Intervalo do log**, a frequência com que os dados são pesquisados e armazenados no log de dados. Quando você clica em Aplicar, o número de dias possíveis de armazenamento é recalculado e exibido na parte superior da tela.

Quando o log estiver cheio, as entradas mais antigas serão excluídas. Para evitar a exclusão automática de dados mais antigos, consulte “Para configurar a rotação do log de dados (Logs > Dados > Rotação):” diretamente abaixo.

Observação: como o intervalo especifica a frequência com que os dados são registrados, *quanto menor o intervalo* maior será o número de vezes que os dados serão registrados e maior será o arquivo de log.

Para configurar a rotação do log de dados (Logs > Dados > Rotação): A rotação faz com que o conteúdo do log de dados seja acrescentado ao arquivo especificado por nome e local. Isso significa que você pode armazenar os dados antes que eles sejam excluídos. Consulte “Para configurar o intervalo de coleta dos dados (Logs > Dados > Intervalo):” diretamente acima.

Use esta opção para configurar a proteção por senha e outros parâmetros.

Campo	Descrição
Servidor FTP	O endereço IP ou nome do host do servidor onde o arquivo residirá.
Nome do usuário Senha	O nome de usuário com senha obrigatória para enviar os dados ao arquivo de repositório. Este usuário deve também ser configurado para ter acesso de leitura e gravação ao arquivo de repositório de dados e ao diretório (pasta) no qual está armazenado.
Caminho do arquivo	O caminho para o arquivo de repositório.
Nome do arquivo	O nome do arquivo de repositório (um arquivo de texto ASCII), por exemplo, <code>datalog.txt</code> . Qualquer dado novo é acrescentado a este arquivo e ele não é sobrescrito.
Nome de arquivo exclusivo	Marque esta caixa de seleção para salvar o log como <code>mmddaaaaa_<filename>.txt</code> , onde <code>filename</code> é o que você especificou no campo Nome do arquivo acima. Qualquer dado novo é acrescentado ao arquivo mas cada dia tem seu próprio arquivo.
Atraso de <i>n</i> horas entre carregamentos.	O número de horas entre carregamentos de dados no arquivo (no máximo 24 horas).
No caso de falha, tentar carregar a cada <i>n</i> minutos.	O número de minutos entre tentativas de carregar os dados no arquivo após um carregamento mal sucedido.
Até <i>n</i> vezes	O número máximo de tentativas para fazer o carregamento após uma tentativa inicial mal sucedida.
até o êxito do carregamento	Tentar fazer o carregamento do arquivo até que a transferência seja concluída.

Como usar FTP ou SCP para recuperar os arquivos de log

Um Administrador ou Usuário de dispositivos pode usar FTP ou SCP para recuperar um arquivo do log de eventos (*event.txt*) ou um arquivo do log de dados (*data.txt*) delimitado por tabulação e importá-lo para uma planilha. Ambos residem na NMC.

- O arquivo relata todos os eventos ou dados registrados desde que o log foi excluído ou (para o log de dados) truncado, porque chegou ao tamanho máximo.
- O arquivo contém informações que o log de eventos ou o log de dados não exibem.
 - A versão do formato do arquivo (primeiro campo)
 - A data e a hora em que o arquivo foi recuperado
 - Os valores de **Nome**, **Contato** e **Local** e o endereço IP da NMC
 - O **Código do evento** exclusivo para cada evento registrado (somente arquivo *event.txt*)
 - A NMC utiliza um ano de quatro dígitos para as entradas do log. É possível selecionar um formato de data de quatro dígitos em seu aplicativo de planilha para exibir todos os quatro dígitos.



Se você estiver usando os protocolos de segurança baseados em criptografia, consulte “Para usar SCP para recuperar os arquivos”. Se estiver usando métodos de autenticação sem criptografia para segurança, consulte “Para usar FTP para recuperar os arquivos”.



Consulte o *Manual de segurança*, disponível no CD de *Utilitários* da placa de gerenciamento de rede e no site (www.apc.com) para obter informações sobre os protocolos e métodos disponíveis para configurar o tipo de segurança necessário.

Para usar SCP para recuperar os arquivos. Ative SSH na NMC. Consulte “Acesso ao console”.

Para recuperar o arquivo *event.txt*, use o seguinte comando:

```
scp <username@hostname> ou <ip_address>:event.txt./event.txt
```

Para recuperar o arquivo *data.txt*, use o seguinte comando:

```
scp <username@hostname> ou <ip_address>:data.txt./data.txt
```

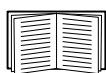
Para usar FTP para recuperar os arquivos. Para usar FTP para recuperar o arquivo *event.txt* ou *data.txt*:

1. Em um prompt de comando, digite `ftp` e o endereço IP da NMC e pressione ENTER.

Se a configuração **Porta** da opção **Servidor FTP** (consulte “Servidor FTP”) tiver sido alterada de seu padrão (21), você precisará usar o valor não padrão no comando FTP.

Para os clientes FTP Windows, use o comando a seguir, incluindo espaços. (Para alguns clientes FTP, você deverá usar dois pontos em vez de um espaço entre o endereço IP e o número da porta.)

```
ftp>open ip_address port_number
```



Para configurar um valor de porta não padrão para melhorar a segurança do servidor FTP, consulte “Servidor FTP”. É possível especificar qualquer porta, de 5001 a 32768.

2. Use o **Nome de usuário** e a **Senha** (diferenciam maiúsculas de minúsculas) para Administrador ou Usuário de dispositivos para fazer login. Para Administrador, `apc` é o padrão para o nome de usuário e a senha. Para o Usuário de dispositivos, os padrões são `device` para nome de usuário e `apc` para a senha.
3. Use o comando `get` para transmitir o texto de um log para sua unidade local.

```
ftp>get event.txt
```

ou

```
ftp>get data.txt
```

4. Você pode usar o comando `del` para limpar o conteúdo de qualquer um dos logs.

```
ftp>del event.txt
```

ou

```
ftp>del data.txt
```

Não será solicitada a confirmação da exclusão.

- Se você limpar o log de dados, o log de eventos registrará um evento do log excluído.
- Se você limpar o log de eventos, um novo arquivo *event.txt* registrará o evento.

5. Digite `quit` no prompt `ftp>` para sair do FTP.

Log do no-break

Caminho: Logs > No-break



Esta opção de menu não está disponível para todos os dispositivos de no-break.

Estas informações provêm de seu dispositivo de no-break e são separadas dos logs de sua NMC. (Elas não estão diretamente relacionadas nem representam um subconjunto da NMC “Log de eventos”).

As informações podem ser úteis para ajudar a equipe de suporte técnico a resolver problemas.

Logs de transferência do no-break Exibe uma tabela dos eventos de transferência armazenados no no-break, inclusive transferências para bateria e transferências para bypass.

Logs de falha do no-break Exibe uma tabela das falhas armazenadas no no-break.

Utilização da energia

Caminho: Logs > Utilização de energia



Esta opção de menu não está disponível para todos os dispositivos de no-break.

Os valores de utilização acumulada de energia de seu no-break são exibidos na parte superior da tela, com uma lista expandida semana a semana na tabela, na parte inferior da tela.

Campo	Descrição
Utilização da energia	A quantidade de energia, em kilowatt-horas, consumida até o momento pelo seu no-break. Por exemplo, um no-break que alimenta uma lâmpada de 350 W durante 1.000 horas consome 350 kWh de potência.
Custo total	O custo total estimado de energia usado até o momento. Por exemplo, uma lâmpada que consome 350 kWh de potência durante 1.000 horas a um preço de R\$ 0,10 por kWh custa R\$ 35 nesse período.
Emissões de CO ₂	A quantidade estimada de CO ₂ liberada pela empresa pública de energia no meio ambiente para fornecer a energia usada até o momento.

Os custos e as emissões de CO₂ variam bastante conforme a fonte de energia e a rede de distribuição. Você pode obter um cálculo aproximado selecionando o seu país na caixa suspensa **Local** ou usar o link “**(editar)**” para inserir seus próprios dados de custo e emissões.

A edição de um local cria um local personalizado e não altera os valores padrão desse local. Por exemplo, se você selecionar **IE-Irlanda** na lista suspensa e depois usar a edição para alterar os dados, será criada uma entrada denominada **Personalizado (IE-Irlanda)** na parte superior da lista suspensa.

Log do firewall

Caminho: Logs > Firewall

Se você criar uma diretiva de firewall, os eventos do firewall serão registrados aqui. Para obter mais informações sobre a implementação de uma diretiva, consulte “Tela Firewall”.

As informações podem ser úteis para ajudar a equipe de suporte técnico a resolver problemas.

As entradas do log contêm informações sobre o tráfego e a ação de regras (permitido, descartado). Quando são registrados aqui, estes eventos não são registrados no log de eventos principal. Consulte “Log de eventos”.

Um log de firewall contém até 50 dos eventos mais recentes. O log de firewall é apagado quando a NMC é reiniciada.

Sobre a placa de gerenciamento de rede 2

Sobre o dispositivo de no-break

Caminho: Sobre > No-break



As informações exibidas em No-break variam conforme o dispositivo usado.

Campo	Descrição
Modelo/Itens em estoque/Número de série	Estes campos identificam seu dispositivo de no-break.
Posição do no-break	A orientação física do no-break, rack ou torre.
Data de fabricação	A data em que seu no-break foi fabricado.
Revisão do firmware	Os números de revisão dos módulos de firmware atualmente instalados no no-break
Revisão do firmware 2	O segundo número de revisão do firmware atualmente instalado no no-break. É usado quando vários processadores exigem versões diferentes.
Classificação da potência aparente	A capacidade total de VA do no-break.
Classificação da potência real	A capacidade total de carga (em Watts) do no-break.
Fase/Classificação da potência aparente	A capacidade de VA de cada fase do no-break. De modo mais técnico, é a potência aparente, presente em cada fase, em Volt-Amps (VA). A potência aparente é o produto entre RMS (root mean square, valor médio quadrático) volts e RMS ampères.
Potência real Classificação/Fase	A capacidade total de carga (em Watts) do no-break. A potência ativa de bypass presente de cada fase em watts (W). A potência ativa é a média temporal do produto instantâneo entre tensão e corrente.
Sobre o software de monitoração de no-break	Contém várias informações sobre o software monitorando diretamente o no-break de modo serial ou em USB.
Itens em estoque da bateria interna/Itens em estoque da bateria externa	Estes campos identificam os números de peças de suas baterias. Isto pode ser útil ao solucionar problemas.

Sobre a NMC e os módulos de firmware

Caminho: Sobre > Rede

Fábrica do hardware: Estas informações sobre o hardware são úteis para solucionar problemas com seu dispositivo de NMC. **Tempo de atividade de gerenciamento** refere-se ao período de tempo em que esta interface de gerenciamento estava sendo executada continuamente; isto é, o período de tempo desde que a NMC foi iniciada aquecida ou a frio.

Módulo do aplicativo, APC OS (AOS, Sistema operacional APC) e Monitor de inicialização: Estas informações são úteis para solucionar problemas e determinar se existe um firmware atualizado disponível, www.apcc.com/tools/download.

Rótulo do campo	Descrição
Nome	O nome do módulo de firmware. O nome do Módulo do aplicativo varia conforme o tipo de dispositivo de no-break, por exemplo, sumx aplica-se a dispositivos Smart-UPS, sy a dispositivos Symmetra. O módulo APC AOS sempre leva o nome de aos e o módulo do monitor de inicialização sempre leva o nome de bootmon .
Versão	O número da versão do módulo de firmware. Os números de versão dos módulos podem variar, mas os módulos compatíveis têm versões conjuntas. Nunca combine módulos de aplicativo com módulos AOS de versões diferentes. Observação: se o módulo do monitor de inicialização precisar de atualização, está incluído um módulo do monitor de inicialização na versão do firmware. Caso contrário, o módulo do monitor de inicialização instalado na placa é compatível com a atualização do firmware. Consulte “Atualização do firmware”.
Data/Hora	A data e hora em que o módulo do firmware foi carregado.

Veja também “Confirmar os números de versão do firmware instalado”.

Tela Suporte

Caminho: Sobre > Suporte

Com esta opção, você pode consolidar vários dados desta interface em um só arquivo compactado para fins de solução de problemas e suporte ao cliente. Os dados contêm os logs de eventos e dados, o arquivo de configuração (consulte “Criação e importação de configurações com o arquivo de configuração”) e informações completas de depuração.

Clique em **Gerar logs** para criar o arquivo e depois em **Download**. Você será perguntado se deseja exibir ou salvar o arquivo compactado.

Utilitário de Configuração do IP do Dispositivo

Capacidades, requisitos e instalação

O Utilitário de Configuração do IP do Dispositivo pode encontrar placas de gerenciamento de rede (NMC) que não contam com IP definido. Depois de detectado, é possível definir as configurações de endereço IP para as placas.

Também é possível pesquisar pelos dispositivos que já estão na rede ao digitar uma faixa de IP para definir a pesquisa. O Utilitário verifica endereços IP no intervalo definido e detecta placas que já contam com endereço IP atribuído por DHCP.



Para informações detalhadas sobre o Utilitário, consulte a Base de Conhecimentos na página de suporte do site www.apc.com e pesquise pelo número FA156064 (o ID do artigo relevante).

Para usar a Opção DHCP 12 (AOS 5.1.5 ou posterior), consulte a Base de conhecimento ID FA156110.

Requisitos do sistema

O Utilitário é compatível com Microsoft Windows 2000, Windows Server® 2003, Windows Server 2012, e em ambas as versões de 32 e 64 bits dos sistemas operacionais Windows XP, Windows Vista, Windows 2008, Windows 7 e Windows 8.

O Utilitário oferece suporte para placas com versão de firmware 3.0.x ou superior e destina-se exclusivamente a IPv4.

Instalação

Para instalar o Utilitário a partir do CD de *Utilitários*:

1. Se a execução automática estiver habilitada, a interface de usuário do CD será iniciada quando você inserir o CD. Caso contrário, abra o arquivo **contents.htm** no CD.
2. Clique em **Utilitário de configuração do IP do dispositivo** e siga as instruções.

Para instalar o Utilitário a partir de um arquivo executável que foi baixado:

1. Acesse www.apc.com/tools/download.
2. Faça o download do Utilitário para configuração IP do dispositivo.
3. Execute o arquivo executável na pasta onde foi feito o download.

Quando instalado, o Utilitário será disponibilizado através das opções de menu do Windows.

Como exportar os valores das configurações

Recuperação e exportação do arquivo .ini

Resumo do procedimento

Um administrador pode recuperar o arquivo .ini de uma placa de gerenciamento de rede 2 (NMC) do no-break e exportá-lo para outra NMC ou para várias NMCs. Siga os passos abaixo, Consulte os detalhes nas seções a seguir.

1. Configure uma NMC com as configurações desejadas e exporte-as, consulte “Criação e importação de configurações com o arquivo de configuração”.
2. Recupere o arquivo .ini da NMC.
3. Personalize o arquivo para alterar as configurações do TCP/IP pelo menos.
4. Use um protocolo de transferência de arquivos ao qual a NMC dá suporte para transferir uma cópia para uma ou mais NMCs. Para transferências para várias NMCs, use um script de SCP ou FTP ou o utilitário do arquivo .ini.

Cada NMC de recebimento usa o arquivo para reconfigurar suas próprias configurações e, em seguida, exclui o arquivo.

Conteúdo do arquivo .ini

O arquivo config.ini que você recupera de uma NMC contém:

- *cabeçalhos de seção e palavras-chave* (somente as compatíveis com o dispositivo específico de no-break/NMC do qual você recupera o arquivo): **Os cabeçalhos de seção** são nomes de categoria incluídos entre colchetes ([]). **As palavras-chave**, sob cada cabeçalho de seção, são etiquetas que descrevem configurações específicas da NMC. Cada palavra-chave é seguida por um sinal de igual e um valor (o padrão ou um valor configurado).
- A palavra-chave **Ignorar**: Com seu valor padrão, esta palavra-chave evita a exportação de uma ou mais palavras-chave e de seus valores específicos do dispositivo. Por exemplo, na seção (NetworkTCP/IP), o valor padrão de Substituir (o endereço MAC da placa de NMC) bloqueia a exportação de valores para o SystemIP, SubnetMask, DefaultGateway e BootMode.

Procedimentos detalhados

Recuperação. Para configurar e recuperar um arquivo .ini para exportar:

1. Se possível, use a interface de uma NMC para ajustá-la com as configurações a serem exportadas. (A edição direta do arquivo .ini pode introduzir erros).
2. Para usar o FTP para recuperar o config.ini da NMC configurada:
 - a. Abra uma conexão com a NMC, usando seu endereço IP:
`ftp> open endereço_ip`
 - b. Faça login usando um nome de usuário e uma senha de administrador.
 - c. Recupere o arquivo config.ini contendo as configurações da NMC:
`ftp> get config.ini`

O arquivo é gravado na pasta a partir da qual você iniciou o FTP.



Para recuperar os valores das configurações das várias NMCs e exportá-los para outras NMCs, consulte as *Notas da versão: Utilitário do arquivo ini, versão 2.0*, disponível no CD de *Utilitários* da placa de gerenciamento de rede e em www.apc.com. Ou consulte também a Base de conhecimento, <http://www.apc.com/site/support/index.cfm/faq/index.cfm>.

Personalização. Deve-se personalizar o arquivo antes de transferi-lo para outra NMC.

1. Use um editor de texto para personalizar o arquivo.
 - Cabeçalhos de seção, palavras-chave e valores predefinidos não diferenciam maiúsculas de minúsculas, mas os valores de sequências de caracteres que definidos diferenciam maiúsculas de minúsculas.
 - Use aspas adjacentes para indicar nenhum valor. Por exemplo, `LinkURL1=""` indica que a URL foi intencionalmente não definida.
 - Coloque entre aspas quaisquer valores que contenham espaços no início ou no final ou que já estejam incluídos entre as aspas.
 - Para exportar eventos agendados, configure os valores diretamente no arquivo `.ini`.
 - Para exportar uma hora do sistema com mais exatidão, se as NMCs de recebimento puderem acessar um servidor NTP, configure `ativado` para `NTPEnable`:

`NTPEnable=enabled`

Opcionalmente, reduza o tempo de transmissão exportando a seção `[Data/hora do sistema]` como um arquivo `.ini` separado.

- Para adicionar comentários, inicie cada linha de comentário por um ponto-e-vírgula (`;`).
2. Copie o arquivo personalizado com outro nome de arquivo na mesma pasta:
 - O nome do arquivo pode conter até 64 caracteres e deverá ter o sufixo `.ini`.
 - Guarde o arquivo personalizado original para uso futuro. *O arquivo que você guardar será o único registro de seus comentários.*

Transferência do arquivo para uma única NMC. Para transferir o arquivo `.ini` para outra placa de gerenciamento de arquivo, realize uma das seguintes opções:

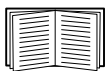
- Na interface de usuário da NMC receptora, selecione **Configuração - Geral - Arquivo de configuração de usuário**. Digite o caminho completo do arquivo, ou use **Procurar** no PC local.
- Use qualquer protocolo de transferência de arquivos para o qual as placas de gerenciamento de rede ofereçam suporte, isso é, FTP, Cliente FTP, SCP ou TFTP. O exemplo a seguir usa FTP:
 - a. Na pasta que contém a cópia do arquivo `.ini` personalizado, use FTP para fazer o login na NMC para a qual está exportando o arquivo `.ini`:

```
ftp> open endereço_ip
```
 - b. Exporte a cópia do arquivo `.ini` personalizado para o diretório raiz da NMC de recebimento:

```
ftp> put nome_de_arquivo.ini
```

Transferência do arquivo para várias NMCs. Siga estas etapas:

- Use FTP ou SCP, mas grave um script que incorpore e repita as etapas usadas para exportar o arquivo para uma única NMC.
- Use um arquivo de processamento em lotes e o utilitário do arquivo `.ini`.



Para criar o arquivo em lotes e usar o utilitário, consulte as *Notas Informativas: Utilitário do arquivo ini, versão 2.0* no CD de *Utilitários* da placa de gerenciamento de rede ou consulte a Base de conhecimento, <http://www.apc.com/site/support/index.cfm/faq/index.cfm>.

O evento de carregamento e as mensagens de erro

O evento e suas mensagens de erro

O evento a seguir ocorre quando a placa de gerenciamento de rede de recebimento termina o uso do arquivo `.ini` para atualizar suas configurações:

```
Configuration file upload complete, with number valid values
```

Se uma palavra-chave, nome de seção ou valor for inválido, o carregamento pela NMC de recebimento será realizado e um texto adicional de evento indicará o erro.

Texto de evento	Descrição
Aviso sobre o arquivo de configuração: Palavra-chave inválida na linha <i>número</i> . Aviso sobre o arquivo de configuração: Valor inválido na linha <i>número</i> .	Uma linha com um valor ou palavra-chave inválida é ignorada.
Aviso sobre o arquivo de configuração: Seção inválida na linha <i>número</i> .	Se um nome de seção for inválido, todos os pares de palavra-chave/valor nessa seção serão ignorados.
Aviso sobre o arquivo de configuração: Palavra-chave encontrada fora de uma seção na linha <i>número</i> .	Uma palavra-chave inserida no início do arquivo (isso é, antes de quaisquer cabeçalhos de seção) será ignorada.
Aviso sobre o arquivo de configuração: Tamanho máximo do arquivo de configuração excedido.	Se o arquivo for muito grande, ocorrerá um carregamento incompleto. Reduza o tamanho do arquivo ou divida-o em dois arquivos e tente carregar novamente.

Mensagens no config.ini

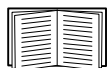
Um dispositivo associado com a NMC da qual você descarregou o arquivo `config.ini` deve ser descoberto com sucesso para que sua configuração seja incluída. Se o dispositivo (como um no-break) não estiver presente ou não for descoberto, o arquivo `config.ini` conterá uma mensagem abaixo do nome da seção apropriada, em vez de palavras-chave e valores. Por exemplo:

```
UPS not discovered  
IEM not discovered
```

Se não desejava exportar a configuração do dispositivo como parte da importação do arquivo `.ini`, ignore essas mensagens.

Erros gerados por valores ignorados

A palavra-chave `Override` seu valor gerarão mensagens de erro no log de eventos quando ela bloquear a exportação de valores.

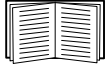


Consulte “Conteúdo do arquivo `.ini`” para obter informações sobre quais valores são ignorados.

Como os valores ignorados são específicos do dispositivo e não são apropriados para exportar para outras NMCs, ignore essas mensagens de erro. Para evitar essas mensagens de erro, exclua as linhas que contêm a palavra-chave `Ignorar` e as linhas que contêm valores ignorados. Não exclua nem altere a linha que contém o cabeçalho da seção.

Tópicos relacionados

Nos sistemas operacionais Windows, em vez de transferir os arquivos .ini, é possível utilizar o Utilitário para configuração do IP do dispositivo para atualizar as configurações básicas de TCP/IP da NMC e ajustar outras configurações por meio da interface de usuário.



Consulte “Utilitário de Configuração do IP do Dispositivo”.

Transferências de arquivos

Atualização do firmware

Ao atualizar o firmware na placa de gerenciamento de rede 2 (NMC) do no-break, serão obtidos os recursos, os aperfeiçoamentos de desempenho e a correção de bugs mais recentes. Para obter o firmware do no-break, consulte a “Tela Atualização de firmware”.

A atualização significa simplesmente colocar os arquivos do módulo na NMC; não haverá instalação. Verifique regularmente em www.apcc.com/tools/download para obter as novas atualizações.

Arquivos do módulo do firmware (placa de gerenciamento de rede 2)

Uma versão do firmware tem três módulos e estes *devem* ser atualizados (isto é, colocados na NMC) na seguinte ordem:

	Módulo	Descrição
1	Um monitor de inicialização (bootmon).	Aproximadamente equivalente ao BIOS de um PC
2	Sistema operacional da APC (AOS)	Pode ser considerado como o sistema operacional da NMC
3	aplicativo	Específico para o tipo de dispositivo de no-break, por exemplo o modelo Smart-UPS, o modelo Symmetra

(Cada módulo contém uma ou mais verificações de redundância cíclica (CRCs) para proteger seus dados contra corrupção).

O módulo monitor de inicialização, o AOS e os nomes dos arquivos do aplicativo compartilham o mesmo formato básico:

```
apc_hardware-version_type_firmware-version.bin
```

- **apc**: Indica o contexto.
- **hardware-version**: hw0n onde n identifica a versão do hardware com a qual é possível utilizar este arquivo.
- **type**: Identifica o módulo.
- **firmware-version**: O número da versão do arquivo.
- **bin**: Indica que este é um arquivo binário.

Métodos de transferência de arquivos de firmware



Atualize primeiramente o módulo de boot (bootmon), em seguida o módulo de AOS e, finalmente, o módulo do aplicativo, transferindo-os para a NMC nesta ordem.

Obtenha a última versão do firmware gratuitamente em www.apcc.com/tools/download. Para atualizar o firmware de uma ou mais NMCs, utilize 1 dos 5 métodos abaixo:

- Para um sistema operacional Windows, use o **Utilitário de atualização do firmware** cujo download pode ser feito a partir do site www.apc.com. Consulte “Uso do utilitário de atualização do firmware”.
- Para qualquer sistema operacional suportado, use **FTP ou SCP** para transferir os módulos individuais do firmware do aplicativo e do AOS. Consulte “Use FTP ou SCP para atualizar uma placa de gerenciamento de rede”.

- Para uma placa de gerenciamento de rede que NÃO esteja em sua rede, use **XMODEM** por meio de uma conexão serial para transferir os módulos individuais de firmware do computador para a NMC. Consulte “Use XMODEM para atualizar uma NMC”.
- Use uma **unidade USB** para transferir os módulos de firmware individuais de seu computador (apenas AP9631). Consulte “Use uma unidade USB para transferir e atualizar os arquivos (somente AP9631)”.
- Para atualizar **múltiplas NMCs**, consulte “Atualizar o firmware em múltiplas placas de gerenciamento de rede” e “Uso do utilitário de atualização do firmware para múltiplas atualizações no Windows”.

Uso do utilitário de atualização do firmware

Este utilitário de atualização do firmware faz parte do pacote de atualização do firmware disponível no site www.apc.com. (Nunca use um utilitário de atualização designado para um produto para atualizar o firmware de outro produto).

Uso do utilitário para atualizações nos sistemas Windows. Em qualquer sistema operacional Windows compatível, o utilitário de atualização do firmware automatiza a transferência dos módulos de firmware, *na ordem correta do módulo*. o utilitário funciona somente com uma NMC que tenha um endereço IPv4.

Descompacte o arquivo de atualização do firmware e clique duas vezes no arquivo .exe. Então digite o endereço IP, o nome do usuário e a senha nos campos da caixa de diálogo e clique **Fazer upgrade agora**. É possível utilizar o botão **Ping** para testar os detalhes digitados. Veja também “Uso do utilitário de atualização do firmware para múltiplas atualizações no Windows”.

Uso do utilitário para atualizações manuais, principalmente em Linux. Em sistemas operacionais que não sejam Windows, o utilitário de atualização do firmware extrai os módulos individuais do firmware, mas não atualiza a NMC. Consulte “Métodos de transferência de arquivos de firmware” para métodos de atualização diferentes após a extração.

Para extrair os arquivos de firmware:

1. Após obter os arquivos do arquivo de atualização do firmware, execute o **Utilitário de atualização do firmware** (o arquivo .exe).
2. Nos prompts, clique em **Avançar**> e, em seguida, especifique o local do diretório para o qual os arquivos serão extraídos.
3. Quando a mensagem **Extração concluída** for exibida, feche a caixa de diálogo.

Use FTP ou SCP para atualizar uma placa de gerenciamento de rede

FTP. Para usar o FTP para atualizar uma NMC pela rede:

- A NMC deve estar na rede com seu IP de sistema, máscara de sub-rede e gateway padrão configurados.
- O servidor FTP deve estar ativado na NMC, consulte “Servidor FTP”.

Para transferir os arquivos, execute estas etapas (este procedimento assume que o bootmon não necessita ser atualizado, mas sempre será necessário atualizar os outros dois):

1. Os arquivos do módulo do firmware devem ser extraídos, consulte “Para extrair os arquivos de firmware:”.
2. Em um computador na rede, abra uma janela de prompt de comando. Vá para o diretório que contém os arquivos de firmware e liste os arquivos:

```
C:\>cd apc
C:\apc>dir
```

Para obter informações do arquivo, consulte “Arquivos do módulo do firmware (placa de gerenciamento de rede 2)”.

3. Abra uma sessão de cliente FTP:

```
C:\apc>ftp
```

4. Digite `open` com o **endereço IP** da NMC e pressione ENTER. Se a configuração **porta** do servidor FTP tiver sido alterada de seu padrão **21**, você precisará usar o valor não padrão no comando FTP.

- Para clientes FTP Windows, separe o número da porta não padrão do endereço IP com um espaço. Por exemplo (mostrando um espaço antes de 21000):
`ftp> open 150.250.6.10 21000`
- Para alguns clientes FTP são necessários os dois pontos [:] em vez de espaço, antes do número de porta.

5. Faça o login como administrador (**apc** é o nome de usuário e senha padrão).

6. Atualize o AOS. (Sempre atualize o AOS antes do módulo de aplicativo).

```
ftp> bin
```

```
ftp> put apc_hw05_aos_ddd.bin (onde ddd é o número da versão do firmware)
```

7. Quando o FTP confirmar a transferência, digite `quit` para fechar a sessão.

8. Depois de 20 segundos, repita de etapa 3 a etapa 7, utilizando o nome do arquivo do módulo de aplicação na etapa 6.

SCP. Para utilizar a cópia segura (SCP, Secure CoPy) para atualizar o firmware para a NMC, siga estas etapas (este procedimento assume que o bootmon não necessita ser atualizado, entretanto, sempre é necessário atualizar os outros dois):

1. Localize os módulos de firmware, consulte “Uso do utilitário para atualizações manuais, principalmente em Linux.”.
2. Use uma linha de comando SCP para transferir o módulo de firmware do AOS para a NMC. O exemplo a seguir usa *ddd* para representar o número da versão do módulo do AOS:

```
scp apc_hw05_aos_ddd.bin apc@158.205.6.185:apc_hw05_aos_ddd.bin
```

3. Use uma linha de comando SCP similar com o nome do módulo do aplicativo para transferir o módulo do firmware do aplicativo para a NMC. (Sempre atualize o AOS antes do módulo de aplicativo).

Use XMODEM para atualizar uma NMC

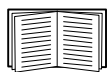
Para usar o XMODEM para atualizar uma NMC que não esteja na rede, você deverá extrair os arquivos de firmware com o Utilitário de atualização de firmware (consulte “Para extrair os arquivos de firmware:”).

Para transferir os arquivos (este procedimento assume que o bootmon não necessita ser atualizado, mas sempre será necessário atualizar os outros dois):

1. Selecione uma porta serial no computador local e desative todos os serviços que estejam utilizando a porta.
2. Conecte o cabo de configuração serial fornecido (código da APC: 940-0299) à porta selecionada e à porta serial da NMC.
3. Execute um programa do tipo terminal como o HyperTerminal e configure a porta selecionada para 57600 bps, 8 bits de dados, sem paridade, 1 bit de parada e sem controle de fluxo.
4. Pressione o botão **Redefinir** na NMC e, em seguida, pressione imediatamente a tecla **Enter** duas vezes, ou até que o prompt do monitor de inicialização seja exibido. `BM>`
5. Digite `XMODEM` e pressione ENTER.
6. No menu do programa tipo terminal, selecione `XMODEM` e, em seguida, selecione o arquivo binário de firmware do AOS para transferir usando o XMODEM. Quando a transferência do XMODEM estiver concluída, o prompt do monitor de inicialização retorna.

(Sempre atualize o AOS antes do módulo de aplicativo).

7. Para instalar o módulo do aplicativo, repita as etapas 5 e 6. Na etapa 6 use o nome do arquivo do módulo do aplicativo.
8. Digite reset ou pressione o botão **Redefinir** para reinicializar a NMC.



Para obter informações sobre o formato usado para os módulos de firmware, consulte “Arquivos do módulo do firmware (placa de gerenciamento de rede 2)”.

Use uma unidade USB para transferir e atualizar os arquivos (somente AP9631)

Antes de iniciar a transferência, certifique-se de que a unidade USB está formatada como FAT32.

1. Faça o download dos arquivos de atualização do firmware e descompacte-os.
2. Crie uma pasta chamada **apcfirm** na unidade USB.
3. Coloque os arquivos descompactados na pasta **apcfirm**.
4. Use um editor de texto para criar um arquivo chamado **upload.rcf**. (A extensão do arquivo deve ser .rcf, não .txt por exemplo).
5. Em **upload.rcf**, adicione uma linha para cada módulo de firmware que deseja atualizar. Por exemplo, para atualizar para a versão 1.0.2 do **bootmon**, versão 5.1.5 do **AOS** e versão 5.1.4 do **aplicativo** Smart-UPS, digite:

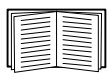
```
BM=apc_hw05_bootmon_102.bin
AOS=apc_hw05_aos_515.bin
APP=apc_hw05_sumx_514.bin
```

6. Coloque o arquivo upload.rcf na pasta **apcfirm** no pen drive.
7. Insira o pen drive na porta USB de sua NMC. Consulte “Painel dianteiro (AP9631)”.
8. Reinicie a NMC e aguarde a placa reiniciar totalmente.
9. Verifique se a atualização foi concluída com êxito usando os procedimentos contidos em “Verificação de atualizações”.

Atualizar o firmware em múltiplas placas de gerenciamento de rede

Use um destes três métodos:

- **Utilitário de atualização de firmware NMC2 em Windows.** Consulte “Uso do utilitário de atualização do firmware para múltiplas atualizações no Windows”.
- **Use FTP ou SCP.** Para atualizar várias NMCs usando um cliente FTP ou usando SCP, grave um script que realize automaticamente o procedimento.
- **Exportar os valores das configurações.** Você pode criar arquivos em lotes e usar um utilitário para recuperar os valores de configuração de várias NMCs e exportá-los para outras NMCs.



Consulte *Notas Informativas: Utilitário do arquivo ini*, disponível no CD de *Utilitários* da placa de gerenciamento de rede e na Base de conhecimento, <http://www.apc.com/site/support/index.cfm/faq/index.cfm>.

Uso do utilitário de atualização do firmware para múltiplas atualizações no Windows. Depois de fazer download do utilitário de atualização a partir da página de downloads da NMC no site www.apc.com, clique duas vezes no arquivo exe para executar o utilitário (que funciona SOMENTE com IPv4) e siga estas etapas para atualizar o firmware da sua NMC:

1. Na caixa de diálogo do utilitário, digite um endereço IP, um nome de usuário e uma senha e selecione o botão **Ping** caso necessite verificar o endereço IP.
2. Selecione o botão **Lista de dispositivos** para abrir o arquivo `iplist.txt`. Aqui, deve-se digitar todos os dispositivos de no-break para atualizar com as seguintes informações: IP, nome de usuário e senha.

Por exemplo,

SystemIP=192.168.0.1

SystemUserName=apc

SystemPassword=apc

É possível utilizar um arquivo `iplist.txt` existente se este existir.

3. Marque a caixa de seleção **Atualizar a partir da lista de dispositivos** para usar o arquivo `iplist.txt`.
4. Selecione o botão **Fazer upgrade agora** para iniciar a(s) atualização(ões) da versão do firmware.
5. Selecione **Exibir log** para verificar qualquer atualização.

Verificação de atualizações

Verificar o sucesso da transferência

Para confirmar se a atualização do firmware foi bem sucedida, é possível utilizar o comando `xferStatus` na interface da linha de comando para exibir o resultado da última transferência. Opcionalmente, é possível utilizar um GET do SNMP para o OID `mfiletransferStatusLastTransferResult`.

Códigos de resultado da última transferência

Possíveis erros de transferência incluem não encontrar o servidor TFTP ou FTP ou quando o servidor recusa o acesso, não encontra ou não reconhece o arquivo de transferência ou um arquivo de transferência corrompido.

Confirmar os números de versão do firmware instalado

Caminho: Sobre - Rede

Use a interface de usuário da Web para verificar as versões dos módulos de firmware atualizados. Também é possível utilizar um GET do SNMP para o OID `sysDescr` do MIB II. Na interface da linha de comando, use o comando `about`.

Adição e alteração de pacotes de idiomas

Utilizando os arquivos de pacote de idiomas da placa de gerenciamento de rede 2, é possível exibir a interface do usuário (UI) em idiomas diferentes. Cada pacote de idiomas contém até cinco idiomas (é por isso que a caixa suspensa **Idioma** possui cinco escolhas de idiomas ao fazer o login).

A UI tem nove idiomas disponíveis: francês, italiano, alemão, espanhol, português brasileiro, russo, coreano, japonês e chinês simplificado.

Os arquivos de pacotes de idiomas estão disponíveis na área de download do firmware da placa de gerenciamento de rede, no site www.apc.com. Os pacotes de idiomas estão incluídos no pacote de atualização do firmware.

Os arquivos para download possuem uma extensão .lpk e a convenção de nomenclatura dos arquivos é:

`<nome do aplicativo>_<versão do aplicativo>_<códigos de idioma>.lpk`

Por exemplo, para um aplicativo trifásico Symmetra, o nome de arquivo seria:

`sy3p_510_esESzhCnjaJAptBrkoKo.lpk`

onde `esESzhCnjaJAptBrkoKo`

representa espanhol, chinês, japonês, português brasileiro e coreano.

O usuário poderá desejar alterar o idioma da UI para um que não esteja atualmente disponível em sua interface de usuário. Para isso, será necessário fazer o download do pacote de idiomas do site e seguir estas etapas:

1. Conecte-se à NMC utilizando FTP.
2. Acesse a pasta **lang** da NMC:
`cd lang`
3. Transfira o pacote de idiomas necessário para a NMC:
`<app name>_<app version>_<language codes>.lpk`
4. Quando o arquivo concluir a transferência, faça o logout do FTP e a NMC será reiniciada.
5. Quando a reinicialização estiver concluída, o novo pacote de idiomas estará pronto para uso.



Qualquer pacote de idiomas atual na placa será *excluído* antes que o novo pacote seja transferido.

Qualquer problema com a transferência do pacote deixará a NMC sem um pacote de idiomas. Neste caso, somente o inglês estará disponível. Se isso acontecer, tente recarregar o novo pacote de idiomas.

Solução de problemas

Problemas de acesso da placa de gerenciamento de rede



Para problemas que não estejam descritos aqui, consulte os fluxogramas de solução de problemas no CD de *Utilitários* da placa de gerenciamento de rede. Clique no link **Solução de problemas** na interface do CD.

Se mesmo assim o problema persistir, consulte “Atendimento mundial ao cliente da APC”.

Problema	Solução
Não foi possível efetuar o comando ping para a NMC	<p>Se o LED de status da NMC ficar verde, tente fazer o ping para outro nó no mesmo segmento de rede da NMC. Se isso não funcionar, o problema não é da NMC. Se o LED de status não ficar verde ou se o teste de ping for bem-sucedido, realize as seguintes verificações:</p> <ul style="list-style-type: none">• Verifique se a NMC está instalada corretamente no no-break.• Verifique todas as conexões de rede.• Verifique os endereços IP da NMC e o NMS.• Se o NMS estiver em uma rede física diferente (ou sub-rede) da NMC, verifique o endereço IP do gateway padrão (ou roteador).• Verifique o número de bits de sub-rede para a máscara de sub-rede da NMC.
Não foi possível alocar a porta de comunicações por meio de um programa tipo terminal	<p>Antes de poder usar um programa tipo terminal para configurar a NMC, deve-se desativar qualquer aplicativo, serviço ou programa que esteja utilizando a porta de comunicações.</p>
Não foi possível acessar a interface da linha de comando por meio de uma conexão serial	<p>Certifique-se de que não tenha alterado a taxa de transmissão em bauds. Tente 2400, 9600, 19200 ou 38400.</p>
Não foi possível acessar remotamente a interface da linha de comando	<ul style="list-style-type: none">• Certifique-se de que esteja utilizando o método de acesso correto, Telnet ou Secure SHell (SSH). Um Administrador pode ativar estes métodos de acesso. Por padrão, o Telnet está ativado. Ativar o SSH desativa automaticamente o Telnet.• Para o SSH, a NMC pode estar criando uma chave do host. A NMC pode levar até um minuto para criar a chave do host e o SSH fica inacessível durante esse tempo.
Não foi possível acessar a interface do usuário (UI)	<ul style="list-style-type: none">• Verifique se o acesso HTTP ou HTTPS está ativado.• Certifique-se de que esteja especificando a URL correta — uma que seja compatível com o sistema de segurança utilizado pela NMC. O SSL exigirá https e não http no início da URL.• Verifique se consegue efetuar um comando ping para a NMC.• Verifique se está usando um navegador Web compatível com a NMC. Consulte “Atendimento mundial ao cliente da APC”.• Se a NMC acabou de ser reinicializada e a segurança SSL estiver sendo configurada, a NMC pode estar gerando um certificado do servidor. A NMC pode levar até um minuto para criar este certificado e o servidor SSL não fica disponível durante esse tempo.

Problemas do SNMP

Problema	Solução
Não foi possível efetuar um GET	<ul style="list-style-type: none"> • Verifique o nome da comunidade (SNMPv1) de leitura (GET) ou a configuração do perfil do usuário (SNMPv3). • Utilize a interface da linha de comando ou a interface do usuário para garantir que o NMS tenha acesso. Consulte “Telas SNMP”.
Não foi possível efetuar um SET	<ul style="list-style-type: none"> • Verifique o nome da comunidade (SNMPv1) de leitura/gravação (SET) ou a configuração do perfil do usuário (SNMPv3). • Utilize a interface da linha de comando ou a interface do usuário para garantir que o NMS tenha acesso (SNMPv1) de gravação (SET) ou que tenha acesso ao endereço IP de destino por meio da lista de controle de acesso (SNMPv3). Consulte “Telas SNMP”.
Não foi possível receber traps no NMS	<ul style="list-style-type: none"> • Certifique-se de que o tipo de trap (SNMPv1 ou SNMPv3) esteja configurado corretamente para o NMS como um receptor de traps. • Para o SNMPv1, consulte o OID mconfigTrapReceiverTable da MIB para verificar se o endereço IP do NMS está relacionado corretamente e se o nome de comunidade definido para o NMS coincide com o nome da comunidade na tabela. Se um dos dois não estiver correto, use SETs para os OIDs mconfigTrapReceiverTable ou use a interface da linha de comando ou a interface do usuário para corrigir a definição do receptor de traps. • Para o SNMPv3, verifique a configuração de perfil do usuário para o NMS e execute um teste de trap. <p>Consulte “Telas SNMP”, “Receptores de traps” e “Tela de teste de traps de SNMP”.</p>
Os traps recebidos em um NMS não são identificados	Consulte a documentação do NMS para verificar se os traps estão corretamente integrados ao banco de dados de alarmes/traps.

Problemas de sincronização

Problema	Solução
Um membro do grupo de controle sincronizado não participa de uma ação sincronizada.	Certifique-se de que o status do membro do grupo esteja configurado como Ativado . Também verifique a capacidade da bateria do membro do grupo, se a ação sincronizada tiver exigido que os no-breaks fossem ligados.
Uma tentativa de adicionar um membro a um grupo de controle sincronizado não funciona.	Os valores de Endereço IP de multicast , Número do grupo de controle sincronizado e versão de firmware deverão coincidir com os dos outros membros do grupo.

Garantia de fábrica de dois anos

Esta garantia aplica-se somente aos produtos adquiridos para uso de acordo com este manual.

Termos da garantia

A APC garante que seus produtos não apresentarão defeitos de materiais nem de fabricação por um período de dois anos a partir da data de compra. A APC consertará ou substituirá os produtos com defeito que estiverem cobertos por esta garantia. Esta garantia não se aplica a equipamento que tenha sofrido danos por acidente, negligência ou uso incorreto, ou que tenha sido alterado ou modificado de alguma forma. O conserto ou a substituição de um produto com defeito não estende o período original da garantia. As peças fornecidas sob os termos desta garantia poderão ser novas ou -recondicionadas pela fábrica.

Garantia intransferível

Esta garantia se aplica somente ao comprador original, que deve ter registrado devidamente o produto. O produto pode ser registrado no site da Web da APC, www.apc.com.

Exclusões

A APC não será responsabilizada, sob os termos desta garantia, se seus testes e exames revelarem que o defeito alegado no produto não existe ou foi causado por uso incorreto, negligência, instalação ou testes inadequados de um usuário final ou de terceiros. Além disso, a APC não será responsabilizada, sob os termos desta garantia, por tentativas não autorizadas de consertar ou modificar uma conexão ou tensão elétrica inadequadas ou erradas, condições de operação inadequadas no local, atmosfera corrosiva, conserto, instalação, exposição ao tempo, casos de força maior, incêndio, roubo ou instalação contrária às recomendações ou especificações da APC ou em qualquer evento em que o número de série da APC tiver sido alterado, rasurado ou removido ou qualquer outra causa além do escopo das indicações de uso.

NÃO EXISTEM GARANTIAS, EXPRESSAS OU IMPLÍCITAS, POR FORÇA DE LEI OU DE QUALQUER OUTRO MODO, DE PRODUTOS VENDIDOS, ASSISTIDOS OU FORNECIDOS SOB ESTE CONTRATO OU EM CONEXÃO COM ESTA GARANTIA. A APC SE ISENTA DE TODAS AS GARANTIAS IMPLÍCITAS DE RESPONSABILIDADE DE COMERCIALIZAÇÃO, SATISFAÇÃO E ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA. AS GARANTIAS EXPRESSAS DA APC NÃO SERÃO AUMENTADAS, REDUZIDAS NEM AFETADAS PELA PRESTAÇÃO DE ASSISTÊNCIA TÉCNICA OU OUTRA ASSESSORIA OU SERVIÇO RELACIONADO AOS PRODUTOS PELA APC E NENHUMA OBRIGAÇÃO OU RESPONSABILIDADE SE ORIGINARÁ DELA. AS PRESENTES GARANTIAS E RECURSOS LEGAIS SÃO EXCLUSIVOS E SUBSTITUEM TODAS AS DEMAIS GARANTIAS E RECURSOS LEGAIS. AS GARANTIAS ACIMA DESCRITAS CONSTITUEM A ÚNICA RESPONSABILIDADE DA APC E A SOLUÇÃO EXCLUSIVA DO COMPRADOR PARA QUALQUER VIOLAÇÃO DE TAIS GARANTIAS. AS GARANTIAS DA APC APLICAM-SE EXCLUSIVAMENTE AO COMPRADOR E NÃO SE ESTENDEM A TERCEIROS.

EM NENHUMA CIRCUNSTÂNCIA, A APC, SEUS DIRETORES, EMPRESAS CONTROLADAS OU FUNCIONÁRIOS SE RESPONSABILIZARÃO POR QUALQUER FORMA DE DANOS INDIRETOS, ESPECIAIS, CONSEQUENTES OU PUNITIVOS DECORRENTES DE USO, MANUTENÇÃO OU INSTALAÇÃO DOS PRODUTOS, QUER ELES DECORRAM DE CONTRATO OU DE DANOS MORAIS, INDEPENDENTEMENTE DE FALHA, NEGLIGÊNCIA OU RESPONSABILIDADE ESTRITA OU A APC TENHA SIDO PREVIAMENTE AVISADA SOBRE A POSSIBILIDADE DE TAIS DANOS. ESPECIFICAMENTE, A APC NÃO SE RESPONSABILIZA POR QUAISQUER CUSTOS, TAIS COMO PERDAS DE VENDAS OU LUCROS CESSANTES, PERDA DO EQUIPAMENTO, IMPOSSIBILIDADE DE USO DO EQUIPAMENTO, PERDA DE PROGRAMAS DE SOFTWARE, PERDA DE DADOS, CUSTOS DE REPOSIÇÃO, RECLAMAÇÕES DE TERCEIROS OU QUALQUER OUTRO CASO.

NENHUM VENDEDOR, FUNCIONÁRIO OU AGENTE DA APC ESTÁ AUTORIZADO A ACRESCENTAR OU ALTERAR OS TERMOS DESTA GARANTIA. OS TERMOS DA GARANTIA PODEM SER MODIFICADOS, SE FOR O CASO, SOMENTE POR ESCRITO E COM A ASSINATURA DE UM EXECUTIVO DA APC E DO DEPARTAMENTO JURÍDICO.

Solicitações de garantia

Clientes com questões sobre solicitações de garantia podem acessar a rede do Serviço de Atendimento ao Cliente da APC através da página de suporte do site da APC, www.apc.com/support. Selecione seu país no menu suspenso de seleção de países na parte superior da página web. Selecione a guia de suporte para obter informações de contato do Serviço de Atendimento ao Cliente em sua região.

Interferência de frequência de rádio



Alterações ou modificações nesta unidade sem a aprovação expressa da parte responsável pela conformidade com as normas podem fazer com que o usuário perca a autorização para operar este equipamento.

EUA—FCC

Este equipamento foi testado e considerado em conformidade com os limites para um dispositivo da Classe A, de acordo com a parte 15 das regras da FCC. Esses limites são projetados de modo a oferecer uma proteção razoável contra interferências prejudiciais quando este equipamento for operado em ambientes de trabalho. Este equipamento gera, usa e pode irradiar energia de frequência de rádio e, se não for instalado e operado de acordo com este manual do usuário, pode causar interferência prejudicial às comunicações por rádio. A operação deste equipamento em uma área residencial provavelmente causará interferência prejudicial. O usuário será totalmente responsável pela correção dessa interferência.

Canadá—ICES

Este aparelho digital da Classe A está em conformidade com o ICES-003 do Canadá.

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

Japão—VCCI

Este é um produto da Classe A com base nas normas do Conselho de Controle Voluntário de Interferência por Equipamento de Tecnologia de Informação (VCCI). Se este equipamento for utilizado em um ambiente doméstico, podem haver interferências de rádio e, nesse caso, pode ser necessário que o usuário tome medidas de correção.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると、電波妨害を引き起こすことがあります。この場合には、使用者が適切な対策を講ずるよう要求されることがあります。

Taiwan—BSMI

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Austrália e Nova Zelândia

Atenção: Este é um produto da Classe A. Em um ambiente doméstico, este produto pode causar interferência de rádio e, nesse caso, pode ser necessário que o usuário tome as medidas adequadas.

União europeia

Este produto está em conformidade com os requisitos de proteção da diretiva 2004/108/EC do conselho da UE relativos à aproximação das leis dos estados membros a respeito da compatibilidade eletromagnética. A APC não pode aceitar responsabilidade por nenhuma falha no cumprimento dos requisitos de proteção que resulte de uma modificação não aprovada do produto.

Este produto foi testado e considerado em conformidade com os limites para equipamentos de tecnologia de informação da Classe A, de acordo com o CISPR 22/padrão europeu EN 55022. Os limites para equipamento da Classe A foram desenvolvidos para ambientes comerciais e industriais para oferecer uma proteção razoável contra interferência com equipamentos de comunicação licenciados.

Atenção: Este é um produto da Classe A. Em um ambiente doméstico, este produto pode causar interferência de rádio e, nesse caso, pode ser necessário que o usuário tome as medidas adequadas.

Coreano 한국

A 급 기기 (업무용 방송통신기기)

이 기기는 업무용 (A 급) 으로 전자파적합등록을 한 기기이오니판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정외의지역에서 사용하는 것을 목적으로 합니다 .

Atendimento mundial ao cliente da APC

O Serviço de Atendimento ao Cliente para este ou qualquer outro produto está disponível, sem custo, de uma das seguintes maneiras:

- Visite o site da APC para acessar documentos na Base de Conhecimentos da APC e para enviar solicitações ao Serviço de Atendimento ao Cliente.
 - www.apc.com (matriz)
Conecte-se aos sites localizados da APC para países específicos, os quais oferecem informações sobre o Serviço de Atendimento ao Cliente.
 - www.apc.com/support/
Suporte global para pesquisas na Base de Conhecimentos da APC e suporte eletrônico.
- Entre em contato com um centro de Serviços de Atendimento ao Cliente da APC por telefone ou e-mail.
 - Centros locais específicos dos países: acesse www.apc.com/support/contact para obter informações sobre meios de contato.

Para obter informações sobre como acessar o Serviço de Atendimento ao Cliente local, entre em contato com o representante ou com outros distribuidores através dos quais o produto foi adquirido.

© 2014 Schneider Electric. Todos os direitos reservados. InfraStruxure, Smart-UPS, Symmetra, PowerNet, MGE, Galaxy e PowerChute são propriedade da Schneider Electric Industries S.A.S., da American Power Conversion Corporation ou de suas empresas afiliadas. Todas as outras marcas comerciais são propriedade de seus respectivos donos.