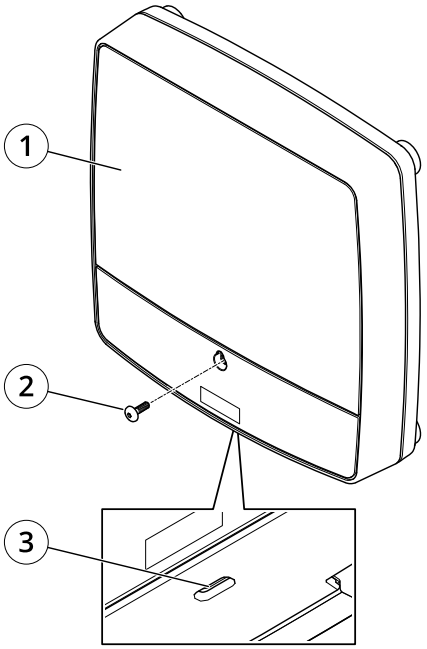
AXIS A1001 & AXIS Entry Manager

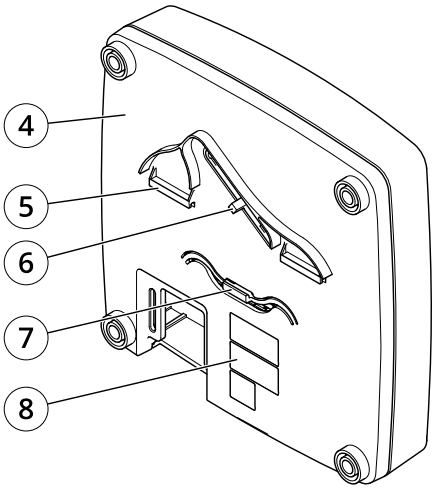
Manual do usuário

Sumário

Sumário

Visão geral do produto

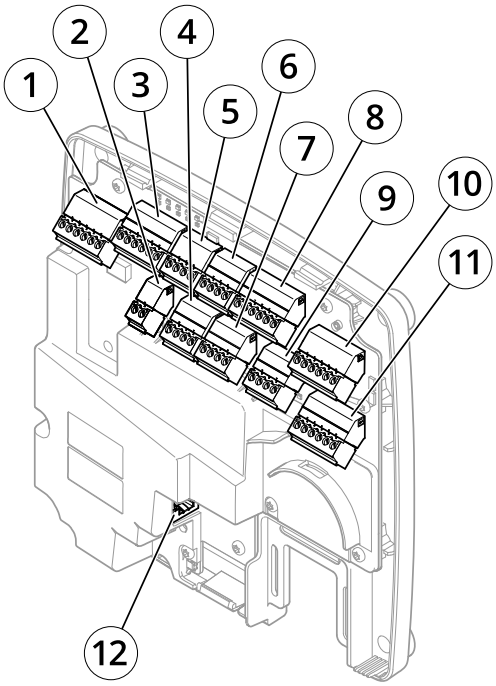




Frente e trás:

1 *Tampa*
2 *Parafuso da tampa*
3 *Slot de remoção da tampa*
4 *Base*
5 *Clipe DIN – superior*
6 *Switch de alarme de violação – trás*
7 *Clipe DIN – inferior*
8 *Número de peça (P/N) e número de série (S/N)*

Visão geral do produto



Interface de E/S:

1 Conector de dados do leitor (READER DATA 1)
10 Conector de dados do leitor (READER DATA 2)
3 Conector de E/S do leitor (READER I/O 1)
8 Conector de E/S do leitor (READER I/O 2)
4 Conector de porta (DOOR IN 1)
7 Conector de porta (DOOR IN 2)
6 Conector auxiliar (AUX)
5 Conector de áudio (AUDIO) (não usado)

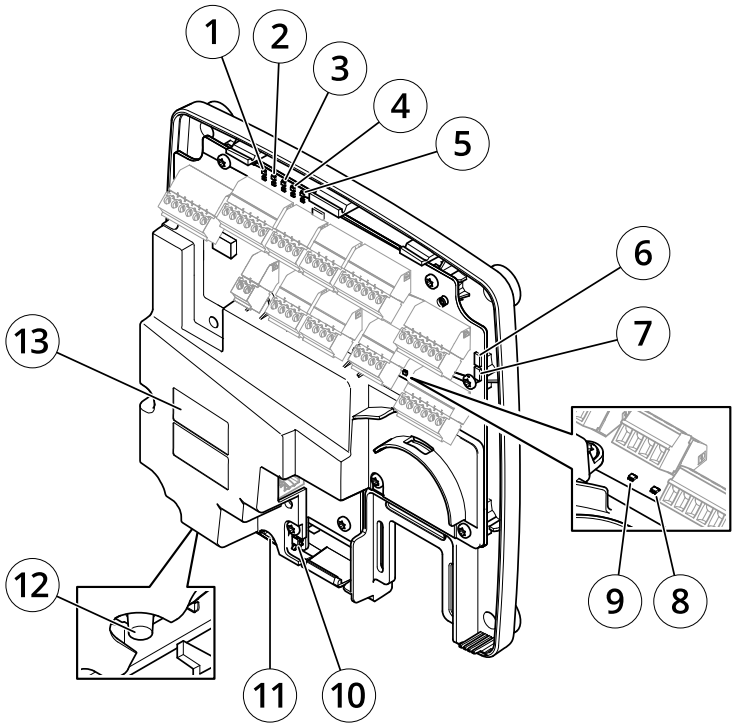
Entradas de alimentação externas:

2 Conector de alimentação (DC IN)
12 Conector de rede (PoE)

Saídas de energia:

9 Conector de trava elétrica (LOCK)
11 Conector de alimentação e relé (PWR, RELAY)

Visão geral do produto



LEDs indicadores, botões e outros hardwares:

1 *LED indicador de energia*
2 *LED indicador de status*
3 *LED indicador de rede*
4 *LED indicador do Leitor 2 (não usado)*
5 *LED indicador do Leitor 1 (não usado)*
6 *Conector header do pino do alarme de violação – frente (TF)*
7 *Conector header do pino do alarme de violação – trás (TB)*
8 *LED indicador de trava*
9 *LED indicador de trava*
10 *Sensor do alarme de violação – frente*
11 *Slot de cartão SD (microSDHC) (não usado)*
12 *Botão de controle*
13 *Número de peça (P/N) e número de série (S/N)*

LEDs indicadores

LED	Cor	Indicação
Rede	Verde	Aceso para conexão a uma rede de 100 Mbps. Pisca quando há atividade na rede.
	Âmbar	Aceso continuamente para uma conexão a uma rede de 10 Mbps. Pisca quando há atividade na rede.
	Apagado	Sem conexão de rede.
Status	Verde	Aceso em verde para operação normal.
	Âmbar	Aceso continuamente durante a inicialização e quando as configurações são restauradas.
	Vermelho	Pisca lentamente para falha na atualização.

Alimentação	Verde	Funcionamento normal.
	Âmbar	Pisca em verde/âmbar durante a atualização do firmware.
Trava	Verde	Sólido quando não energizado.
	Vermelho	Sólido quando energizado.
	Apagado	Flutuando.

Observação

- O LED de status pode ser configurado para piscar enquanto um evento está ativo.
- O LED de status pode ser configurado para piscar para identificar a unidade. Vá para **Setup > Additional Controller Configuration > System Options > Maintenance (Configurar > Configuração de controlador adicional > Opções do sistema > Manutenção)** .

Conectores e botões

Interface de E/S

Conectores de dados do leitor
Dois blocos de terminais de 6 pinos com suporte aos protocolos RS485 e Wiegand para comunicação com o leitor. Para obter especificações, consulte *página 70*.

Conectores de E/S do leitor
Dois blocos de terminais com 6 pinos para entrada e saída do leitor. Além do ponto de referência de 0 VCC e da alimentação (saída CC), o conector de E/S do leitor fornece a interface para:

- Entrada digital – Para conexão, por exemplo, alarmes de violação do leitor.
- Saída digital – Para conexão, por exemplo, beepers e LEDs do leitor.

Para obter especificações, consulte *página 70*.

Conectores de porta
Dois blocos de terminais com 4 pinos para conectar dispositivos de monitoramento de porta e solicitar sair de dispositivos (REX). Para obter especificações, consulte *página 71*.

Conector auxiliar
Bloco de terminais de E/S configurável com 4 pinos Use com dispositivos externos em combinação com, por exemplo, alarmes de violação, acionamento de eventos e notificações de alarmes. Além do ponto de referência de 0 VCC e alimentação (saída CC), o conector auxiliar fornece a interface para:

- Entrada digital – Uma entrada de alarme para conectar dispositivos que podem alternar entre um circuito aberto e fechado, por exemplo, sensores PIR ou detectores de quebra de vidros.
- Saída digital – Para conectar dispositivos externos como alarmes, sirenes ou luzes de arrombamento. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX® ou por uma regra de ação.

Para obter especificações, consulte *página 72*.

Entradas de alimentação externas

OBSERVAÇÃO

O produto deve ser conectado com um cabo de rede blindado (STP). Todos os cabos que conectam o produto à rede devem ser blindados (STP) e usados somente da forma para a qual foram projetados. Certifique-se de que os dispositivos de rede sejam instalados de acordo com as instruções do fabricante. Para obter informações sobre requisitos regulatórios, consulte .

Conector de alimentação
bloco de terminais com 2 pinos para entrada de energia CC. Use uma fonte de alimentação limitada compatível com os requisitos

de tensão de segurança extra baixa (SELV) e com potência de saída nominal restrita a ≤ 100 W ou corrente de saída nominal limitada a ≤ 5 A. Para obter especificações, consulte *página 72*.

Conector de rede
Conector Ethernet RJ45. Compatível com Power over Ethernet (PoE). Para obter especificações, consulte *página 73*.

Saídas de energia

Conector de trava de alimentação

Bloco de terminais com 4 pinos para conectar uma ou duas travas. O conector de trava também pode ser usado para alimentar dispositivos externos. Para obter especificações, consulte *página 73*.

Conector de energia e relé

Bloco de terminais com 6 pinos para conectar energia e relé do controlador de porta a dispositivos externos como travas e sensores. Para obter especificações, consulte *página 73*.

Botões e outros tipos de hardware

Conector header de pino de alarme de violação
Dois conectores headers com 2 pinos para desconectar alarmes de violação frontal e traseiro. Para obter especificações, consulte *página 74*.

Botão de controle
O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte *página 65*.
- Conectar a um serviço do AXIS Video Hosting System. Consulte *página 59*. Para conectar, mantenha o botão apertado por aproximadamente 1 segundo até o LED de status piscar em verde.
- Conexão ao AXIS Internet Dynamic DNS Service. Consulte *página 59*. Para conectar, mantenha o botão pressionado por aproximadamente 3 segundos.

Instalação

Para assistir a este vídeo, vá para a versão Web deste documento.

help.axis.com/?&tpiaId=19467&section=product-overview

Vídeo de instalação do produto.

Como acessar o produto

Para instalar o produto Axis, consulte o guia de instalação fornecido com o produto.

Acesso ao dispositivo

1. Abra um navegador e insira o endereço IP ou o nome de host do dispositivo Axis.

   Se você não souber o endereço IP, use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede.

2. Insira o nome de usuário e a senha. Ao acessar o dispositivo pela primeira vez, você deverá definir a senha de root. Consulte .
3. O AXIS Entry Manager é aberto no navegador. Se estiver usando um computador, você será levado para a página Visão geral. Se estiver usando um dispositivo móvel, você será levado para a página de acesso móvel.

Sobre a página de acesso móvel

A página de acesso móvel mostra o status das portas e fechaduras conectadas ao controlador de porta. Você pode testar o travamento e o destravamento. Atualize a página para ver o resultado.

Um link leva você ao Axis Entry Manager.

Observação

- O Axis Entry Manager não oferece suporte a dispositivos móveis.
- Se você continuar para o Axis Entry Manager, não haverá link de volta para a página de acesso móvel.

Como acessar o produto da Internet

Um roteador de rede permite que os produtos em uma rede privada (LAN) compartilhem uma única conexão com a Internet. Isso é feito ao encaminhar tráfego da rede privada para a Internet.

A maioria dos roteadores são pré-configurados para impedir tentativas de acesso à rede privada (LAN) da rede pública (Internet).

Se o produto Axis estiver localizado em uma intranet (LAN) e você desejar torná-lo disponível do outro lado (WAN) de um roteador NAT (Network Address Translator), ative **NAT traversal**. Com NAT traversal configurado corretamente, todo o tráfego HTTP para uma porta HTTP externa no roteador NAT será encaminhado para o produto.

Como ativar o recurso NAT traversal

- Vá para **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado)**.
- Clique em **Enable (Ativar)**.
- Configure manualmente seu roteador NAT para permitir acesso da Internet.

Consulte também AXIS Internet Dynamic DNS Service em *www.axiscam.net*

Observação

- Nesse contexto, um "roteador" diz respeito a qualquer dispositivo de roteamento de rede, como um roteador NAT, roteador de rede, gateway de Internet, roteador de banda larga, dispositivo de compartilhamento de banda larga ou um software, como um firewall.
- Para que o NAT traversal funcione, ele deverá ser compatível com o roteador. O roteador também deverá oferecer suporte a UPnP®.

Como acessar o produto

Como definir a senha do usuário root

Para acessar o produto Axis, você deverá definir a senha para o usuário administrador padrão **root**. Isso é feito na caixa de diálogo **Configure Root Password (Configurar senha do root)**, aberta quando o produto é acessado pela primeira vez.

Para evitar a violação da confidencialidade da rede, a senha do root poderá ser definida através de uma conexão HTTPS criptografada, o que exigirá um certificado HTTPS. O HTTPS (Hypertext Transfer Protocol over SSL) é um protocolo usado para criptografar tráfego entre navegadores da Web e servidores. O certificado HTTPS garante a troca criptografada de informações. Consulte *HTTPS na página 55*.

O nome de usuário do administrador padrão **root** é permanente e não pode ser excluído. Se a senha do usuário root for perdida, o produto deverá ser restaurado para as configurações padrão de fábrica. Consulte *Redefinição para as configurações padrão de fábrica na página 65*.

Para definir a senha, insira-a diretamente na caixa de diálogo.

A página Overview (Visão geral)

A página Overview (Visão geral) do AXIS Entry Manager mostra informações sobre o nome, endereço MAC, endereço IP e versão do firmware do controlador de porta. Ele também permite a você identificar o controlador de porta na rede ou no sistema.

Na primeira vez que acessar o produto Axis, a página Overview (Visão geral) irá avisá-lo para configurar o hardware, definir a data e hora, configurar as opções de rede e configurar o controlador de porta como parte de um sistema ou uma unidade autônoma. Para obter mais informações sobre como configurar o sistema, consulte *Configuração – Passo a passo na página 12*.

Para retornar para a página Overview (Visão geral) das outras páginas Web do produto, clique em **Overview (Visão geral)** na barra de menus.

Configuração do sistema

Para abrir as páginas de configuração do produto, clique em **Setup (Configuração)** no canto superior direito da página de visão geral.

O produto Axis pode ser configurado por administradores. Para obter mais informações sobre os usuários e administradores, consulte *página 32*, *página 41* e *página 55*.

Configuração – Passo a passo

Antes de começar a usar o sistema de controle de acesso, você deve concluir as etapas de configuração a seguir:

1. Se inglês não for seu primeiro idioma, talvez você queira que o AXIS Entry Manager use um idioma diferente. Consulte *Seleção de um idioma na página 12*.
2. Defina a data e a hora. Consulte *página 12*.
3. Configure as opções de rede. Consulte *página 14*.
4. Configure o controlador de porta e os dispositivos conectados, como leitores, travas e dispositivos de solicitação de saída (REX). Consulte *Configurar o hardware na página 14*.
5. Verifique as conexões de hardware. Consulte *página 21*.
6. Configuração de cartões e formatos. Consulte *página 22*.
7. Configure o sistema do controlador de porta. Consulte *Gerenciar controladores de porta de rede na página 27*.

Para obter informações sobre como configurar e gerenciar portas, agendamentos, usuários e grupos do sistema, consulte *Gerenciamento de acesso na página 32*.

Para obter informações sobre as recomendações de manutenção, consulte *Instruções de manutenção na página 30*.

Observação

Para adicionar ou remover controladores de porta, adicionar, remover ou editar usuários ou configurar o hardware, mais da metade dos controladores de porta no sistema devem estar **online**. Para verificar o status do controlador de porta, vá para **Setup > Manage Network Door Controllers in System (Configuração > Gerenciar controladores de porta de rede no sistema)**.

Seleção de um idioma

O idioma padrão do AXIS Entry Manager é inglês, mas é possível alternar para qualquer um dos idiomas incluídos no firmware do produto. Para obter informações sobre o firmware mais recente disponível, consulte *www.axis.com*

Você pode alternar entre idiomas em qualquer uma das páginas Web do produto.

Para alternar entre idiomas, clique em lista suspensa idioma  e selecione um idioma. Todas as páginas Web e páginas de ajuda do produto são exibidas no idioma selecionado.

Observação

- Quando você alterna o idioma, o formato de data também muda para um formato comumente usado no idioma selecionado. O formato correto é exibido nos campos de dados.
- Se você redefinir o produto para as configurações padrão de fábrica, o AXIS Entry Manager retornará para o idioma inglês.
- Se você restaurar o produto, o AXIS Entry Manager continuará a usar o idioma selecionado.
- Se você reiniciar o produto, o AXIS Entry Manager continuará a usar o idioma selecionado.
- Se você atualizar o firmware, o AXIS Entry Manager continuará a usar o idioma selecionado.

Configuração da data e hora

Se o controlador de porta é parte de um sistema, as configurações de data e hora são distribuídas para todos os controladores de porta. Isso significa que as configurações são enviadas para os outros controladores no sistema, independentemente se você sincroniza com um servidor NTP, define a data e a hora manualmente ou obtém a data e a hora do computador. Caso não consiga ver as alterações, tente atualizar a página em seu navegador. Para obter mais informações sobre como gerenciar um sistema de controladores de porta, consulte *Gerenciar controladores de porta de rede na página 27*.

Para definir a data e a hora do produto Axis, vá para **Setup > Date & Time (Configuração > Data e hora)**.

Você pode definir a data e a hora das seguintes formas:

- Obtenha a data e a hora de um servidor NTP. Consulte *página 13*.
- Definir a data e a hora manualmente. Consulte *página 13*.
- Obter a data e a hora do computador. Consulte *página 13*.

Current controller time (Hora atual do controlador) exibe a data e a hora atuais do controlador de porta (formato de 24 horas).

As mesmas opções para data e hora também estão disponíveis nas páginas System Options (Opções do sistema). Vá para **Setup > Additional Controller Configuration > System Options > Date & Time (Configuração > Configuração de controlador adicional > Opções do sistema > Data e hora)**.

Obtenção da data e hora de um servidor Network Time Protocol (NTP)

1. Vá para **Setup > Date & Time (Configuração > Data e hora)**.
2. Selecione seu **Timezone (Fuso horário)** na lista suspensa.
3. Se o horário de verão é usado em sua região, selecione **Adjust for daylight saving (Ajustar para horário de verão)**.
4. Selecione **Synchronize with NTP (Sincronizar com NTP)**.
5. Selecione o endereço DHCP padrão ou insira o endereço de um servidor NTP.
6. Clique em **Save (Salvar)**.

Quando a sincronização é feita com um servidor NTP, a data e a hora são atualizadas continuamente porque os dados são enviados do servidor NTP. Para obter informações sobre as configurações de NTP, consulte *Configuração de NTP na página 60*.

Se você usa um nome de host para o servidor NTP, um servidor de DNS deverá ser configurado. Consulte *Configuração de DNS na página 60*.

Configuração manual da data e hora

1. Vá para **Setup > Date & Time (Configuração > Data e hora)**.
2. Se o horário de verão é usado em sua região, selecione **Adjust for daylight saving (Ajustar para horário de verão)**.
3. Selecione **Set date & time manually (Definir data e hora manualmente)**.
4. Insira a data e a hora desejadas.
5. Clique em **Save (Salvar)**.

Ao configurar manualmente a data e a hora, elas serão definidas uma vez e não serão atualizadas automaticamente. Isso significa que, se a data e a hora precisarem ser atualizadas, as alterações deverão ser feitas manualmente porque não há nenhuma conexão a um servidor NTP externo.

Obtenção da data e da hora do computador

1. Vá para **Setup > Date & Time (Configuração > Data e hora)**.

2. Se o horário de verão é usado em sua região, selecione **Adjust for daylight saving (Ajustar para horário de verão)**.
3. Selecione **Set date & time manually (Definir data e hora manualmente)**.
4. Clique em **Sync now and save (Sincronizar agora e salvar)**.

Quando a hora do computador é usada, a data e a hora são sincronizadas com a hora do computador uma vez. Elas não serão atualizadas automaticamente. Isso significa que, se você alterar a data e a hora no computador usado para gerenciar o sistema, a sincronização deverá ser feita novamente.

Configuração das opções de rede

Para configurar as opções básicas de rede, vá para **Setup > Network Settings (Configuração > Configurações de rede)** ou para **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Básicas)**.

Para obter mais informações sobre as configurações de rede, consulte *Rede na página 57*.

Configurar o hardware

Antes de gerenciar as portas e andares, o hardware deverá ser configurado nas páginas de configuração de hardware.

Você pode conectar leitores, travas e outros dispositivos ao produto Axis antes de concluir a configuração do hardware. No entanto, será mais fácil conectar dispositivos se você concluir a configuração do hardware primeiro. Isso ocorre, pois um gráfico de pinagem de hardware estará disponível quando a configuração for concluída. O gráfico de pinagem de hardware é um guia sobre como conectar dispositivos aos pinos e pode ser usado como uma folha de referência para manutenção. Para obter instruções de manutenção, consulte *página 30*.

Se estiver configurando o hardware pela primeira vez, selecione um dos seguintes métodos:

- Importe um arquivo de configuração de hardware. Consulte *página 14*.
- Crie uma nova configuração de hardware. Consulte *página 15*.

Observação

Se o hardware do produto não tiver sido configurado antes ou tiver sido excluído, **Hardware Configuration (Configuração de hardware)** estará disponível no painel de notificação na página de visão geral.

Como importar um arquivo de configuração de hardware

A configuração de hardware do produto Axis pode ser concluída mais rapidamente ao importar um arquivo de configuração de hardware.

Ao exportar o arquivo de um produto e importá-lo em outros, você poderá fazer várias cópias da mesma configuração de hardware sem repetir as mesmas etapas. Você também pode armazenar arquivos exportados como backups e usá-los para restaurar configurações de hardware. Para obter mais informações, consulte *Como exportar um arquivo de configuração de hardware na página 15*.

Para importar um arquivo de configuração de hardware:

1. Vá para **Setup > Hardware Configuration (Configurar > Configuração de hardware)**.
2. Clique em **Import hardware configuration (Importar configuração de hardware)** ou, se uma configuração de hardware já existir, **Reset and import hardware configuration (Redefinir e importar configuração de hardware)**.
3. Na caixa de diálogo do navegador exibida, localize e selecione o arquivo de configuração de hardware (*.json) em seu computador.
4. Clique em **OK**.

Como exportar um arquivo de configuração de hardware

A configuração de hardware do produto Axis pode ser exportada para criar várias cópias da mesma configuração de hardware. Você também pode armazenar arquivos exportados como backups e usá-los para restaurar configurações de hardware.

Observação

Não é possível exportar a configuração de hardware de andares.

As configurações de rede sem fio não são incluídas na exportação da configuração de hardware.

Para exportar um arquivo de configuração de hardware:

1. Vá para **Setup > Hardware Configuration (Configurar > Configuração de hardware)**.
2. Clique em **Export hardware configuration (Exportar configuração de hardware)**.
3. Dependendo do navegador, talvez seja necessário passar por uma caixa de diálogo para concluir a exportação.

   A menos que especificado de outra forma, o arquivo exportado (*.json) é salvo na pasta de download padrão. Você pode selecionar uma pasta de download nas configurações de usuário do navegador da Web.

Criação de uma nova configuração de hardware

Siga as instruções de acordo com suas necessidades:

- *Como criar uma nova configuração de hardware sem periféricos na página 15*
- *Como criar uma nova configuração de hardware para travas sem fio na página 19*
- *Como criar uma nova configuração de hardware com controle de elevador (AXIS A9188) na página 20*

Como criar uma nova configuração de hardware sem periféricos

1. Vá para **Setup > Hardware Configuration (Configurar > Configuração de hardware)** e clique em **Start new hardware configuration (Iniciar nova configuração de hardware)**.
2. Insira um nome para o produto Axis.
3. Selecione o número de portas conectadas e clique em **Next (Avançar)**.
4. Configure os monitores de porta (sensores de posição de porta) e travas de acordo com seus requisitos e clique em **Next (Avançar)**. Para obter mais informações sobre as opções disponíveis, consulte *Como configurar monitores de portas e travas na página 15*.
5. Configure os leitores e dispositivos REX que serão usados e clique em **Finish (Concluir)**. Para obter mais informações sobre as opções disponíveis, consulte *Como configurar leitores e dispositivos REX na página 18*.
6. Clique em **Close (Fechar)** ou no link para exibir o gráfico de pinos do hardware.

Como configurar monitores de portas e travas

Após selecionar uma opção de porta na nova configuração de hardware, você poderá configurar monitores e travas de portas.

1. Se um monitor de portas for usado, selecione **Door monitor (Monitor de portas)** e, em seguida, selecione a opção que corresponde a como os circuitos de monitor de portas serão conectados.
2. Se a trava da porta precisar ser travada imediatamente após a porta abrir, selecione **Cancel access time once door is opened (Cancelar o tempo de acesso uma vez que a porta é aberta)**.

   Se deseja atrasar o retravamento, defina o tempo de atraso em milissegundos em **Relock time (Tempo para retravamento)**.
3. Especifique as opções de tempo do monitor de portas ou, se nenhum monitor de portas for usado, as opções de tempo da trava.

4. Selecione as opções que correspondem à forma como os circuitos de travas serão conectados.
5. Se um monitor de travas for usado, selecione **Lock monitor (Monitor de travas)** e, em seguida, selecione as opções que correspondem à forma como os circuitos de monitor de travas serão conectados.
6. Se as conexões de entrada dos leitores, dispositivos REX e monitores de portas precisarem ser supervisionadas, selecione **Enable supervised inputs (Ativar entradas supervisionadas)**.

   Para obter mais informações, consulte *Como usar entradas supervisionadas na página 18*.

Observação

- A maioria das opções de trava, monitor de portas e leitor podem ser alteradas sem redefinir e iniciar uma nova configuração de hardware. Vá para **Setup > Hardware Reconfiguration (Configuração > Reconfiguração de hardware)**.
- Você pode conectar um monitor de travas por controlador de porta. Assim, se você usar portas com travas duplas, somente uma das travas poderá ter um monitor de travas. Se duas portas estiverem conectadas ao mesmo controlador de porta, os monitores de portas não poderão ser usados.
- As travas motorizadas devem ser configuradas como travas secundárias.

Sobre opções do monitor de portas e tempo

As seguintes opções do monitor de portas estão disponíveis:

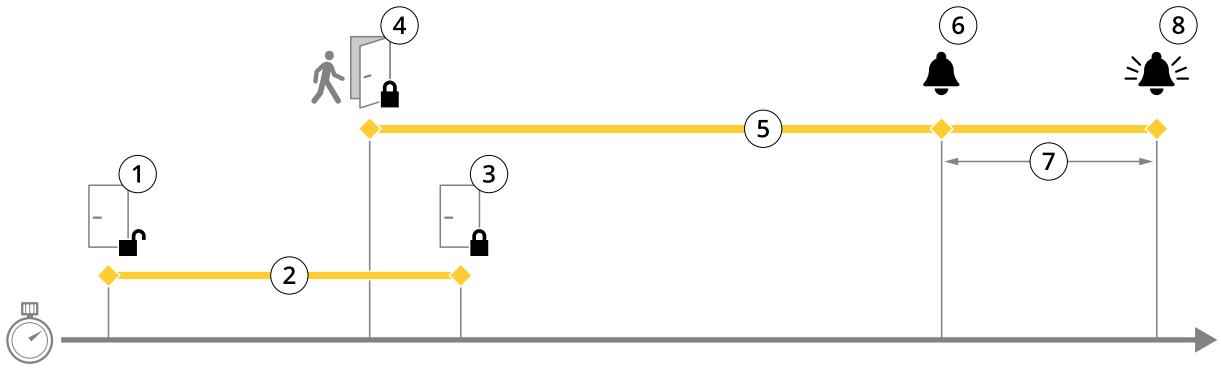
- **Door monitor (Monitor de portas)** – Selecionada por padrão. Cada porta possui seu próprio monitor de portas que, por exemplo, emitirá um sinal quando a porta é forçada ou permanece aberta por muito tempo. Desmarque a opção se nenhum monitor de portas for usado.
  - **Open circuit = Closed door (Circuito aberto = Porta fechada)** – Selecione se o circuito do monitor de portas é normalmente aberto. O monitor de portas fornece o sinal de porta aberta quando o circuito está fechado. O monitor de portas fornece o sinal de porta fechada quando o circuito está aberto.
  - **Open circuit = Open door (Circuito aberto = Porta aberta)** – Selecione se o circuito do monitor de portas é normalmente fechado. O monitor de portas fornece o sinal de porta aberta quando o circuito está aberto. O monitor de portas fornece o sinal de porta fechada quando o circuito está fechado.
- **Cancel access time once door is opened (Cancelar o tempo de acesso uma vez que a porta é aberta)** – Selecione essa opção para impedir entradas não autorizadas. A trava será acionada assim que o monitor de portas indicar que a porta foi aberta.

As seguintes opções de tempo de porta estão sempre disponíveis:

- **Access time (Tempo de acesso)** – Defina o número de segundos que a porta deve permanecer destravada após o acesso ser concedido. A porta permanece destravada até ser aberta ou até o tempo definido ser atingido. A porta será travada assim que fechar, independentemente se o tempo de acesso expirou ou não.
- **Long access time (Tempo de acesso longo)** – Defina o número de segundos que a porta deve permanecer destravada após o acesso ser concedido. O tempo de acesso longo sobrescreve o tempo de acesso já definido e será ativado para usuários com tempo de acesso longo selecionado. Consulte *Credenciais de usuário na página 42*.

Selecione **Door monitor (Monitor de portas)** para disponibilizar as seguintes opções de tempo de porta:

- **Open too long time (Aberta há muito tempo)** – Defina o número de segundos em que a porta pode permanecer aberta. Se a porta ainda estiver aberta quando o tempo definido for atingido, o alarme de porta aberta há muito tempo será acionado. Configure uma regra de ação para definir a ação que deve ser disparada pelo evento de porta aberta há muito tempo.
- **Pre-alarm time (Tempo pré-alarme)** – Um pré-alarme é um sinal de alerta que é acionado antes que o tempo de aberta há muito tempo seja atingido. Ele informa o administrador e avisa, dependendo de como a regra de ação foi configurada, à pessoa que está entrando pela porta que a porta deve ser fechada para evitar o acionamento do alarme de porta aberta há muito tempo. Defina o número de segundos antes de o alarme de aberta há muito tempo ser acionado em que o sistema deve emitir o sinal de alerta pré-alarme. Para desativar o pré-alarme, defina o tempo de pré-alarme como 0.



1 *Acesso concedido – a trava abre*
2 *Hora de acesso*
3 *Nenhuma ação realizada – a trava fecha*
4 *Ação realizada (porta aberta) – fecha as travas ou permanece destravada até que a porta feche*
5 *Aberta por muito tempo*
6 *O pré-alarme é acionado*
7 *Tempo de pré-alarme*
8 *O alarme de aberta há muito tempo é acionado*

Para obter informações sobre como configurar uma regra de ação, consulte *Como configurar regras de ação na página 48*.

Sobre opções de travamento

As seguintes opções de circuito de travamento estão disponíveis:

- 12 V
  - **Fail-secure (Segurança contra falhas)** – Selecione para travas que permanecerão bloqueadas durante quedas de energia. Ao aplicar corrente elétrica, a trava será desbloqueada.
  - **Fail-safe (Segurança contra falhas)** – Selecione para travas que serão desbloqueadas durante quedas de energia. Ao aplicar corrente elétrica, a trava será bloqueada.
- **Relay (Relé)** – Somente pode ser usado em uma trava por controlador de porta. Se duas portas estiverem conectadas ao controlador de porta, um relé somente poderá ser usado na trava da segunda porta.
  - **Relay open = Locked (Relé aberto = Bloqueado)** – Selecione para travas que permanecerão bloqueadas quando o relé for aberto (segurança contra falhas). Quando o relé fechar, a trava será desbloqueada.
  - **Relay open = Unlocked (Relé aberto = Desbloqueado)** – Selecione para travas que serão desbloqueadas durante quedas de energia (segurança contra falhas). Quando o relé fechar, a trava será bloqueada.
- **None (Nenhuma)** – Disponível somente para a trava 2. Selecione se apenas uma trava será usada.

As seguintes opções de monitor de travas estão disponíveis para configurações de uma porta:

- **Lock monitor (Monitor de travas)** – Selecione para disponibilizar os controles do monitor de travas. Em seguida, selecione a trava que será monitorada. Um monitor de travas somente poderá ser usado em portas de trava dupla e não poderá ser usado se duas portas estiverem conectadas ao controlador de porta.
  - **Open circuit = Locked (Circuito aberto = Bloqueado)** – Selecione se o circuito de monitor de travas está normalmente fechado. O monitor de travas fornece o sinal de destravamento de porta quando o circuito está fechado. O monitor de travas fornece o sinal de travamento de porta quando o circuito está aberto.
  - **Open circuit = Unlocked (Circuito aberto = Desbloqueado)** – Selecione se o circuito do monitor de travas está normalmente aberto. O monitor de travas fornece o sinal de destravamento de porta quando o circuito está aberto. O monitor de travas fornece o sinal de travamento de porta quando o circuito está fechado.

Como configurar leitores e dispositivos REX

Após configurar os monitores de portas e travas na nova configuração de hardware, você poderá configurar os leitores e dispositivos de solicitação de saída (REX).

1. Se um leitor for usado, marque a caixa de seleção e, em seguida, selecione as opções que correspondem ao protocolo de comunicação do leitor.
2. Se um dispositivo REX, como um botão, sensor ou barra de empurrar for usado, marque a caixa de seleção e, em seguida, selecione a opção que corresponde a como os circuitos do dispositivo REX serão conectados.

   Se o sinal REX não influenciar a abertura da porta (por exemplo, para portas com alças mecânicas ou barras de empurrar), selecione **REX does not unlock door (REX não destrava porta)**.
3. Ao conectar mais de um leitor ou dispositivo REX ao controlador de porta, execute as duas etapas anteriores novamente até cada leitor ou dispositivo REX ter as configurações corretas.

Sobre opções de leitor e dispositivo REX

As seguintes opções de leitor estão disponíveis:

- **Wiegand** – Selecione para leitores que usam protocolos Wiegand. Em seguida, selecione o controle de LED compatível com o leitor. Leitores com controle de LED único, geralmente alternam entre vermelho e verde. Leitores com controle de LED duplo usam fios diferentes para os LEDs vermelhos e verdes. Isso significa que os LEDs são controlados de forma independente. Quando ambos os LEDs estão ativados, a luz é exibida em âmbar. Consulte as informações do fabricante sobre qual controle de LED é compatível com o leitor.
- **OSDP, RS485 half-duplex** – Selecione para leitores RS485 com suporte a half-duplex. Consulte as informações do fabricante sobre protocolos compatíveis com o leitor.

As seguintes opções de dispositivo REX estão disponíveis:

- **Active low (Baixo ativo)** – Selecione se ativar o dispositivo REX fechará o circuito.
- **Active high (Alto ativo)** – Selecione se ativar o dispositivo REX abrirá o circuito.
- **REX does not unlock door (REX não destrava porta)** – Selecione se o sinal REX não influenciará a abertura de portas (por exemplo, para portas com alças mecânicas ou barras de empurrar). O alarme de abertura forçada de porta não será acionado desde que o usuário abra a porta no tempo de acesso. Desmarque se a porta tiver que ser destravada automaticamente quando o usuário ativar o dispositivo REX.

Observação

A maioria das opções de trava, monitor de portas e leitor pode ser alterada sem redefinir e iniciar uma nova configuração de hardware. Vá para **Setup > Hardware Reconfiguration (Configuração > Reconfiguração de hardware)**.

Como usar entradas supervisionadas

Relatório de entradas supervisionadas sobre o status da conexão entre o controlador de porta e os leitores, dispositivos REX e monitores de portas. Se a conexão for interrompida, um evento será ativado.

Para usar entradas supervisionadas:

1. Instale resistores de fim de linha em todas as entradas supervisionadas usadas. Consulte o diagrama de conexão em *página 75*.
2. Vá para **Setup > Hardware Reconfiguration (Configuração > Reconfiguração de hardware)** e selecione **Enable supervised inputs (Ativar entradas supervisionadas)**. Você também pode ativar entradas supervisionadas durante a configuração de hardware.

Sobre a compatibilidade de entradas supervisionadas

Os seguintes conectores oferecem suporte a entradas supervisionadas:

- Conector de E/S do leitor – sinal de violação. Consulte *página 70*.
- Conector de porta. Consulte *página 71*.

Leitores e switches que podem ser usados com entradas supervisionadas incluem:

- Leitores e switches com pull-up interno de 1 kΩ para 5 V.
- Leitores e switches sem pull-up interno.

Como criar uma nova configuração de hardware para travas sem fio

1. Vá para **Setup > Hardware Configuration (Configurar > Configuração de hardware)** e clique em **Start new hardware configuration (Iniciar nova configuração de hardware)**.
2. Insira um nome para o produto Axis.
3. Na lista de periféricos, selecione um fabricante para um gateway sem fio.
4. Se você desejar conectar uma porta com fio, marque a caixa de seleção **1 Door (1 Porta)** e clique em **Next (Avançar)**. Se nenhuma porta estiver incluída, clique em **Finish (Concluir)**.
5. Dependendo do fabricante da sua trava, prossiga segundo um dos tópicos:
   - **ASSA Aperio**: clique no link para exibir o gráfico de pinos de hardware ou clique em **Close (Fechar)** e vá para **Setup > Hardware Reconfiguration (Configurar > Reconfiguração de hardware)** para concluir a configuração, consulte *Adição de portas e dispositivos Assa Aperio™ na página 19*
   - **SmartIntego**: clique no link para exibir o gráfico de pinos de hardware ou em **Click here to select wireless gateway and configure doors (Clique aqui para selecionar gateway sem fio e configurar portas)** para concluir a configuração, consulte *Como configurar o SmartIntego na página 27*.

Adição de portas e dispositivos Assa Aperio™

Para que uma porta sem fio seja adicionada ao sistema, ela precisa ser pareada ao hub de comunicação Assa Aperio conectado por meio do Aperio PAP (ferramenta de aplicativo de programação Aperio).

Para adicionar uma porta sem fio:

1. Vá para **Setup (Configurar)** > **Hardware Reconfiguration (Reconfiguração de hardware)**.
2. Em portas sem fio e dispositivos, clique em **Add door (Adicionar porta)**.
3. No campo **Door name (Nome da porta)**: Insira um nome descritivo.
4. No campo **ID** em **Lock (Trava)**: Insira o endereço com 6 caracteres do dispositivo que você deseja adicionar. O endereço do dispositivo está impresso no rótulo do produto.
5. Opcionalmente, em **Door position sensor (Sensor de posição da porta)**: Escolha **Built in door position sensor (Sensor integrado de posição da porta)** ou **External door position sensor (Sensor externo de posição da porta)**.

Observação

Ao usar um sensor externo de posição da porta (DPS), certifique-se de que o dispositivo de trava Aperio ofereça suporte à detecção de estado da maçaneta da porta antes de configurá-lo.

6. Opcionalmente, no campo **ID** em **Door position sensor (Sensor de posição da porta)**: Insira o endereço com 6 caracteres do dispositivo que você deseja adicionar. O endereço do dispositivo está impresso no rótulo do produto.
7. Clique em **Add (Adicionar)**.

Como criar uma nova configuração de hardware com controle de elevador (AXIS A9188)

Importante

Antes de criar uma configuração de HW, você precisa adicionar um usuário no AXIS A9188 Network I/O Relay Module. Vá para a interface Web A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferências > Configuração de dispositivo adicional > Configuração básica > Usuários > Adicionar > Configuração de usuário)**.

Observação

No máximo 2 AXIS 9188 Network I/O Relay Modules podem ser configurados com cada Axis Network Door Controller

1. No A1001, vá para **Setup > Hardware Configuration (Configurar > Configuração de hardware)** e clique em **Start new hardware configuration (Iniciar nova configuração de hardware)**.
2. Insira um nome para o produto Axis.
3. Na lista de periféricos, selecione **Elevator control (Controle de elevador)** para incluir um AXIS A9188 Network I/O Relay Module e clique em **Next (Avançar)**.
4. Insira um nome para o leitor conectado.
5. Selecione o protocolo do leitor que será usado e clique em **Finish (Concluir)**.
6. Clique em **Network Peripherals (Periféricos de rede)** para concluir a configuração, consulte *Como adicionar e configurar periféricos de rede na página 20* ou clique no link para ir para o gráfico de pinos de hardware.

Como adicionar e configurar periféricos de rede

Importante

- Antes de configurar os periféricos de rede, é necessário adicionar um usuário ao AXIS A9188 Network I/O Relay Module. Vá para a interface Web da AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferências > Configuração de dispositivo adicional > Configuração básica > Usuários > Adicionar > Configuração de usuário)**.
- Não adicione outro AXIS A1001 Network Door Controller como um periférico de rede.

1. Vá para **Setup > Network Peripherals (Configuração > Periféricos de rede)** para adicionar um dispositivo
2. Encontre seus dispositivos em **Discovered devices (Dispositivos descobertos)**.
3. Clique em **Add this device (Adicionar este dispositivo)**.
4. Insira um nome para o dispositivo
5. Insira o nome de usuário e a senha da AXIS A9188
6. Clique em **Add (Adicionar)**.

Observação

Você pode adicionar manualmente periféricos de rede inserindo o endereço MAC ou endereço IP na caixa de diálogo **Manually add device (Adicionar dispositivo manualmente)**.

Importante

Se desejar excluir um agendamento, certifique-se primeiro de que ele não esteja sendo usado pelo módulo de relé e E/S de rede.

Como configurar E/S e relés em periféricos de rede

Importante

Antes de configurar os periféricos de rede, é necessário adicionar um usuário ao AXIS A9188 Network I/O Relay Module. Vá para a interface Web da AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferências > Configuração de dispositivo adicional > Configuração básica > Usuários > Adicionar > Configuração de usuário)**.

1. Vá para **Setup > Network Peripherals (Configuração > Periféricos rede)** e clique na linha **Added devices (Dispositivos adicionados)**.
2. Escolha quais E/S e relés serão definidos como andar.
3. Clique em **Set as floor (Definir como andar)** e insira um nome.
4. Clique em **Add (Adicionar)**.

O andar agora está visível na guia **Floor (Andar)** em **Access Management (Gerenciamento de acesso)**.

Observação

No AXIS entry Manager, você pode adicionar no máximo 16 andares.

Verifique as conexões de hardware

Quando a instalação e a configuração do hardware estiverem concluídas, e em qualquer momento durante o ciclo de vida do controlador de porta, você poderá verificar a função dos monitores de portas, módulos de relé de E/S de rede, travas e leitores conectados.

Para verificar a configuração e acessar os controles de verificação, vá para **Setup > Hardware Connection Verification (Configuração > Verificação da conexão de hardware)**.

Portas de controles de verificação

- **Door state (Estado da porta)** – Verifique o estado atual do monitor de portas, alarmes de porta e travas. Clique em **Get current state (Obter estado atual)**.
- **Lock (Travar)** – Aciona a trava manualmente. As travas principais e secundárias, se houver alguma, serão afetadas. Clique em **Lock (Travar)** ou **Unlock (Destravar)**.
- **Lock (Travar)** – Aciona manualmente a trava para conceder acesso. Somente travas principais serão afetadas. Clique em **Access (Acesso)**.
- **Reader: Feedback (Leitor: Feedback)** – Verifique o feedback do leitor, por exemplo, sons e sinais de LED, para diferentes comandos. Selecione o comando e clique em **Test (Testar)**. Os tipos de feedback disponíveis dependem do leitor. Para obter mais informações, consulte *Feedback do leitor na página 53*. Consulte também as instruções do fabricante.
- **Reader: Tampering (Leitor: Violação)** – Obtenha informações sobre a última tentativa de violação. A primeira tentativa de violação será registrada quando o leitor for instalado. Clique em **Get last tampering (Obter a última violação)**.
- **Reader: Card swipe (Leitor: Passagem de cartão)** – Obtenha informações sobre o último cartão utilizado ou outro tipo de token de usuário aceito pelo leitor. Clique em **Get last credential (Obter a última credencial)**.
- **REX** – Obtenha informações sobre a última vez em que a solicitação para sair do dispositivo (REX) foi pressionada. Clique em **Get last REX (Obter último REX)**.

Controles de verificação de andares

- **Floor state (Estado do andar)** – Verifica o estado atual do acesso ao andar. Clique em **Get current state (Obter estado atual)**.

- **Floor lock & unlock (Travar e destravar andar)** – Aciona manualmente o acesso ao andar. As travas principais e secundárias, se houver alguma, serão afetadas. Clique em **Lock (Travar)** ou **Unlock (Destravar)**.
- **Floor access (Acesso ao andar)** – Conceda manualmente acesso temporário ao andar. Somente travas principais serão afetadas. Clique em **Access (Acesso)**.
- **Elevator Reader: Feedback (Leitor do elevador: Feedback)** – Verifique o feedback do leitor, por exemplo, sons e sinais de LED, para diferentes comandos. Selecione o comando e clique em **Test (Testar)**. Os tipos de feedback disponíveis dependem do leitor. Para obter mais informações, consulte *Feedback do leitor na página 53*. Consulte também as instruções do fabricante.
- **Elevator Reader: Tampering (Leitor do elevador: Violação)** – Obtenha informações sobre a última tentativa de violação. A primeira tentativa de violação será registrada quando o leitor for instalado. Clique em **Get last tampering (Obter a última violação)**.
- **Elevator Reader: Card swipe (Leitor do elevador: Passagem de cartão)** – Obtenha informações sobre o último cartão utilizado ou outro tipo de token de usuário aceito pelo leitor. Clique em **Get last credential (Obter a última credencial)**.
- **REX** – Obtenha informações sobre a última vez em que a solicitação para sair do dispositivo (REX) foi pressionada. Clique em **Get last REX (Obter último REX)**.

Configuração de cartões e formatos

O controlador de porta possui alguns formatos de cartão comumente usado predefinidos que você pode usar como são ou modificá-los conforme necessário. Você também pode criar formatos de cartão personalizados. Cada formato de cartão possui um conjunto de regras diferentes – mapas de campo – para o modo como as informações armazenadas no cartão são organizadas. Ao definir um formato de cartão, você informa ao sistema como interpretar as informações que o controlador obtém do leitor. Para obter informações sobre quais formatos de cartão são aceitos pelo leitor, consulte as instruções do fabricante.

Para ativar formatos de cartão:

1. Vá para **Setup > Configure cards and formats (Configuração > Configurar cartões e formatos)**.
2. Selecione um ou mais formatos de cartão correspondentes ao formato de cartão usado pelos leitores conectados.

Para criar novos formatos de cartão:

1. Vá para **Setup > Configure cards and formats (Configuração > Configurar cartões e formatos)**.
2. Clique em **Add card format (Adicionar formato de cartão)**.
3. Na caixa de diálogo **Add card format (Adicionar formato de cartão)**, insira um nome, uma descrição e o tamanho em bits do formato de cartão. Consulte *Descrições de formatos de cartão na página 23*.
4. Clique em **Add field map (Adicionar mapa de campos)** e insira as informações necessárias nos campos. Consulte *Mapas de campos na página 23*.
5. Para adicionar vários mapas de campo, repita a etapa anterior.

Para expandir um item na lista **Card formats (Formatos de cartão)** e exibir as descrições e os mapas de campos do formato do cartão, clique em  .

Para editar um formato de cartão, clique em  e altere as descrições de formato de cartão e mapa de campos conforme necessário. Em seguida, clique em **Save (Salvar)**.

Para excluir um mapa de campos na caixa de diálogo **Edit card format (Editar formato de cartão)** ou **Add card format (Adicionar formato de cartão)**, clique em

Para excluir um formato de cartão, clique em  .

Importante

- Todas as alterações nos formatos de cartão aplicam-se a todo o sistema de controladores de porta.
- Você só pode ativar e desativar os formatos de cartão se pelo menos um controlador de porta no sistema foi configurado com pelo menos um leitor. Consulte *Configurar o hardware na página 14* e *Como configurar leitores e dispositivos REX na página 18*.
- Dois formatos de cartão com o mesmo tamanho em bits não podem estar ativos ao mesmo tempo. Por exemplo, se você definiu dois formatos de cartão de 32 bits, "Formato A" e "Format B", e "Formato A" estiver ativado, você não poderá ativar o "Formato B" sem antes desativar o "Formato A".
- Se nenhum dos formatos de cartão tiverem sido ativados, você poderá usar os tipos de identificação **Card raw only (Somente raw do cartão)** e **Card raw and PIN (Raw do cartão e PIN)** para identificar um cartão e conceder acesso aos usuários. No entanto, não recomendamos fazer isso, pois fabricantes de leitores ou configurações de leitor diferentes podem gerar dados raw diferentes.

Descrições de formatos de cartão

- **Name (Nome)** (obrigatório) – Insira um nome descritivo.
- **Description (Descrição)** – Insira informações adicionais conforme desejado. Essas informações estão visíveis somente nas caixas de diálogo **Edit card format (Editar formato de cartão)** e **Add card format (Adicionar formato de cartão)**.
- **Bit length (Tamanho em bits)** (obrigatório) – Insira o tamanho em bits do formato de cartão. Ele deve ser um valor entre 1 e 1000000000.

Mapas de campos

- **Name (Nome)** (obrigatório) – Insira o nome do mapa de campos sem usar espaços, por exemplo, `ParidadeÍmpar`.

  Exemplos de mapas de campos comuns incluem:

  - `Parity` – Bits de paridade são usados na detecção de erros. Os bits de paridade são normalmente adicionados no inicio ou no final de uma string de código binária para indicar se o número de bits é par ou ímpar.
  - `EvenParity` – Bits de paridade par garantem que há um número par de bits na string. Os bits que têm o valor 1 são contados. Se a contagem já for par, o valor do bit de paridade é definido como 0. Se a contagem for ímpar, o valor do bit de paridade par é definido como 1, tornando a contagem total um número par.
  - `OddParity` – Bits de paridade ímpar garantem que há um número ímpar de bits na string. Os bits que têm o valor 1 são contados. Se a contagem já for ímpar, o valor do bit de paridade ímpar é definido como 0. Se a contagem for par, o valor do bit de paridade é definido como 1, tornando a contagem total um número ímpar.
  - `FacilityCode` – Os códigos de local algumas vezes são usados para verificar se o token corresponde ao lote de credenciais de usuário final solicitado. Em sistemas de controle de acesso mais antigos, o código de local era usado para uma validação degradada, permitindo a entrada de qualquer funcionário no lote de credenciais que havia sido codificado com um código de local correspondente. Esse nome de mapa de campos, o qual diferencia maiúsculas de minúsculas, é necessário para o produto realizar a validação do código de local.
  - `CardNr` – O número do cartão ou ID de usuário é o que é mais comumente validado em sistemas de controle de acesso. Esse nome de mapa de campos, o qual diferencia maiúsculas de minúsculas, é necessário para o produto realizar a validação do número do cartão.
  - `CardNrHex` – Os dados binários do número do cartão são codificados como números hexadecimais em caracteres minúsculos no produto. Eles são usados principalmente para soluções de problemas quando você não está recebendo o número de cartão esperado do leitor.

- **Range (Intervalo)** (obrigatório) – Insira o intervalo de bits do mapa de campos, por exemplo, 1, 2 – 17, 18 – 33 e 34.
- **Encoding (Codificação)** (obrigatório) – Selecione o tipo de codificação de cada mapa de campos.
  - **BinLE2Int** – Os dados são codificados como números inteiros na ordem de bits little endian. Integer significa que ele precisa ser um número inteiro (sem decimais). A ordem de bits little endian significa que o primeiro bit é o menor (menos significativo).

- **BinBE2Int** – Os dados são codificados como números inteiros na ordem de bits big endian. Integer significa que ele precisa ser um número inteiro (sem decimais). A ordem de bits big endian significa que o primeiro bit é o maior (mais significativo).
- **BinLE2Hex** – Os dados binários são codificados como números hexadecimais em caracteres minúsculos em ordem de bits little endian. O sistema hexadecimal, também conhecido como sistema de números de base 16, consiste em 16 símbolos exclusivos: os números 0 – 9 e as letras a – f. A ordem de bits little endian significa que o primeiro bit é o menor (menos significativo).
- **BinBE2Hex** – Os dados binários são codificados como números hexadecimais em caracteres minúsculos em ordem de bits big endian. O sistema hexadecimal, também conhecido como sistema de números de base 16, consiste em 16 símbolos exclusivos: os números 0 – 9 e as letras a – f. A ordem de bits big endian significa que o primeiro bit é o maior (mais significativo).
- **BinLEIBO2Int** – Os dados binários são codificados da mesma forma que no BinLE2Int, mas os dados raw do cartão são lidos na ordem de bytes invertida em uma sequência de vários bytes antes que os mapas de campos sejam removidos para codificação.
- **BinBEIBO2Int** – Os dados binários são codificados assim como no BinBE2Int, mas os dados raw do cartão são lidos na ordem de bytes invertida em uma sequência de vários bytes antes que os mapas de campos sejam removidos para codificação.

Para obter informações sobre quais mapas de campos seu formato de cartão utiliza, consulte as instruções do fabricante.

Código de local predefinido

Códigos de local são às vezes usados para verificar se o token corresponde ao sistema de controle de acesso do local. Muitas vezes, todos os tokens emitidos para um único local possuem o mesmo código de local. Insira um código de local predefinido para facilitar o registro manual de um lote de cartões. O código de local predefinido é preenchido automaticamente durante a adição de usuários. Consulte*Credenciais de usuário na página 42*

Para criar um código de local predefinido:

1. Vá para **Setup > Configure cards and formats (Configuração > Configurar cartões e formatos)**.
2. Em **Preset facility code (Código de local predefinido)**: Insira um código de local.
3. Clique em **Set facility code (Definir código de local)**.

Configuração de serviços

A opção Configure Services (Configurar serviços) na página Setup (Configuração) é usada para acessar a configuração de dispositivos externos que podem ser usados com o controlador de porta.

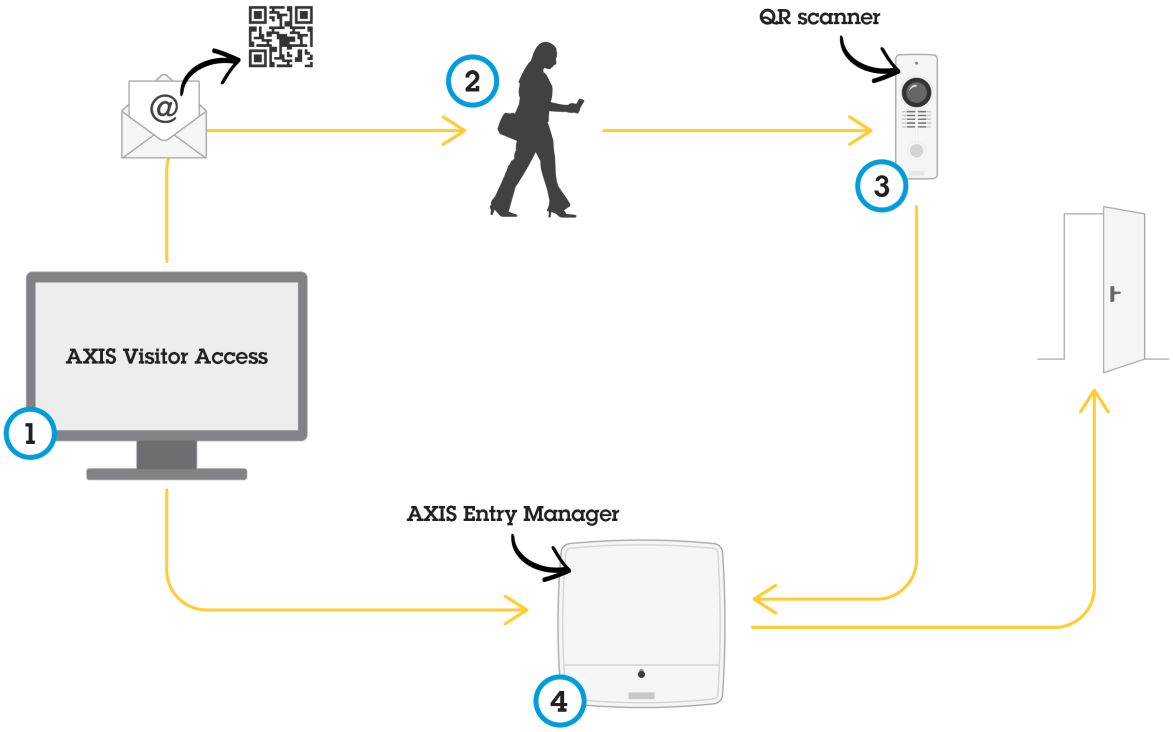
AXIS Visitor Access

Com o AXIS Visitor Access, credenciais temporárias podem ser criadas na forma de um QR Code. Uma câmera de rede ou um porteiro eletrônico conectado ao sistema de controle de acesso faz a leitura do QR Code.

O serviço consiste em:

- um controlador de porta Axis com AXIS Entry Manager e firmware versão 1.65.2 ou superior
- uma câmera de rede ou um porteiro eletrônico Axis com o aplicativo leitor de QR Code instalado
- um PC Windows® com o aplicativo AXIS Visitor Access instalado

Configuração do sistema



Uso do serviço AXIS Visitor Access

O usuário cria um convite no AXIS Visitor Access (1) e envia o convite para o endereço de email do visitante. Ao mesmo tempo, as credenciais de desbloqueio da porta são criadas e armazenadas no controlador de porta Axis conectado (4). O visitante mostra o QR Code incluído no convite na câmera de rede ou no porteiro eletrônico (3), o qual pede ao controlador de porta (4) para desbloquear a porta para o visitante.

QR Code é marca registrada da Denso Wave, inc.

Pré-requisitos do AXIS Visitor Access

Antes de usar o serviço AXIS Visitor Access service, você precisará:

- configurar o hardware do controlador de porta,
- de uma câmera de rede ou de um porteiro eletrônico Axis conectado à mesma rede que o controlador de porta, colocada em local acessível ao visitante e próximo à porta,
- do pacote de instalação do AXIS Visitor Access. Ele está disponível em *axis.com*,
- duas contas de usuário adicionais no controlador de porta, somente para uso pelo serviço AXIS Visitor Access. Uma delas é necessária para o aplicativo AXIS Visitor Access e outra para o aplicativo leitor de QR Code. Para saber como criar contas de usuário, consulte *Usuários na página 55*.

Importante

- Você só pode conectar o serviço AXIS Visitor Access a um único controlador de porta no sistema inteiro.
- Com o serviço AXIS Visitor Access, só é possível endereçar portas controladas pelo controlador de porta conectado. Não é possível endereçar outras portas no sistema.
- Use o aplicativo AXIS Visitor Access para modificar e excluir visitantes. Não use o AXIS Entry Manager.
- Se você alterar a senha da conta de usuário usada para o AXIS Visitor Access, você também precisará atualizá-la no AXIS Visitor Access.
- Se você alterar a senha da conta de usuário usada para o aplicativo leitor de QR Code, será necessário configurar o leitor de QR Code novamente.

Configuração do AXIS Visitor Access

Você deve instalar o aplicativo de leitor de QR na câmera de rede ou no porteiro eletrônico Axis ao configurar o serviço AXIS Visitor Access. Não é necessário fazer uma instalação separada.

1. Na página Web do controlador de porta, vá para **Setup > Configure Services > Settings (Configuração > Configurar serviços > Configurações**.
2. Clique em **Start new setup (Iniciar nova configuração)**.
3. Siga as instruções para finalizar a configuração.

Importante

Se desejar impor o uso de HTTPS, certifique-se de que o controlador de porta comunique-se via HTTPS. Caso contrário, o aplicativo não poderá se comunicar com o controlador de porta.

4. No computador que será usado para criar credenciais temporárias, instale e configure o aplicativo AXIS Visitor Access.

SmartIntego

SmartIntego é uma solução sem fio que aumenta o número de portas com as quais um controlador de porta pode lidar.

Pré-requisitos do SmartIntego

Os seguintes pré-requisitos devem ser atendidos antes de prosseguir com a configuração do SmartIntego:

- Um arquivo csv precisa ser criado. O arquivo csv contém informações sobre o GatewayNode e as portas usados em sua solução SmartIntego. O arquivo é criado em um software independente fornecido pelo parceiro SimonsVoss.
- A configuração de hardware do SmartIntego foi concluída, consulte *Como criar uma nova configuração de hardware para travas sem fio na página 19*.

Observação

- A ferramenta Configuração do SmartIntego deve conter a versão 2.1.6452.23485, compilação 2.1.6452.23485 (8/31/2017 1:02:50 PM) ou posterior.
- O Advanced Encryption Standard (AES) não é compatível com o SmartIntego e deve, assim, ser desativado na ferramenta Configuração do SmartIntego.

Como configurar o SmartIntego

Observação

- Certifique-se de que os pré-requisitos listados foram atendidos.
- Para obter maior visibilidade do status da bateria, vá para **Setup (Configurar)** > **Configure event and alarms logs (Configurar logs de eventos e alarmes)**, e adicione **Door — Battery alarm (Porta — Alarme da bateria)** ou **IdPoint — Battery alarm (IdPoint — Alarme da bateria)** como um alarme.
- As configurações do monitor de portas estão disponíveis no arquivo CSV importado. Não é necessário alterar essa configuração em uma instalação normal.

1. Clique em **Browse... (Procurar...)**, selecione o arquivo CSV e clique em **Upload file (Carregar arquivo)**.
2. Selecione um GatewayNode e clique em **Next (Avançar)**.
3. Uma visualização da nova configuração é mostrada. Desative os monitores de portas, se necessário.
4. Clique em **Configure (Configurar)**.
5. Uma visão geral das portas incluídos na configuração é mostrada. Clique em **Settings (Configurações)** para configurar cada porta individualmente.

Como reconfigurar o SmartIntego

1. Clique em **Setup (Configuração)** no menu superior.
2. Clique em **Configure Services (Configurar serviços)** > **Settings (Configurações)**.
3. Clique em **Re-configure (Reconfigurar)**.
4. Clique em **Browse... (Procurar...)**, selecione o arquivo CSV e clique em **Upload file (Carregar arquivo)**.
5. Selecione um GatewayNode e clique em **Next (Avançar)**.
6. Uma visualização da nova configuração é mostrada. Desative os monitores de portas, se necessário.

Observação

As configurações do monitor de portas estão disponíveis no arquivo CSV importado. Não é necessário alterar essa configuração em uma instalação normal.

7. Clique em **Configure (Configurar)**.
8. Uma visão geral das portas incluídos na configuração é mostrada. Clique em **Settings (Configurações)** para configurar cada porta individualmente.

Gerenciar controladores de porta de rede

A página de gerenciamento de controladores de porta de rede no sistema mostra informações sobre o controlador de porta, seu status no sistema e outros controladores de porta que fazem parte do sistema. Ele também permite que o administrador altere a configuração do sistema, adicionando e removendo controladores de porta.

Importante

Todos os controladores de porta em um sistema devem ser conectados à mesma rede e ser configurados para uso em um único site.

Para gerenciar controladores de porta, vá para **Setup > Manage Network Door Controllers in System (Configuração > Gerenciar controladores de porta de rede no sistema)**.

A página de gerenciamento de controladores de porta de rede no sistema inclui os seguintes painéis:

- **System status of this controller (Status do sistema deste controlador)** – Mostra o status do sistema do controlador de porta e permite alternar entre os modos de sistema e autônomo. Para obter mais informações, consulte *Status do sistema do controlador de porta na página 28*.
- **Network door controllers in system (Controladores de porta de rede no sistema)** – Mostra informações sobre os controladores de porta no sistema e inclui controles para adicionar e remover um controlador do sistema. Para obter mais informações, consulte *Controladores de porta conectados no sistema na página 28*.

Status do sistema do controlador de porta

O status do sistema determinará se o controlador de porta poderá fazer parte de um sistema de controladores de porta. O status do sistema do controlador de porta é exibido no painel **System status for this controller (Status do sistema para este controlador)**.

Se o controlador de porta não estiver no modo autônomo e você desejar impedir que ele seja adicionado a um sistema, clique em **Activate standalone mode (Ativar modo autônomo)** para entrar no modo autônomo.

Se o controlador de porta estiver no modo autônomo, mas você pretender adicioná-lo a um sistema, clique em **Deactivate standalone mode (Desativar modo autônomo)**.

Modos do sistema

- **This controller is not part of a system and not in standalone mode (Este controlador não é parte de um sistema e não está no modo autônomo)** – O controlador de porta não foi configurado como parte de um sistema e não está no modo autônomo. Isso significa que o controlador de porta está aberto e pode ser adicionado a um sistema por qualquer outro controlador de porta dentro da mesma rede. Para impedir que o controlador de porta seja adicionado a um sistema, ative o modo autônomo.
- **This controller is set to standalone mode (Este controlador está configurado no modo autônomo)** – O controlador de porta não é parte de um sistema. Ele não pode ser adicionado a um sistema por outros controladores de porta de rede nem adicionar outros controladores de porta ele mesmo. O modo autônomo é geralmente usado em instalações pequenas com apenas um controlador de porta e uma ou duas portas. Para permitir que o controlador de porta seja adicionado em um sistema, desative o modo autônomo.
- **This controller is part of a system (Este controlador é parte de um sistema)** – O controlador de porta é parte de um sistema distribuído. No sistema distribuído, os usuários, grupos, portas e agendamentos são compartilhados entre os controladores conectados.

Controladores de porta conectados no sistema

O painel **Network door controllers in system (Controladores de porta de rede no sistema)** fornece controles para as seguintes alterações do sistema:

- Adicione um controlador de porta a um sistema, consulte *Adicionar controladores de porta ao sistema na página 29*.
- Remova um controlador de porta de um sistema, consulte *Remover controladores de porta do sistema na página 30*.

Lista de controladores de porta conectados

O painel **Network door controllers in system (Controladores de porta de rede no sistema)** também inclui uma lista que mostra as seguintes informações de ID e status sobre os controladores de porta conectados no sistema:

- **Name (Nome)** – O nome do controlador de porta definido pelo usuário. Se o administrador não definiu um nome durante a configuração do hardware, o nome padrão será mostrado.
- **IP address (Endereço IP)**
- **MAC address (Endereço MAC)**
- **Status (Status)** – O controlador de porta do qual você acessa o sistema mostrará o status **This controller (Este controlador)**. Os outros controladores de porta no sistema mostrarão o status **Online (Online)**.
- **Firmware version (Versão do firmware)**

Para abrir as páginas Web de outro controlador de porta, clique no endereço IP do controlador.

Para atualizar a lista, clique em **Refresh list of controllers (Atualizar lista de controladores)**.

Observação

Todos os controladores em um sistema devem sempre ter a mesma versão do firmware. Use o Axis Device Manager para fazer uma atualização de firmware em paralelo em todos os controladores no sistema inteiro.

Adicionar controladores de porta ao sistema

Importante

Ao parear controladores de porta, todas as configurações de gerenciamento de acesso no controlador de porta adicionado serão excluídas e substituídas por configurações de gerenciamento de acesso do sistema.

Para adicionar um controlador de porta ao sistema na lista de controladores de porta:

1. Vá para **Setup > Manage Network Door Controllers in System (Configuração > Gerenciar controladores de porta de rede no sistema)**.
2. Clique em **Add controllers to system from list (Adicionar controladores ao sistema da lista)**.
3. Selecione o controlador de porta que deseja adicionar.
4. Clique em **Add (Adicionar)**.
5. Para adicionar mais controladores de porta, repita as etapas acima.

Para adicionar um controlador de porta ao sistema por seu endereço IP ou MAC conhecido:

1. Vá para **Manage Devices (Gerenciar dispositivos)**.
2. Clique em **Add controller to system by IP or MAC address (Adicionar controlador ao sistema por endereço IP ou MAC.**
3. Insira o endereço IP ou MAC.
4. Clique em **Add (Adicionar)**.
5. Para adicionar mais controladores de porta, repita as etapas acima.

Quando o pareamento estiver concluído, todos os usuários, portas, agendamentos e grupos serão compartilhados por todos os controladores de porta no sistema.

Para atualizar a lista, clique em **Refresh list of controllers (Atualizar lista de controladores)**.

Remover controladores de porta do sistema

Importante

- Antes de remover um controlador de porta do sistema, redefina sua configuração de hardware. Se você ignorar esta etapa, todas as portas relacionadas ao controlador de porta permanecerão no sistema e não poderão ser excluídas.
- Ao remover um controlador de porta de um sistema de dois controladores, ambos os controladores de porta alternarão automaticamente para o modo autônomo.

Para remover um controlador de porta do sistema:

1. Acesse o sistema através do controlador de porta que deseja remover e vá para **Setup > Hardware Configuration (Configuração > Configuração de hardware)**.
2. Clique em **Reset hardware configuration (Redefinir configuração de hardware)**.
3. Após a configuração de hardware ser redefinida, vá para **Setup > Manage Network Door Controllers in System (Configuração > Gerenciar controladores de porta de rede no sistema)**.
4. Na lista **Network door controllers in system (Controladores de porta de rede no sistema)**, identifique o controlador de porta que você deseja remover e clique em **Remove from system (Remover do sistema)**.
5. Uma caixa de diálogo abrirá lembrando de redefinir a configuração de hardware do controlador de porta. Clique em **Remove controller (Remover controlador)** para confirmar.
6. Uma caixa de diálogo será aberta solicitando que você confirme se deseja remover o controlador de porta. Clique em **OK** para confirmar. O controlador de porta removido está agora no modo autônomo.

Observação

- Quando um controlador de porta for removido do sistema, todas as suas configurações de gerenciamento de acesso serão removidas.
- Somente controladores de porta online podem ser removidos.

Modo de configuração

O modo de configuração é o modo padrão quando você acessa o dispositivo pela primeira vez. Quando o modo de configuração está desativado, a maioria dos recursos de configuração do dispositivo permanece oculta.

Importante

Desativar o modo de configuração não deve ser considerado um recurso de segurança. Seu objetivo é prevenir erros de configuração, e não impedir que usuários mal-intencionados alterem configurações vitais.

Como desativar o modo de configuração

1. Vá para **Setup (Configuração)** > **Disable Configuration Mode (Desativar modo de configuração)**.
2. Insira um PIN e selecione **OK**.

Observação

O PIN não é obrigatório.

Como ativar o modo de configuração

1. Vá para **Setup (Configuração)** > **Enable Configuration Mode (Ativar modo de configuração)**.
2. Insira o PIN e selecione **OK**.

Observação

Caso não lembre do PIN, você poderá ativar o modo de configuração inserindo `http://[endereço IP]/webapp/pacs/index.shtml#resetConfigurationMode`.

Instruções de manutenção

Para manter o sistema de controle de acesso funcionando sem problemas, a Axis recomenda efetuar manutenção regular do sistema de controle de acesso, incluindo controladores de porta e dispositivos conectados.

Efetue manutenção pelo menos uma vez por ano. O procedimento de manutenção sugerido inclui, mas não está limitado a, as seguintes etapas:

- Certifique-se de que todas as conexões entre o controlador de porta e os dispositivos externos estejam seguras.
- Verifique todas as conexões de hardware. Consulte *Portas de controles de verificação na página 21*.
- Verifique se o sistema, incluindo os dispositivos externos conectados, está funcionando corretamente.
  - Passe um cartão e teste os leitores, as portas e as travas.
  - Se o sistema incluir dispositivos REX, sensores ou outros dispositivos, também teste-os.
  - Se ativados, teste os alarmes de violação.

Se os resultados de qualquer uma das etapas acima indicarem falhas ou comportamento inesperado:

- Teste os sinais dos fios usando equipamentos apropriados e verifique se os fios ou cabos estão danificados de alguma forma.
- Substitua todos os cabos e fios danificados ou com falha.
- Após a substituição de cabos e fios, verifique todas as conexões de hardware novamente. Consulte *Portas de controles de verificação na página 21*.

- Certifique-se de que todos os agendamentos de acesso, portas, grupos e usuários estejam atualizados.
- Se o controlador de porta não estiver se comportando como o esperado, consulte *Solução de problemas na página 67* e *Manutenção na página 63* para obter mais informações.

Gerenciamento de acesso

Sobre os usuários

No AXIS Entry Manager, os usuários são as pessoas que foram registradas como proprietários de um ou mais tokens (tipos de identificação). Cada pessoa deverá ter um perfil de usuário exclusivo para ter acesso a portas no sistema de controle de acesso. O perfil de usuário é composto por credenciais que dizem ao sistema quem é o usuário e quando e como ele obtém acesso a portas. Para obter mais informações, consulte *Criação e edição de usuários na página 41*.

Os usuários neste contexto não devem ser confundidos com administradores. Administrators (Administradores) têm acesso irrestrito a todas as configurações. E, no contexto de gerenciamento do sistema de controle de acesso, as páginas Web do produto (AXIS Entry Manager), os administradores algumas vezes também são chamados de usuários. Para obter mais informações, consulte *Usuários na página 55*.

A página Access Management (Gerenciamento de acesso)

A página Access Management (Gerenciamento de acesso) permite a você configurar e gerenciar usuários, grupos, portas e agendamentos do sistema. Para abrir a página Access Management (Gerenciamento de acesso), clique em **Access Management (Gerenciamento de acesso)**.

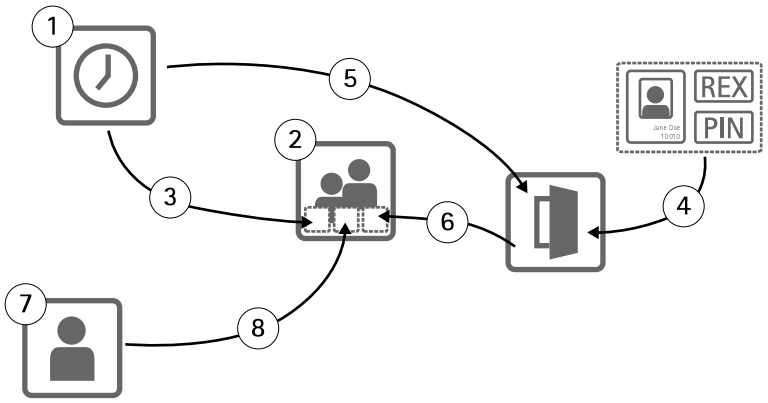
Para adicionar usuários a grupos e aplicar agendamentos de acesso e portas, arraste os itens para seus respectivos destinos nas listas **Groups (Grupos)** e **Doors (Portas)**.

Observação

As mensagens que necessitam de ação são mostradas em texto vermelho.

Escolha de um fluxo de trabalho

A estrutura de gerenciamento de acesso é flexível, permitindo a você desenvolver um fluxo de trabalho que atenda às suas necessidades. Este é um exemplo de fluxo de trabalho:



1. Crie agendamentos de acesso. Consulte *página 33*.
2. Crie grupos. Consulte *página 35*.
3. Aplique agendamentos de acesso a grupos.
4. Adicione tipos de identificação a portas ou andares. Consulte *página 36* e *página 37*.
5. Aplique agendamentos de acesso a cada tipo de identificação.
6. Aplique portas ou andares a grupos.

7. Crie usuários. Consulte *página 41*.
8. Adicione usuários a grupos.

Para obter exemplos aplicados desse fluxo de trabalho, consulte *Combinações de agendamentos de acesso de exemplo na página 43*.

Criar e editar agendamentos de acesso

Agendamentos de acesso são usados para definir regras gerais sobre quando portas podem ou não ser acessadas. Elas também são usadas para definir regras sobre quando grupos podem ou não acessar as portas no sistema. Para obter mais informações, consulte *Tipos de agendamento de acesso na página 33*.

Para criar um novo agendamento de acesso:

1. Vá para **Access Management (Gerenciamento de acesso)**.
2. Na guia **Access Schedules (Agendamentos de acesso)**, clique em **Add new schedule (Adicionar novo agendamento)**.
3. Na caixa de diálogo **Add access schedule (Adicionar agendamento de acesso)**, insira o nome do agendamento.
4. Para criar um agendamento de acesso regular, selecione **Addition Schedule (Agendamento de adição)**.

   Ou para criar um agendamento de subtração, selecione **Subtraction Schedule (Agendamento de subtração)**.

   Para obter mais informações, consulte *Tipos de agendamento de acesso na página 33*.
5. Clique em **Save (Salvar)**.

Para expandir um item na lista **Access Schedules (Agendamentos de acesso)**, clique em . Os agendamentos de adição são mostrados em texto verde e os agendamentos de subtração são mostrados em texto vermelho escuro.

Para exibir o calendário de um agendamento acesso, clique em .

Para editar o nome de um agendamento acesso ou um item de agendamento, clique em e faça as alterações. Em seguida, clique em **Save (Salvar)**.

Para excluir um agendamento de acesso, clique em .

Observação

O controlador de porta possui alguns agendamentos de acesso comumente usados predefinidos que podem ser usados como exemplos ou modificados conforme necessário. No entanto, o agendamento de acesso predefinido **Sempre** não pode ser modificado ou excluído.

Tipos de agendamento de acesso

Há dois tipos de agendamentos de acesso:

- **Addition schedule (Agendamento de adição)** – Agendamentos de acesso regulares que definem quando portas podem ser acessadas. Agendamentos de adição típicos são horário de funcionamento, horário comercial, depois do expediente ou horário noturno.
- **Subtraction schedule (Agendamento de subtração)** – Exceções a agendamentos de acesso regulares. Em geral, elas são usadas para restringir o acesso durante um período específico que ocorre dentro do período de tempo de um agendamento regular (agendamento de adição). Por exemplo, agendamentos de subtração podem ser usados para negar acesso ao edifício durante feriados públicos em dias da semana.

Ambos os tipos de agendamentos de acesso podem ser usados em dois níveis:

- **Identification type schedules (Agendamentos de tipo de identificação)** – Determine quando e como leitores concedem acesso a uma porta aos usuários. Cada tipo de identificação deve ser conectado a um agendamento de acesso que informa ao sistema quando conceder acesso a usuários com esse tipo de identificação específica. Vários agendamentos de

adição e agendamentos de subtração podem ser adicionados a cada tipo de identificação. Para obter informações sobre tipos de identificação, consulte *página 37*.

- **Group schedules (Agendamentos de grupo)** – Determine quando, mas não como, membros de um grupo receberão acesso a uma porta. Cada grupo deve estar conectado a um ou mais agendamentos de acesso que informam ao sistema quando conceder acesso a seus membros. Vários agendamentos de adição e agendamentos de subtração podem ser adicionados a cada grupo. Para obter informações sobre grupos, consulte *página 35*.

Agendamentos de grupo podem restringir direitos de acesso de entrada, mas não estender direitos de acesso de entrada ou saída além do que agendamentos de tipo de identificação permitem. Em outras palavras, se o tipo de identificação de um agendamento restringir o acesso de entrada ou saída em horários específicos, um agendamento de grupo não poderá substituir esse agendamento de tipo de identificação. No entanto, se um agendamento de grupo for mais restritivo sobre acesso do que o agendamento de tipo de identificação, o agendamento de grupo substituirá o agendamento de tipo de identificação.

Agendamentos de tipo de identificação e grupo podem ser combinados de várias formas para atingir diferentes resultados. Para obter combinações de agendamento de acesso de exemplo, consulte *página 43*.

Adicionar itens de agendamento

Agendamentos de adição e subtração podem ser eventos únicos (isolados) ou eventos recorrentes.

Para adicionar um item de agendamento a um agendamento de acesso:

1. Expanda o agendamento de acesso na lista **Access Schedules (Agendamentos de acesso)**.
2. Clique em **Add schedule item (Adicionar item de agendamento)**.
3. Insira o nome do item agendado.
4. Selecione **One time (Uma vez)** ou **Recurrence (Recorrência)**.
5. Defina a duração nos campos de tempo. Consulte *Opções de tempo na página 34*.
6. Para eventos de agendamento recorrente, selecione os parâmetros **Recurrence pattern (Padrão de recorrência)** e **Range of recurrence (Intervalo de recorrência)**. Consulte *Opções de padrão de recorrência na página 34* e *Opções de intervalo de recorrência na página 35*.
7. Clique em **Save (Salvar)**.

Opções de tempo

As seguintes opções de tempo estão disponíveis:

- **All day (Dia inteiro)** – Selecione esta opção para eventos que durem as 24 horas do dia. Em seguida, insira o **Start (Início)** desejado.
- **Start (Início)** – Clique no campo de tempo e selecione a hora desejada. Se necessário, clique no campo de data e selecione o mês, o dia e o ano desejados. Você também pode digitar a data diretamente no campo.
- **End (Término)** – Clique no campo de tempo e selecione a hora desejada. Se necessário, clique no campo de data e selecione o mês, o dia e o ano desejados. Você também pode digitar a data diretamente no campo.

Opções de padrão de recorrência

As seguintes opções de padrão de recorrência estão disponíveis:

- **Yearly (Anual)** – Selecione para repetir a cada ano.
- **Weekly (Semanal)** – Selecione para repetir a cada semana.
- Recorrência todas as semanas às **Segundas-feiras**, **Terças-feiras**, **Quartas-feiras**, **Quintas-feiras**, **Sextas-feiras**, **Sábados** e **Domingos** – Selecione os dias para repetição.

Opções de intervalo de recorrência

O seguinte intervalo de opções de recorrência está disponível:

- **Primeira ocorrência** – Clique no campo de data e selecione o mês, o dia e o ano desejados. Você também pode digitar a data diretamente no campo.
- **No end date (Sem data de término)** – Selecione para repetir a ocorrência indefinidamente.
- **End by (Terminar em)** – Clique no campo de data e selecione o mês, o dia e o ano desejados. Você também pode digitar a data diretamente no campo.

Criar e editar grupos

Grupos permitem que você gerencie usuários e seus direitos de acesso de forma coletiva e eficiente. Um grupo consiste em credenciais que informam ao sistema os usuários do grupo e quando e como membros do grupo têm acesso às portas.

Cada usuário deve pertencer a um ou mais grupos. Para adicionar um usuário a um grupo, arraste e solte o usuário no grupo desejado na lista **Groups (Grupos)**. Para obter mais informações, consulte *Criação e edição de usuários na página 41*.

Para criar um novo grupo:

1. Vá para **Access Management (Gerenciamento de acesso)**.
2. Na guia **Groups (Grupos)**, clique em **Add new group (Adicionar novo grupo)**.
3. Na caixa de diálogo **Add Group (Adicionar grupo)**, insira as credenciais do grupo. Consulte *Credenciais de grupo na página 35*.
4. Clique em **Save (Salvar)**.

Para expandir um item na lista **Groups (Grupos)** e exibir seus membros, direitos de acesso a portas e agendamentos, clique em  .

Para editar um nome de grupo ou a data de validade, clique em  e faça as alterações. Em seguida, clique em **Save (Salvar)**.

Para verificar quando e como um grupo pode acessar determinadas portas, clique em  .

Para excluir um grupo ou membros do grupo, portas ou agendamentos de um grupo, clique em  .

Credenciais de grupo

As seguintes credenciais estão disponíveis para grupos:

- **Name (Nome)** (obrigatório)
- **Valid from (Válido de)** e **Valid to (Válido até)** – Insira as datas entre as quais as credenciais do grupo serão válidas. Clique no campo de data e selecione o mês, o dia e o ano desejados. Você também pode digitar a data diretamente no campo.
- **Whitelist (Lista branca)** – Usuários de um grupo na lista branca sempre podem acessar as portas no grupo, até mesmo em caso de falha de energia ou de rede. Como os usuários do grupo sempre têm acesso às portas, os agendamentos e intervalos de agendamento não se aplicam. Não há suporte ao tempo de acesso longo para um usuário que abre uma porta em um grupo na lista branca. Somente portas com travas sem fio que oferecem suporte à funcionalidade de lista branca podem ser adicionadas ao grupo.

Observação

- Para poder salvar o grupo, você deve inserir o **Name (Nome)** do grupo.
- Valido de e válido até para um usuário não se aplicam quando o usuário é adicionado ao grupo de lista branca.
- Sincronizar credenciais na lista branca a uma trava sem fio algumas vezes é um pouco demorado e interfere com os procedimentos de abertura normal da porta. Evite adicionar ou remover grandes números de credenciais em um sistema em horários de pico. Quando a sincronização das credenciais atualizadas com a trava é concluída, o log de eventos mostra `SyncOngoing: false` para a trava.

Gerenciar portas

As regras gerais para cada porta são gerenciadas na guia **Doors (Portas)**. As regras incluem adicionar tipos de identificação que determinam como os usuários terão acesso à porta e agendamentos de acesso que determinam quando cada tipo de identificação é válido. Para obter mais informações, consulte *Tipos de identificação na página 37* e *Criar e editar agendamentos de acesso na página 33*.

Antes que você possa gerenciar uma porta, adicione-a ao sistema de controle de acesso concluindo a configuração de hardware, consulte *Configurar o hardware na página 14*.

Para gerenciar uma porta:

1. Vá para **Access Management (Gerenciamento de acesso)** e selecione a guia **Doors (Portas)**.
2. Na lista **Doors (Portas)**, clique em ▶ perto da porta que deseja editar.
3. Arraste a porta para pelo menos um grupo. Se a lista **Groups (Grupos)** estiver vazia, crie um novo grupo. Consulte *Criar e editar grupos na página 35*.
4. Clique em **Add identification type (Adicionar tipo de identificação)** e selecione quais credenciais os usuários precisam apresentar ao leitor para receber acesso à porta. Consulte *Tipos de identificação na página 37*.

   Adicione pelo menos um tipo de identificação à cada porta.
5. Para adicionar vários tipos de identificação, repita a etapa anterior.

   Se ambos os tipos de identificação **Card number only (Somente número do cartão)** e **PIN only (Somente PIN)** forem adicionados, os usuários poderão escolher passar o cartão ou inserir seu PIN para acessar a porta. No entanto, se, em vez disso, somente o tipo de identificação **Card number and PIN (Número do cartão e PIN)** for adicionado, os usuários deverão passar seus cartões e inserir seus PINs para acessar a porta.
6. Para definir quando as credenciais são válidas, arraste um agendamento para cada tipo de identificação.

Para destravar portas, travar portas ou conceder acesso temporário manualmente, clique em uma das ações manuais de porta conforme necessário. Consulte *Uso de ações manuais de portas na página 38*.

Observação

Controles para destravar portas, travar portas ou conceder acesso temporário manualmente não estão disponíveis para portas/dispositivos sem fio.

Para expandir um item na lista **Doors (Portas)**, clique em ▶.

Para editar uma porta ou nome de leitor, clique em ✎ e faça as alterações. Em seguida, clique em **Save (Salvar)**.

Para verificar o leitor, tipo de identificação e combinações de agendamento de acesso, clique  .

Para verificar a função das travas conectadas às portas, clique nos controles de verificação. Consulte *Portas de controles de verificação na página 21*.

Para excluir tipos de identificação ou agendamentos de acesso, clique em ⊖.

Tipos de identificação

Tipos de identificação são dispositivos de armazenamento de credenciais portáteis, peças de informação memorizadas ou várias combinações de ambos que determinam como os usuários receberão acesso à porta. Tipos de identificação comuns incluem tokens, como cartões ou chaveiros, números de identificação pessoal (PINs) e dispositivos de solicitação de saída (REX).

Para obter mais informações sobre credenciais, consulte *Credenciais de usuário na página 42*.

Os seguintes tipos de identificação estão disponíveis:

- **Facility code only (Somente código de local)** – O usuário pode acessar a porta usando um cartão ou outro token com o código de local aceito pelo leitor.
- **Card number only (Somente número do cartão)** – O usuário pode acessar a porta usando somente um cartão ou outro token aceito pelo leitor. O número do cartão é um número exclusivo que, normalmente, é impresso no cartão. Consulte as informações do fabricante do cartão sobre onde localizar seu número. O número do cartão também pode ser recuperado pelo sistema. Passe o cartão em um leitor conectado, selecione o leitor na lista e clique em **Retrieve (Recuperar)**.
- **Card raw only (Somente raw do cartão)** – O usuário pode acessar a porta usando somente um cartão ou outro token aceito pelo leitor. As informações são armazenadas como dados raw no cartão. Os dados raw do cartão podem ser recuperados pelo sistema. Passe o cartão em um leitor conectado, selecione o leitor na lista e clique em **Retrieve (Recuperar)**. Use este tipo de identificação somente se um número de cartão não puder ser localizado.
- **PIN only (Somente PIN)** – O usuário pode acessar a porta usando apenas um número de identificação pessoal (PIN) de quatro dígitos.
- **Facility code and PIN (Código de local e PIN)** – O usuário precisa do cartão ou outro token com o código de local aceito pelo leitor e um PIN para acessar a porta. O usuário deve apresentar as credenciais na ordem especificada (cartão seguido pelo PIN).
- **Card number and PIN (Número do cartão e PIN)** – O usuário precisa do cartão ou outro token aceito pelo leitor e um PIN para acessar a porta. O usuário deve apresentar as credenciais na ordem especificada (cartão seguido pelo PIN).
- **Card raw and PIN (Raw do cartão e PIN)** – O usuário precisa do cartão ou outro token aceito pelo leitor e um PIN para obter acesso à porta. Use este tipo de identificação somente se um número de cartão não puder ser localizado. O usuário deve apresentar as credenciais na ordem especificada (cartão seguido pelo PIN).
- **REX** – O usuário pode acessar a porta ao ativar uma solicitação para sair (REX) do dispositivo, como um botão, sensor ou barra de empurrar.
- **License plate only (Somente placa de licença)** – O usuário pode acessar a porta usando apenas um número de placa de licença para um veículo.

Adicionar estados de destravamento agendados

Para manter automaticamente uma porta destravada por um período específico de tempo, você pode adicionar um estado **Scheduled unlock (Agendar destravamento)** a uma porta e aplicar um agendamento de acesso a ele.

Por exemplo, para manter uma porta destravada durante o horário comercial:

1. Vá para **Access Management (Gerenciamento de acesso)** e selecione a guia **Doors (Portas)**.
2. Clique em ▶ perto do item de lista **Doors (Portas)** que você deseja editar.
3. Clique em **Add scheduled unlock (Adicionar destravamento agendado)**.
4. Selecione **Unlock state (Estado de destravamento)** (**unlocked (destravada)** ou **unlock both locks (destravar ambas as travas)** dependendo se a porta possui uma ou duas travas.
5. Clique em **OK**.
6. Aplique o agendamento de acesso **Office hours (Horário comercial)** predefinido ao estado **Scheduled unlock (Destravamento agendado)**.

Para verificar quando a porta está destravada, clique em .

Para excluir um estado de destravamento agendado ou agendamento de acesso, clique em .

Uso de ações manuais de portas

Portas podem ser desbloqueadas ou bloqueadas e acesso temporário pode ser concedido na guia **Doors (Portas)** através de **Manual door actions (ações manuais de portas)**. As ações manuais de portas disponíveis para uma porta específica dependem de como a porta foi configurada.

Para usar as ações manuais de portas:

1. Vá para **Access Management (Gerenciamento de acesso)** e selecione a guia **Doors (Portas)**.
2. Na lista **Doors (Portas)**, clique em perto da porta que deseja controlar.
3. Clique na ação de porta necessária. Consulte *Ações manuais de portas na página 38*.

Observação

Para usar as ações manuais de portas, você precisa abrir a página de gerenciamento de acesso por meio do controlador de porta ao qual a porta específica está conectada. Se você abrir a página de gerenciamento de acesso por meio de um controlador de porta diferente, em vez de usar as ações manuais de portas, haverá um link para a página de visão geral do controlador de porta ao qual a porta específica está conectada. Clique no link, vá para **Access Management (Gerenciamento de acesso)** e selecione a guia **Doors (Portas)**.

Ações manuais de portas

As seguintes ações manuais de portas estão disponíveis:

- **Get door status (Obter status da porta)** – Verifique o estado atual do monitor de portas, alarmes de porta e travas.
- **Access (Acesso)** – Conceda acesso de usuários à porta. O horário de acesso determinado se aplica. Consulte *Como configurar monitores de portas e travas na página 15*.
- **Unlock (Destravar)** (uma trava) ou **Unlock both locks (Destravar ambas)** (duas travas) – Destrave a porta. A porta permanece destravada até você pressionar **Lock (Travar)** ou **Lock both locks (Travar ambas)**, um estado de porta agendado ser ativado ou o controlador de porta ser reiniciado.
- **Lock (Travar)** (uma trava) ou **Lock both locks (Travar ambas)** (duas travas) – Trave a porta.
- **Unlock second lock and lock primary (Destravar trava secundária e travar principal)** – Essa opção está disponível somente se a porta foi configurada com uma trava secundária. Destravar a porta. A trava secundária permanece destravada até você pressionar **Double lock (Trava dupla)** ou um estado de porta agendado ser ativado.

Gerenciamento de andares

Se você instalou um AXIS 9188 Network I/O Relay Module em seu sistema, os andares podem ser gerenciados de forma semelhante ao gerenciamento de portas.

Observação

Se você usa um A1001 no modo de cluster com eventos globais ativados, certifique-se de usar nomes descritivos exclusivos para cada andar. Por exemplo, *Elevador A, Andar 1"*.

Observação

No máximo 2 AXIS 9188 Network I/O Relay Modules podem ser configurados com cada A1001 Network Door Controller.

As regras gerais para cada andar são gerenciadas na guia **Floors (Andares)**. As regras incluem adicionar tipos de identificação que determinam como os usuários terão acesso ao andar e agendamentos de acesso que determinam quando cada tipo de identificação é

válido. Para obter mais informações, consulte *Tipos de identificação para andares na página 39* e *Criar e editar agendamentos de acesso na página 33*.

Antes que você possa gerenciar um andar, adicione-o ao sistema de controle de acesso concluindo a configuração de hardware, consulte *Configurar o hardware na página 14*.

Para gerenciar um andar:

1. Vá para **Access Management (Gerenciamento de acesso)** e selecione a guia **Floors (Andares)**.
2. Na lista **Floors (Andares)**, clique em perto do andar que deseja editar.
3. Arraste o andar para pelo menos um grupo. Se a lista **Groups (Grupos)** estiver vazia, crie um novo grupo. Consulte *Criar e editar grupos na página 35*.
4. Clique em **Add identification type (Adicionar tipo de identificação)** e selecione quais credenciais os usuários precisam apresentar ao leitor para receber acesso ao andar. Consulte *Tipos de identificação para andares na página 39*.

   Adicione pelo menos um tipo de identificação à cada andar.
5. Para adicionar vários tipos de identificação, repita a etapa anterior.

   Se ambos os tipos de identificação **Card number only (Somente número do cartão)** e **PIN only (Somente PIN)** forem adicionados, os usuários poderão escolher passar o cartão ou inserir seu PIN para acessar a porta. No entanto, se, em vez disso, somente o tipo de identificação **Card number and PIN (Número do cartão e PIN)** for adicionado, os usuários deverão passar seus cartões e inserir seus PINs para acessar a porta.
6. Para definir quando as credenciais são válidas, arraste um agendamento para cada tipo de identificação.

Para destravar andares, travar andares ou conceder acesso temporário manualmente, clique em uma das ações manuais de andar conforme necessário. Consulte *Uso de ações manuais de andar na página 40*.

Observação

Controles para destravar andares, travar andares ou conceder acesso temporário manualmente não estão disponíveis para portas/dispositivos sem fio.

Para expandir um item na lista **Floors (Andares)**, clique em .

Para editar um andar ou nome de leitor, clique em e faça as alterações. Em seguida, clique em **Save (Salvar)**.

Para verificar o leitor, tipo de identificação e combinações de agendamento de acesso, clique .

Para verificar a função das travas conectadas aos andares, clique nos controles de verificação. Consulte *Controles de verificação de andares na página 21*.

Para excluir tipos de identificação ou agendamentos de acesso, clique em .

Tipos de identificação para andares

Tipos de identificação são dispositivos de armazenamento de credenciais portáteis, pedaços de informações memorizados ou várias combinações de ambos que determinam como os usuários receberão acesso ao andar. Tipos de identificação comuns incluem tokens, como cartões ou chaveiros, números de identificação pessoal (PINs) e dispositivos de solicitação de saída (REX).

Para obter mais informações sobre credenciais, consulte *Credenciais de usuário na página 42*.

Os seguintes tipos de identificação estão disponíveis:

- **Facility code only (Somente código do local)** – O usuário pode acessar o andar usando um cartão ou outro token com o código do local aceito pelo leitor.

- **Card number only (Somente número do cartão)** – O usuário pode acessar o andar usando somente um cartão ou outro token aceito pelo leitor. O número do cartão é um número exclusivo que, normalmente, é impresso no cartão. Consulte as informações do fabricante do cartão sobre onde localizar seu número. O número do cartão também pode ser recuperado pelo sistema. Passe o cartão em um leitor conectado, selecione o leitor na lista e clique em **Retrieve (Recuperar)**.
- **Card raw only (Somente raw do cartão)** – O usuário pode acessar o andar usando somente um cartão ou outro token aceito pelo leitor. As informações são armazenadas como dados raw no cartão. Os dados raw do cartão podem ser recuperados pelo sistema. Passe o cartão em um leitor conectado, selecione o leitor na lista e clique em **Retrieve (Recuperar)**. Use este tipo de identificação somente se um número de cartão não puder ser localizado.
- **PIN only (Somente PIN)** – O usuário pode acessar o andar usando apenas um número de identificação pessoal (PIN) de quatro dígitos.
- **Facility code and PIN (Código do local e PIN)** – O usuário precisa do cartão ou outro token com o código do local aceito pelo leitor e um PIN para obter acesso ao andar. O usuário deve apresentar as credenciais na ordem especificada (cartão seguido pelo PIN).
- **Card number and PIN (Número do cartão e PIN)** – O usuário precisa do cartão ou outro token aceito pelo leitor e um PIN para obter acesso ao andar. O usuário deve apresentar as credenciais na ordem especificada (cartão seguido pelo PIN).
- **Card raw and PIN (Raw do cartão e PIN)** – O usuário precisa do cartão ou outro token aceito pelo leitor e um PIN para obter acesso ao andar. Use este tipo de identificação somente se um número de cartão não puder ser localizado. O usuário deve apresentar as credenciais na ordem especificada (cartão seguido pelo PIN).
- **REX** – o usuário pode acessar o andar ativando um dispositivo de solicitação para sair (REX), como um botão, sensor ou barra de empurrar.

Adicionar estados de destravamento agendados

Para manter automaticamente um andar acessível para qualquer pessoa por um período específico, você pode adicionar um estado **Scheduled unlock (Destravamento agendado)** a um andar e aplicar um agendamento de acesso a ele.

Por exemplo, para manter um andar acessível para qualquer pessoa durante o horário comercial:

1. Vá para **Access Management (Gerenciamento de acesso)** e selecione a guia **Floors (Andares)**.
2. Clique em  próximo ao item da lista **Floors (Andares)** que você deseja editar.
3. Clique em **Add scheduled unlock (Adicionar destravamento agendado)**.
4. Selecione o **Unlock state (Estado de destravamento)** (**unlocked** (destravado) ou **unlock both locks (destravar ambas as travas)** dependendo se o andar possui uma ou duas travas.
5. Clique em **OK**.
6. Aplique o agendamento de acesso **Office hours (Horário comercial)** predefinido ao estado **Scheduled unlock (Destravamento agendado)**.

Para verificar quando o andar está acessível, clique em  .

Para excluir um estado de destravamento agendado ou agendamento de acesso, clique em  .

Uso de ações manuais de andar

Os andares podem ter diferentes acessibilidades, restritos ou acessíveis para todas as pessoas. Acesso temporário pode ser concedido na guia **Floors (Andares)** via **Manual floor actions (Ações manuais de andar)**. As ações manuais de andar disponíveis para um andar específico dependem de como o andar foi configurado.

Para usar as ações manuais de andar:

1. Vá para **Access Management (Gerenciamento de acesso)** e selecione a guia **Floors (Andares)**.

2. Na lista **Floors (Andares)**, clique em perto do andar que deseja controlar.
3. Clique na ação de andar necessária. Consulte *Ações manuais de andar na página 41*.

Observação

Para usar as ações manuais de porta andar, você precisa abrir a página de gerenciamento de acesso por meio do controlador de andar ao qual o andar específico está conectado. Se você abrir a página de gerenciamento de acesso por meio de um controlador de andar diferente, em vez de usar as ações manuais de andar, haverá um link para a página de visão geral do controlador de andar ao qual o andar específico está conectado. Clique no link, vá para **Access Management (Gerenciamento de acesso)** e selecione a guia **Floors (Andares)**.

Ações manuais de andar

As seguintes ações manuais de andar estão disponíveis:

- **Get floor status (Obter status do andar)** – Verifique o estado atual do relé conectado a um andar.
- **Access (Acesso)** – Conceda acesso de usuários ao andar. O horário de acesso determinado se aplica. Consulte *Como configurar monitores de portas e travas na página 15*.
- **Unlock (Destravar)** – O andar torna-se totalmente acessível a todas as pessoas até você pressionar **Lock (Travar)**, um estado de andar agendado é ativado ou o controlador de porta é reiniciado.
- **Lock (Travar)** – O andar torna-se inacessível a todas as pessoas até você pressionar **Unlock (Destravar)**, um estado de andar agendado é ativado ou o controlador de porta é reiniciado.

Criação e edição de usuários

Cada pessoa deverá ter um perfil de usuário exclusivo para ter acesso a portas no sistema de controle de acesso. O perfil de usuário é composto por credenciais que dizem ao sistema quem é o usuário e quando e como ele obtém acesso às portas.

Para ser capaz de gerenciar os direitos de acesso de usuários de forma eficiente, cada usuário deverá pertencer a um ou mais grupos. Para obter mais informações, consulte *Criar e editar grupos*.

Para criar um novo perfil de usuário:

1. Vá para **Access Management (Gerenciamento de acesso)**.
2. Selecione a guia **Users (Usuários)** e clique em **Add new user (Adicionar novo usuário)**.
3. Na caixa de diálogo **Add User (Adicionar usuário)**, insira as credenciais do usuário. Consulte *Credenciais de usuário na página 42*.
4. Clique em **Save (Salvar)**.
5. Arraste o usuário para um ou mais grupos na lista **Groups (Grupos)**. Se a lista **Groups (Grupos)** estiver vazia, crie um novo grupo. Consulte *Criar e editar grupos na página 35*.

Para expandir um item na lista **Users (Usuários)** e exibir as credenciais do usuário, clique em .

Para encontrar um usuário específico, insira um filtro no campo de filtragem de usuários. Para forçar correspondências exatas, circunde o texto do filtro com aspas duplas, por exemplo, "John" ou "potter, virginia".

Para editar as credenciais do usuário, clique em e altere as credenciais conforme necessário. Em seguida, clique em **Save (Salvar)**.

Para excluir um usuário, clique em .

Importante

Se um usuário foi criado via AXIS Visitor Manager, não edite-o nem o exclua no AXIS Entry Manager. Para obter mais informações sobre o AXIS Visitor Manager e o serviço de leitor de QR Code, consulte *AXIS Visitor Access na página 24*.

Credenciais de usuário

As seguintes credenciais estão disponíveis para usuários:

- **First name (Nome)** (obrigatório)
- **Last name (Sobrenome)**
- **Valid from (Válido de)** e **Valid until (Válido até)** – Insira as datas entre as quais as credenciais do usuário serão válidas. Clique no campo de data e selecione o mês, o dia e o ano desejados. Você também pode digitar a data diretamente no campo.
- **Suspend credential (Suspender credencial)** – Selecione para suspender a credencial. Quando suspensa, o usuário não poderá acessar quaisquer portas no sistema por meio dessa credencial. Desmarque para conceder acesso ao usuário novamente. A suspensão visa ser temporária. Se o acesso ao usuário tiver que ser negado permanentemente, será melhor excluir o perfil do usuário.
- **PIN**(obrigatório sem número de cartão ou raw de cartão) – Insira o número de identificação pessoal de quatro dígitos (PIN) selecionado ou atribuído ao usuário.
- **Facility code (Código de local)** Insira um código para verificar o sistema de controle de acesso da instalação. Se um código de local predefinido for inserido, este campo será preenchido automaticamente, consulte *Código de local predefinido na página 24*
- **Card number (Número do cartão)** (obrigatório sem PIN ou raw de cartão) – Insira o número do cartão. Consulte as informações do fabricante do cartão sobre onde localizar seu número. O número do cartão também pode ser recuperado pelo sistema. Passe o cartão em um leitor conectado, selecione o leitor na lista e clique em **Retrieve (Recuperar)**.
- **Card raw (Raw do cartão)** (obrigatório sem PIN ou número do cartão) – Insira os dados raw do cartão. Os dados podem ser recuperados pelo sistema. Passe o cartão em um leitor conectado, selecione o leitor na lista e clique em **Retrieve (Recuperar)**. Use este tipo de identificação somente se um número de cartão não puder ser localizado.
- **Long access time (Tempo de acesso longo)** – Selecione para substituir o tempo de acesso existente e permitir que a porta seja aberta pelo tempo de acesso longo para o usuário, consulte *Sobre opções do monitor de portas e tempo na página 16*
- **License plate (Placa de licença)** (esta credencial não está disponível em uma instalação de controlador de porta padrão) – Quando esta credencial for ativada por software de parceiros, insira o número da placa de licença para o veículo do usuário. Essa credencial só pode ser usada junto com o software do parceiro Axis e uma câmera com software de reconhecimento de placa de licença. Para obter mais informações, entre em contato com seu parceiro ou representante de vendas Axis.

Observação

O botão **Retrieve (Recuperar)** estará disponível somente se a configuração de hardware tiver sido concluída e um ou mais leitores estiverem conectados ao controlador.

Importar usuários

Os usuários podem ser adicionados ao sistema ao importar um arquivo de texto em formato de valores separados por vírgulas (CSV). Recomenda-se importar usuários quando for necessário adicionar vários usuários ao mesmo tempo.

Antes que você possa importar usuários, crie e salve um arquivo (*. csv ou *. txt) no formato CSV correto. Separe valores com vírgulas, sem espaços e cada usuário com uma quebra de linha.

Exemplo

```
jane,doe,1234,12345678,abc123
john,doe,5435,87654321,cde321
```

Para importar usuários:

1. Vá para **Setup > Import Users (Configuração > Importar usuários)**.
2. Localize e selecione o arquivo *.csv ou *.txt com a lista de usuários.
3. Selecione a opção de credencial correta para cada coluna.

4. Para importar os usuários no sistema, clique em **Import users (Importar usuários)**.
5. Verifique se cada coluna contém o tipo de credencial correto.
6. Se as colunas estiverem corretas, clique em **Start importing users (Iniciar importação de usuários)**. Se as colunas estiverem incorretas, clique em **Cancel (Cancelar)** e comece novamente.
7. Quando a importação estiver concluída, clique em **OK**.

As seguintes opções de credenciais estão disponíveis:

- **First name (Nome)**
- **Last name (Sobrenome)**
- **PIN code (Código PIN)**
- **Card number (Número do cartão)**
- **License plate (Placa de licença)**
- **Unassigned (Não atribuído)** – Valores que não serão importados. Selecione esta opção para ignorar uma determinada coluna.

Para obter mais informações sobre credenciais, consulte *Criação e edição de usuários*.

Exportar usuários

A página de exportação mostra uma lista de valores separados por vírgulas (CSV) de todos os usuários no sistema. A lista pode ser usada para importar os usuários para outro sistema.

Para exportar a lista de usuários:

1. Abra um editor de texto simples e crie um novo documento.
2. Vá para **Setup > Export Users (Configuração > Exportar usuários)**
3. Selecione e copie todos os valores na página.
4. Cole os valores no documento de texto.
5. Salve o documento como um arquivo de valores separados por vírgulas (* csv) ou como um arquivo de texto (*. txt).

Combinações de agendamentos de acesso de exemplo

Agendamentos de tipo de identificação e grupo podem ser combinados de várias formas para atingir diferentes resultados. Os exemplos abaixo seguem o fluxo de trabalho descrito em *página 32*.

Exemplo

Para criar uma combinação de agendamento que

- sempre conceda acesso a vigilantes a uma porta,
  - usando seus cartões durante o turno diurno (segunda a sexta-feira, da 6h às 16h.), enquanto
  - usam seus cartões e PIN antes e após o turno diurno e que
- conceda acesso a funcionários do turno diurno à mesma porta,
  - usando seus cartões somente durante o turno diurno:

1. Crie um **Addition schedule (Agendamento de adição)** chamado **Day shift hours (Horário do turno diurno)**. Consulte *página 33*.

2. Crie um **Schedule item (Item de agendamento)** de turno diurno com recorrência de segunda à sexta-feira das 6h às 16h.
3. Crie dois grupos, um **Group (Grupo)** chamado **Guards (Vigilantes)** e um **Group (Grupo)** chamado **Day shift personnel (Funcionários do turno diurno)**. Consulte *página 35*.
4. Arraste o agendamento de acesso predefinido **Sempre** para o grupo **Guards (Vigilantes)**.
5. Arraste o agendamento de acesso **Day shift hours (Horário do turno diurno)** para o grupo **Day shift personnel (Funcionários do turno diurno**.
6. Adicione os tipos de identificação **Card number and PIN (Número do cartão e PIN)** e **Card number only (Somente número do cartão)** ao leitor da porta.
7. Arraste o agendamento de acesso predefinido **Sempre** para o tipo de identificação **Card number and PIN (Número do cartão e PIN)**.
8. Arraste o agendamento de acesso **Day shift hours (Horário do turno diurno)** para o tipo de identificação **Card number only (Somente número do cartão)**
9. Arraste a porta para os dois grupos. Em seguida, adicione usuários aos grupos conforme necessário. Consulte *página 41*.

Exemplo

Para criar uma combinação de agendamento que

- sempre conceda acesso a vigilantes a uma porta,
  - usando seus cartões durante o turno diurno (segunda a sexta-feira, da 6h às 16h.), enquanto
  - usam seus cartões e PIN antes e após o turno diurno e que
- conceda acesso a funcionários diurnos à mesma porta todos os dias entre 6h e 16h,
  - usando seus cartões somente durante o turno diurno, ao
  - usar seus cartões e PIN durante noites e fins de semana:

1. Crie um **Addition schedule (Agendamento de adição)** chamado **Day shift hours (Horário do turno diurno)**. Consulte *página 33*.
2. Crie um **Schedule item (Item de agendamento)** de turno diurno com recorrência de segunda à sexta-feira das 6h às 16h.
3. Crie um **Subtraction schedule (Agendamento de subtração)** chamado **Nights & weekends (Noites e fins de semana)**.
4. Crie um **Schedule item (Item de agendamento)** para noites e fins de semana com recorrência de domingo a sábado das 16h às 6h.
5. Arraste o agendamento predefinido **Sempre** e o agendamento de acesso **Nights & weekends (Noites e fins de semana)** para o grupo **Day shift personnel (Funcionários do turno diurno)**.
6. Crie dois grupos, um **Group (Grupo)** chamado **Guards (Vigilantes)** e um **Group (Grupo)** chamado **Day shift personnel (Funcionários do turno diurno)**. Consulte *página 35*.
7. Arraste o agendamento de acesso predefinido **Sempre** para o grupo **Guards (Vigilantes)** e o grupo **Day shift personnel (Funcionários do turno diurno)**.
8. Arraste o agendamento de acesso **Nights & weekends** (Noites e fins de semana) para o grupo **Day shift personnel** (Funcionários do turno diurno).
9. Adicione os tipos de identificação **Card number and PIN (Número do cartão e PIN)** e **Card number only (Somente número do cartão)** ao leitor da porta.
10. Arraste o agendamento de acesso predefinido **Sempre** para o tipo de identificação **Card number and PIN (Número do cartão e PIN)**.

11. Arraste o agendamento de acesso **Day shift hours (Horário do turno diurno)** para o tipo de identificação **Card number only (Somente número do cartão)**
12. Arraste a porta para os dois grupos. Em seguida, adicione usuários aos grupos conforme necessário. Consulte *página 41*.

Configuração de alarmes e eventos

Eventos que ocorrem no sistema, por exemplo, quando um usuário passa um cartão ou um dispositivo REX é ativado, são registrados no log de eventos. Eventos registrados podem ser configurados para acionar alarmes e tais alarmes são registrados no log de alarmes.

- Exiba o log de eventos. Consulte *página 46*.
- Exporte o log de eventos. Consulte *página 46*
- Exiba o log de alarmes. Consulte *página 47*.
- Configure os logs de eventos e alarmes. Consulte *página 47*.

Alarmes também podem ser configurados para acionar ações como notificações por email. Para obter mais informações, consulte *Como configurar regras de ação na página 48*.

Exibir o log de eventos

Para exibir eventos registrados, vá para **Event Log (Log de eventos)**.

Se eventos globais estiverem ativados, você poderá abrir o log de eventos de qualquer controlador de porta no sistema. Para obter mais informações sobre eventos globais, consulte *Configurar o evento e logs de alarme na página 47*.

Para expandir um item no log de eventos e visualizar os detalhes do evento, clique em  .

A aplicação de filtros para o log de eventos facilita encontrar eventos específicos. Para filtrar a lista, selecione um ou mais filtros de log de eventos e clique em **Apply filters (Aplicar filtros)**. Para obter mais informações, consulte *Filtros do log de eventos na página 46*.

Como um administrador, você pode ter mais interesse em alguns eventos do que em outros. Assim, você pode escolher quais eventos devem ser registrados, e para quais controladores. Para obter mais informações, consulte *Opções do log de eventos na página 47*.

Filtros do log de eventos

Você pode restringir o escopo do log de eventos selecionando um ou mais dos seguintes filtros:

- Usuário – Filtre por eventos relacionados a um usuário selecionado.
- Porta e andar – Filtre por eventos relacionados a uma porta ou a um andar específico.
- Tópico – Filtro por tipo de evento.
- Origem – Filtre por eventos de um controlador selecionado. Disponível somente em um cluster de controlador e quando eventos globais estão ativados.
- Data e hora – Filtre o log de eventos por um intervalo de data e hora.

Exportação do log de eventos

Para exportar eventos registrados no log, vá para **Event Log (Log de eventos)**:

1. Clique em  .
2. Selecione o formato de exportação no menu suspenso para iniciar a exportação.

Observação

O formato CSV é aceito por todos os navegadores. O formato XLSX pode ser usado no Chrome™ e no Internet Explorer®.

Observação

Após a conclusão de uma exportação, o botão de exportação muda de  para  . Para iniciar outra exportação, atualize a página Web. O botão de exportação muda de volta para  .

Exibir o log de alarmes

Para exibir os alarmes acionados, vá para **Alarm Log (Log de alarmes)**. Se eventos globais estiverem ativados, você poderá abrir o log de alarmes de qualquer controlador de porta no sistema. Para obter mais informações sobre eventos globais, consulte *Configurar o evento e logs de alarme na página 47*.

Para expandir um item no log de alarmes e exibir os detalhes do alarme, por exemplo, identidade de porta e estado, clique em  .

Para remover um alarme da lista após verificar a causa do alarme, clique em **Acknowledge (Confirmar)**. Para remover todos os alarmes, clique em **Acknowledge all alarms (Confirmar todos os alarmes)**.

Como um administrador, talvez alguns eventos sejam necessários para acionar alarmes. Assim, você poderá escolher quais eventos deverão acionar alarmes e para quais controladores. Para obter mais informações, consulte *Opções do log de alarmes na página 48*.

Configurar o evento e logs de alarme

A página de configuração de evento e logs de alarme permite que você defina quais eventos devem estar registrados e acionar alarmes.

Para compartilhar eventos e alarmes entre todos os controladores conectados, selecione **Global events (Eventos globais)**. Quando eventos globais estiverem ativados, você apenas precisará abrir uma página de log de eventos e uma página de log de alarmes para gerenciar ao mesmo tempo eventos e alarmes de todos os controladores de porta no sistema. Eventos globais estão ativados por padrão.

Se você desativar eventos globais, será necessário abrir uma página de log de eventos e uma página de log de alarmes para cada controlador de porta individual e gerenciar seus eventos e alarmes separadamente.

Importante

Cada vez que você ativar ou desativar eventos globais, o log de eventos será limpo. Isso significa que todos os eventos antes desse momento serão removidos e o log de eventos será iniciado.

Alarmes também podem ser configurados para acionar ações como notificações por email. Para obter mais informações, consulte *Como configurar regras de ação na página 48*.

Opções do log de eventos

Para definir quais eventos devem ser incluídos no log de eventos, vá para **Setup > Configure Event and Alarm Logs (Configuração > Configure logs de eventos e alarmes)**.

As seguintes opções de log de eventos estão disponíveis:

- **No logging (Nenhum registro)** – Desative o log de eventos. O evento não será registrado ou incluído no log de eventos.
- **Log for all sources (Registre para todas as fontes)** – Ative o log de eventos em todos os controladores de porta. O evento será registrado para todos os controladores e incluído no log de eventos.
- **Log for selected sources (Registre para fontes selecionadas)** – Ative o log de eventos em controladores de porta selecionados. O evento será registrado para todos os controladores selecionados e incluído no log de eventos. Selecione essa opção para eventos que serão combinados com a opção de log de alarme **No alarms (Sem alarmes)** ou **Log alarm for selected controllers (Registre alarme para controladores selecionados)**.

  Na lista **Configure event logging (Configure log de eventos)**, clique em **Select controllers** (Selecione controladores) no item do log de eventos que deseja ativar. A caixa de diálogo **Device Specific Event Logging (Log de eventos específico de dispositivo)** é aberta. Em **Log event (Registre evento)**, selecione os controladores que devem ter o registro de alarme ativado e clique em **Save (Salvar)**.

Opções do log de alarmes

Para definir quais eventos devem acionar um alarme, vá para **Setup > Configure Event and Alarm Logs (Configuração > Configurar logs de eventos e alarmes)**.

As seguintes opções para acionar e registrar alarmes estão disponíveis:

- **No alarms (Sem alarmes)** – Desative o log de alarmes. O evento não acionará alarmes nem será incluído no log de alarmes.
- **Log alarm for all sources (Registrar alarme para todas as fontes)** – Ative o log de alarmes em todos os controladores de porta. O evento acionará um alarme e será incluído no log de alarmes.
- **Log alarm for selected sources (Registrar alarme para fontes selecionadas)** – Ative o log de alarmes nos controladores de porta selecionados. O evento acionará um alarme e será incluído no log de alarmes.

  Na lista **Configure alarm logging (Configurar log de alarmes)**, clique em **Select sources (Selecionar fontes_** sob o item de log do alarme que deseja ativar. A caixa de diálogo **Device Specific Alarm Triggering (Acionamento de alarme específico de dispositivo)** é aberta. Em **Trigger alarm (Acionar alarme)**, selecione os controladores de porta que devem ter o registro de alarme ativado e clique em **Save (Salvar)**.

Como configurar regras de ação

As páginas de eventos permitem que você configure o produto Axis para executar ações quando diferentes eventos ocorrem. Por exemplo, o produto pode enviar uma notificação por email ou ativar uma porta de saída quando um alarme é acionado. O conjunto de condições que define como e quando a ação é acionada é chamado regra de ação. Se várias condições forem definidas, todas elas deverão ser atendidas para acionar a ação.

Para obter mais informações sobre os acionadores e ações disponíveis, consulte *Acionadores na página 49* e *Ações na página 51*.

Este exemplo descreve como configurar uma regra de ação para enviar uma notificação por email quando qualquer alarme é acionado.

1. Configure os alarmes. Consulte *Configurar o evento e logs de alarme na página 47*.
2. Vá para **Setup > Additional Controller Configuration > Events > Schedules (Configuração > Configuração de controlador adicional > Eventos > Regras de ação)** e clique em **Add (Adicionar)**.
3. Selecione **Enable rule (Ativar regra)** e insira um nome descritivo para a regra.
4. Selecione **Event Logger (Registrador de eventos)** na lista suspensa **Trigger (Acionador)**.
5. Opcionalmente, selecione um **Schedule (Agendamento)** e **Additional conditions (Condições adicionais)**. Consulte abaixo.
6. Em **Actions (Ações)**, selecione **Send Notification (Enviar notificação)** na lista suspensa **Type (Tipo)**.
7. Selecione um destinatário de email na lista suspensa. Consulte *Como adicionar destinatários na página 51*.

Este exemplo descreve como configurar uma regra de ação para ativar uma porta de saída quando a abertura da porta é forçada.

1. Vá para **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Configuração > Configuração de controlador adicional > Opções do sistema > Portas e dispositivos > Portas de E/S)**.
2. Selecione **Output (Saída)** na lista suspensa **I/O Port Type (Tipo de porta de E/S)** e insira um **Name (Nome)**.
3. Selecione o **Normal state (Estado normal)** da porta de E/S e clique em **Save (Salvar)**.
4. Vá para **Events > Action Rules (Eventos > Regras de ação)** e clique em **Add (Adicionar)**.
5. Selecione **Door (Porta)** na lista suspensa **Trigger (Acionador)**.
6. Selecione **Door Alarm (Alarme da porta)** na lista suspensa.
7. Selecione a porta desejada na lista suspensa.
8. Selecione **DoorForcedOpen** na lista suspensa.

9. Opcionalmente, selecione um **Schedule (Agendamento)** e **Additional conditions (Condições adicionais)**. Consulte abaixo.
10. Em **Actions (Ações)**, selecione **Output Port (Porta de saída)** na lista suspensa **Type (Tipo)**.
11. Selecione a porta de saída desejada na lista suspensa **Port (Porta)**.
12. Defina o estado **Active (Ativo)**.
13. Selecione **Duration (Duração)** e **Go to opposite state after (Ir para o estado oposto após)**. Em seguida, insira a duração desejada da ação.
14. Clique em **OK**.

Para usar mais de um acionador para a regra de ação, selecione **Additional conditions (Condições adicionais)** e clique em **Add (Adicionar)** para adicionar outros acionadores. Ao usar condições adicionais, todas as condições deverão ser atendidas para acionar a ação.

Para evitar que uma ação seja acionada várias vezes, um tempo **Wait at least (Aguardar pelo menos)** poderá ser definido. Insira o tempo em horas, minutos e segundos, durante os quais o acionador deverá ser ignorado antes que a regra de ação possa ser utilizada novamente.

Para obter mais informações, consulte a Ajuda integrada do produto.

Acionadores

Os **acionadores** e **condições** da regra de ação disponível incluem:

- **Ponto de acesso**
  - **Ativação de ponto de acesso** – Inicia uma regra de ação quando um dispositivo de ponto de acesso como um leitor ou dispositivo REX é configurado, por exemplo, quando a configuração de hardware é concluída ou um tipo de identificação é adicionado.
- **Configuração**
  - **Ponto de acesso alterado** – Inicia uma regra de ação quando a configuração de um dispositivo de ponto de acesso como um leitor ou dispositivo REX é alterada, por exemplo, quando o hardware é configurado ou um tipo de identificação é editado.
  - **Remoção de ponto de acesso** – Inicia uma regra de ação quando a configuração de hardware de um ponto de acesso como um leitor ou dispositivo REX é redefinida.
  - **Alteração em área** – Não oferecido nesta versão do AXIS Entry Manager. Deve ser configurado por um cliente como um sistema de gerenciamento de acesso, por meio da interface de programação de aplicativos VAPIX®, que oferece suporte a esse recurso e usa dispositivos capazes de fornecer os sinais necessários. Inicia a regra de ação quando uma área de acesso é alterada.
  - **Remoção de área** – Não oferecido nesta versão do AXIS Entry Manager. Deve ser configurado por um cliente como um sistema de gerenciamento de acesso, por meio da interface de programação de aplicativos VAPIX®, que oferece suporte a esse recurso e usa dispositivos capazes de fornecer os sinais necessários. Inicia a regra de ação quando uma área de acesso é removida do sistema.
  - **Alteração em porta** – Inicia uma regra de ação quando as opções de configuração da porta, por exemplo, nome da porta, são alteradas ou quando uma porta é adicionada ao sistema. Isso pode ser usado, por exemplo, para enviar uma notificação quando uma porta é instalada e configurada.
  - **Remoção de porta** – Inicia uma regra de ação quando uma porta é removida do sistema. Isso pode ser usado, por exemplo, para enviar uma notificação quando uma porta é removida do sistema.
- **Porta**
  - **Alarme de bateria** – Inicia uma regra de ação quando a bateria de uma porta sem fio está fraca ou esgotada.

- **Alarme de porta** – Inicia uma regra de ação quando o monitor de portas indica que a porta foi forçada para abrir, a porta está aberta há muito tempo ou se a porta apresenta algum tipo de falha. Isso pode ser usado, por exemplo, para enviar uma notificação quando alguém está tentando forçar uma entrada.
- **Monitor de trava dupla da porta** – Inicia uma regra de ação somente quando o estado da trava secundária muda para travada ou destravada.
- **Monitor de trava da porta** – Inicia uma regra de ação quando o estado da trava normal muda para travada ou destravada. Por exemplo, uma falha é acionada quando o monitor de portas detecta que a porta está aberta, mas a trava ainda está travada.
- **Modo da porta** – Inicia uma regra de ação quando a porta muda de estado, por exemplo, quando a porta foi acessada ou bloqueada ou quando ela está no modo de bloqueio. Para obter descrições mais detalhadas desses modos, consulte a ajuda online.
- **Monitor de portas** – Inicia a regra de ação quando o estado do monitor de portas muda. Isso pode ser usado, por exemplo, para enviar uma notificação quando um monitor de portas indica que a porta foi aberta ou fechada.
- **Violação de porta** – Inicia uma regra de ação quando o monitor de portas detecta que a conexão foi interrompida, por exemplo, se alguém cortou os fios do monitor de portas. Para usar esse acionador, certifique-se de que a opção **Ativar entradas supervisionadas** esteja selecionada e que os resistores de terminação estejam instalados nas portas de entrada de conectores de portas relevantes. Para obter mais informações, consulte *Como usar entradas supervisionadas na página 18*.
- **Alerta de porta** – Inicia uma regra de ação antes do alarme de porta aberta há muito tempo disparar. Isso pode ser usado, por exemplo, para enviar um sinal de alerta informando que o controlador de porta enviará um alarme real de porta aberta há muito tempo se a porta não for fechada dentro do período configurado para acionamento do alarme. Para obter mais informações sobre o tempo de porta aberta há muito tempo, consulte *Como configurar monitores de portas e travas na página 15*.
- **Trava obstruída** – Inicia uma regra de ação quando uma trava de porta sem fio é bloqueada fisicamente.

- **Registrador de eventos** – Registra todos os eventos no controlador de portas, por exemplo, quando um usuário passa um cartão ou abre uma porta. Se a opção **Eventos globais** estiver ativada, o registrador de eventos acompanhará todos os eventos em todos os controladores do sistema. Para definir quais alarmes e eventos podem iniciar uma regra de ação, vá para **Configuração > Configurar Logs de eventos e alarmes**. O registrador de eventos é compartilhado pelo sistema e pode armazenar até 30.000 eventos. Quando o limite é atingido, o registrador de eventos usa a regra "primeiro a chegar, primeiro a sair" (FIFO). Isso significa que o primeiro evento é o primeiro a ser sobrescrito.
  - **Alarme** – Inicia uma regra de ação quando um dos alarmes especificados é acionado. O administrador do sistema pode configurar quais eventos são mais importantes que outros e definir se um evento específico deve acionar um alarme ou não.
  - **Alarmes descartados** – Inicia uma regra de ação quando não é possível escrever novos registros de alarme nos logs de alarmes. Por exemplo, se houver um número demasiadamente grande de alarmes a ponto de o registrador de eventos não conseguir acompanhar. Quando um alarme é descartado, uma notificação pode ser enviada para o operador.
  - **Eventos descartados** – Inicia uma regra de ação quando novos registros de eventos não podem ser escritos nos logs de eventos. Por exemplo, se houver um número demasiadamente grande de eventos a ponto de o registrador de eventos não conseguir acompanhar. Quando um evento é descartado, uma notificação pode ser enviada para o operador.
- Hardware
  - **Rede** – Inicia uma regra de ação quando a conexão de rede é perdida. Selecione **Sim** para iniciar a regra de ação quando a conexão de rede é perdida. Selecione **Não** para iniciar regra de ação quando a conexão de rede é restaurada. Selecione **Endereço IPv4/v6 removido** ou **Novo endereço IPv4/v6** para acionar uma regra de ação quando o endereço IP mudar.
  - **Conexão com par** – Inicia uma regra de ação quando o produto Axis estabeleceu conexão com outro controlador de porta, se a conexão de rede entre os dispositivos é perdida ou se o pareamento de controladores de porta falhou. Isso pode ser usado, por exemplo, para enviar uma notificação de que um controlador de porta perdeu sua conexão de rede.

- **Sinal de entrada**
  - **Porta de entrada digital** – Inicia uma regra de ação quando uma porta de E/S recebe um sinal de um dispositivo conectado. Consulte *Portas de E/S na página 63*.
  - **Acionador manual** – Inicia uma regra de ação quando o acionador manual é ativado. Ele pode ser usado por clientes como sistemas de gerenciamento de acesso, por meio da interface de programação de aplicativos VAPIX®, para iniciar ou parar manualmente a regra de ação.
  - **Entradas virtuais** – Inicia uma regra de ação quando uma das entradas virtuais muda de estado. Ele pode ser usado por clientes como sistemas de gerenciamento de acesso, por meio da interface de programação de aplicativos VAPIX®, para disparar ações. As entradas virtuais podem, por exemplo, ser conectadas a botões na interface do usuário do sistema de gerenciamento.
- **Agendamento**
  - **Intervalo** – Inicia uma regra de ação na hora de início agendada e permanece ativo até a hora de término do agendamento ser atingida.
  - **Pulso** – Inicia uma regra de ação quando um evento único ocorre. Ou seja, um evento que ocorre em um instante específico e não possui duração.
- **Sistema**
  - **Sistema pronto** – Inicia uma regra de ação quando o sistema está no estado de pronto. Por exemplo, o produto Axis pode detectar o estado do sistema e enviar uma notificação quando o sistema iniciou.

    Selecione **Sim** para iniciar a regra de ação quando o produto está no estado pronto. Observe que a regra será iniciada somente quando todos os serviços necessários, como o sistema de eventos, tiverem iniciado.
- **Tempo**
  - **Recorrência** – Inicia uma regra de ação monitorando as recorrências que você criou. Você pode usar esse acionador para iniciar ações recorrentes, como enviar notificações a cada hora. Selecione um padrão de recorrência ou crie um novo. Para obter mais informações sobre como configurar um padrão de recorrência, consulte *Como configurar recorrências na página 53*.
  - **Usar agendamento** – Inicia uma regra de ação de acordo com o agendamento selecionado. Consulte *Como criar agendamentos na página 52*.

Ações

Você pode configurar várias ações:

- **Output Port (Porta de saída)** – Ative uma porta de E/S para controlar um dispositivo externo.
- **Send Notification (Enviar notificação)** – Envie uma mensagem de notificação para um destinatário.
- **Status LED (LED de status)** – O LED de status pode ser configurado para piscar pela duração da regra de ação ou por um número definido de segundos. O LED de status pode ser usado durante a instalação e configuração para validar visualmente se as configurações do acionador, por exemplo, de porta aberta há muito tempo, funcionam corretamente. Para definir a cor em que o LED de status pisca, selecione uma **LED Color (Cor do LED)** na lista suspensa.

Como adicionar destinatários

O produto pode enviar mensagens para notificar destinatários sobre eventos e alarmes. No entanto, antes que o produto possa enviar mensagens de notificação, é necessário definir um ou mais destinatários. Para obter informações sobre as opções disponíveis, consulte *Tipos de destinatários na página 52*.

Para adicionar um destinatário:

1. Vá para **Setup > Additional Controller Configuration > Events > Recipients (Configuração > Configuração de controlador adicional > Eventos > Destinatários)** e clique em **Add (Adicionar)**.

2. Insira um nome descritivo.
3. Selecione um **Type (Tipo)** de destinatário.
4. Insira as informações necessárias para o tipo de destinatário.
5. Clique em **Test (Testar)** para testar a conexão com o destinatário.
6. Clique em **OK**.

Tipos de destinatários

Os seguintes tipos de destinatários estão disponíveis:

HTTP

HTTPS

Email

TCP

Como configurar destinatários de email

Destinatários de email podem ser configurados ao selecionar um dos provedores de email listados, ou mediante a especificação do servidor SMTP, porta e autenticação usadas por, por exemplo, um servidor de email corporativo.

Observação

Alguns provedores de email possuem filtros de segurança que impedem os usuários de receber ou exibir grandes quantidades de anexos, emails agendados e itens semelhantes. Verifique a política de segurança do provedor de email para evitar problemas de entrega e contas de email bloqueadas.

Para configurar um destinatário de email usando um dos provedores listados:

1. Vá para **Events > Recipients (Eventos > Destinatários)** e clique em **Add (Adicionar)**.
2. Insira um **Name (Nome)** e selecione **Email** na lista **Type (Tipo)**.
3. Insira os endereços de email para o envio de emails no campo **To (Para)**. Use vírgulas para separar vários endereços.
4. Selecione o provedor de email na lista **Provider (Provedor)**.
5. Insira o ID de usuário e a senha para a conta de email.
6. Clique em **Test (Testar)** para enviar um email de teste.

Para configurar um destinatário de email usando, por exemplo, um servidor de email corporativo, siga as instruções acima, mas selecione **User defined (Definido pelo usuário)** como **Provider (Provedor)**. Insira o endereço de email a ser exibido como remetente no campo **From (De)**. Selecione **Advanced settings (Configurações avançadas)** e especifique o endereço do servidor SMTP, porta e método de autenticação. Opcionalmente, selecione **Use encryption (Usar criptografia)** para enviar emails através de uma conexão criptografada. O certificado do servidor pode ser validado usando os certificados disponíveis no produto Axis. Para obter informações sobre como carregar certificados, consulte *Certificados na página 56*.

Como criar agendamentos

Os agendamentos podem ser usados como acionadores de regras de ação ou condições adicionais. Use um dos agendamentos predefinidos ou crie um novo agendamento como descrito a seguir.

Para criar um novo agendamento:

1. Vá para **Setup > Additional Controller Configuration > Events > Schedules (Configuração > Configuração de controlador adicional > Eventos > Agendamentos)** e clique em **Add (Adicionar)**.

2. Insira um nome descritivo e as informações necessárias para um agendamento diário, semanal, mensal ou anual.
3. Clique em **OK**.

Para usar o agendamento em uma regra de ação, selecione o agendamento na lista suspensa **Schedule** (Agendamento) na página Action Rule Setup (Configuração de regras de ação).

Como configurar recorrências

Recorrências são usadas para acionar regras de ação repetidamente, por exemplo, a cada 5 minutos ou a cada hora.

Para configurar uma recorrência:

1. Vá para **Setup > Additonal Controller Configuration > Events > Recurrences (Configuração > Configuração de controlador adicional > Eventos > Recorrências)** e clique em **Add (Adicionar)**.
2. Insira um nome descritivo e um padrão de recorrência.
3. Clique em **OK**.

Para usar a recorrência em uma regra de ação, selecione **Time (Tempo)** na lista suspensa **Trigger (Acionador)** na página de configuração de regras de ação e, em seguida, selecione a recorrência na segunda lista suspensa.

Para modificar ou remover recorrências, selecione a recorrência na **Recurrences List (Lista de recorrências)** e clique em **Modify (Modificar)** ou **Remove (Remover)**.

Feedback do leitor

Leitores usam LEDs e beepers para enviar mensagens de feedback ao usuário (a pessoa acessando ou tentando acessar a porta). O controlador de porta pode acionar um número de mensagens de feedback, algumas das quais são pré-configuradas no controlador de porta e compatíveis com a maioria dos leitores.

Leitores têm diferentes comportamentos de LED, mas normalmente eles usam diferentes sequências de luzes sólidas e luzes piscando em vermelho, verde e âmbar.

Leitores também podem usar beepers de um passo para enviar mensagens, utilizando diferentes sequências de sinais de beeper curtos e longos.

A tabela a seguir mostra os eventos que estão pré-configurados no controlador de porta para acionar o feedback de leitor e seus sinais de feedback de leitor típico. Sinais de feedback para leitores AXIS são apresentados no Guia de Instalação fornecido com o leitor AXIS.

Evento	Wiegand LED duplo	Wiegand LED único	OSDP	Padrão do beeper	Estado
Ocioso[1]	Apagado	Vermelho	Vermelho	Silencioso	Normal
PIN necessário	Piscando em vermelho/verde	Piscando em vermelho/verde	Piscando em vermelho/verde	Dois bipes curtos	PIN necessário
Acesso concedido	Verde	Verde	Verde	Bipe	Acesso concedido
Acesso negado	Vermelho	Vermelho	Vermelho	Bipe	Acesso negado

1. Estado ocioso é inserido quando a porta está fechada e a trava está bloqueada.

Mensagens de feedback diferentes das acimas devem ser configuradas por um cliente como um sistema de gerenciamento de acesso, através da interface de programação de aplicativos VAPIX®, que oferece suporte a este recurso e usa leitores que podem fornecer os sinais necessários. Para obter mais informações, consulte as informações do usuário fornecidas pelo desenvolvedor do sistema de gerenciamento de acesso e fabricante do leitor.

Relatórios

A página Reports (Relatórios) permite a você exibir, imprimir e exportar relatórios que contêm diferentes tipos de informações sobre o sistema. Para obter mais informações sobre quais relatórios estão disponíveis, consulte *Tipos de relatórios na página 54*.

Exibição, impressão e exportação de relatórios

Para abrir a página Reports (Relatórios), clique em **Reports (Relatórios)**.

Para exibir um relatório, clique em **View and print (Exibir e imprimir)**.

Para imprimir um relatório:

1. Clique em **View and print (Exibir e imprimir)**.
2. Selecione as colunas que devem ser incluídas no relatório. Todas as colunas são selecionadas por padrão.
3. Se desejar restringir o escopo do relatório, insira um filtro no campo filtro relevantes. Por exemplo, você pode filtrar os usuários pelo grupo ao qual eles pertencem, portas por seus agendamentos ou grupos pelas portas às quais eles têm acesso.

   Para forçar correspondências exatas, circunde o texto do filtro com aspas duplas, por exemplo, "John".
4. Se desejar classificar os itens de relatório em uma ordem diferente, clique em  na coluna relevante. Para alterar entre ordem padrão e inversa, alterne os botões de classificação.

   ▲ Mostra os itens na ordem padrão (crescente).

   ▼ Mostra os itens na ordem inversa (decrescente).
5. Clique em **Print selected columns (Imprimir colunas selecionadas)**.

Para exportar um relatório, clique em **Export CSV file (Exportar arquivo CSV)**.

O relatório é exportado como um arquivo de valores separados por vírgulas (CSV) e inclui todos os itens e colunas possíveis para o tipo de relatório. A menos que especificado de outra forma, o arquivo exportado (*. csv) é salvo na pasta de download padrão. Você pode selecionar uma pasta de download nas configurações de usuário do navegador da Web.

Observação

Somente os usuários que possuem credenciais são mostrados em relatórios.

Tipos de relatórios

Os seguintes tipos de relatórios estão disponíveis:

- Agendamentos de acesso. Para obter mais informações sobre tipos e opções de agendamentos de acesso, consulte *página 33* e *página 34*.
- Grupos. Para obter mais informações sobre credenciais de grupos, consulte *página 35*.
- Portas. Para obter mais informações sobre portas e tipos de identificação, consulte *página 36* e *página 37*.
- Usuários. Para obter mais informações sobre credenciais de usuários, consulte *página 42*.
- Controlador de porta. Para obter mais informações sobre controladores conectados e seus tipos de ID, consulte *página 28*. Para obter mais informações sobre opções de tempo de monitores de portas, consulte *página 17*.

Opções do sistema

Segurança

Usuários

O controle de acesso de usuários é ativado por padrão e pode ser configurado em **Setup > Additional Controller Configuration > System Options > Security > Users (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > Usuários)**. Um administrador pode configurar outros usuários fornecendo a eles nomes de usuário e senhas.

A lista de usuários exibe os usuários autorizados e grupos de usuários (níveis de acesso):

- **Administrators (Administradores)** têm acesso irrestrito a todas as configurações. O administrador pode adicionar, modificar e remover outros usuários.

Observação

Observe que, quando a opção **Encrypted & unencrypted (Criptografada e não criptografada)** for selecionada, o servidor Web criptografará a senha. Essa é a opção padrão para uma nova unidade ou uma redefinição de unidade para as configurações padrão de fábrica.

Em **HTTP/RTSP Password Settings (Configurações de senha HTTP/RTSP)**, selecione o tipo de senha que será permitido. Talvez seja necessário permitir senhas não criptografadas, se houver clientes visualizadores que não ofereçam suporte a criptografia, ou se você tiver atualizado o firmware e os clientes existentes oferecerem suporte a criptografia, mas precisarem fazer login novamente e serem configurados para usar essa funcionalidade.

ONVIF

ONVIF é um fórum aberto do setor que fornece e promove interfaces padronizadas para interoperabilidade efetiva de produtos de segurança física baseados em IP.

Ao criar um usuário, você ativa a comunicação ONVIF automaticamente. Use o nome de usuário e a senha com toda a comunicação ONVIF com o produto. Para obter mais informações, consulte *www.onvif.org*

Filtro de endereços IP

A filtragem de endereços IP é ativada na página **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > Filtro de endereços IP)**. Uma vez ativada, acessos do endereço IP listado serão permitidos ou negados ao produto Axis. Selecione **Allow (Permitir)** ou **Deny (Negar)** na lista e clique em **Apply (Aplicar)** para ativar a filtragem de endereços IP.

O administrador pode adicionar até 256 entradas de endereço IP à lista (uma única entrada pode conter vários endereços IP).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer), ou HTTP over SSL) é um protocolo da Web que fornece navegação criptografada. HTTPS também pode ser usado por usuários e clientes para verificar se o dispositivo correto está sendo acessado. O nível de segurança fornecido pelo HTTPS é considerado adequado para a maioria das trocas comerciais.

O produto Axis pode ser configurado para exigir HTTPS quando os administradores fizerem login.

Para usar HTTPS, um certificado HTTPS deve ser instalado primeiro. Vá para **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > Certificados)** para instalar e gerenciar certificados. Consulte *Certificados na página 56*.

Para ativar HTTPS no produto Axis:

1. Vá para **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > HTTPS)**

2. Selecione um certificado HTTPS na lista de certificados instalados.
3. Opcionalmente, clique **Ciphers (Codificadores)** e selecione os algoritmos de criptografia a serem usados para SSL.
4. Defina a **HTTPS Connection Policy (Política de conexão HTTPS)** para os diferentes grupos de usuários.
5. Clique em **Save (Salvar)** para ativar as configurações.

Para acessar o produto Axis através do protocolo desejado, no campo de endereço em um navegador, digite `https://` para o protocolo HTTPS e `http://` para o protocolo HTTP.

A porta de HTTPS pode ser alterada na página **System Options > Network > TCP/IP > Advanced (Opções do sistema > Rede > TCP/IP > Avançado)**.

IEEE 802.1X

IEEE 802.1X é um padrão para Controle de Admissão em Rede baseado em porta que fornece autenticação segura de dispositivos em rede com e sem fio. IEEE 802.1X é baseado em EAP (Extensible Authentication Protocol).

Para acessar uma rede protegida por IEEE 802.1X, os dispositivos devem ser autenticados. A autenticação é executada por um servidor de autenticação, geralmente, um **servidor RADIUS**. Exemplos são FreeRADIUS e Microsoft Internet Authentication Service.

Na implementação da Axis, o produto Axis e o servidor de autenticação se identificam com certificados digitais usando EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). Os certificados são fornecidos por uma **Autoridade de Certificação** (CA). Você precisa de:

- Um certificado de CA para autenticar o servidor de autenticação.
- Um certificado de cliente assinado por CA para autenticar o produto Axis.

Para criar e instalar certificados, vá para **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > Certificados)**. Consulte *Certificados na página 56*.

Para permitir que o produto acesse uma rede protegida por IEEE 802.1 X:

1. Vá para **Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > IEEE 802.1X)**
2. Selecione um **CA Certificate (Certificado de CA)** e um **Client Certificate (Certificado de cliente)** na lista de certificados instalados.
3. Em **Settings (Configurações)**, selecione a versão EAPOL e forneça a identidade EAP associada ao certificado de cliente.
4. Marque a caixa para ativar IEEE 802.1 X e clique em **Save (Salvar)**.

Observação

Para que a autenticação funcione corretamente, as configurações de data e hora no produto Axis deverão ser sincronizadas com um servidor NTP. Consulte *Data e hora na página 57*.

Certificados

Os certificados são usados para autenticar dispositivos em uma rede. Aplicações típicas incluem a navegação na Web criptografada (HTTPS), proteção de rede via IEEE 802.1 X e mensagens de notificação, por exemplo, via email. Dois tipos de certificados podem ser usados com o produto Axis:

Certificados de servidor/cliente – Para autenticar o produto Axis. Um certificado de **servidor/cliente** pode ser autoassinado ou emitido por uma Autoridade de Certificação (CA). Um certificado autoassinado oferece proteção limitada e pode ser usado antes que um certificado emitido por uma CA tenha sido obtido.

Certificados CA – Para autenticar certificados de pares, por exemplo, o certificado de um servidor de autenticação caso o produto Axis esteja conectado a uma rede IEEE 802.1X protegida. O produto Axis é enviado com vários certificados CA pré-instalados.

Observação

- Se o produto for redefinido para o padrão de fábrica, todos os certificados, exceto certificados CA pré-instalados, serão removidos.
- Se o produto for redefinido para o padrão de fábrica, todos os certificados CA pré-instalados que foram removidos serão reinstalados.

Como criar um certificado autoassinado

1. Vá para **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > Certificados)**.
2. Clique em **Create self-signed certificate (Clique em criar certificado autoassinado)** e forneça as informações solicitadas.

Como criar e instalar um certificado assinado por CA

1. Crie um certificado autoassinado, consulte .
2. Vá para **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > Certificados)**.
3. Clique em **Create certificate signing request (Criar solicitação de assinatura de certificado)** e forneça as informações solicitadas.
4. Copie a solicitação em formato PEM e envie para a autoridade de certificação de sua escolha.
5. Quando o certificado assinado for devolvido, clique em **Install certificate (Instalar certificado)** e carregar o certificado.

Como instalar certificados CA adicionais

1. Vá para **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > Certificados)**.
2. Clique em **Install certificate (Instalar certificado)** e carregue o certificado.

Data e hora

As configurações de data e hora do produto Axis são definidas em **Setup > Additional Controller Configuration > System Options > Date & Time (Configuração > Configuração de controlador adicional > Opções do sistema > Data e hora)**.

Current Server Time (Hora do servidor atual) exibe a data e a hora atuais (relógio de 24 horas).

Para alterar as configurações de data e hora, selecione o **Time mode (Modo de hora)** em **New Server Time (Nova hora do servidor)**:

- **Synchronize with computer time (Sincronizar com hora do computador)** – Define a data e a hora de acordo com o relógio do computador. Com essa opção, a data e a hora serão definidas uma vez e não serão atualizadas automaticamente.
- **Synchronize with NTP Server (Sincronizar com servidor NTP)** – Obtém a data e a hora de um servidor NTP. Com essa opção, configurações de data e hora são atualizadas continuamente. Para obter informações sobre as configurações de NTP, consulte *Configuração de NTP na página 60*.

  Se estiver usando um nome de host para o servidor NTP, um servidor de DNS deverá ser configurado. Consulte *Configuração de DNS na página 60*.
- **Set manually (Definir manualmente)** – Permite definir manualmente a data e a hora.

Se estiver usando um servidor NTP, selecione seu **Time zone (Fuso horário)** na lista suspensa. Se necessário, marque **Automatically adjust for daylight saving time changes (Ajustar automaticamente para horário de verão)**.

Rede

Configurações de TCP/IP básicas

O produto Axis oferece suporte a IP versão 4 (IPv4).

O produto Axis pode obter um endereço IPv4 das seguintes formas:

- **Endereço IP dinâmico** – A opção **Obtain IP address via DHCP (Obter endereço IP via DHCP)** é selecionada por padrão. Isso significa que o produto Axis é configurado para obter o endereço IP automaticamente via Dynamic Host Configuration Protocol (DHCP).

  O DHCP permite que os administradores de rede gerenciem e automatizem centralmente a atribuição de endereços IP.

- **Endereço IP estático** – Para usar um endereço IP estático, selecione **Use the following IP address (Usar o seguinte endereço IP)** e especifique o endereço IP, a máscara de sub-rede e o roteador padrão. Em seguida, clique em **Save (Salvar)**.

O DHCP só deverá ser habilitado quando a notificação de endereço IP dinâmica estiver sendo usada, ou se o DHCP puder atualizar um servidor DNS que torne possível acessar o produto Axis pelo nome (nome de host).

Se DHCP estiver ativado e o produto não puder ser acessado, execute o AXIS IP Utility para procurar produtos Axis conectados na rede, ou redefina o produto para as configurações padrão de fábrica e, em seguida, execute a instalação novamente. Para obter informações sobre como redefinir o dispositivo para o padrão de fábrica, consulte *página 65*.

ARP/Ping

O endereço IP do produto pode ser atribuído usando ARP e Ping. Para obter instruções, consulte *Atribua um endereço IP usando ARP/Ping na página 58*.

O serviço ARP/Ping é ativado por padrão, mas será desativado automaticamente dois minutos após o produto ser iniciado ou assim que um endereço IP for atribuído. Para reatribuir endereço IP usando ARP/Ping, o produto deverá ser reiniciado para ativar ARP/Ping por mais dois minutos.

Para desativar o serviço, vá para **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Básicas)** e desmarque a opção **Enable ARP/Ping setting of IP address (Ativar configuração ARP/Ping de endereço IP)**.

A execução de ping do produto ainda será possível quando o serviço for desativado.

Atribua um endereço IP usando ARP/Ping

O endereço IP do dispositivo pode ser atribuído usando ARP/Ping. O comando deve ser emitido em 2 minutos a partir da alimentação conectada.

1. Adquira um endereço IP estático gratuito no mesmo segmento de rede que o computador.
2. Localize o número de série (S/N) na etiqueta do dispositivo.
3. Abra um prompt de comandos e insira os seguintes comandos:

   Sintaxe do Unix/Linux

   ```
   arp -s <endereço IP> <número de série> temp
   ping -s 408 <endereço IP>
   ```

   Exemplo do Linux/Unix

   ```
   arp -s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   Sintaxe do Windows (isso pode exigir que você execute o prompt de comandos como um administrador)

   ```
   arp -s <endereço IP> <número de série>
   ```

```
ping -l 408 -t <endereço IP>
```

Exemplo do Windows (isso pode necessitar que você execute o prompt de comandos como um administrador)

```
arp -s 192.168.0.125 00-40-8c-18-10-00
ping -l 408 -t 192.168.0.125
```

4. Reinicie o dispositivo ao desconectar e reconectar o conector de rede.
5. Feche o prompt de comandos quando o dispositivo responder com `Reply from 192.168.0.125:...` (`Resposta de 192.168.0.125:...` ou semelhante.
6. Abra um navegador e digite `http://<endereço IP>` no campo de endereço.

Para obter outros métodos de atribuição de endereço IP, consulte o documento *How to assign an IP address and access your device (Como atribuir um endereço IP e acessar o dispositivo)* em *www.axis.com/support*

Observação

- Para abrir um prompt de comandos no Windows, abra o menu **Start (Iniciar)** procure `cmd`.
- Para usar o comando ARP no Windows 8/Windows 7/Windows Vista, clique com o botão direito do mouse sobre o ícone de prompt de comandos e selecione **Run as administrator (Executar como administrador)**.
- Para abrir um prompt de comandos do Mac OS X, abra o **Terminal utility (utilitário Terminal)** de **Application > Utilities (Aplicativo > Utilitários)**.

AXIS Video Hosting System (AVHS)

O AVHS usado em conjunto com um serviço AVHS fornece acesso fácil e seguro via Internet a gerenciamento de controladores e logs de qualquer lugar. Para obter mais informações e ajuda sobre provedores de serviços AVHS locais, acesse www.axis.com/hosting

As configurações de AVHS são definidas em **Setup > Additional Controller Configuration > System Options > Network > TCP IP > Basic (Configuração > Controlador adicional > Configuração > Opções do sistema > Rede > TCP/IP > Básicas)**. A possibilidade de conectar a um serviço AVHS está ativada por padrão. Para desativá-la, desmarque a caixa **Enable AVHS (Ativar AVHS)**.

One-click enabled (Um clique ativado) – Pressione e mantenha pressionado o botão de controle do produto (consulte *Visão geral do produto na página 4*) por aproximadamente 3 segundos para conectar a um serviço AVHS pela Internet. Uma vez registrado, **Sempre** será ativado e seu produto Axis permanecerá conectado ao serviço AVHS. Se o produto não for registrado em até 24 horas quando o botão for pressionado, ele será desconectado do serviço AVHS.

Sempre – O produto Axis tentará constantemente conectar a um serviço AVHS pela Internet. Uma vez registrado, ele permanecerá conectado ao serviço. Esta opção poderá ser usada quando o produto já estiver instalado e não for conveniente ou possível usar a instalação de um clique.

Observação

O suporte a AVHS depende da disponibilidade de assinaturas de provedores de serviços.

AXIS Internet Dynamic DNS Service

O AXIS Internet Dynamic DNS Service atribui um nome de host para facilitar o acesso ao produto. Para obter mais informações, consulte *www.axiscam.net*

Para registrar o produto Axis com o AXIS Internet Dynamic DNS Service, vá para **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Básicas)**. Em **Services (Serviços)**, clique no botão **Settings (Configurações)** do AXIS Internet Dynamic DNS Service (requer acesso à Internet). O nome de domínio atualmente registrado no AXIS Internet Dynamic DNS Service para o produto pode ser removido a qualquer momento.

Observação

O AXIS Internet Dynamic DNS Service requer IPv4.

Configurações de TCP/IP avançadas

Configuração de DNS

DNS (Domain Name Service) fornece a tradução de nomes de host em endereços IP. As configurações de DNS são definidas em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado)**.

Selecione **Obtain DNS server address via DHCP (Obter endereço de servidor DNS via DHCP)** para usar as configurações de DNS fornecidas pelo servidor DHCP.

Para fazer configurações manuais, selecione **Use the following DNS server address (Usar o seguinte endereço de servidor DNS)** e especifique o seguinte:

Nome de domínio – Insira os domínios para procurar o nome de host usado pelo produto Axis. Vários domínios podem ser separados por ponto e vírgula. O nome de host sempre é a primeira parte de um nome de domínio totalmente qualificado, por exemplo, `myserver` é o nome de host no nome do domínio totalmente qualificado `myserver.mycompany.com` onde `mycompany.com` é o nome de domínio.

Servidor DNS primário/secundário – Insira os endereços IP dos servidores DNS primários e secundários. O servidor DNS secundário é opcional e usado quando o primário está indisponível.

Configuração de NTP

NTP (Network Time Protocol) é usado para sincronizar os tempos do relógio de dispositivos em uma rede. As configurações NTP são definidas em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado)**.

Selecione **Obtain NTP server address via DHCP (Obter endereço de servidor NTP via DHCP)** para usar as configurações de NTP fornecidas pelo servidor DHCP.

Para fazer configurações manuais, selecione **Use the following NTP server address (Usar o seguinte endereço de servidor NTP)** e insira o nome de host ou endereço IP do servidor NTP.

Configuração de nome do host

O produto Axis pode ser acessado usando um nome de host em vez de um endereço IP. O nome do host é, em geral, o mesmo que o nome de DNS atribuído. O nome do host é configurado em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado)**.

Selecione **Obtain host name via IPv4 DHCP (Obter nome de host via DHCP IPv4)** para usar o nome de host fornecido pelo servidor DHCP em execução em IPv4.

Selecione **Use the host name (Usar o nome de host)** para definir o nome de host manualmente.

Selecione **Enable dynamic DNS updates (Ativar atualizações de DNS dinâmicas)** para atualizar dinamicamente servidores DNS locais sempre que o endereço IP do produto Axis for alterado. Para obter mais informações, consulte a Ajuda online.

Endereço IPv4 local do link

Link-Local Address (Endereço local do link) é ativado por padrão e atribui ao produto Axis um endereço IP adicional que pode ser usado para acessar o produto por meio de outros hosts no mesmo segmento da rede local. O produto pode ter um IP local do link e um endereço IP estático ou fornecido por DHCP ao mesmo tempo.

Esta função pode ser desativada em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado)**.

Opções do sistema

HTTP

A porta HTTP usada pelo produto Axis pode ser alterada em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado)**. Além da configuração padrão, 80, qualquer porta no intervalo 1024–65535 pode ser usada.

HTTPS

A porta HTTPS usada pelo produto Axis pode ser alterada em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado**. Além da configuração padrão, 443, qualquer porta no intervalo 1024–65535 pode ser usada.

Para ativar HTTPS, vá para **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Configuração > Configuração de controlador adicional > Opções do sistema > Segurança > HTTP)**. Para obter mais informações, consulte *HTTPS na página 55*.

NAT traversal (mapeamento de portas) para IPv4

Um roteador de rede permite que dispositivos em uma rede privada (LAN) compartilhem uma única conexão com a Internet. Isso é feito ao encaminhar tráfego da rede privada para o "exterior", isto é, a Internet. A segurança na rede privada (LAN) é aumentada, pois a maioria dos roteadores é pré-configurada para impedir tentativas de acesso à rede privada (LAN) da rede pública (Internet).

Use **NAT traversal** quando o produto Axis estiver localizado em uma intranet (LAN) e você desejar disponibilizá-lo do outro lado (WAN) de um roteador NAT. Com NAT traversal configurado corretamente, todo o tráfego HTTP para uma porta HTTP externa no roteador NAT será encaminhado para o produto.

O NAT traversal é configurado em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado)**.

Observação

- Para que o NAT traversal funcione, isso deverá ser compatível com o roteador. O roteador também deverá oferecer suporte a UPnP®.
- Nesse contexto, um roteador corresponde a qualquer dispositivo de roteamento de rede, como um roteador NAT, roteador de rede, gateway de Internet, roteador de banda larga, dispositivo de compartilhamento de banda larga ou um software como um firewall.

Ativar/Desativar – Quando ativado, o produto Axis tentará configurar o mapeamento de portas em um roteador NAT em sua rede, usando UPnP. Observe que UPnP deverá ser ativado no produto (consulte **Setup > Additional Controller Configuration > System Options > Network > UPnP (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > UPnP)**).

Use roteador NAT manualmente selecionado – Selecione esta opção para selecionar um roteador NAT manualmente e insira o endereço IP para o roteador no campo. Se nenhum roteador for especificado, o produto procurará automaticamente roteadores NAT em sua rede. Se mais de um roteador for encontrado, o roteador padrão será selecionado.

Porta HTTP alternativa – Selecione esta opção para definir manualmente uma porta HTTP externa. Insira uma porta na faixa de 1024 a 65535. Se o campo de porta estiver vazio ou contiver a configuração padrão, que é 0, um número de porta será selecionado automaticamente ao habilitar NAT traversal.

Observação

- Uma porta HTTP alternativa pode ser usada ou estar ativa mesmo se NAT traversal estiver desativado. Isso será útil se seu roteador NAT não oferecer suporte a UPnP e você precisar configurar manualmente encaminhamento de porta no roteador NAT.
- Se você tentar inserir manualmente uma porta que já está em uso, outra porta disponível será selecionada automaticamente.
- Quando a porta for selecionada automaticamente, ela será exibida neste campo. Para alterar isso, insira um novo número de porta e clique em **Save (Salvar)**.

FTP

O servidor FTP em execução no produto Axis permite o upload de novo firmware, aplicativos de usuário, etc. O servidor FTP pode ser desativado em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado)**.

RTSP

O servidor RTSP em execução no produto Axis permite que um cliente que esteja conectando inicie um stream de evento. O número da porta RTSP pode ser alterado em **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Avançado**. A porta padrão é 554.

Observação

Streams de eventos não estarão disponíveis se o servidor RTSP estiver desativado.

SOCKS

SOCKS é um protocolo de proxy rede. O produto Axis pode ser configurado para usar um servidor SOCKS para alcançar redes no outro lado de um firewall ou servidor proxy. Essa funcionalidade é útil quando o produto Axis está localizado em uma rede local atrás de um firewall e notificações, uploads, alarmes, etc. precisam ser enviados para um destino fora da rede local (por exemplo, a Internet).

SOCKS é configurado em **Setup > Additional Controller Configuration > System Options > Network > SOCKS (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > SOCKS)**. Para obter mais informações, consulte a Ajuda online.

QoS (Qualidade do Serviço)

QoS (Qualidade do Serviço) garante um determinado nível de um recurso especificado para tráfego selecionado em uma rede. Uma rede com QoS prioriza tráfego de rede e oferece uma maior confiabilidade da rede, ao controlar a quantidade de largura de banda que um aplicativo pode usar.

As configurações de QoS são definidas em **Setup > Additional Controller Configuration > System Options > Network > QoS (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > QoS)**. Usando valores de DSCP (Differentiated Services Codepoint), o produto Axis poderá marcar tráfego de eventos/alarmes e tráfego de gerenciamento.

SNMP

O Simple Network Management Protocol (SNMP) possibilita o acesso e o gerenciamento remotos de dispositivos de rede. Uma comunidade SNMP é o grupo de dispositivos e a estação de gerenciamento que executam SNMP. Nomes de comunidades são usados para identificar grupos.

Para ativar e configurar SNMP no produto Axis, vá para a página **Setup > Additional Controller Configuration > System Options > Network > SNMP (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > SNMP)**.

Dependendo do nível de segurança necessário, selecione a versão em SNMP a ser usada.

Interceptações são usadas pelo produto Axis para enviar mensagens a um sistema de gerenciamento sobre eventos importantes e alterações de status. Selecione **Enable traps (Ativar interceptações)** e insira o endereço IP para onde a mensagem de interceptação deve ser enviada e a **Trap community (Comunidade de interceptação)** que deve receber a mensagem.

Observação

Se HTTPS estiver ativado, SNMP v1 e SNMP v2c deverão ser desativados.

Traps for SNMP v1/v2 (Interceptações para SNMP v1/v2) são usadas pelo produto Axis para enviar mensagens para um sistema de gerenciamento sobre eventos importantes e alterações de status. Selecione **Enable traps (Ativar interceptações)** e insira o endereço IP para onde a mensagem de interceptação deve ser enviada e a **Trap community (Comunidade de interceptação)** que deve receber a mensagem.

As seguintes interceptações estão disponíveis:

- Partida a frio

- Partida a quente
- Link ativo
- Falha de autenticação

SNMP v3 fornece criptografia e senhas seguras. Para usar interceptações com SNMP v3, um aplicativo de gerenciamento SNMP v3 é necessário.

Para utilizar SNMP v3, HTTPS deve estar ativado, consulte *HTTPS na página 55*. Para ativar SNMP v3, marque a caixa e forneça a senha inicial do usuário.

Observação

A senha inicial pode ser definida somente uma vez. Se a senha for perdida, o produto Axis deverá ser redefinido como o padrão de fábrica, consulte *Redefinição para as configurações padrão de fábrica na página 65*.

UPnP

O produto Axis inclui suporte a UPnP®. O UPnP está ativado por padrão e o produto é detectado automaticamente por sistemas operacionais e clientes que oferecem suporte a esse protocolo.

UPnP pode ser desativado em **Setup > Additional Controller Configuration > System Options > Network > UPnP (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > UPnP)**.

Bonjour

O produto Axis inclui suporte ao Bonjour. O Bonjour está ativado por padrão e o produto é detectado automaticamente por sistemas operacionais e clientes que oferecem suporte a esse protocolo.

O Bonjour pode ser desativado em **Setup > Additional Controller Configuration > System Options > Network > Bonjour (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > Bonjour)**.

Portas e dispositivos

Portas de E/S

O conector auxiliar no produto Axis oferece duas portas de entrada e saída configuráveis para conexão de dispositivos externos. Para obter informações sobre como conectar dispositivos externos, consulte o Guia de Instalação, disponível em *www.axis.com*

As portas de E/S são configuradas em **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Configuração > Configuração de controlador adicional > Opções do sistema > Portas e dispositivos > Portas de E/S**. Selecione a direção da porta (**Input (Entrada)** ou **Output (Saída)**). As portas podem receber nomes descritivos e seus **Normal states (Estados normais)** podem ser configurados como **Open circuit (Circuito aberto)** ou **Grounded circuit (Circuito aterrado)**.

Status das portas

A lista na página **System Options > Ports & Devices > Port Status (Opções do sistema > Portas e dispositivos > Status das portas)** mostra o status das portas de entrada e saída do produto.

Manutenção

O produto Axis oferece várias funções de manutenção. Elas estão disponíveis em **Setup > Additional Controller Configuration > System Options > Maintenance (Configuração > Configuração de controlador adicional > Opções do sistema > Manutenção)**.

Clique em **Restart (Reiniciar)** para executar uma reinicialização correta se o produto Axis não estiver se comportando como o esperado. Isso não afetará nenhuma das configurações atuais.

Observação

Uma reinicialização limpa todas as entradas no Relatório do servidor.

Clique em **Restore (Restaurar)** para redefinir a maioria das configurações para os valores padrão de fábrica. As seguintes configurações não serão afetadas:

- o protocolo de inicialização (DHCP ou estático)
- o endereço IP estático
- o roteador padrão
- a máscara de sub-rede
- a hora do sistema
- as configurações de IEEE 802.1X

Clique em **Default (Padrão)** para redefinir todas as configurações, incluindo o endereço IP, para os valores padrão de fábrica. Este botão deve ser usado com cuidado. O produto Axis também pode ser redefinido com o padrão de fábrica usando o botão de controle, consulte *Redefinição para as configurações padrão de fábrica na página 65*.

Para obter informações sobre a atualização de firmware, consulte *Como atualizar o firmware na página 67*.

Backup dos dados do aplicativo

Vá para **Setup > Create a backup (Configuração > Criar um backup)** para criar um backup dos dados do aplicativo. Os dados copiados para o backup incluem usuários, credenciais, grupos e agendamentos. Quando você cria um backup, um arquivo com os dados é salvo localmente em seu computador.

Vá para **Setup > Upload a backup (Configuração > Carregar um backup)** para usar um arquivo de backup criado anteriormente para restaurar os dados do aplicativo. Antes de carregar o arquivo de backup, é necessário restaurar as configurações padrão de fábrica do dispositivo. Para obter instruções, consulte *Redefinição para as configurações padrão de fábrica na página 65*.

Suporte

Visão geral do suporte

A página **Setup > Additional Controller Configuration > System Options > Support > Support Overview (Configuração > Configuração de controlador adicional > Opções do sistema > Suporte > Visão geral do suporte)** fornece informações sobre solução de problemas e contato, se você precisar de assistência técnica.

Consulte também *Solução de problemas na página 67*.

Visão geral do sistema

Para obter uma visão geral do status e configurações do produto Axis, vá para **Setup > Additional Controller Configuration > System Options > Support > System Overview (Configuração > Configuração de controlador adicional > Opções do sistema > Suporte > Visão geral do sistema)**. Informações que podem ser encontradas aqui incluem a versão do firmware, endereço IP, configurações de rede e segurança, as configurações de eventos, itens de log recentes.

Logs e relatórios

A página **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports (Configuração > Configuração de controlador adicional > Opções do sistema > Suporte > Logs e relatórios)** gera logs e relatórios úteis para análise do sistema e solução de problemas. Ao entrar em contato com o suporte da Axis, forneça um relatório do servidor com a sua consulta.

Log do sistema – Fornece informações sobre eventos do sistema.

Log de acesso – Lista todas as tentativas sem êxito de acessar o produto. O log de acesso também pode ser configurado para listar todas as conexões com o produto (veja abaixo).

Exibir relatório do servidor – Fornece informações sobre o status do produto em uma janela pop-up. O log de acesso é incluído automaticamente no relatório do servidor.

Baixar relatório do servidor – Cria um arquivo .zip que contém um arquivo de texto do relatório do servidor completo no formato UTF-8. Selecione a opção **Include snapshot from Live View (Incluir instantâneo da Visualização ao vivo)** para incluir um instantâneo da Live View do produto. O arquivo .zip deve sempre ser incluído nos contatos com o suporte.

Lista de parâmetros – Mostra os parâmetros do produto e suas configurações atuais. Isso pode ser útil ao solucionar problemas ou entrar em contato com o suporte da Axis.

Lista de conexões – Lista todos os clientes que atualmente estão acessando streams de mídia.

Relatório de panes – Gera um arquivo com informações de depuração. A geração do relatório poderá demorar vários minutos.

Os níveis de log para os logs do sistema e acesso são definidos em **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration (Configuração > Configuração de controlador adicional > Opções do sistema > Suporte > Logs e relatórios > Configuração)**. O log de acesso pode ser configurado para listar todas as conexões com o produto (selecione Mensagens críticas, avisos e informações).

Avançado

Scripting

Scripting permite que os usuários experientes personalizem e usem seus próprios scripts.

OBSERVAÇÃO

O uso inadequado pode causar comportamento inesperado e perda de contato com o produto Axis.

A Axis recomenda enfaticamente que você não use esta função a menos que entenda as consequências. O suporte da Axis não fornece assistência para problemas com scripts personalizados.

Para abrir o Script Editor, vá para **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Configuração > Configuração de controlador adicional > Opções do sistema > Avançado > Scripting)**. Se um script causar problemas, redefina o produto para suas configurações padrão de fábrica, consulte *página 65*.

Para obter mais informações, consulte *www.axis.com/developer*

Upload de arquivos

Arquivos, por exemplo, páginas da Web e imagens, podem ser carregados no produto Axis e usados como configurações personalizadas. Para carregar um arquivo, vá para **Setup > Additional Controller Configuration > System Options > Advanced > File Upload (Configuração > Configuração de controlador adicional > Opções do sistema > Avançado > Upload de arquivos)**.

Arquivos carregados são acessados via `http://<endereço ip>/local/<usuário>/<nome de arquivo>` onde `<usuário>` é o grupo de usuários selecionado (administrador) para o arquivo carregado.

Redefinição para as configurações padrão de fábrica

Importante

A restauração das configurações padrão de fábrica. deve ser feita com muito cuidado. Uma redefinição para os padrões de fábrica restaura todas as configurações, inclusive o endereço IP, para os valores padrão de fábrica.

Para redefinir o produto para as configurações padrão de fábrica:

1. Desconecte a alimentação do produto.
2. Mantenha o botão de controle pressionado enquanto reconecta a alimentação. Consulte *Visão geral do produto na página 4*.
3. Mantenha o botão de controle pressionado por 25 segundos até que o LED indicador de status se torne âmbar pela segunda vez.

4. Solte o botão de controle. O processo estará concluído quando o LED indicador de status tornar-se verde. O produto foi então redefinido para as configurações padrão de fábrica. Se não houver um servidor DHCP disponível na rede, o endereço IP padrão será `192.168.0.90`.
5. Use as ferramentas de software de instalação e gerenciamento, atribua um endereço IP, defina a senha e acesse o produto.

Também é possível redefinir os parâmetros para os valores padrão de fábrica através da interface Web. Vá para **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Configurar > Configuração de controlador adicional > Configurar > Opções do sistema > Manutenção)** e clique em **Default (Padrão)**.

Solução de problemas

Como verificar o firmware atual

Firmware é o software que determina a funcionalidade dos dispositivos de rede. Uma de suas primeiras ações ao solucionar um problema deve ser verificar a versão do firmware atual. A versão mais recente pode conter uma correção que soluciona seu problema específico.

A versão do firmware atual do produto Axis é exibida na página de visão geral.

Como atualizar o firmware

Importante

- Seu distribuidor reserva-se o direito de cobrar por quaisquer reparos atribuíveis à atualização com falha do usuário.
- Configurações predefinidas e personalizadas são salvas quando o firmware é atualizado (fornecendo os recursos disponíveis no novo firmware), embora isso não seja garantido pela Axis Communications AB.
- Se você instalar uma versão anterior do firmware, será necessário restaurar as configurações padrão de fábrica do produto.

Observação

- Após a conclusão do processo de atualização, o produto será reiniciado automaticamente. Se você reiniciar o produto manualmente após a atualização, aguarde 5 minutos mesmo que suspeite que a atualização tenha falhado.
- Como o banco de dados de usuários, grupos, credenciais e outros dados são atualizados após uma atualização de firmware, a primeira inicialização poderá levar alguns minutos para ser concluída. O tempo necessário depende da quantidade de dados.
- Ao atualizar o produto Axis com o último firmware, o produto receberá a última funcionalidade disponível. Sempre leia as instruções de atualização e notas de versão disponíveis com cada nova versão antes de atualizar o firmware.

Controladores de porta autônomos:

1. Baixe o último arquivo de firmware para seu computador, disponível gratuitamente em *www.axis.com/support*
2. Vá para **Setup > Additional Controller Configuration > System Options > Maintenance (Configuração > Configuração de controlador adicional > Opções do sistema > Manutenção)** nas páginas da Web do produto.
3. Em **Upgrade Server (Atualizar servidor)**, clique em **Choose file (Escolher arquivo)** e localize o arquivo em seu computador.
4. Se você desejar que o produto restaure automaticamente as configurações padrão de fábrica após a atualização, marque a caixa de seleção **Default (Padrão)**.
5. Clique em **Upgrade (Atualizar)**.
6. Aguarde aproximadamente 5 minutos enquanto o produto está sendo atualizado e reiniciado. Em seguida, desmarque o cache do navegador da Web.
7. Acesse o produto.

Controladores de porta em um sistema:

Você pode usar o AXIS Device Manager ou a AXIS Camera Station para atualizar todos os controladores de porta em um sistema. Consulte *www.axis.com* para obter mais informações.

Importante

- Não selecione atualização sequencial.

Observação

- Todos os controladores em um sistema sempre devem possuir a mesma versão de firmware.
- Atualize todos os controladores em um sistema ao mesmo tempo, usando a opção paralela no AXIS Device Manager ou na AXIS Camera Station.

Procedimento de recuperação de emergência

Se a conexão de rede ou alimentação for perdida durante a atualização, o processo falhará e o produto poderá não responder. Se o indicador de status vermelho estiver piscando, isso indicará uma falha na atualização. Para recuperar o produto, siga as etapas abaixo. O número de série está na etiqueta do produto.

1. No **UNIX/Linux**, digite o seguinte na linha de comando:

   ```
   arp -s <endereço IP> <número de série> temp
   ping -l 408 <endereço IP>
   ```

   No **Windows**, digite o seguinte em um prompt de comando/DOS (isso pode exigir que você execute o prompt de comando como um administrador):

   ```
   arp -s <endereço IP> <número de série>
   ping -l 408 -t <endereço IP>
   ```

2. Se o produto não responder em 30 segundos, reinicie e aguarde uma resposta. Pressione CTRL+C para parar o Ping.
3. Abra um navegador e digite o endereço IP do produto. Na página aberta, use o botão **Browse (Procurar)** para selecionar o arquivo de atualização a ser usado. Em seguida, clique em **Load (Carregar)** para reiniciar o processo de atualização.
4. Após a conclusão da atualização (1–10 minutos), o produto será reiniciado automaticamente e exibirá verde sólido no indicador de Status.
5. Reinstale o produto, fazendo referência ao Guia de Instalação.

Se o procedimento de recuperação de emergência não colocar o produto em funcionamento novamente, entre em contato com o suporte da Axis em *www.axis.com/support*

Sintomas, possíveis causas e ações corretivas

Problemas na atualização do firmware	
Falha na atualização do firmware	Se a atualização do firmware falhar, o produto recarregará o firmware anterior. Verifique o arquivo de firmware e tente novamente.

Problemas na configuração do endereço IP	
Ao usar ARP/Ping	Tente instalar novamente. O endereço IP deverá ser definido em dois minutos após a aplicação da alimentação ao produto. Certifique-se de que a duração do ping seja definida como 408. Para obter instruções, consulte o Guia de Instalação na página do produto em *axis.com*.
O produto está localizado em uma sub-rede diferente	Se o endereço IP destinado ao produto e o endereço IP do computador usado para acessar o produto estiverem localizados em sub-redes diferentes, você não será capaz de definir o endereço IP. Entre em contato com o administrador de rede para obter um endereço IP.

Solução de problemas

O endereço IP está sendo usado por outro dispositivo	Desconecte o produto Axis da rede. Execute o comando ping (em uma janela de comando/DOS, digite `ping` e o endereço IP do produto): • Se você receber: `Reply from <endereço IP>: bytes=32; time=10...`, isso significa que o endereço IP já pode estar sendo usado por outro dispositivo na rede. Obtenha um novo endereço IP junto ao administrador da rede e reinstale o produto. • Se você receber: `Request timed out`, isso significa que o endereço IP está disponível para uso com o produto Axis. Verifique todo o cabeamento e reinstale o produto.
Possível conflito de endereço IP com outro dispositivo na mesma sub-rede	O endereço IP estático no produto Axis é usado antes que o DHCP defina um endereço dinâmico. Isso significa que, se o mesmo endereço IP estático padrão também for usado por outro dispositivo, poderá haver problemas para acessar o produto.

O produto não pode ser acessado por um navegador

Não é possível fazer login	Quando HTTPS estiver ativado, certifique-se de que o protocolo correto (HTTP ou HTTPS) seja usado ao tentar fazer login. Talvez seja necessário digitar manualmente `http` ou `https` no campo de endereço do navegador. Se a senha do usuário root for perdida, o produto deverá ser restaurado para as configurações padrão de fábrica. Consulte *Redefinição para as configurações padrão de fábrica na página 65*.
O endereço IP foi alterado pelo DHCP	Os endereços IP obtidos de um servidor DHCP são dinâmicos e podem mudar. Se o endereço IP tiver sido alterado use o AXIS IP Utility ou o AXIS Device Manager para localizar o produto na rede. Identifique o produto usando seu modelo ou número de série ou nome de DNS (se um nome tiver sido configurado). Se necessário, um endereço IP estático poderá ser atribuído manualmente. Para obter instruções, consulte o documento *How to assign an IP address and access your device (Como atribuir um endereço IP e acessar seu dispositivo)* na página do produto em *axis.com*
Erro de certificado ao usar IEEE 802.1X	Para que a autenticação funcione corretamente, as configurações de data e hora no produto Axis deverão ser sincronizadas com um servidor NTP. Consulte *Data e hora na página 57*.

O produto está acessível local, mas não externamente

Configuração do roteador	Para configurar o roteador para permitir tráfego de dados para o produto Axis, ative o recurso NAT traversal que tentará configurar automaticamente o roteador para permitir acesso ao produto Axis, consulte *NAT traversal (mapeamento de portas) para IPv4 na página 61*. O roteador deverá oferecer suporte a UPnP®.
Proteção de firewall	Verifique o firewall da Internet junto ao administrador da rede.
Roteadores padrão necessários	Verifique se é necessário definir as configurações do roteador em **Setup > Network Settings (Configuração > Configurações de rede)** ou **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuração > Configuração de controlador adicional > Opções do sistema > Rede > TCP/IP > Básicas)**.

Status e LEDs indicadores de rede estão piscando em vermelho rapidamente

Falha de hardware	Entre em contato com seu revendedor Axis.

Produto não inicializa

Produto não inicializa	Se o produto não inicializar, mantenha o cabo de rede conectado e reinserira o cabo de alimentação no midspan.

Especificações

Conectores

Para obter informações sobre as posições dos conectores, consulte .

Para obter diagramas de conexão e informações sobre o gráfico de pinos de hardware gerado através da configuração do hardware, consulte *Diagramas de conexão na página 74* e *Configurar o hardware na página 14*.

A seção a seguir descreve as especificações técnicas dos conectores.

Conector de dados do leitor

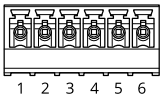
Bloco de terminais com 6 pinos e suporte aos protocolos RS485 e Wiegand para comunicação com o leitor.

As portas RS485 são compatíveis com:

- RS485 com 2 fios half duplex
- RS485 com 4 fios full duplex

As portas Wiegand são compatíveis com:

- Wiegand com 2 fios



Função		Pino	Observações
RS485	A-	1	Para RS485 full duplex Para RS485 half duplex
	B+	2	
RS485	A-	3	Para RS485 full duplex Para RS485 half duplex
	B+	4	
Wiegand	D0 (Dados 0)	5	Para Wiegand
	D1 (Dados 1)	6	

Importante

As portas RS485 possuem uma taxa de transmissão de 9600 Bit/s.

Importante

O comprimento de cabo máximo recomendado é 30 m (98,4 pés).

Importante

Os circuitos de saída nesta seção possuem potência Classe 2 limitada.

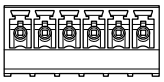
Conector de E/S do leitor

Bloco de terminais com 6 pinos para:

- Alimentação auxiliar (saída CC)
- Entrada digital

- Saída digital
- 0 VCC (-)

O pino 3 nos conectores de E/S do leitor podem ser supervisionados. Se a conexão for interrompida, um evento será ativado. Para usar entradas supervisionadas, instale resistores terminadores. Use o diagrama de conexão para entradas supervisionadas. Consulte *página 75*.



Função	Pino	Observações	Especificações
0 VCC (-)	1		0 VCC
Saída CC	2	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	12 VCC Carga máx. = 300 mA
Configurável (entrada ou saída)	3–6	Entrada digital — Conecte ao pino 1para ativar ou deixe aberta (desconectada) para desativar.	0 a 40 VCC (máx.)
		Saída digital — Conecte ao pino 1 para ativar ou deixe flutuando (desconectado) para desativar. Se usado com uma carga indutiva, por exemplo, um relé, um diodo deverá ser conectado em paralelo à carga para proporcionar proteção contra transientes de tensão.	0 a 40 VCC máx., dreno aberto, 100 mA

Importante

O comprimento de cabo máximo recomendado é 30 m (98,4 pés).

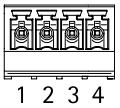
Importante

Os circuitos de saída nesta seção possuem potência Classe 2 limitada.

Conector de porta

Dois blocos de terminais com 4 pinos para monitoramento de dispositivos de portas (entrada digital).

Todos os pinos de entrada de porta podem ser supervisionados. Se a conexão for interrompida, um alarme será acionado. Para usar entradas supervisionadas, instale resistores terminadores. Use o diagrama de conexão para entradas supervisionadas. Consulte *página 75*.



Função	Pino	Observações	Especificações
0 VCC (-)	1, 3		0 VCC
Entrada	2, 4	Para comunicação com o monitor de portas. Entrada digital – Conecte ao pino 1 ou 3, respectivamente para ativar ou deixe-o flutuando (desconectado) para desativar. Observação: este pino pode ser usado somente para entrada.	0 a máx. 40 VCC

Importante

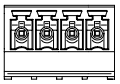
O comprimento de cabo máximo recomendado é 30 m (98,4 pés).

Conector auxiliar

Bloco de terminais de E/S configurável com 4 pinos para:

- Alimentação auxiliar (saída CC)
- Entrada digital
- Saída digital
- 0 VCC (-)

Para obter um diagrama de conexão de exemplo, consulte *Diagramas de conexão na página 74*.



Função	Pino	Observações	Especificações
0 VCC (-)	1		0 VCC
Saída CC	2	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	3,3 VCC Carga máx. = 100 mA
Configurável (entrada ou saída)	3–4	Entrada digital — Conecte ao pino 1para ativar ou deixe aberta (desconectada) para desativar.	0 a 40 VCC (máx.)
		Saída digital — Conecte ao pino 1 para ativar ou deixe flutuando (desconectado) para desativar. Se usado com uma carga indutiva, por exemplo, um relé, um diodo deverá ser conectado em paralelo à carga para proporcionar proteção contra transientes de tensão.	0 a 40 VCC máx., dreno aberto, 100 mA

Importante

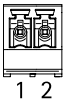
O comprimento de cabo máximo recomendado é 30 m (98,4 pés).

Importante

Os circuitos de saída nesta seção possuem potência Classe 2 limitada.

Conector de alimentação

Bloco de terminais com 2 pinos usado para entrada de alimentação CC. Use uma fonte de alimentação limitada compatível com os requisitos de tensão de segurança extra baixa (SELV) e com potência de saída nominal restrita a ≤ 100 W ou corrente de saída nominal limitada a ≤ 5 A.



Função	Pino	Observações	Especificações
0 VCC (-)	1		0 VCC
Entrada CC	2	Para controlador de alimentação sem usar Power over Ethernet. Observação: Esse pino pode ser usado somente como entrada de energia.	10 – 28 VCC, máx. 36 W Carga máxima nas saídas = 14 W

Conector de rede

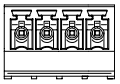
Conector Ethernet RJ45. Use cabos Category 5e ou superior.

Função	Especificações
Energia e Ethernet	Power over Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3, 44–57 VCC Carga máx. em saídas = 7,5 W

Conector de trava de alimentação

Bloco de terminais com 4 pinos para alimentar uma ou duas travas (saída CC). O conector de trava também pode ser usado para alimentar dispositivos externos.

Conecte travas e cargas aos pinos de acordo com o gráfico de pinos de hardware gerado através da configuração do hardware.



Função	Pino	Observações	Especificações
0 VCC (-)	1, 3		0 VCC
0 VCC, flutuação, ou 12 VCC	2, 4	Para controlar até duas travas de 12 V. Use o gráfico de pinos de hardware. Consulte *Configurar o hardware na página 14*.	12 VCC Carga total máx. = 500 mA

OBSERVAÇÃO

Se a trava for não polarizada, recomendamos adicionar um diodo flyback externo.

Importante

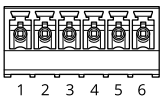
Os circuitos de saída nesta seção possuem potência Classe 2 limitada.

Conector de energia e relé

Bloco de terminais com 6 pinos e relé interno para:

- Dispositivos externos
- Alimentação auxiliar (saída CC)
- 0 VCC (-)

Conecte travas e cargas aos pinos de acordo com o gráfico de pinos de hardware gerado através da configuração do hardware.



Função	Pino	Observações	Especificações
0 VCC (-)	1, 4		0 VCC
Relé	2–3	Para conectar dispositivos de relé. Use o gráfico de pinos de hardware. Consulte *Configurar o hardware na página 14*. Os dois pinos de relé estão galvanicamente separados do resto do circuito.	Corrente máx. = 700 mA Tensão máx. = +30 VCC
12 VCC	5	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	Tensão máx. = +12 VCC Carga máx. = 500 mA
24 VCC	6	Não usado	

OBSERVAÇÃO

Se a trava for não polarizada, recomendamos adicionar um diodo flyback externo.

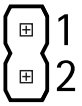
Importante

Os circuitos de saída nesta seção possuem potência Classe 2 limitada.

Conector header de pinos do alarme de violação

Dois conectores header de 2 pinos para bypass:

- Alarme de violação traseiro (TB)
- Alarme de violação frontal (TF)



Função	Pino	Observações
Alarme de violação traseiro	1–2	Para efetuar bypass do alarme de violação frontal e traseiro simultaneamente, conecte jumpers entre TB 1, TB 2 e TF 1, TF 2 respectivamente. Efetuar bypass dos alarmes de violação significa que o sistema não identificará quaisquer tentativas de violação.
Alarme de violação frontal	1–2	

Observação

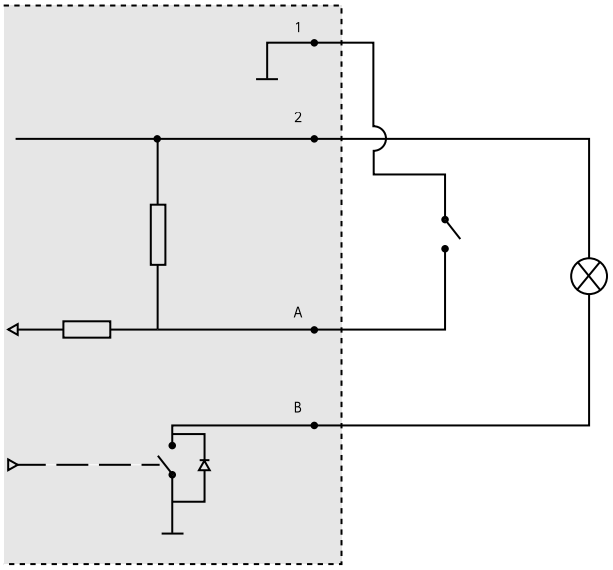
Ambos os alarmes de violação frontal e traseiro estão conectados por padrão. O acionador de abertura da caixa poderá ser configurado para executar uma ação se o controlador de porta for aberto ou removido da parede ou teto. Para obter informações sobre como configurar alarmes e eventos, consulte *Configuração de alarmes e eventos na página 46*.

Diagramas de conexão

Conecte dispositivos de acordo com o gráfico de pinos de hardware gerado através da configuração de hardware. Para obter mais informações sobre a configuração de hardware e o gráfico de pinos de hardware, consulte *Configurar o hardware na página 14*.

Especificações

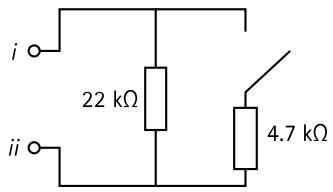
Conector auxiliar



1 *0 VCC (-)*
2 *Saída CC: 3,3 V, máx. 100 mA*
A *E/S configurada como entrada*
B *E/S configurada como saída*

Entradas supervisionadas

Para usar entradas supervisionadas, instale resistores terminadores de acordo com o diagrama abaixo.



i *Entrada*

ii *0 VCC (-)*

Observação

Recomenda-se usar cabos blindados e trançados. Conecte a blindagem a 0 VCC.

Informações sobre segurança

Níveis de perigo

⚠PERIGO

Indica uma situação perigosa que, se não evitada, irá resultar em morte ou lesões graves.

⚠AVISO

Indica uma situação perigosa que, se não evitada, poderá resultar em morte ou lesões graves.

⚠CUIDADO

Indica uma situação perigosa que, se não evitada, poderá resultar em lesões leves ou moderadas.

OBSERVAÇÃO

Indica uma situação perigosa que, se não evitada, poderá resultar em danos à propriedade.

Outros níveis de mensagens

Importante

Indica informações significativas que são essenciais para o produto funcionar corretamente.

Observação

Indica informações úteis que ajudam a obter o máximo do produto.

Manual do usuário
AXIS A1001 & AXIS Entry Manager

Ver. M25.2
Data: Dezembro 2023
Nº da peça T10010336