AXIS Secure Entry for XProtect

Manual do Usuário

Índice

Controle de acesso

O controle de acesso é uma solução que combina controle de acesso físico com videomonitoramento. Essa integração permite a configuração de um sistema de controle de acesso Axis diretamente a partir do Management Client. O sistema integra-se perfeitamente ao XProtect, permitindo que os operadores monitorem o acesso e realizem ações de controle de acesso no Smart Client.

Observação

Requisitos

- VMS versão 2024 R1 ou posterior.
- Licenças do XProtect Access, consulte *licenças de acesso*.
- Instalar o AXIS Optimizer no servidor de eventos e no Management Client.

As portas 53459 e 53461 serão abertas para tráfego de entrada (TCP) durante a instalação do AXIS Optimizer através do AXIS Secure Entry.

Configuração do controle de acesso

Observação

Antes de começar, faça o seguinte:

- Atualize o software do controlador de porta. Consulte a tabela abaixo para saber quais são as versões mínima e recomendada do AXIS OS para a sua versão do VMS.
- Confirme se a data e a hora estão corretas.

Versão do AXIS Optimizer	Versão mínima do AXIS OS	Versão recomendada do AXIS OS
5.6	12.6.94.1	12.6.94.1

Para adicionar um controlador de porta em rede Axis ao seu sistema:

1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control (Navegação no site > Axis Optimizer > Controle de acesso)**.
2. Em **Configuration (Configuração)**, selecione **Devices (Dispositivos)**.
3. Selecione **Discovered devices (Dispositivos descobertos)** para ver a lista de unidades que você pode adicionar ao sistema.
4. Selecione as unidades que deseja adicionar.
5. Clique em **+ Add (+ Adicionar)** na janela pop-up e forneça as credenciais do controlador.

Observação

Você verá os controladores adicionados na guia **Management (Gerenciamento)**.

Para adicionar manualmente um controlador ao sistema, clique em **+ Add (+ Adicionar)** na guia **Management (Gerenciamento)**.

Para integrar sua atualização ao VMS sempre que você adicionar, remover ou editar o nome de um controlador de porta:

- Vá para **Site Navigation** > **Access control(Navegação no site > Controle de acesso)** e clique na integração do controle de acesso.
- Clique em **Refresh Configuration (Atualizar configuração)** na guia **General settings (Configurações gerais)**.

Fluxo de trabalho para configurar o controle de acesso

1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control (Navegação no site > Axis Optimizer > Controle de acesso)**.
2. Para editar os perfis de identificação predefinidos ou criar um novo perfil de identificação, consulte .
3. Para usar uma configuração personalizada para formatos de cartões e tamanhos de PIN, consulte .

4. Adicione uma porta e aplique um perfil de identificação à porta. Consulte .
5. Adicione uma zona e adicione portas à zona. Consulte .

Compatibilidade do software do dispositivo para controladores de porta

Importante

Ao atualizar o AXIS OS no seu controlador de porta, lembre-se:

- **Versões do AXIS OS compatíveis:** As versões do AXIS OS compatíveis listadas acima só se aplicam quando se atualiza a partir da versão do VMS original recomendada e quando o sistema tem uma porta. Se o sistema não atender a essas condições, você deverá atualizar para a versão do AXIS OS recomendada para a versão específica do VMS.
- **Versão mínima compatível do AXIS OS:** A versão mais antiga do AXIS OS instalada no sistema determina a versão mínima suportada do AXIS OS, com um limite de duas versões anteriores.
- **Atualização para uma versão do AXIS OS superior àquela recomendada:** Suponha que você atualize para uma versão do AXIS OS superior àquela recomendada para uma versão específica do VMS. Você sempre poderá fazer downgrade e retornar para a versão recomendada do AXIS OS sem nenhum problema, desde que esteja dentro dos limites de suporte definidos para a versão do VMS.
- **Recomendações futuras do AXIS OS:** Siga sempre a versão do AXIS OS recomendada para a respectiva versão do VMS, a fim de garantir a estabilidade do sistema e total compatibilidade.

Integração do controle de acesso

Para integrar o controle de acesso ao VMS:

1. Vá para **Site Navigation** > **Access Control (Navegação no site > Controle de acesso)**.
2. Clique com o botão direito do mouse em **Access Control (Controle de acesso)** e clique em **Create new... (Criar novo...)**.
3. Na caixa de diálogo **Create Access Control System Integration (Criar integração do sistema de controle de acesso)**:
   - Insira um nome para a integração.
   - Selecione **AXIS Secure Entry** no menu suspenso em **Integration plug-in (Plug-in da integração)**.
   - Clique em **Next (Avançar)** até ver a caixa de diálogo **Associate cameras (Associar câmeras)**. Para associar câmeras a pontos de acesso de portas:
     - Clique no seu dispositivo em **Cameras (Câmeras)** para ver as listas de câmeras configuradas no sistema XProtect.
     - Selecione e arraste uma câmera até o ponto de acesso ao qual deseja associá-la.
     - Clique em **Close (Fechar)** para fechar a caixa de diálogo.

Observação

- Para obter mais informações sobre a integração do controle de acesso no XProtect, consulte *Usando controle de acesso no XProtect Smart Client*.
- Para obter mais informações sobre as propriedades de controle de acesso, como configurações gerais, portas e câmeras associadas, eventos de controle de acesso e assim por diante, consulte *Propriedades de controle de acesso*.

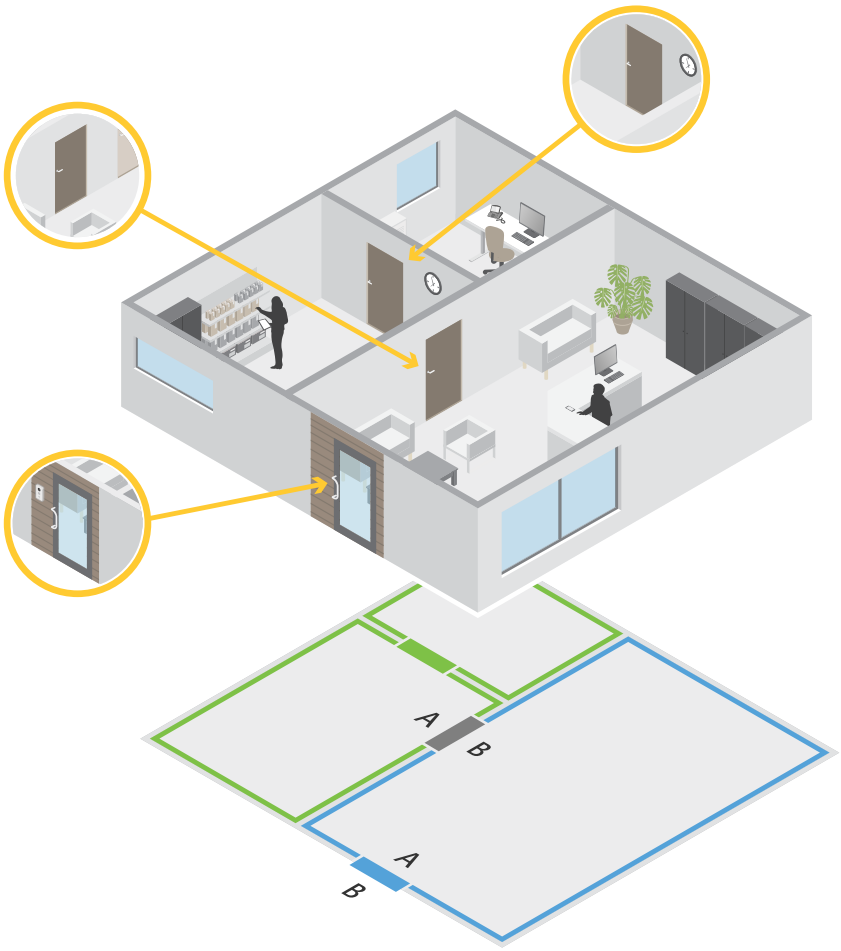
Portas e zonas

Vá para **Site Navigation** > **Axis Optimizer** >**Access control** > **Doors and zones (Navegação no site > Axis Optimizer > Controle de acesso > Portas e zonas)** para obter uma visão geral e configurar portas e zonas.

Gráfico de PIN	Exiba a tabela de pinagem do controlador associado a uma porta. Se desejar imprimir a tabela de pinagem, clique em **Print (Imprimir)**.
Identification profile: (Perfil de identificação:	Altere o perfil de identificação nas portas.
Secure Channel (Canal seguro)	Ative ou desative o OSDP Secure Channel para um leitor específico.

Portas	
Nome	O nome da porta.
Controle de porta	O controlador de porta conectado à porta.
Lado A	A zona na qual o lado A da porta está localizado.
Lado B	A zona na qual o lado B da porta está localizado.
Identification profile: (Perfil de identificação:	O perfil de identificação aplicado à porta.
Formatos de cartão e PIN	Mostra o tipo de formatos de cartões ou comprimento do PIN.
Status	O status da porta. • **Online:** A porta está online e funciona corretamente. • **Leitor offline:** O leitor na configuração da porta está offline. • **Erro do leitor:** O leitor na configuração de porta não oferece suporte a canais seguros ou o canal seguro está desativado para o leitor.
Zonas	
Nome	O nome da zona.
Número de portas	O número de portas incluídas na zona.

Exemplo de portas e zonas



- Existem duas zonas: zona verde e zona azul.
- Existem três portas: porta verde, porta azul e porta marrom.
- A porta verde é uma porta interna na zona verde.
- A porta azul é uma porta de perímetro somente para a zona azul.
- A porta marrom é uma porta de perímetro para a zona verde e a zona azul.

Adicionar uma porta

Observação

- Você pode configurar um controlador de porta com uma porta com duas fechaduras ou duas portas com uma trava cada.
- Se um controlador de porta não tiver portas e você estiver usando uma nova versão do Axis Optimizer com um software mais antigo no controlador, o sistema impedirá que você adicione uma porta. No entanto, o sistema permite novas portas em controladores de sistema com software mais antigo se já houver uma porta existente.

Criar uma configuração de porta para adicionar uma porta:

1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones (Navegação no site > Axis Optimizer > Controle de acesso > Portas e zonas)**.
2. Clique em + **Add door (Adicionar porta)**.

3. Insira um nome de porta.
4. No menu suspenso **Controller (Controlador)**, selecione um controlador de porta. O controlador fica cinza quando não é possível adicionar outra porta quando está offline ou o HTTPS não está ativo.
5. No menu suspenso **Door type (Tipo de porta)**, selecione o tipo de porta que deseja criar.
6. Clique **Next (Avançar)** para ir para a página configuração da porta.
7. Selecione uma porta de relé no menu suspenso **Primary lock (Trava principal)**.
8. Para configurar duas travas na porta, selecione uma porta de relé no menu suspenso **Secondary lock (Trava secundária)**.
9. Selecione um perfil de identificação. Consulte .
10. Configure as opções da porta. Consulte .
11. Configure uma porta com monitoramento. Consulte .
12. Clique em **Salvar**.

Copie uma configuração de porta existente para adicionar uma porta:

1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones (Navegação no site > Axis Optimizer > Controle de acesso > Portas e zonas)**.
2. Clique em **Add door (Adicionar porta)**.
3. Insira um nome de porta.
4. No menu suspenso **Controller (Controlador)**, selecione um controlador de porta.
5. Clique em **Next** (Próximo).
6. Selecione uma configuração de porta existente no menu suspenso **Copy configuration (Copia configuração)**. Ele mostra as portas conectadas, e o controlador fica cinza se for configurado com duas portas ou uma porta com duas fechaduras.
7. Altere as configurações, se desejar.
8. Clique em **Salvar**.

Para editar uma porta:

1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones** > **Doors (Navegação no site > Axis Optimizer > Controle de acesso > Portas e zonas > Portas)**.
2. Selecione uma porta na lista.
3. Clique em **Edit (Editar)**.
4. Altere as configurações e clique em **Save (Salvar)**.

Para remover uma porta:

1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones** > **Doors (Navegação no site > Axis Optimizer > Controle de acesso > Portas e zonas > Portas)**.
2. Selecione uma porta na lista.
3. Clique em **Remove (Remover)**.
4. Clique em **Sim**.

Para integrar sua atualização ao VMS sempre que você adicionar, remover ou editar o nome de uma porta:

1. Vá para **Site Navigation** > **Access control(Navegação no site > Controle de acesso)** e clique na integração do controle de acesso.
2. Clique em **Refresh Configuration (Atualizar configuração)** na guia **General settings (Configurações gerais)**.

Configurações da porta

1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones (Navegação no site > Axis Optimizer > Controle de acesso > Portas e zonas)**.
2. Selecione a porta que deseja editar.
3. Clique em **Edit (Editar)**.

Tempo de acesso (s)	Defina o número de segundos que a porta permanece destravada após o acesso ser concedido. A porta permanece destravada até a porta abrir ou até a hora definida terminar. A porta trava quando fecha mesmo quando o tempo de acesso é deixado.
Open-too-long time (sec) (Aberta por muito tempo (s))	Válido somente se você configurou um monitor de porta. Defina o número de segundos em que a porta permanece aberta. Se a porta estiver aberta quando a hora definida terminar, ela aciona o alarme de porta aberta há muito tempo. Configure uma regra de ação para definir a ação que deve ser disparada pelo evento de porta aberta há muito tempo.
Hora de acesso longa (s)	Defina o número de segundos que a porta permanece destravada após o acesso ser concedido. O tempo de acesso longo substitui o tempo de acesso para portadores de cartões com essa configuração ativada.
Long open-too-long time (sec) (Tempo de Aberta por muito tempo (s))	Válido somente se você configurou um monitor de porta. Defina o número de segundos em que a porta permanece aberta. Se a porta estiver aberta quando a hora definida terminar, ela aciona o evento de porta aberta há muito tempo. O tempo aberto por muito tempo sobrescreve o tempo aberto e longo já definido para os portadores de cartões se você ativar a configuração **Long access time (Tempo de acesso longo)**.
Tempo de retardo de novo travamento (ms)	Defina o tempo em (milissegundos) durante o qual a porta permanecerá destravada após ser aberta ou fechada.
Relock (Travar novamente)	• **After opening (Após a abertura):** Válido somente se você adicionou um monitor de porta. • **After closing (Após o fechamento):** Válido somente se você adicionou um monitor de porta.

Nível de segurança da porta

Você pode adicionar os seguintes recursos de segurança à porta:

Regra das duas pessoas – A regra das duas pessoas exige que duas pessoas utilizem uma credencial válida para obter acesso.

Dupla passagem – A dupla passagem permite que um titular de cartão substitua o estado atual de uma porta. Por exemplo, ele pode usá-la para travar ou destravar uma porta fora da programação regular, o que é mais conveniente do que entrar no sistema para destravar a porta. A dupla passagem não afeta uma programação

existente. Por exemplo, se uma porta estiver programada para travar na hora do fechamento e um funcionário sair para o intervalo de almoço, a porta ainda será travada de acordo com a programação.

Você pode configurar o nível de segurança enquanto está adicionando uma nova porta ou fazer isso em uma porta existente.

Para adicionar **Two-person rule (Regra das duas pessoas)** a uma porta existente:

1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones (Navegação no site > Axis Optimizer > Controle de acesso > Portas e zonas)**.
2. Selecione a porta para a qual deseja configurar um nível de segurança.
3. Clique em **Edit (Editar)**.
4. Clique em **Nível de segurança**.
5. Ative **Two-person rule (Regra das duas pessoas)**.
6. Clique em **Aplicar**.

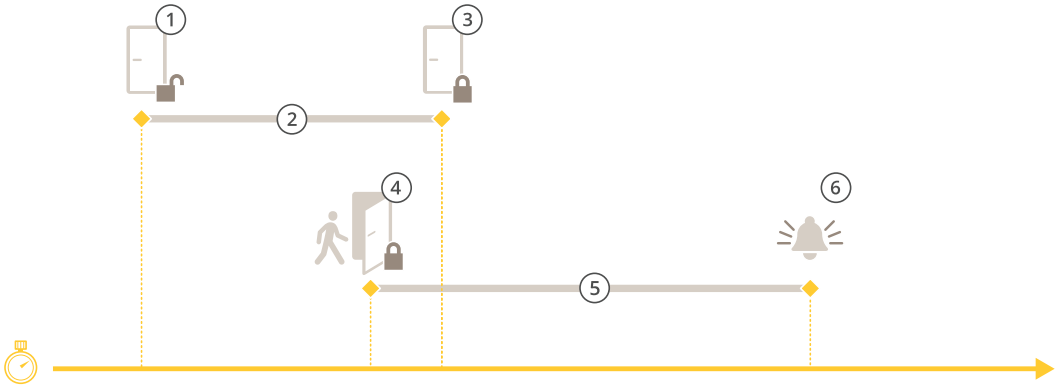
Regra das duas pessoas	
Laterais A e **B**	Selecione em quais lados da porta a regra será usada.
Programações	Selecione quando a regra estiver ativa.
Tempo limite (segundos)	O tempo limite é o tempo máximo permitido entre as passagens do cartão ou outro tipo de credencial válida.

Para adicionar **Dupla passagem** a uma porta existente:

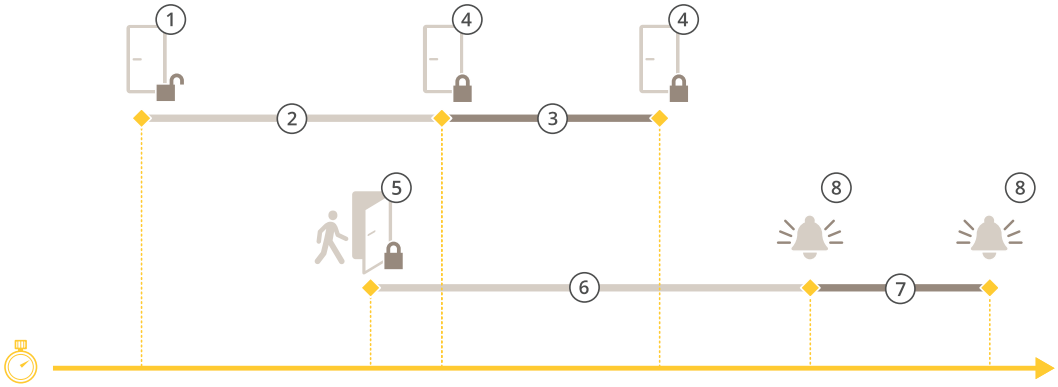
1. Vá para **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones (Navegação no site > Axis Optimizer > Controle de acesso > Portas e zonas)**.
2. Selecione a porta para a qual deseja configurar um nível de segurança.
3. Clique em **Edit (Editar)**.
4. Clique em **Nível de segurança**.
5. Ative **Double-swipe (Dupla passagem)**.
6. Clique em **Aplicar**.
7. Aplique **Double-swipe (Dupla passagem)** a um portador de cartão.
   7.1. Vá para **Cardholder management (Gerenciamento de portadores de cartões)**.
   7.2. Clique em ⋮ no portador do cartão que deseja editar e clique em **Edit (Editar)**.
   7.3. Clique em **More (Mais)**.
   7.4. Selecione **Allow double-swipe (Permitir dupla passagem)**.
   7.5. Clique em **Aplicar**.

Dupla passagem	
Tempo limite (segundos)	O tempo limite é o tempo máximo permitido entre as passagens do cartão ou outro tipo de credencial válida.

Opções de tempo



1 *Acesso concedido – a trava abre*
2 *Tempo 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 alarme de aberta há muito tempo é acionado*



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

Adicionar um monitor de porta

Um monitor de porta é um interruptor de posição de porta que monitora o estado físico de uma porta. Você pode optar por adicionar um monitor de porta à sua porta e configurar a forma de conectar os circuitos do monitor de porta.

1. Vá para a página de configuração de porta. Consulte
2. Em **Sensores**, clique em **Adicionar**.
3. Selecione **Sensor de monitor de portas**.

4. Selecione a porta de E/S à qual deseja conectar o monitor de porta.
5. Em **Door open if (Porta aberta se)**, selecione como os circuitos do monitor de porta serão conectados.
6. Para ignorar as alterações de estado da entrada digital antes de entrar em um novo estado estável, defina um horário **Debounce time (Tempo de debounce)**.
7. Para acionar um evento quando ocorre uma interrupção na conexão entre o controlador de porta e o monitor de porta, ative **Supervised input (Entrada supervisionada)**. Consulte .

Abertura da porta se	
Circuito aberto	O circuito do monitor de porta é normalmente fechado. O monitor de porta envia à porta um sinal de aberto quando o circuito está aberto. O monitor de porta envia à porta um sinal fechado quando o circuito está fechado.
Circuito fechado	O circuito do monitor de porta é normalmente aberto. O monitor de porta envia à porta um sinal de aberto quando o circuito está fechado. O monitor de porta envia à porta um sinal de fechado quando o circuito está aberto.

Adicionar uma porta com monitoramento

Uma porta com monitoramento é um tipo de porta que permite saber se ela está aberta ou fechada. Por exemplo, você pode usar esse recurso em uma porta de segurança contra incêndio que não requer trava, mas que requer que você saiba se a porta está aberta.

Uma porta com monitoramento é diferente de uma porta comum com um monitor de porta. Uma porta comum com monitor de porta suporta travas e leitores, mas requer um controlador de porta. Uma porta com monitoramento suporta um sensor de posição da porta, mas requer apenas um módulo de relé de E/S em rede conectado a um controlador de porta. Você pode conectar até cinco sensores de posição da porta a um módulo de relé de E/S em rede.

Observação

Uma porta com monitoramento requer um AXIS A9210 Network I/O Relay Module com o software mais recente, incluindo o aplicativo AXIS Monitoring Door ACAP.

Para configurar uma porta com monitoramento:

1. Faça a instalação do AXIS A9210 e atualize-o com a versão mais recente do AXIS OS.
2. Instale os sensores de posição da porta.
3. No VMS, vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas)**.
4. Clique em **Add door (Adicionar porta)**.
5. Insira um nome.
6. Em **Type (Tipo)**, selecione **Monitoring door (Porta com monitoramento)**.
7. Em **Device (Dispositivo)**, selecione o seu módulo de relé de E/S em rede.
8. Clique em **Next** (Próximo).
9. Em **Sensors (Sensores)**, clique em **+ Add (+ Adicionar)** e selecione **Door position sensor (Sensor de posição da porta)**.
10. Selecione a E/S conectada ao sensor de posição da porta.
11. Clique em **Adicionar**.

Adicionar um leitor

Você pode configurar um controlador de porta para usar dois leitores com cabos. Selecione para adicionar um leitor em um lado ou em ambos os lados de uma porta.

Se você aplicar uma configuração personalizada dos formatos de cartões ou um tamanho de PIN a um leitor, será possível vê-la em **Card formats (Formatos de cartões)** em **Configuration > Access control > Doors and zones (Configuração > Controle de acesso > Portas e zonas)**. Consulte .

1. Vá para a página de configuração de porta. Consulte .
2. Em um lado da porta, clique em **Add (Adicionar)**.
3. Selecione **Card reader (Leitor de cartões)**.
4. Selecione o **Reader type (Tipo de leitor)**.
5. Para usar uma configuração personalizada de comprimento de PIN para este leitor.
   5.1. Clique em **Advanced (Avançado)**.
   5.2. Ative **Custom PIN length (Tamanho do PIN personalizado)**.
   5.3. Defina os valores de **Min PIN length (Tamanho mínimo do PIN)**, **Max PIN length (Tamanho máximo do PIN)** e **End of PIN character (Caractere de fim de PIN)**.
6. Para usar um formato de cartão personalizado para este leitor.
   6.1. Clique em **Advanced (Avançado)**.
   6.2. Ative **Custom card formats (Formatos de cartões personalizados)**.
   6.3. Selecione os formatos de cartões que deseja usar para o leitor. Se um formato de cartão com o mesmo comprimento de bits já estiver em uso, você deverá desativá-lo primeiro. Um ícone de aviso é exibido no cliente quando a configuração do formato de cartão é diferente da configuração do sistema configurada.
7. Clique em **Adicionar**.
8. Para adicionar um leitor ao outro lado da porta, faça esse procedimento novamente.

Tipo de leitor	
OSDP RS485 half duplex	Para leitores de RS485, selecione **OSDP RS485 half duplex** e uma porta de leitor.
Wiegand	Para leitores que usam protocolos Wiegand, selecione **Wiegand** e selecione uma porta de leitor.

Wiegand	
Controle LED	Selecione **Single wire (Fio único)** ou **Dual wire (R/G) (Fio duplo (R/G))**. Leitores com controle de LED duplo usam fios diferentes para os LEDs vermelhos e verdes.
Alerta de adulteração	Selecione quando a entrada de violação do leitor estiver ativo. • **Open circuit (Circuito aberto)**: O leitor envia para a porta o sinal de violação quando o circuito está aberto. • **Closed circuit (Circuito fechado)**: O leitor envia para a porta o sinal de violação quando o circuito está fechado.

Tempo de debounce de violação	Para ignorar as alterações de estado da entrada de violação do leitor antes de entrar em um novo estado estável, defina um horário **Tamper debounce time (Tempo de debounce de violação)**.
Entrada supervisionada	Ative para acionar um evento quando houver uma interrupção na conexão entre o controlador de porta e o leitor. Consulte .

Adicionar um dispositivo REX

Você pode optar por adicionar uma solicitação para sair (REX) do dispositivo em um lado ou em ambos os lados da porta. Um dispositivo REX pode ser um sensor PIR, um botão REX ou uma barra de empurrar.

1. Vá para a página de configuração de porta. Consulte .
2. Em um lado da porta, clique em **Add (Adicionar)**.
3. Selecionar **REX device (Dispositivo REX)**.
4. Selecione a porta de E/S à qual deseja conectar o dispositivo REX. Se houver apenas uma porta disponível, ela será selecionada automaticamente.
5. Selecione qual **Action (Ação)** que será acionada quando a porta receber o sinal do REX.
6. Em **REX active (REX ativo)**, selecione a conexão dos circuitos do monitor de porta.
7. Para ignorar as alterações de estado da entrada digital antes de entrar em um novo estado estável, defina um horário **Debounce time (ms) (Tempo de debounce (ms))**.
8. Para acionar um evento quando uma interrupção na conexão entre o controlador de porta e o dispositivo REX ocorrer, ative **Supervised input (Entrada supervisionada)**. Consulte .

Ação	
Desbloquear porta	Selecione para destravar a porta quando ela receber o sinal REX.
Nenhuma	Selecione se não desejar acionar nenhuma ação quando a porta receber o sinal REX.

REX ativo	
Circuito aberto	Selecione se o circuito REX for normalmente fechado. O dispositivo REX envia o sinal quando o circuito está aberto.
Circuito fechado	Selecione se o circuito REX for normalmente aberto. O dispositivo REX envia o sinal quando o circuito está fechado.

Adicionar uma zona

Uma zona é uma área física específica com um grupo de portas. Você pode criar zonas e adicionar portas às zonas. Há dois tipos de portas:

- **Perimeter door (Porta de perímetro):** Os portadores de cartões entram ou saem da zona através desta porta.
- **Internal door (Porta interna):** Uma porta interna na zona.

Observação

Uma porta de perímetro pode pertencer a duas zonas. Uma porta interna só pode pertencer a uma zona.

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas > Zonas)**.
2. Clique em **Add zone (Adicionar zona)**.
3. Insira um nome de zona.
4. Clique em **Add door (Adicionar porta)**.
5. Selecione as portas que deseja adicionar à zona e clique em **Add (Adicionar)**.
6. A porta está configurada para ser uma porta de perímetro por padrão. Para alterá-la, selecione **Internal door (Porta interna)** no menu suspenso.
7. Uma porta de perímetro usa a lateral da porta A como entrada da zona por padrão. Para alterá-la, selecione **Leave (Deixar)** no menu suspenso.
8. Para remover uma porta da zona, selecione-a e clique em **Remove (Remover)**.
9. Clique em **Salvar**.

Para editar uma zona:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas > Zonas)**.
2. Selecione uma zona na lista.
3. Clique em **Edit (Editar)**.
4. Altere as configurações e clique em **Save (Salvar)**.

Para remover uma zona:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas > Zonas)**.
2. Selecione uma zona na lista.
3. Clique em **Remove (Remover)**.
4. Clique em **Sim**.

Nível de segurança da zona

Você pode adicionar o seguinte recurso de segurança a uma zona:

Anti-passback – Impede que as pessoas usem as mesmas credenciais que alguém que entrou em uma área antes delas. Ele impõe que uma pessoa primeiro saia da área antes de poder usar suas credenciais novamente.

Observação

- Com o anti-passback, todas as portas da zona devem ter sensores de posição da porta para que o sistema possa registrar que um usuário abriu a porta após passar o cartão.
- Se um controlador de porta ficar offline, o anti-passback funcionará desde que todas as portas da zona pertençam ao mesmo controlador de porta. No entanto, se as portas na zona pertencerem a diferentes controladores de porta que ficarem offline, o anti-passback deixará de funcionar.

Você pode configurar o nível de segurança enquanto adiciona uma nova zona ou fazer isso em uma zona existente. Para adicionar um nível de segurança a uma zona existente:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas)**.
2. Selecione a zona para a qual deseja configurar um nível de segurança.
3. Clique em **Edit (Editar)**.
4. Clique em **Nível de segurança**.
5. Ative os recursos de segurança que deseja adicionar à porta.

6. Clique em **Aplicar**.

Anti-passback	
Log violation only (Soft) (Apenas registrar violações (Soft))	Use essa opção se desejar permitir que uma segunda pessoa entre na porta usando as mesmas credenciais da primeira pessoa. Esta opção resulta somente em um alarme do sistema.
Negar acesso (Hard)	Use essa opção se desejar impedir que o segundo usuário entre na porta se estiver usando as mesmas credenciais da primeira pessoa. Esta opção resulta também em um alarme do sistema.
Tempo limite (segundos)	A quantidade de tempo até que o sistema permita que um usuário entre novamente. Insira 0 se não quiser tempo limite, o que significa que a zona terá anti-passback até que o usuário saia da zona. Use o tempo limite **0** com **Negar acesso (Hard)** apenas se todas as portas na zona tiverem leitores de ambos os lados.

Entradas supervisionadas

As entradas supervisionadas podem acionar um evento quando há interrupção na conexão com um controlador de portas.

- Conexão entre o controlador de porta e o monitor de porta. Consulte .
- Conexão entre o controlador de porta e o leitor que usa os protocolos Wiegand. Consulte .
- Conexão entre o controlador de porta e o dispositivo REX. Consulte .

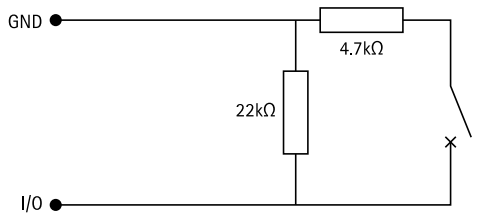
Para usar entradas supervisionadas:

1. Instale os resistores de fim de linha próximos ao dispositivo periférico conforme o possível segundo o diagrama de conexão.
2. Vá para a página de configuração de um leitor, um monitor de porta ou um dispositivo REX, ative **Supervised input (Entrada supervisionada)**.
3. Se você seguiu o diagrama de conexão paralela primeiro, selecione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Conexão paralela primeiro com um resistor paralelo de 22 KΩ e um resistor serial de 4,7 KΩ)**.
4. Se você tiver seguido o diagrama de conexão serial primeiro, selecione **Serial first connection (Conexão serial primeiro)** e selecione um valor de resistor no menu suspenso **Resistor values (Valores de resistor)**.

Diagramas de conexão

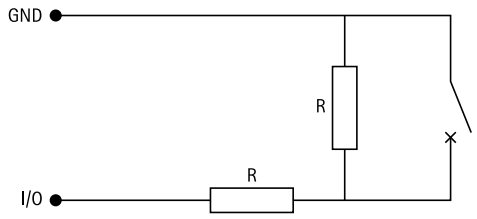
Conexão paralela primeiro

Os valores dos resistores devem ser 4,7 kΩ e 22 kΩ.



Conexão serial primeiro

Os valores dos resistores devem ser iguais e estão dentro do alcance de 1-10 kΩ.



Ações manuais

Você pode realizar as seguintes ações manual em portas e zonas:

Redefinir – Retorna às regras configuradas do sistema.

Conceder acesso – Destrava uma porta ou zona por 7 segundos e, em seguida, trava novamente.

Unlock (Destrancar) – Mantém a porta destravada até você reiniciar.

Travamento – Mantém a porta travada até que o sistema conceda acesso ao portador de um cartão.

Travamento – Ninguém entra ou sai até que você reinicie ou destrave.

Para realizar uma ação manual:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas)**.
2. Selecione a porta ou zona na qual deseja realizar uma ação manual.
3. Clique em qualquer uma das ações manuais.

Formatos de cartão e PIN

Um formato de cartão define como um cartão armazena dados. Trata-se de uma tabela de conversão entre os dados recebidos e os dados validados no sistema. Cada formato de cartão possui um conjunto de regras diferentes para como organizar as informações armazenadas. Ao definir um formato de cartão, você informa ao sistema como interpretar as informações que o controlador obtém do leitor de cartões.

Há formatos de cartões comumente usados estão disponíveis para uso como estão ou para edição conforme o necessário. Você também pode criar formatos de cartão personalizados.

Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN (Navegação no site > AXIS Optimizer > Controle de acesso > Formatos de cartão e PIN)** para criar, editar ou ativar formatos de cartões. Você também pode configurar o PIN.

Os formatos de cartões personalizados podem conter os seguintes campos de dados usados para a validação de credenciais.

Número do cartão – Um subconjunto dos dados binários da credencial codificados como números decimais ou hexadecimais. Use o número do cartão para identificar um cartão ou um portador específico.

Código da instalação – Um subconjunto dos dados binários da credencial codificados como números decimais ou hexadecimais. Use o código de instalação para identificar um cliente final ou um site específico.

Para criar um formato de cartão:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN (Navegação no site > AXIS Optimizer > Controle de acesso > Formatos de cartão e PIN)**.
2. Clique em **Add card format (Adicionar formato de cartão)**.
3. Insira um nome de formato de cartão.
4. No campo **Bit length (Comprimento de bits)**, insira um comprimento de bits entre 1 e 256.
5. Selecione **Invert bit order (Inverter ordem de bits)** se desejar inverter a ordem dos bits de dados recebidos do leitor de cartões.

6. Selecione **Invert byte order (Inverter ordem de bytes)** se desejar inverter a ordem dos bytes dos dados recebidos do leitor de cartões. Essa opção está disponível somente quando você especifica um comprimento de bits que pode ser dividido por oito.
7. Selecione e configure os campos de dados como ativos no formato do cartão. O **Card number (Número do cartão)** ou o **Facility code (Código da instalação)** devem estar ativos no formato do cartão.
8. Clique em **OK**.
9. Para ativar o formato do cartão, marque a caixa de seleção na frente do nome do formato do cartão.

Observação

- 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, somente um deles poderá estar ativo. Desativar o formato do cartão para ativar o outro.
- Você só pode ativar e desativar os formatos de cartão se o controlador de porta foi configurado com pelo menos um leitor.

ⓘ	Clique em ⓘ para ver um exemplo da saída após inverter a ordem de bits.
Alcance	Defina o intervalo de bits dos dados para o campo de dados. O intervalo deve estar dentro do que você especificou para **Bit length (Comprimento de bits)**.
Formato da saída	Selecione o formato de saída dos dados para o campo de dados. **Decimal**: Também conhecido como sistema numérico de posição de base 10, consiste nos números de 0 a 9. **Hexadecimal**: também conhecido como sistema numérico posicional de base 16, consiste em 16 símbolos únicos: os números de 0 a 9 e as letras de a a f.
Ordem de bits do subintervalo	Selecione a ordem de bits. **Little endian**: O primeiro bit é a menor (menos significativa). **Big endian**: O primeiro bit é a maior (mais significativa).

Para editar um formato de cartão:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN (Navegação no site > AXIS Optimizer > Controle de acesso > Formatos de cartão e PIN)**.
2. Selecione um formato de cartão e clique em .
3. Se você editar um formato de cartão predefinido, é possível editar **Invert bit order (Inverter ordem dos bits)** e **Invert byte order (Inverter ordem dos bytes)**.
4. Clique em **OK**.

Somente os formatos de cartões personalizados podem ser removidos. Para remover um formato de cartão personalizado:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN (Navegação no site > AXIS Optimizer > Controle de acesso > Formatos de cartão e PIN)**.
2. Selecione um formato de cartão personalizado, clique em e em **Yes (Sim)**.

Para redefinir um formato de cartão predefinido:

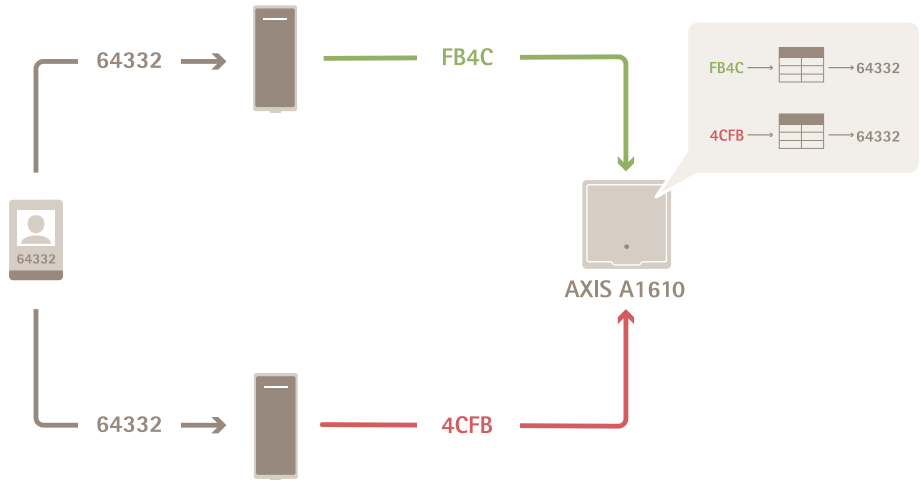
1. Vá para **Site Navigation > AXIS Optimizer > Access control > Card formats and PIN (Navegação no site > AXIS Optimizer > Controle de acesso > Formatos de cartão e PIN)**.
2. Clique em para redefinir um formato de cartão para o mapa de campos padrão.

Para configurar o tamanho do PIN:

1. Vá para **Site Navigation > AXIS Optimizer > Access control > Card formats and PIN (Navegação no site > AXIS Optimizer > Controle de acesso > Formatos de cartão e PIN)**.
2. Em **PIN configuration (Configuração do PIN)**, clique em .
3. Especifique os valores de **Min PIN length (Tamanho mínimo do PIN)**, **Max PIN length (Tamanho máximo do PIN)** e **End of PIN character (Caractere de fim de PIN)**.
4. Clique em **OK**.

Configurações de formato de cartão

Visão geral



- O número do cartão em decimal é `64332`.
- Um leitor transfere o número do cartão para o número hexadecimal `FB4C`. O outro leitor o transfere para o número hexadecimal `4CFB`.
- O AXIS A1610 Network Door Controller recebe o `FB4C` e o transfere para o número decimal `64332` de acordo com as configurações de formato de cartão no leitor.
- O AXIS A1610 Network Door Controller recebe o `4CFB`, o altera para `FB4C` invertendo a ordem dos bytes e o transfere para o número decimal `64332` de acordo com as configurações de formato de cartão no leitor.

Inverter ordem de bits

Após a inversão da ordem de bits, os dados do cartão recebidos do leitor são lidos da direita para a esquerda.

Inverter ordem de bytes

Um grupo de oito bits é um byte. Após a inversão da ordem de bytes, os dados do cartão recebidos do leitor são lidos da direita para a esquerda byte a byte.

Formato de cartão Wiegand padrão de 26 bits

1 *Paridade líder*
2 *Código da instalação*
3 *Número do cartão*
4 *Paridade final*

Perfis de identificação

Um perfil de identificação é uma combinação de tipos de identificação e agendamentos. Você pode aplicar um perfil de identificação a uma ou mais portas para definir como e quando um titular de cartão pode acessar uma porta.

Os tipos de identificação são portadores das informações de credencial necessárias para acessar uma porta. Tipos de identificação comuns são tokens, números de identificação pessoal (PINs), impressões digitais, mapas faciais e dispositivos REX. Um tipo de identificação pode possuir um ou mais tipos de informações.

As programações, também conhecidas como **Perfis de tempo**, são criadas no Management Client. Para configurar perfis de tempo, consulte *Perfis de tempo (explicação)*.

Os tipos de identificação aceitos são: Cartão, PIN e REX.

Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles (Navegação no site > AXIS Optimizer > Controle de acesso > Perfis de identificação)**.

Há cinco perfis de identificação padrão disponíveis para serem usados como estão ou editá-los conforme o necessário.

Cartão – Os portadores de cartões precisam deslizar o cartão para acessar a porta.

Cartão e PIN – Os portadores de cartões precisam deslizar o cartão e digitar o PIN para acessar a porta.

PIN – Os portadores de cartões precisam digitar o PIN para acessar a porta.

Cartão ou PIN – Os portadores de cartões precisam deslizar o cartão ou digitar o PIN para acessar a porta.

Placa de licença – Os portadores de cartões devem dirigir em direção à câmera em um veículo com placa de licença aprovada.

Para criar um perfil de identificação:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles (Navegação no site > AXIS Optimizer > Controle de acesso > Perfis de identificação)**.
2. Clique em **Create identification profile (Criar perfil de identificação)**.
3. Digite um nome para o perfil de identificação.
4. Selecione **Include facility code for card validation (Incluir código da instalação para validação do cartão)** para usar o código da instalação como um dos campos de validação da credencial. Este campo

estará disponível somente se você tiver ativado **Facility code (Código da instalação)** em **Access management > Settings (Gerenciamento de acesso > Configurações)**.

5. Configure o perfil de identificação para um lado da porta.
6. No outro lado da porta, repita as etapas anteriores.
7. Clique em **OK**.

Para editar um perfil de identificação:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles (Navegação no site > AXIS Optimizer > Controle de acesso > Perfis de identificação)**.
2. Selecione um perfil de identificação e clique em .
3. Para alterar o nome do perfil de identificação, digite um novo nome.
4. Faça suas edições na lateral da porta.
5. Para editar o perfil de identificação no outro lado da porta, repita as etapas anteriores.
6. Clique em **OK**.

Para remover um perfil de identificação:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles (Navegação no site > AXIS Optimizer > Controle de acesso > Perfis de identificação)**.
2. Selecione um perfil de identificação e clique em .
3. Se o perfil de identificação é usado em uma porta, selecione outro perfil de identificação para a porta.
4. Clique em **OK**.

Editar perfil de identificação	
×	Para remover um tipo de identificação e o cronograma relacionado.
Tipo de identificação	Para alterar um tipo de identificação, selecione um ou mais tipos no menu suspenso **Identification type (Tipo de identificação)**.
Programação	Para alterar um cronograma, selecione um ou mais agendamentos no menu suspenso **Schedule (Cronograma)**.
+ **Adicionar**	Adicione um tipo de identificação e o cronograma relacionado, clique em **Add (Adicionar)** e defina os tipos de identificação e cronogramas.

Comunicação criptografada

OSDP Secure Channel

O Secure Entry é compatível com o OSDP (Open Supervised Device Protocol) Secure Channel para criptografia de linha ativa entre o controlador e os leitores Axis.

Para ativar o OSDP Secure Channel para todo um sistema:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Encrypted communication (Navegação no site > AXIS Optimizer > Controle de acesso > Comunicação criptografada)**.
2. Insira sua chave de criptografia principal e clique em **OK**.

3. Ative o **OSDP Secure Channel**. Essa opção está disponível somente após você inserir a chave de criptografia principal.
4. Por padrão, a chave de criptografia principal gera uma chave do OSDP Secure Channel. Para definir manualmente a chave do OSDP Secure Channel:
   4.1. Em **OSDP Secure Channel**, clique em .
   4.2. Desmarque a opção **Use main encryption key to generate OSDP Secure Channel key (Usar a chave de criptografia principal para gerar a chave OSDP Secure Channel)**.
   4.3. Insira a chave do OSDP Secure Channel e clique em **OK**.

Para ativar ou desativar o OSDP Secure Channel para um leitor específico, consulte *Portas e zonas)*.

Multisservidor BETA

Os subservidores conectados podem, com multisservidor, usar os portadores de cartão globais e grupos de portadores de cartão pelo servidor principal.

Observação

- Um sistema pode comportar até 64 subservidores.
- Isso requer que o servidor principal e os subservidores estejam na mesma rede.
- No servidor principal e nos subservidores, certifique-se de configurar o Firewall do Windows para permitir conexões TCP de entrada na porta de entrada segura. A porta padrão é 53461.

Fluxo de trabalho

1. Configure um servidor como um subservidor e gere o arquivo de configuração. Consulte .
2. Configure um servidor como um servidor principal e importe o arquivo de configuração dos subservidores. Consulte .
3. Configure os portadores e grupos de portadores de cartões globais no servidor principal. Consulte e .
4. Exiba e monitore portadores e grupos de portadores globais do subservidor. Consulte .

Gerar o arquivo de configuração do subservidor

1. No subservidor, vá para **AXIS Optimizer** > **Access control** > **Multi server (AXIS Optimizer > Controle de acesso > Multisservidor)**.
2. Clique em **Sub server (Subservidor)**.
3. Clique em **Generate logs (Gerar logs)**. Isso gera um arquivo de configuração no formato.json.
4. Clique em **Download (Baixar)** e escolha um local para salvar o arquivo.

Importar o arquivo de configuração para o servidor principal

1. No servidor principal, vá para **AXIS Optimizer** > **Access control** > **Multi server (AXIS Optimizer > Controle de acesso > Multisservidor)**.
2. Clique em **Main server (Servidor principal)**.
3. Clique em **+ Add (Adicionar)** e vá para o arquivo de configuração gerado a partir do subservidor.
4. Insira o nome do servidor, o endereço IP e o número da porta do subservidor.
5. Clique em **Import (Importar)** para adicionar o subservidor.
6. O estado do subservidor mostra `Connected`.

Revogar um subservidor

Você só pode revogar um subservidor antes de importar o arquivo de configuração para um servidor principal.

1. No servidor principal, vá para **AXIS Optimizer** > **Access control** > **Multi server (AXIS Optimizer > Controle de acesso > Multisservidor)**.
2. Clique em **Sub server (Subservidor)**e em **Revoke server (Revogar servidor)**.
   Agora você poderá configurar este servidor como um servidor principal ou um subservidor.

Remover um subservidor

Após importar o arquivo de configuração de um subservidor, o subservidor será conectado ao servidor principal.

Para remover um subservidor:

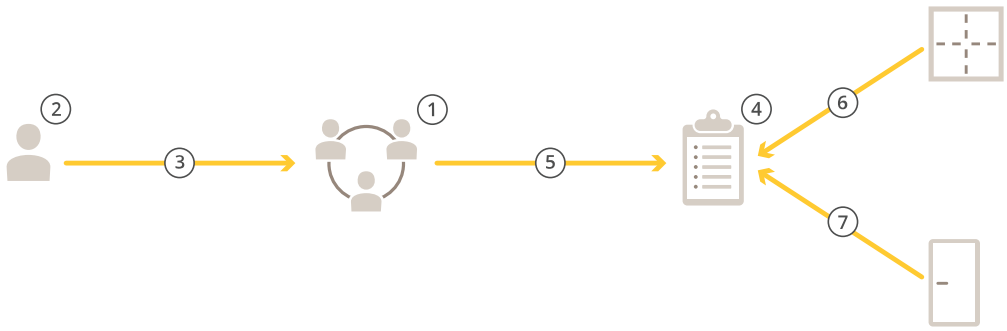
1. No servidor principal:
   1.1. Vá para **Access management** > **Dashboard (Gerenciamento de acesso > Painel)**.
   1.2. Altere os titulares e grupos de cartões globais para portadores de cartões locais e grupos.
   1.3. Vá para **AXIS Optimizer** > **Access control** > **Multi server (AXIS Optimizer > Controle de acesso > Multisservidor)**.
   1.4. Clique em **Main server (Servidor principal)** para mostrar a lista de subservidores.
   1.5. Selecione o subservidor e clique em **Delete (Excluir)**.
2. No subservidor:
   – Vá para **AXIS Optimizer** > **Access control** > **Multi server (AXIS Optimizer > Controle de acesso > Multisservidor)**.
   – Clique em **Sub server (Subservidor)**e **Revoke server (Revogar servidor)**.

Gerenciamento de acesso

A guia Access Management (Gerenciamento de acesso) permite configurar e gerenciar portadores de cartões, grupos e regras de acesso.

Fluxo de trabalho do gerenciamento de acesso

A estrutura de gerenciamento de acesso é flexível, que permite desenvolver um fluxo de trabalho adequado às suas necessidades. A seguir está um exemplo de fluxo de trabalho:



1. Adicione grupos. Consulte .
2. Adicione portadores de cartões. Consulte .
3. Adicione portadores de cartões a grupos.
4. Adicione regras de acesso. Consulte .
5. Aplique grupos a regras de acesso.
6. Aplique zonas a regras de acesso.
7. Aplique portas a regras de acesso.

Adicionar um portador de cartão

Um portador de cartão é uma pessoa com um ID exclusivo registrado no sistema. Configure um titular de cartão com credenciais que identifique a pessoa e quando e como conceder acesso à pessoa às portas.

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management (Navegação no site > AXIS Optimizer > Controle de acesso > Gerenciamento de portadores de cartões)**.
2. Vá para **Cardholders (Portadores de cartões)** e clique em **+ Add (+ Adicionar)**.
3. Insira o nome e o sobrenome do portador do cartão e clique em **Next (Avançar)**.
4. Opcionalmente, clique em **Advanced (Avançado)** e selecione as opções desejadas.
5. Adicione uma credencial ao portador do cartão. Consulte
6. Clique em **Salvar**.
7. Adicionar o portador do cartão a um grupo.
   7.1. Em **Groups (Grupos)**, selecione o grupo ao qual deseja adicionar o portador do cartão e clique em **Edit (Editar)**.
   7.2. Clique em **+ Add (+ Adicionar)** e selecione o portador do cartão que deseja adicionar ao grupo. Você pode selecionar vários portadores de cartões.
   7.3. Clique em **Adicionar**.
   7.4. Clique em **Salvar**.

Avançada	
Tempo de acesso longo	Selecione para permitir que o titular do cartão tenha um tempo de acesso longo e tempo muito aberto e longo quando houver um monitor de porta instalado.
Suspender portador de cartão	Selecione para suspender o titular do cartão.
Permitir dupla passagem	Selecione para permitir que o portador do cartão anule o estado atual de uma porta. Por exemplo, ele podem usá-la para destravar uma porta fora da programação regular.
Isenta de bloqueio	Selecione para permitir que o titular do cartão tenha acesso durante o bloqueio.
Exempt from anti-passback (Isenta de antirretorno)	Selecione para dar a um titular de cartão uma isenção da regra antirretorno. O antirretorno impede que as pessoas usem as mesmas credenciais que alguém que entrou em uma área antes delas. A primeira pessoa deverá primeiro sair da área antes que suas credenciais possam ser usadas novamente.
Portador de cartão global	Selecione para possibilitar a exibição e o monitor do titular do cartão nos subservidores. Essa opção está disponível somente para portadores de cartões criados no servidor principal. Consulte .

Adicionar credenciais

Você pode adicionar os seguintes tipos de credenciais a um portador de cartão:

- PIN
- Cartão
- Placa de licença

- Telefone celular

Para adicionar uma credencial de placa de licença a um portador de cartão:

1. Em **Credentials (Credenciais)**, clique em **+ Add (+ Adicionar)** e selecione **License plate (Placa de licença)**.
2. Insira um nome de credencial que descreva o veículo.
3. Insira o número da placa de licença do veículo.
4. Defina a data de início e término da credencial.
5. Clique em **Adicionar**.

Veja um exemplo em .

Para adicionar uma credencial de PIN a um portador de cartão:

1. Em **Credentials (Credenciais)**, clique em **+ Add (+ Adicionar)** e selecione **PIN**.
2. Insira um PIN.
3. Para usar um PIN de emergência para acionar um alarme silencioso, ative **Duress PIN (PIN de emergência)** e insira um PIN de emergência.
4. Clique em **Adicionar**.

Uma credencial de PIN é sempre válida. Você também pode configurar um PIN de emergência que abra a porta e dispare um alarme silencioso no sistema.

Para adicionar uma credencial de cartão a um portador de cartão:

1. Em **Credentials (Credenciais)**, clique em **+ Add (+ Adicionar)** e selecione **Card (Cartão)**.
2. Para inserir manualmente os dados do cartão, insira um nome de cartão, um número de cartão e um comprimento de bits.

Observação

O comprimento de bits só pode ser configurado quando você cria um formato de cartão com um comprimento de bits específico que não está no sistema.

3. Para obter automaticamente os dados dos cartões com o último cartão utilizado:
   3.1. Selecione uma porta no menu suspenso **Select reader (Selecionar leitor)**.
   3.2. Passe o cartão no leitor conectado a essa porta.
   3.3. Clique em **Get last swiped card data from the door's reader(s) (Obter os dados do último cartão utilizado nos leitores da porta)**.
4. Insira um código de local. Este campo estará disponível somente se você tiver ativado **Facility code (Código da instalação)** em **Access management > Settings (Gerenciamento de acesso > Configurações)**.
5. Defina a data de início e término da credencial.
6. Clique em **Adicionar**.

Data de expiração	
Válido de	Defina uma data e hora para quando a credencial deve ser válida.
Válido até	Selecione uma opção no menu suspenso.

Válido até	
Sem data de término	A credencial nunca expira.
Data	Defina uma data e hora em que a credencial expira.

Válido até	
Desde o primeiro uso	Selecione em quanto tempo a credencial expira após o primeiro uso. Selecione os dias, os meses, os anos ou o número de vezes após o primeiro uso.
Desde o último uso	Selecione em quanto tempo a credencial expira após o último uso. Selecione dias, meses ou anos após o último uso.

Usar o número de placa de licença como credencial

Esse exemplo mostra como usar um controlador de porta, uma câmera com o AXIS License Plate Verifier e o número de placa de licença de um veículo como credenciais para conceder acesso.

1. Adicione o controlador de porta e a câmera ao AXIS Secure Entry for XProtect.
2. Defina a data e a hora para os novos dispositivos com a opção **Synchronize with server computer time (Sincronizar com a data/hora do computador servidor)**.
3. Atualize o software nos novos dispositivos para a versão mais recente disponível.
4. Adicione uma nova porta conectada ao seu controlador de porta. Consulte .
   4.1. Adicione um leitor em **Side A (Lado A)**. Consulte .
   4.2. Em **Door settings (Configurações da porta)**, selecione **AXIS License Plate Verifier** como **Reader type (Tipo de leitor)** e insira um nome para o leitor.
   4.3. Opcionalmente, adicione um dispositivo leitor ou REX em **Side B (Lado B)**.
   4.4. Clique em **OK**.
5. Instale e ative o AXIS License Plate Verifier em sua câmera. Consulte o *Manual do usuário do AXIS License Plate Verifier*.
6. Inicie o AXIS License Plate Verifier.
7. Configure o AXIS License Plate Verifier.
   7.1. Vá para **Configuration > Access control > Encrypted communication (Configuração > Controle de acesso > Comunicação criptografada)**.
   7.2. Em **External Peripheral Authentication Key (Chave de autenticação de periférico externo)**, clique em **Show authentication key (Mostrar chave de autenticação)** e em **Copy key (Copiar chave)**.
   7.3. Abra o AXIS License Plate Verifier na interface Web da câmera.
   7.4. Não faça a configuração.
   7.5. Vá para **Settings (Configurações)**.
   7.6. Em **Access control (Controle de acesso)**, selecione **Secure Entry** como **Type (Tipo)**.
   7.7. Em **IP address (Endereço IP)**, insira o endereço do controlador de porta.
   7.8. Em **Authentication key (Chave de autenticação)**, cole a chave de autenticação que você copiou antes.
   7.9. Clique em **Conectar**.
   7.10. Em **Door controller name (Nome do controlador de porta)**, selecione seu controlador de porta.
   7.11. Em **Reader name (Nome do leitor)**, selecione o leitor que você adicionou anteriormente.
   7.12. Ative a integração.
8. Adicione o portador de cartão ao qual você deseja conceder acesso. Consulte .
9. Adicione as credenciais da placa de licença ao novo titular do cartão. Consulte .
10. Adicione uma regra de acesso. Consulte .

10.1. Adicionar um cronograma.

10.2. Adicione o portador de cartão ao qual você deseja conceder acesso à placa de licença.

10.3. Adicione a porta com o leitor do AXIS License Plate Verifier.

Adicionar um grupo

Grupos permitem que você portadores de cartões e suas regras de acesso de forma coletiva e eficiente.

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management (Navegação no site > AXIS Optimizer > Controle de acesso > Gerenciamento de portadores de cartões)**.
2. Vá para **Groups (Grupos)** e clique em **+ Add (+ Adicionar)**.
3. Insira um nome e, opcionalmente, as iniciais do grupo.
4. Selecione **Global group (Grupo global)** para permitir a visualização e o monitoramento do titular do cartão nos subservidores. Essa opção está disponível somente para portadores de cartões criados no servidor principal. Consulte .
5. Adicione portadores de cartões ao grupo:
   5.1. Clique em **+ Adicionar**.
   5.2. Selecione os portadores de cartões que deseja adicionar e clique em **Add (Adicionar)**.
6. Clique em **Salvar**.

Adicionar uma regra de acesso

Uma regra de acesso define as condições que devem ser atendidas para o acesso ser concedido.

Uma regra de acesso consiste em:

Portadores de cartões e grupos de portadores de cartões – a quem conceder acesso.

Portas e zonas – onde o acesso se aplica.

Programações – quando conceder acesso.

Para adicionar uma regra de acesso:

1. Vá para **Access control** > **Cardholder management (Controle de acesso > Gerenciamento de portadores de cartões)**.
2. Em **Access rules (Regras de acesso)**, clique em **+ Add (+ Adicionar)**.
3. Insira um nome para a regra de acesso e clique em **Next (Avançar)**.
4. Configure os titulares e os grupos do cartão:
   4.1. Em **Cardholders (Portadores de cartões)** ou **Groups (Grupos)**, clique em **+ Add (+ Adicionar)**.
   4.2. Selecione os portadores de cartões ou grupos e clique em **Add (Adicionar)**.
5. Configurar as portas e as zonas:
   5.1. Em **Doors (Portas)** ou **Zones (Zonas)**, clique em **+ Add (+ Adicionar)**.
   5.2. Selecione as portas ou zonas e clique em **Add (Adicionar)**.
6. Configure os cronogramas:
   6.1. Em **Schedules (Programações)**, clique em **Add (+ Adicionar)**.
   6.2. Selecione uma ou mais programações e clique em **Add (Adicionar)**.
7. Clique em **Salvar**.

Uma regra de acesso que não contenha um ou mais dos componentes descritos acima está incompleta. Você pode exibir todas as regras de acesso incompletas na guia **Incomplete (Incompleto)**.

Destravar portas e zonas manualmente

Para obter informações sobre ações manuais, como destravar manualmente uma porta, consulte .

Para obter informações sobre ações manuais, como destravar manualmente uma zona, consulte .

Exportar relatórios de configuração do sistema

Você pode exportar relatórios que contêm diferentes tipos de informações sobre o sistema. O AXIS Secure Entry for XProtect exporta o relatório como um arquivo de valores separados por vírgulas (CSV) e o salva na pasta de download padrão. Para exportar um relatório:

1. Vá para **Reports** > **System configuration (Relatórios > Configuração do sistema)**.
2. Selecione os relatórios que deseja exportar e clique em **Download (Baixar)**.

Cardholders details (Detalhes dos portadores de cartões)	Inclui informações sobre os portadores de cartões, credenciais, validação do cartão e última transação.
Cardholders access (Acesso dos portadores de cartões)	Inclui informações de portadores de cartões e informações sobre os grupos de portadores de cartões, regras de acesso, portas e zonas relacionados ao portador de cartão.
Cardholders group access (Acesso de grupos de portadores de cartões)	Inclui o nome do grupo de portadores de cartões e informações sobre os portadores de cartões, regras de acesso, portas e zonas relacionados ao grupo de portadores de cartões.
Regra de acesso	Inclui o nome da regra de acesso e informações sobre os portadores de cartões, grupos de portadores de cartões, portas e zonas relacionados à regra de acesso.
Door access (Acesso à porta)	Inclui o nome da porta e informações sobre os portadores de cartões, grupos de portadores de cartões, regras de acesso e zonas relacionados à porta.
Zone access (Acesso à zona)	Inclui o nome da zona e informações sobre os portadores de cartões, grupos de portadores de cartões, regras de acesso e portas relacionados à zona.

Criar relatórios de atividade de portadores de cartões

Um relatório de lista de presença lista os portadores de cartões dentro de uma zona específica, ajudando a identificar quem está presente em um determinado momento.

Um relatório de conferência lista os portadores de cartões dentro de uma zona específica, ajudando a identificar quem está seguro e quem está ausente durante emergências. Ajuda os gestores de edifícios a localizar funcionários e visitantes após evacuações. Um ponto de conferência é um leitor designado onde o pessoal se reúne durante emergências, gerando um relatório das pessoas que estão dentro e fora do site. O sistema marca os portadores de cartões como ausentes até que eles se apresentem em um ponto de conferência ou até que alguém os marque manualmente como seguros.

Tanto os relatórios de lista de presença quanto os de conferência exigem zonas para rastrear os portadores dos cartões.

Para criar e executar um relatório de lista de presença ou de conferência:

1. Vá para **Reports** > **Cardholder activity (Relatórios > Atividade do portador do cartão)**.

2. Clique em **+ Add (+ Adicionar)** e selecione **Roll call / Mustering (Lista de presença/conferência)**.
3. Insira um nome para o relatório.
4. Selecione quais zonas incluir no relatório.
5. Selecione os grupos que deseja incluir no relatório.
6. Se desejar um relatório de conferência, selecione **Mustering point (Ponto de conferência)** e um leitor para o ponto de conferência.
7. Selecione um período de tempo para o relatório.
8. Clique em **Salvar**.
9. Selecione o relatório e clique em **Run (Executar)**.

Estado do relatório de lista de presença	Descrição
Present (Presente)	O portador do cartão entrou na zona especificada e não saiu até o momento da execução do relatório.
Not present (Não presente)	O portador do cartão saiu da zona especificada e não entrou novamente até o momento da execução do relatório.

Estado do relatório de conferência	Descrição
Safe (Seguro)	O portador do cartão passou o cartão no ponto de conferência.
Ausente	O portador do cartão não passou o cartão no ponto de conferência.

Configurações de gerenciamento de acesso

Para personalizar os campos de portadores de cartões usados no painel de gerenciamento de acesso:

1. Na guia **Access management (Gerenciamento de acesso)**, clique em **Settings** > **Custom cardholder fields (Configurações > Campos personalizados de portador de cartão)**.
2. Clique em **+ Add (+ Adicionar)** e insira um nome. Você pode adicionar até 6 campos personalizados.
3. Clique em **Adicionar**.

Para usar o código de instalação para verificar seu sistema de controle de acesso:

1. Na guia **Access management (Gerenciamento de acesso)**, clique em **Settings** > **Facility code (Configurações > Código da instalação)**.
2. Selecione **Facility code on (Código da instalação em)**.

Observação

Você também deve selecionar **Incluir código da instalação para validação** de cartões ao configurar perfis de identificação. Consulte .

Importação e exportação

Importar portadores de cartões

Essa opção importa portadores de cartões, grupos de portadores, credenciais e fotos de portadores de um arquivo CSV. Para importar fotos de portadores de cartões, certifique-se de que o servidor tenha acesso às fotos.

Quando você importa portadores de cartões, o sistema de gerenciamento de acesso salva automaticamente a configuração do sistema, incluindo toda a configuração do hardware, e exclui qualquer configuração salva anteriormente.

Opções de importação	
Novo	Essa opção remove os portadores existentes e adiciona novos portadores de cartões.
ATUALIZAR	Esta opção atualiza os portadores existentes e adiciona novos portadores de cartões.
Adicionar	Essa opção mantém os portadores existentes e adiciona novos portadores de cartões. Os números do cartão e os IDs dos portadores de cartões são únicos e só podem ser usados uma vez.

1. Na guia **Access management (Gerenciamento de acesso)**, clique em **Import and export (Importar e exportar)**.
2. Clique em **Import cardholders (Importar portadores de cartões)**.
3. Selecione **New (Novo)**, **Update (Atualizar)** ou **Add (Adicionar)**.
4. Clique em **Next** (Próximo).
5. Clique em **Choose a file (Escolher um arquivo)** e vá para o arquivo CSV. Clique em **Open (Abrir)**.
6. Insira um delimitador de coluna, selecione um identificador exclusivo e clique em **Next (Avançar)**.
7. Atribua um título a cada coluna.
8. Clique em **Import (Importar)**.

Configurações de importação	
A primeira linha é o cabeçalho	Selecione se o arquivo CSV contém um cabeçalho de coluna.
Delimitador de coluna	Insira um formato de delimitador de coluna para o arquivo CSV.
Identificador exclusivo	O sistema usa **Cardholder ID (ID de portador de cartão)** para identificar um portador de cartão por padrão. Você também pode usar o nome e o sobrenome ou o endereço de email. O identificador exclusivo impede a importação de registros de pessoas duplicados.
Formato do número do cartão	**Allow both hexadecimal and number (Permitir tanto hexadecimal quanto número)** sejam selecionados por padrão.

Exportar portadores de cartões

Esta opção exporta os dados de portadores de cartão no sistema para um arquivo CSV.

1. Na guia **Access management (Gerenciamento de acesso)**, clique em **Import and export (Importar e exportar)**.
2. Clique em **Export cardholders (Exportar portadores de cartões)**.
3. Escolha um local de download e clique em **Save (Salvar)**.

O AXIS Secure Entry for XProtect atualiza as fotos dos portadores de cartões em `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` sempre que a configuração é alterada.

Desfazer importação

O sistema salva automaticamente suas configurações quando você importa portadores de cartões. A opção **Undo import (Desfazer importação)** redefine os dados de portadores de cartões e todas as configurações de hardware para o estado anterior à última importação de portadores de cartões.

1. Na guia **Access management (Gerenciamento de acesso)**, clique em **Import and export (Importar e exportar)**.
2. Clique em **Undo import (Desfazer importação)**.
3. Clique em **Sim**.

Fazer backup e restaurar

Os backups automáticos são realizados todas as noites. Os três arquivos de backup mais recentes são armazenados em C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup. Para restaurar esses arquivos:

1. Mova o arquivo de backup para C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry \restore.
2. Reinicie o AXIS Secure Entry usando um destes métodos:
   - Inicie o programa MSC (Serviços), localize o "AXIS Optimizer Secure Entry Service" e reinicie.
   - Reinicie o computador.

T10234037_pt

2025-10 (M3.2)