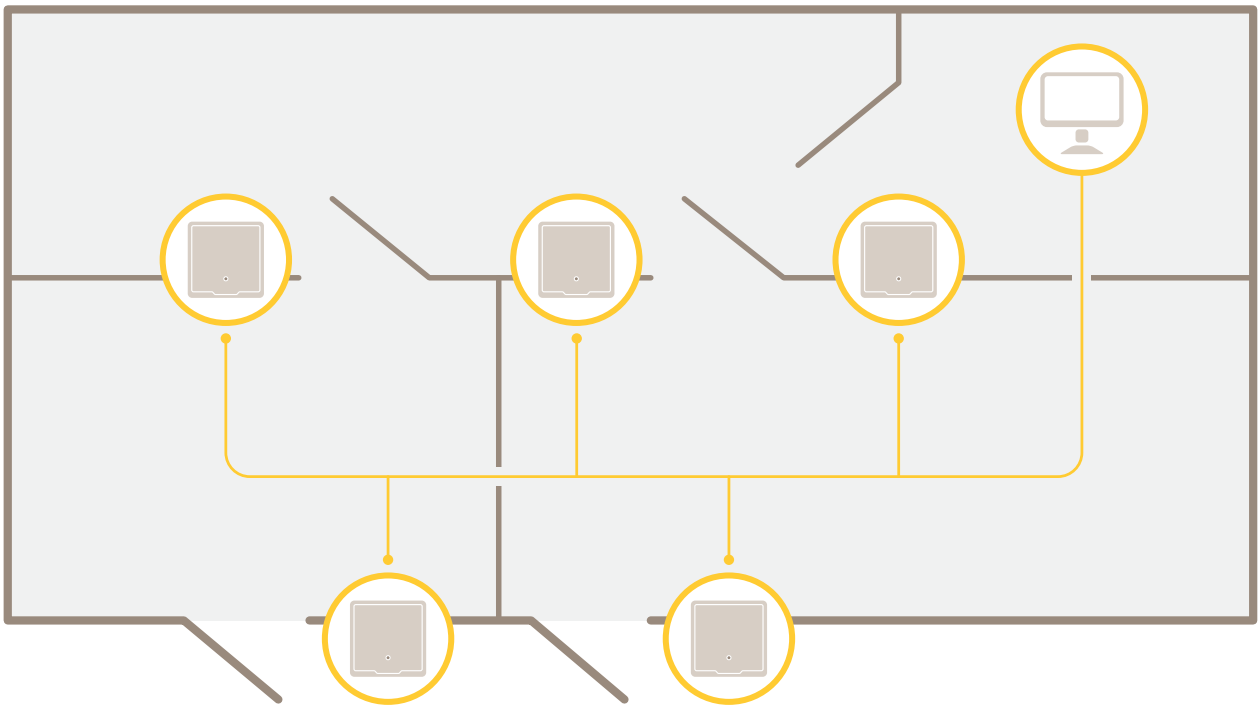
AXIS A1601 Network Door Controller

Manual do Usuário

Índice

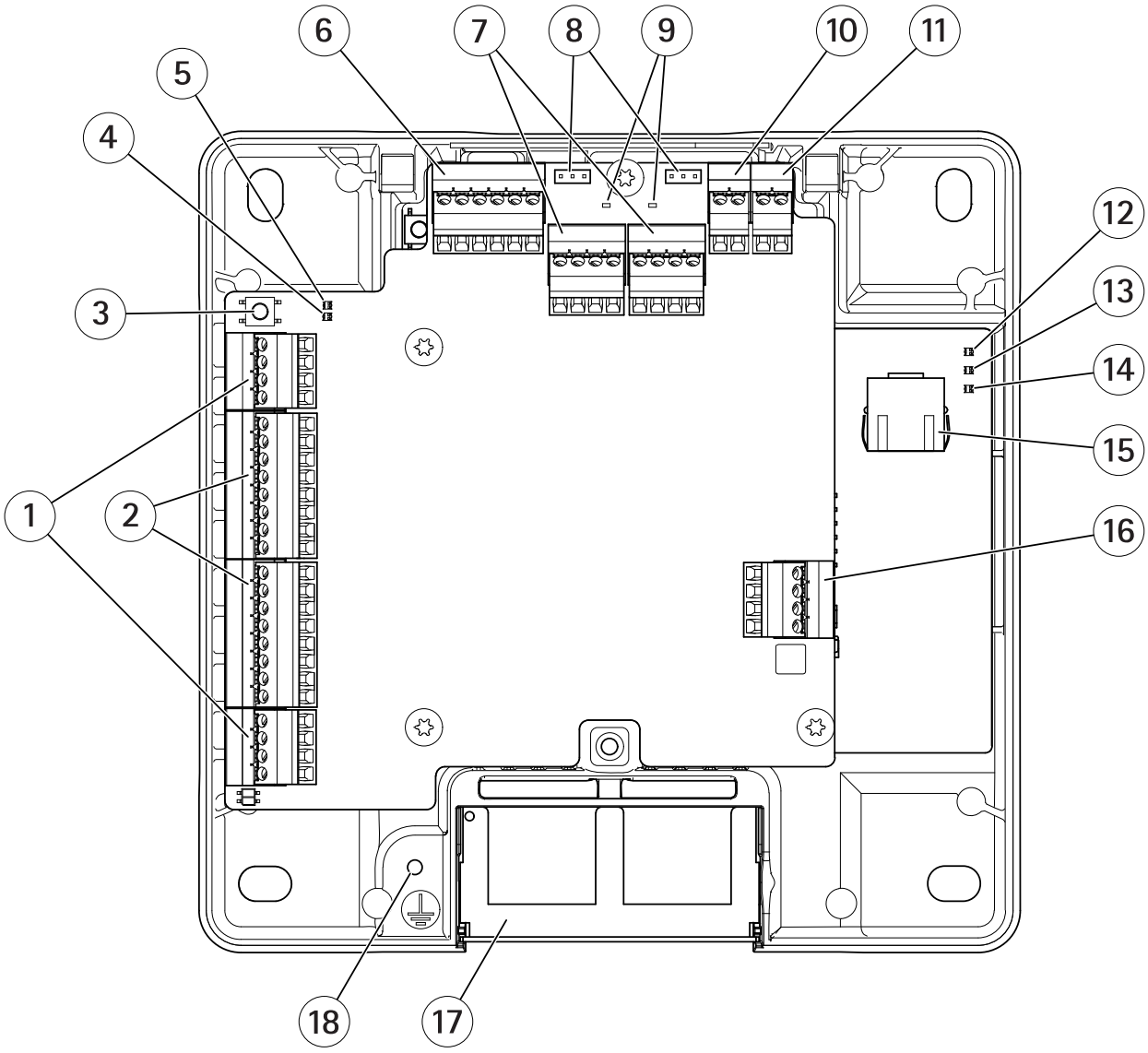
Visão geral da solução



O controlador de porta em rede pode ser facilmente conectado à e alimentado pela sua rede IP existente sem a necessidade de cabeamento especial.

Cada controlador de porta em rede é um dispositivo inteligente que pode ser montado facilmente próximo a uma porta. Ela pode alimentar e controlar até quatro leitores.

Visão geral do produto



1 (2x)
2 (2x)
3
4 LED de excesso de corrente no leitor
5 LED de excesso de corrente no relé
6
7 (2x)
8 Jumper do relé (2x)
9 LED do relé (2x)
10
11
12 LED de energia
13 LED de estado
14 LED de rede
15
16
17 Cobertura do cabo reversível
18 Posição de aterramento

Encontre o dispositivo na rede

Para encontrar dispositivos Axis na rede e atribuir endereços IP a eles no Windows®, use o AXIS IP Utility ou o AXIS Device Manager. Ambos os aplicativos são grátis e podem ser baixados de *axis.com/support*.

Para obter mais informações sobre como encontrar e atribuir endereços IP, acesse *Como atribuir um endereço IP e acessar seu dispositivo*.

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. A página Web do dispositivo será aberta em seu navegador. A página inicial é chamada Visão geral.

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.

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®.

Senhas seguras

Importante

Use HTTPS (que é ativado por padrão) para definir sua senha ou outras configurações confidenciais pela rede. O HTTPS permite conexões de rede seguras e criptografadas, protegendo assim dados confidenciais, como senhas.

A senha do dispositivo é a proteção primária para seus dados e serviços. Os dispositivos Axis não impõem uma política de senhas, pois os produtos podem ser usados em vários tipos de instalações.

Para proteger seus dados, recomendamos enfaticamente que você:

- Use uma senha com pelo menos 8 caracteres, preferencialmente criada por um gerador de senhas.
- Não exponha a senha.

- Altere a senha em um intervalo recorrente pelo menos uma vez por ano.

Como definir a senha do usuário root

Para acessar o produto Axis, você precisa 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 assegura a troca criptografada de informações. Consulte .

O nome do usuário administrador padrão **root** é permanente e não pode ser excluído. Se a senha do root for perdida ou esquecida, o produto deverá ser redefinido para as configurações padrão de fábrica. Consulte .

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

A página Overview (Visão geral)

A página Overview (Visão geral) na página Web do produto mostra informações sobre o nome, endereço MAC, endereço IP e versão do firmware do controlador de porta. Ela também permite a você identificar o controlador de porta na rede.

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 e configurar as opções de rede. Para obter mais informações sobre como configurar o sistema, consulte .

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 .

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 a página Web do produto use um idioma diferente. Consulte .
2. Defina a data e a hora. Consulte .
3. Configure as opções de rede. Consulte .
4. Configure o controlador de porta e os dispositivos conectados, como leitores, travas e dispositivos de solicitação de saída (REX). Consulte .
5. Verifique as conexões de hardware. Consulte .
6. Configuração de cartões e formatos. Consulte .

Para obter informações sobre as recomendações de manutenção, consulte .

Seleção de um idioma

O idioma padrão da página Web do produto 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, a página Web do produto retornará para o idioma inglês.
- Se você restaurar ou reiniciar o produto, ou atualizar o firmware, a página Web continuará a usar o idioma selecionado.

Configuração da data e hora

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 .
- Definir a data e a hora manualmente. Consulte .
- Obter a data e a hora do computador. Consulte .

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 (Opções do sistema > Data e hora) **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 .
Se você usa um nome de host para o servidor NTP, um servidor de DNS deverá ser configurado. Consulte .

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 .

Configurar o 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 .

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

- Importe um arquivo de configuração de hardware. Consulte .
- Crie uma nova configuração de hardware. Consulte .

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 .

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

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 .
5. Configure os leitores e dispositivos REX que serão usados e clique em **Finish (Concluir)**. Para obter mais informações sobre as opções disponíveis, consulte .
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 .

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.

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 porta fornece o sinal de porta aberta quando o circuito está aberto. O monitor de porta 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:

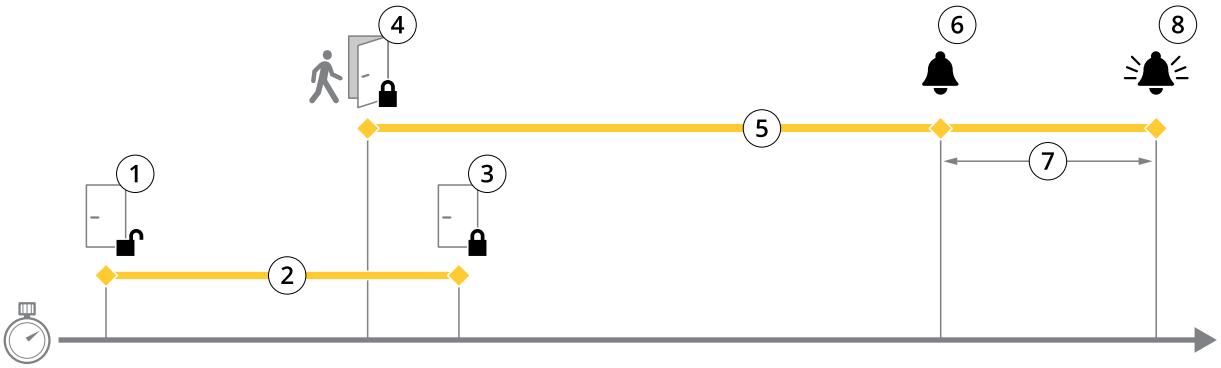
- **Access time (Tempo de acesso)** – Defina o número de segundos que a porta deve permanecer destravada após o acesso ser concedido. A porta permanece destravada até ser aberta ou até o tempo

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.

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 *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 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 .

Sobre opções de travamento

As seguintes opções de circuito de travamento estão disponíveis:

- **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.
- **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. Os leitores com controle LED duplo utilizam fios diferentes para os LEDs vermelho e verde. Isso significa que os LEDs são controlados independentemente um do outro. 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 podem ser alteradas 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 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 .
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

A seguinte função é compatível com entradas supervisionadas:

- Monitor de portas. Consulte .

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
   - **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 .

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 **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. Na página Web do controlador de porta, 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 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 **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 **Adicionar**.

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 . Consulte também as instruções do fabricante.
- **Reader: Tampering** (Leitor: Manipulação) – Obtenha informações sobre a última tentativa de manipulação. 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 de 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 . Consulte também as instruções do fabricante.
- **Elevator Reader: Tampering** (Leitor de elevador: Manipulação) – Obtenha informações sobre a última tentativa de manipulação. 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 de 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 .
4. Clique em **Add field map (Adicionar mapa de campos)** e insira as informações necessárias nos campos. Consulte .
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 ,255mm,sfx)=″graphics:graphic3ABB581B156855197F72986FC9756501″ 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 ,255mm,sfx)=″graphics:graphic2945EA6CEF5875E874297866EE32EB45″

Para excluir um formato de cartão, clique em ,255mm,sfx)=″graphics:graphic2945EA6CEF5875E874297866EE32EB45″.

Importante

- Você só pode ativar e desativar os formatos de cartão se o controlador de porta foi configurado com pelo menos um leitor. Consulte e .
- 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, `OddParity` (Paridade ímpar).
  Exemplos de mapas de campos comuns incluem:
  - `Parity` (Paridade) – 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` (Paridade ímpar) – 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 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` (Paridade par) – 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 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` (Código do local) – 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` (Número do cartão) – 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` (Número de cartão hexadecimal) – 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 numérico de base 16, consiste em 16 símbolos únicos: 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 numérico de base 16, consiste em 16 símbolos únicos: 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.

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.

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 .

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.

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 .
- 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 .

- Se o controlador de porta não estiver se comportando como o esperado, consulte e para obter mais informações.

Configuração de 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.

- Exiba o log de eventos. Consulte .
- Exporte o log de eventos. Consulte .
- Configure o log de eventos. Consulte .

Exibir o log de eventos

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

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 .

Como um administrador, você pode ter mais interesse em alguns eventos do que em outros. Portanto, você pode escolher quais eventos devem ser conectados. Para obter mais informações, consulte .

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.
- Data e hora – Filtre o log de eventos por um intervalo de data e hora.

Configurar o log de eventos

A página Configure event log (Configurar log de eventos) permite definir quais eventos serão registrados.

Opções do log de eventos

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

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. O evento será registrado e incluído no log de eventos.

Como configurar regras de ação

As páginas de eventos permitem que você configure o produto Axis para executar ações quando diferentes eventos ocorrem. 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 a ajuda integrada do produto.

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)**. Veja 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.

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 .

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 **Teste** para testar a conexão com o destinatário.
6. Clique em **OK**.

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 .

Como criar agendamentos

Os agendamentos podem ser usados como acionadores de regras de ação ou como 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 simples	OSDP	Padrão do beeper	Estado
Ocioso[1]	Desligado	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

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.

1. *O estado ocioso é inserido quando a porta está fechada e a trava está bloqueada.*

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 endereço 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 .

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 do:

- 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 .

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 .

Certificados

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.

Rede

Configurações de TCP/IP básicas

O produto Axis oferece suporte a IP versão 4 (IPv4) e IP versão 6 (IPv6).

O produto Axis pode obter um endereço IP 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 .

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) por aproximadamente 3 segundos para conectar a um serviço AVHS pela Internet. Uma vez registrado, **Always (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 do nome do host

O produto Axis pode ser acessado usando um nome de host em vez de um endereço IP. O nome de host é normalmente igual ao nome DNS atribuído. O nome de 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 do 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)**.

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 .

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 executado no produto Axis ativa o upload de novo firmware, aplicativos de usuário, etc. O servidor de 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 de 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 estações de gerenciamento que executam o SNMP. Os 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 . 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 .

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 fornece quatro portas de entrada e saída configuráveis para a conexão de dispositivos externos.

O conector externo fornece duas portas de entrada e saída configuráveis para a conexão de dispositivos externos.

Você pode configurar as portas de E/S 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)**). Você pode atribuir nomes descritivos às portas 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 .

Para obter informações sobre a atualização de firmware, consulte .

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 .

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** 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).

Avançada

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 .

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 **(Opções do sistema > Avançado > Upload de arquivos) Setup > Additional Controller Configuration > System Options > Advanced > File Upload** (Preferências > Configuração de dispositivo adicional > Opções do sistema > Avançado > Upload de arquivos).

Arquivos carregados são acessados via `http://<ip address>/local/<user>/<file name>` onde `<user>` é o grupo de usuários selecionado (administrador) para o arquivo carregado.

Solução de problemas

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 .
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 indicador do LED de estado ficar 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)**.

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 depois de uma atualização de firmware, a primeira inicialização pode 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.

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 **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.

Sintomas, possíveis causas e ações corretivas

Problemas ao atualizar o firmware	
Falha na atualização do firmware	Se a atualização do firmware falha, o produto recarrega 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 o comprimento do ping esteja configurado 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 da rede para obter um endereço IP.
O endereço IP está sendo usado por outro dispositivo	Desconecte o produto Axis da rede. Execute o comando ping (em uma janela do Command/DOS, digite `ping` e o endereço IP do produto): • Se você receber: `Reply from <IP address>: bytes=32; time=10...`, 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`, 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 o 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 .

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 pelo nome de DNS (se um nome foi 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 .

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 . 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)**.

Especificações

O texto marcado com **UL** é válido somente para instalações UL 293 ou UL 294.

Indicadores de LED

LED	Cor	Indicação
Rede	Verde	Aceso para conexão a uma rede de 100 Mbps. Pisca para atividade de rede.
	Âmbar	Aceso continuamente para uma conexão a uma rede de 10 Mbps. Pisca para atividade de rede.
	Apagado	Sem conexão de rede.
Status	Verde	Aceso em verde para operação normal.
	Âmbar	Aceso durante a inicialização e na restauração de configurações.
	Vermelho	Pisca lentamente para falha na atualização.
Alimentação	Verde	Funcionamento normal.
	Âmbar	Pisca em verde/âmbar durante a atualização do firmware.
Excesso de corrente no relé	Vermelho	Aceso quando há um curto-circuito ou se um excesso de corrente foi detectado.
	Apagado	Funcionamento normal.
Excesso de corrente no leitor	Vermelho	Aceso quando há um curto-circuito ou se um excesso de corrente foi detectado.
	Apagado	Funcionamento normal.
Relé	Verde	Relé ativo.[2]
	Apagado	Relé inativo.

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)**.

Botões

Botão de controle

O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte .

Conectores

Conector de rede

Conector Ethernet RJ45 com Power over Ethernet Plus (PoE+).

UL: A alimentação Power over Ethernet (PoE) deve ser fornecida por um injetor Power over Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3 ou Power over Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Classe 4 com limitação

2. Relé está ativo quando COM está conectado a NO.

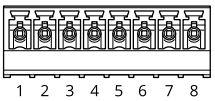
de potência, listado pelo padrão UL 294 e que seja capaz de fornecer 44 – 57 VCC, 15,4 W/30 W. O Power over Ethernet (PoE) foi avaliado pelo UL com um AXIS T8133 Midspan 30 W de 1 porta.

Conector do leitor

Dois blocos de terminais com 8 pinos com suporte aos protocolos RS485 e Wiegand para comunicação com o leitor.

Os valores de saída de alimentação especificados são compartilhados entre as portas dos dois leitores. Isso significa que 486 mA a 12 VCC são reservados para todos os leitores conectados ao controlador de porta.

Selecione o protocolo que será usado na página Web do produto.



Configurado para RS485

Função	Pino	Observação	Especificações
Terra CC (GND)	1		0 VCC
Saída CC (+12 V)	2	Fornece energia para o leitor.	12 VCC, máx. 486 mA combinados para ambos os leitores
RX/TX	3–4	Full duplex: RX. Half duplex: RX/TX.	
TX	5–6	Full duplex: TX.	
Configurável (entrada ou saída)	7–8	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 VCC máx.
		Saída digital — Se usada com uma carga indutiva (por exemplo, um relé), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão.	0 a 30 VCC máx., dreno aberto, 100 mA

Importante

- Quando o leitor é alimentado pelo controlador, o comprimento de cabo qualificado é de até 200 m (656 ft).
- Quando o leitor não é alimentado pelo controlador, o comprimento de cabo qualificado para dados do leitor é de até 1000 m (3280,8 pés) quando os seguintes requisitos de cabo são atendidos: 1 par trançado com proteção AWG 24. 120 ohm de impedância.

Configurado para Wiegand

Função	Pino	Observação	Especificações
Terra CC (GND)	1		0 VCC

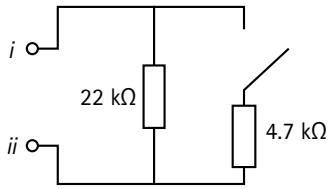
Saída CC (+12 V)	2	Fornece energia para o leitor.	12 VCC, máx. 486 mA combinados para ambos os leitores
D0	3		
D1	4		
O	5–6	Saída digital, dreno aberto	
Configurável (entrada ou saída)	7–8	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 VCC máx.
		Saída digital — Se usada com uma carga indutiva (por exemplo, um relé), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão.	0 a 30 VCC máx., dreno aberto, 100 mA

Importante

- Quando o leitor é alimentado pelo controlador, o comprimento de cabo qualificado é de até 150 m (500 ft).
- Quando o leitor não é alimentado pelo controlador, o comprimento de cabo qualificado para dados do leitor é de até 150 m (500 pés) quando o seguinte requisito de cabo é atendido: AWG 22.

Entradas supervisionadas

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



i Entrada

ii 0 VCC (-)

UL: As entradas supervisionadas não foram avaliadas pelo UL para uso contra invasores. Somente o monitor de porta e o REX oferecem suporte à supervisão com resistores terminadores.

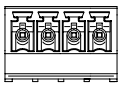
Observação

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

Conector de porta

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

O monitor de porta oferece suporte à supervisão com resistores terminadores. 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 .



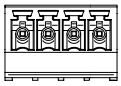
Função	Pino	Observações	Especificações
Terra CC	1, 3		0 VCC
Entrada	2, 4	Para comunicação com o monitor da porta. Entrada digital ou Entrada supervisionada – Conecte ao pino 1 ou 3 respectivamente para ativar ou deixe flutuante (desconectada) para desativar.	0 a 30 VCC máx.

Importante

O comprimento de cabo qualificado é de até 200 m (656 pés) quando o seguinte requisito de cabo é atendido: 24 AWG.

Conector do relé

Dois blocos de terminais com 4 pinos para relés C que podem ser usados, por exemplo, para controlar uma trava ou uma interface para um portão.



Função	Pino	Observações	Especificações
Terra CC (GND)	1		0 VCC
NO	2	normalmente aberto. Para conectar dispositivos de relé. Conecte uma trava de segurança contra falhas entre o terra NO e o terra CC. Os dois pinos de relé são galvanicamente separados do resto do circuito se os jumpers não forem usados.	Corrente máxima = 2 A por relé Tensão máxima = 30 V CC
COM	3	Comum	
NC	4	normalmente fechado. Para conectar dispositivos de relé. Conecte uma trava fail-safe entre o terra NC e o terra CC. Os dois pinos de relé são galvanicamente separados do resto do circuito se os jumpers não forem usados.	

Jumper de alimentação do relé

Quando o jumper de alimentação está instalado, ele conecta a alimentação 12 VCC ou 24 VCC ao pino COM do relé.

Ele pode ser usado para conectar uma trava entre os pinos GND e NO ou GND e NC.

Fonte de alimentação	Potência máxima em 12 VCC[3]	Potência máxima em 24 VCC[3]
ENTRADA CC	1600 mA	800 mA
PoE	800 mA	400 mA

OBSERVAÇÃO

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

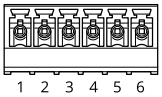
Conector auxiliar

Use o conector auxiliar com dispositivos externos em combinação com, por exemplo, detecção de movimento, 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 – Para conectar dispositivos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas/janelas e detectores de quebra de vidros.

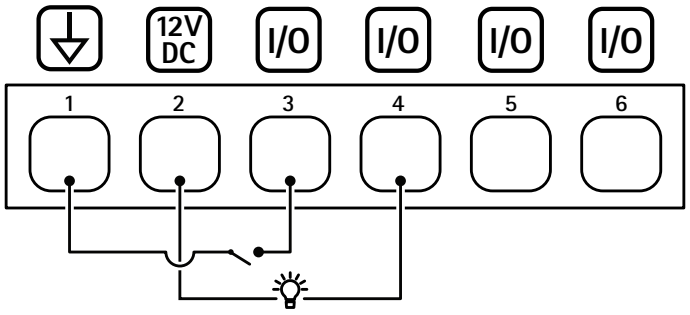
Saída digital – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativo do VAPIX® ou pela página da web do produto.

Bloco de terminais com 6 pinos



Função	Pino	Observações	Especificações
Terra CC	1		0 VCC
Saída CC	2	Pode ser usada para alimentar equipamentos auxiliares. Observação: esse pino pode ser usado somente como saída de energia.	12 V CC Carga máxima = 50 mA para cada E/S
Configurável (entrada ou saída)	3–6	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 VCC máx.
		Saída digital – Conectado internamente ao pino 1 (terra CC) quando ativo, flutuante (desconectado) quando inativo. Se usada com uma carga indutiva (por exemplo, um relé), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão. Cada E/S é capaz de alimentar uma carga externa de 12 VCC, 50 mA (máx.), se uma saída interna de 12 VCC (pino 2) é usada. No caso do uso de conexões de dreno abertas em conjunto com uma fonte de alimentação externa, as E/S podem gerenciar um fornecimento CC de 0 – 30 VCC, 100 mA.	0 a 30 VCC máx., dreno aberto, 100 mA

3. A energia é compartilhada entre os dois relés e a E/S AUX de 12 VCC.

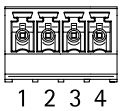


1 *Terra CC*
2 *Saída CC 12 V*
3 *E/S configurada como entrada*
4 *E/S configurada como saída*
5 *E/S configurável*
6 *E/S configurável*

Conector externo

Bloco de terminais com 4 pinos para dispositivos externos, por exemplo, detectores de quebra de vidros ou incêndio.

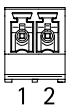
UL: O conector não foi avaliado pelo UL para uso em alarme antifurto/de incêndio.



Função	Pino	Observações	Especificações
Terra CC	1, 3		0 VCC
Configurável (entrada ou saída)	2, 4	Entrada digital – Conecte ao pino 1 ou 3 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 VCC máx.
		Saída digital – Conecte ao pino 1 ou 3 para ativar ou deixe aberta (desconectada) para desativar. Se usada com uma carga indutiva (por exemplo, um relé), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão.	0 a 30 VCC máx., dreno aberto, 100 mA

Conector de energia

Bloco de terminais com 2 pinos para entrada de energia CC Use uma fonte de energia com limitação (LPS) compatível com os requisitos de voltagem 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.	10,5 – 28 VCC, máx. 36 W

UL: Alimentação CC a ser fornecida por uma fonte de alimentação UL 294, UL 293 ou UL 603 relacionada, dependendo do aplicativo, com as classificações apropriadas.

Conector de entrada da bateria de backup.

Para uma solução de backup usando uma bateria com carregador integrado. Entrada 12 VCC.

UL: O conector não foi avaliado pelo UL.

Importante

Quando a entrada da bateria é usada, um fusível externo de abertura lenta de 3 A deve ser conectado em série.

Função	Pino	Observações	Especificações
0 VCC (-)	1		0 VCC
Entrada de bateria	2	Para alimentar o controlador de porta quando outras fontes de alimentação não estão disponíveis. Observação: Esse pino pode ser usado somente como entrada de energia da bateria. Somente para conexão com o UPS.	11 – 13,7 VCC, máx. 36 W

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.

A interface Web

Para alcançar a interface Web do dispositivo, digite o endereço IP do dispositivo em um navegador da Web.

Observação

Esta seção é válida somente para o AXIS A1601 Network Door Controller com firmware do AXIS Camera Station Secure Entry.

Mostre ou oculte o menu principal.

Acesse as notas de versão.

Acesse a ajuda do produto.

Altere o idioma.

Defina o tema claro ou escuro.

O menu de usuário contém:

- Informações sobre o usuário que está conectado.
- **Alterar conta**: Saia da conta atual e faça login em uma nova conta.
- **Desconectar**: Faça logout da conta atual.

O menu de contexto contém:

- **Analytics data (Dados de analíticos)**: Aceite para compartilhar dados de navegador não pessoais.
- **Feedback (Comentários)**: Compartilhe qualquer feedback para nos ajudar a melhorar sua experiência de usuário.
- **Legal**: veja informações sobre cookies e licenças.
- **About (Sobre)**: veja informações do dispositivo, incluindo versão e número de série do AXIS OS.

Status

Status de sincronização de horário

Mostra as informações de sincronização de NTP, incluindo se o dispositivo está em sincronia com um servidor NTP e o tempo restante até a próxima sincronização.

NTP settings (Configurações de NTP): Exiba e atualize as configurações de NTP. Leva você para a página **Time and location (Hora e local)** na qual é possível alterar as configurações de NTP.

Informações do dispositivo

Mostra as informações do dispositivo, incluindo versão e o número de série do AXIS OS.

Upgrade AXIS OS (Atualizar o AXIS OS): atualize o software em seu dispositivo. Abre a página Maintenance (Manutenção), na qual é possível atualizar.

Dispositivo

Alarmes

Device motion (Movimento do dispositivo): Ative para acionar um alarme no sistema quando um movimento do dispositivo for detectado.

Caixa de proteção aberta : Ative para acionar um alarme no sistema quando a abertura de uma caixa de controlador de porta é detectada. Desative essa configuração para controladores de porta barebone.

Violação externa: : Ative para acionar um alarme no sistema quando uma violação externa é detectada. Por exemplo, quando alguém abre ou fecha o gabinete externo.

- **Entrada supervisionada** : Ligue para monitorar o estado de entrada e configure os resistores de fim de linha.
  - Para usar a primeira conexão paralela, selecione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Conexão paralela primeiro com um resistor de 22 kΩ em paralelo e um resistor de 4,7 kΩ em série)**.
  - Para usar a primeira conexão serial, selecione **Serial first connection (Primeira conexão serial)** e selecione um valor de resistor na lista suspensa **Resistor values (Valores de resistor)**.

Periféricos

Leitores

Adicionar leitor: Clique para adicionar um leitor.

AXIS A4612: É possível adicionar até 16 leitores Bluetooth ao controlador, sem necessidade de licença.

- **Nome**: Insira um nome para o leitor.
- **Leitor**: Selecione um leitor na lista suspensa.
- **Endereço IP**: Insira o endereço IP do leitor manualmente.
- **Username (Nome de usuário)**: Insira o nome de usuário do leitor.
- **Senha**: Insira a senha do leitor.
- **Ignore server certificate verification (Ignorar verificação do certificado do servidor)**: Ative para ignorar a verificação.
- **Portas de E/S e relés**: Expanda para a configuração das portas de E/S e dos relés.
  - **Porta**: Mostra o nome da porta.
  - **Direction (Direção)**: Indica que é uma porta de entrada ou saída.
  - **Normal state (Estado normal)**: Clique em  para circuito aberto e  para circuito fechado.

AXIS License Plate Verifier (É necessário reconfigurar no AXIS Camera Station)

- **Nome**: Insira um nome para o leitor.
- **API-key** (Chave API): Insira a chave API.
- **Generate** (Gerar): Clicar para gerar a chave API.
- **Copy API-key** (Copiar a chave API): Clique para copiar a chave API e salvar em um local seguro.

Leitor de código de barras AXIS (É necessário reconfigurar no AXIS Camera Station)

- **Nome**: Insira um nome para o leitor.
- **API-key** (Chave API): Insira a chave API.
- **Generate** (Gerar): Clicar para gerar a chave API.
- **Copy API-key** (Copiar a chave API): Clique para copiar a chave API e salvar em um local seguro.

Leitor de intercomunicação Axis (É necessário reconfigurar no AXIS Camera Station)

- **Nome**: Insira um nome para o leitor.
- **Leitor**: Selecione um leitor na lista suspensa.
- **Endereço IP**: Insira o endereço IP do leitor manualmente.
- **Username (Nome de usuário)**: Insira o nome de usuário do leitor.
- **Senha**: Insira a senha do leitor.
- **Ignore server certificate verification (Ignorar verificação do certificado do servidor)**: Ative para ignorar a verificação.

Edit (Editar): Selecione um leitor e clique em **Edit** (Editar) para fazer alterações no leitor selecionado.

Excluir: Selecione os leitores e clique em **Delete** (Excluir) para excluir os leitores selecionados.

Fechaduras sem fio

É possível conectar até 16 bloqueadores sem fio ASSA ABLOY Aperio utilizando o AH30 Communication Hub. É necessária uma licença para bloqueador sem fio.

Observação

É necessário realizar a instalação do AH30 Communication Hub no lado seguro.

Conectar o hub de comunicação: Clique para conectar as fechaduras sem fio.

Atualizar

Upgrade readers (Atualizar leitores): Clique para atualizar o software do leitor. Você só pode atualizar leitores compatíveis quando eles estão on-line.

Atualizar conversores: Clique para atualizar o software do conversor. Você só pode atualizar conversores compatíveis quando eles estão on-line.

Sistema

Hora e local

Data e hora

O formato de hora depende das configurações de idioma do navegador da Web.

Observação

Recomendamos sincronizar a data e a hora do dispositivo com um servidor NTP.

Synchronization (Sincronização): Selecione uma opção para sincronização da data e da hora do dispositivo.

- **Data e hora automática (PTP)**: Sincronize usando o protocolo de tempo de precisão.
- **Automatic date and time (manual NTS KE servers) (Data e hora automáticas (servidores NTS KE manuais))**: Sincronizar com os servidores estabelecimentos de chave NTP seguros conectados ao servidor DHCP.
  - **Manual NTS KE servers (Servidores NTS KE manuais)**: Insira o endereço IP de um ou dois servidores NTP. Quando você usa dois servidores NTP, o dispositivo sincroniza e adapta sua hora com base na entrada de ambos.
  - **Certificados NTS KE CA confiáveis**: Selecione os certificados CA confiáveis a serem usados para sincronização segura de hora NTS KE ou deixe como nenhum.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Automatic date and time (NTP servers using DHCP) (Data e hora automáticas (servidores NTP usando DHCP))**: sincronize com os servidores NTP conectados ao servidor DHCP.
  - **Fallback NTP servers (Servidores NTP de fallback)**: insira o endereço IP de um ou dois servidores de fallback.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Automatic date and time (manual NTP servers) (Data e hora automáticas (servidores NTP manuais))**: sincronize com os servidores NTP de sua escolha.
  - **Manual NTP servers (Servidores NTP manuais)**: Insira o endereço IP de um ou dois servidores NTP. Quando você usa dois servidores NTP, o dispositivo sincroniza e adapta sua hora com base na entrada de ambos.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Custom date and time (Data e hora personalizadas)**: defina manualmente a data e a hora. Clique em **Get from system (Obter do sistema)** para obter as configurações de data e hora uma vez em seu computador ou dispositivo móvel.

Fuso horário: Selecione qual fuso horário será usado. A hora será ajustada automaticamente para o horário de verão e o horário padrão.

- **DHCP**: Adota o fuso horário do servidor DHCP. O dispositivo deve estar conectado a um servidor DHCP para que você possa selecionar esta opção.
- **Manual**: Selecione um fuso horário na lista suspensa.

Observação

O sistema usa as configurações de data e hora em todas as gravações, logs e configurações do sistema.

Rede

IPv4

Assign IPv4 automatically (Atribuir IPv4 automaticamente): Selecionar a opção de IP de IPv4 automático (DHCP) para permitir que a rede atribua seu endereço IP, máscara de sub-rede e roteador automaticamente, sem a necessidade de configuração manual. Recomendamos o uso da atribuição automática de IP (DHCP) para a maioria das redes.

Endereço IP: Insira um endereço IP exclusivo para o dispositivo. Endereços IP estáticos podem ser atribuídos aleatoriamente em redes isoladas, desde que cada endereço seja único. Para evitar conflitos, é altamente recomendável entrar em contato o administrador da rede antes de atribuir um endereço IP estático.

Máscara de sub-rede: Insira a máscara de sub-rede para definir quais endereços estão dentro da rede local. Qualquer endereço fora da rede local passa pelo roteador.

Router (Roteador): Insira o endereço IP do roteador padrão (gateway) usado para conectar dispositivos conectados a diferentes redes e segmentos de rede.

Fallback to static IP address if DHCP isn't available (Retornar como contingência para o endereço IP estático se o DHCP não estiver disponível): Selecione se você deseja adicionar um endereço IP estático para usar como contingência se o DHCP não estiver disponível e não puder atribuir um endereço IP automaticamente.

Observação

Se o DHCP não estiver disponível e o dispositivo usar um fallback de endereço estático, o endereço estático será configurado com um escopo limitado.

IPv6

Assign IPv6 automatically (Atribuir IPv6 automaticamente): Selecione para ativar o IPv6 e permitir que o roteador de rede atribua um endereço IP ao dispositivo automaticamente.

Nome de host

Assign hostname automatically (Atribuir nome de host automaticamente): Selecione para permitir que o roteador de rede atribua um nome de host ao dispositivo automaticamente.

Nome de host: Insira o nome de host manualmente para usar como uma maneira alternativa de acessar o dispositivo. O relatório do servidor e o log do sistema usam o nome de host. Os caracteres permitidos são A – Z, a – z, 0 – 9 e -.

Ative as atualizações de DNS dinâmicas: Permita que o dispositivo faça a atualização automática dos registros do servidor de nomes de domínio sempre que o endereço IP for alterado.

Registrar o nome do DNS: Digite um nome de domínio exclusivo que aponte para o endereço IP de seu dispositivo. Os caracteres permitidos são A – Z, a – z, 0 – 9 e -.

TTL: O tempo de vida (TTL) define por quanto tempo um registro DNS permanecerá válido até que precise ser atualizado.

Servidores DNS

Assign DNS automatically (Atribuir o DNS automaticamente): Selecione para permitir que o servidor DHCP atribua domínios de pesquisa e endereços de servidor DNS ao dispositivo automaticamente. Recomendamos utilizar DNS (DHCP) automático para a maioria das redes.

Search domains (Domínios de pesquisa): Ao usar um nome de host que não está totalmente qualificado, clique em **Add search domain (Adicionar domínio de pesquisa)** e insira um domínio para pesquisar o nome de domínio usado pelo dispositivo.

DNS servers (Servidores DNS): Clique em **Add DNS server (Adicionar servidor DNS)** e insira o endereço IP do servidor DNS. Esse servidor fornece a tradução dos nomes de host em endereços IP na sua rede.

Observação

Se o DHCP estiver desativado, recursos que dependem da configuração automática de rede, como nome de host, servidores DNS, NTP e outros, podem parar de funcionar.

HTTP e HTTPS

O HTTPS é um protocolo que fornece criptografia para solicitações de páginas de usuários e para as páginas retornadas pelo servidor Web. A troca de informações de criptografia é regida pelo uso de um certificado HTTPS que garante a autenticidade do servidor.

Para usar HTTPS no dispositivo, é necessário instalar certificado HTTPS. Vá para **System > Security (Sistema > Segurança)** para criar e instalar certificados.

Allow access through (Permitir acesso via): Selecione se um usuário tem permissão para se conectar ao dispositivo via protocolos **HTTP**, **HTTPS** ou **HTTP and HTTPS (HTTP e HTTPS)**.

Observação

Se você exibir páginas da Web criptografadas via HTTPS, talvez haja uma queda no desempenho, especialmente quando uma página é solicitada pela primeira vez.

HTTP port (Porta HTTP): Insira a porta HTTP que será usada. O dispositivo permite a porta 80 ou qualquer porta no intervalo 1024 – 65535. Se você estiver conectado como um administrador, também poderá inserir qualquer porta no intervalo 1 – 1023. Se você usar uma porta nesse intervalo, receberá um aviso.

HTTPS port (Porta HTTPS): Insira a porta HTTPS que será usada. O dispositivo permite a porta 443 ou qualquer porta no intervalo 1024 – 65535. Se você estiver conectado como um administrador, também poderá inserir qualquer porta no intervalo 1 – 1023. Se você usar uma porta nesse intervalo, receberá um aviso.

Certificate (Certificado): Selecione um certificado para ativar o HTTPS para o dispositivo.

Protocolos de descoberta de rede

Bonjour®: Ative para permitir a descoberta automática na rede.

Nome Bonjour: Insira um nome amigável para ser visível na rede. O nome padrão é o nome do dispositivo e seu endereço MAC.

UPnP®: Ative para permitir a descoberta automática na rede.

Nome UPnP: Insira um nome amigável para ser visível na rede. O nome padrão é o nome do dispositivo e seu endereço MAC.

WS-Discovery: Ative para permitir a descoberta automática na rede.

LLDP e CDP: Ative para permitir a descoberta automática na rede. Desligar as configurações LLDP e o CDP pode afetar a negociação de energia PoE. Para resolver quaisquer problemas com a negociação de energia PoE, configure a chave PoE somente para negociação de energia PoE de hardware.

Conexão com a nuvem com apenas um clique

O One-Click Cloud Connect (O3C), em conjunto com um serviço O3C, fornece acesso via Internet fácil e seguro a vídeo ao vivo e gravado a partir de qualquer local. Para obter mais informações, consulte *axis.com/end-to-end--solutions/hosted-services*.

Allow O3C (Permitir O3):

- **Um clique**: Esta é a opção padrão. Para se conectar ao O3C, pressione o botão de controle no dispositivo. Dependendo do modelo do dispositivo, pressione e solte ou pressione e segure, até que o LED status pisque. Registre o dispositivo no serviço O3C dentro de 24 horas para ativar **Always (Sempre)** e permanecer conectado. Se não se registrar, o dispositivo será desconectado do O3C.
- **Sempre**: O dispositivo tenta continuamente conectar a um serviço O3C pela Internet. Depois de registrar o dispositivo, ele permanece conectado. Use essa opção se o botão de controle estiver fora de alcance.
- **Não**: Desconecta o serviço O3C.

Proxy settings (Configurações de proxy): Se necessário, insira as configurações de proxy para conectar ao servidor proxy.

Host: Insira o endereço do servidor proxy.

Porta: Insira o número da porta usada para acesso.

Login e **Senha**: Se necessário, insira um nome de usuário e uma senha para o servidor proxy.

Authentication method (Método de autenticação):

- **Básico**: Este método é o esquema de autenticação mais compatível para HTTP. Ele é menos seguro do que o método de **Digest**, pois ele envia o nome de usuário e a senha não criptografados para o servidor.
- **Digest**: Esse método é mais seguro porque sempre transfere a senha criptografada pela rede.
- **Auto**: Essa opção permite que o dispositivo selecione o método de autenticação automaticamente dependendo dos métodos suportados. Ela prioriza o método **Digest** sobre o método **Básico**.

Owner authentication key (OAK) (Chave de autenticação do proprietário (OAK): Clique em **Get key (Obter chave)** para buscar a chave de autenticação do proprietário. Isso só será possível se o dispositivo estiver conectado à Internet sem um firewall ou proxy.

SNMP

O Simple Network Management Protocol (SNMP) possibilita o acesso e o gerenciamento remotos de dispositivos de rede.

SNMP: Selecione a versão de SNMP que deve ser utilizada.

- **v1 and v2c (v1 e v2c)**:
  - **Read community (Comunidade de leitura)**: Insira o nome da comunidade que tem acesso somente de leitura a todos os objetos SNMP suportados. O valor padrão é **public**.
  - **Write community (Comunidade de gravação)**: Insira o nome da comunidade que tem acesso de leitura ou gravação em todos os objetos SNMP suportados (exceto objetos somente leitura). O valor padrão é **gravação**.
  - **Activate traps (Ativar interceptações)**: Ative para ativar o relatório de interceptações. O dispositivo usa interceptações para enviar mensagens sobre eventos importantes ou alterações de status para um sistema de gerenciamento. Na interface Web, você pode configurar interceptações para SNMP v1 e v2c. As interceptações serão desativadas automaticamente se você mudar para SNMP v3 ou desativar o SNMP. Se você usa SNMP v3, é possível configurar interceptações via aplicativo de gerenciamento do SNMP v3.
  - **Trap address (Endereço da interceptação)**: Insira o endereço IP ou nome de host do servidor de gerenciamento.
  - **Trap community (Comunidade de interceptação)**: Insira a comunidade que é usada quando o dispositivo envia uma mensagem de interceptação para o sistema de gerenciamento.
  - **Traps (Interceptações)**:
    - **Cold start (Partida a frio)**: Envia uma mensagem de interceptação quando o dispositivo é iniciado.
    - **Link up (Link ativo)**: Envia uma mensagem de interceptação quando um link muda de inativo para ativo.
    - **Link down (Link inativo)**: Envia uma mensagem de interceptação quando um link muda de ativo para inativo.
    - **Falha de autenticação**: Envia uma mensagem de interceptação quando uma tentativa de autenticação falha.

Observação

Todas as interceptações MIB de vídeo Axis são habilitados quando você ativa as interceptações SNMP v1 e v2c. Para obter mais informações, consulte *AXIS OS portal > SNMP*.

- **v3**: O SNMP v3 é uma versão mais segura que fornece criptografia e senhas seguras. Para usar o SNMP v3, recomendamos ativar o HTTPS, pois as senhas serão enviadas via HTTPS. Isso também impede que partes não autorizadas acessem interceptações SNMP v1 e v2c não criptografadas. Se você usa SNMP v3, é possível configurar interceptações via aplicativo de gerenciamento do SNMP v3.
  - **Password for the account "initial" (Senha para a conta "initial")**: Insira a senha do SNMP para a conta chamada "initial". Embora a senha possa ser enviada sem ativar o HTTPS, isso não é recomendável. A senha do SNMP v3 só pode ser definida uma vez e, preferivelmente, quando o HTTPS está ativado. Após a senha ser definida, o campo de senha não será mais exibido. Para definir a senha novamente, o dispositivo deverá ser redefinido para as configurações padrões de fábrica.

Clientes conectados

Mostra o número de conexões e os clientes conectados.

View details (Exibir detalhes): Exiba e atualize a lista dos clientes conectados. A lista mostra o endereço IP, o protocolo, a porta e o PID/Processo de cada conexão.

Segurança

Certificados

Certificados são usados para autenticar dispositivos em uma rede. O dispositivo oferece suporte a dois tipos de certificados:

- **Certificados cliente/servidor**
  Um certificado cliente/servidor valida a identidade do produto e 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**
  Você pode usar um certificado de CA para autenticar um certificado de par, por exemplo, para validar a identidade de um servidor de autenticação quando o dispositivo se conecta a uma rede protegida por IEEE 802.1X. O dispositivo possui vários certificados de CA pré-instalados.

Os seguintes formatos são aceitos:

- Formatos de certificado: .PEM, .CER e .PFX
- Formatos de chave privada: PKCS#1 e PKCS#12

Importante

Se você redefinir o dispositivo para o padrão de fábrica, todos os certificados serão excluídos. Quaisquer certificados de CA pré-instalados serão reinstalados.

Adicionar certificado : Clique para adicionar um certificado. Um guia passo a passo é aberto.

- **Mais** : Mostrar mais campos para preencher ou selecionar.
- **Secure keystore (Armazenamento de chaves seguro)**: Selecione para usar **Trusted Execution Environment (SoC TEE)**, **Secure element** (Elemento seguro) ou **Trusted Platform Module 2.0** para armazenar de forma segura a chave privada. Para obter mais informações sobre qual armazenamento de chaves seguro selecionar, acesse *help.axis.com/axis-os#cryptographic-support*.
- **Tipo da chave**: Selecione o algoritmo de criptografia padrão ou diferente na lista suspensa para proteger o certificado.

O menu de contexto contém:

- **Certificate information (Informações do certificado)**: Exiba as propriedades de um certificado instalado.
- **Delete certificate (Excluir certificado)**: Exclua o certificado.
- **Create certificate signing request (Criar solicitação de assinatura de certificado)**: Crie uma solicitação de assinatura de certificado para enviar a uma autoridade de registro para se aplicar para um certificado de identidade digital.

Secure keystore (Armazenamento de chaves seguro) :

- **Trusted Execution Environment (SoC TEE)**: Selecione para usar o SoC TEE para armazenamento de chaves seguro.
- **Secure element (CC EAL6+, FIPS 140-3 Level 3) (Elemento seguro [CC EAL6+, FIPS 140-3 Nível 3])** : Selecione para usar o elemento seguro no armazenamento de chaves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Nível 2)** : Selecione para usar TPM 2.0 para armazenamento de chaves seguro.

Controle de acesso à rede e criptografia

IEEE 802.1x

O IEEE 802.1x é um padrão do IEEE para controle de admissão em redes baseado em portas que fornece autenticação segura de dispositivos em rede com e sem fio. O IEEE 802.1x é baseado no EAP (Extensible Authentication Protocol).

Para acessar uma rede protegida pelo IEEE 802.1x, os dispositivos de rede devem se autenticar. A autenticação é executada por um servidor de autenticação, geralmente, um servidor RADIUS (por exemplo, FreeRADIUS e Microsoft Internet Authentication Server).

IEEE 802.1AE MACsec

O IEEE 802.1AE MACsec é um padrão IEEE para segurança de controle de acesso à mídia (MAC) que define a confidencialidade e integridade de dados sem conexão para protocolos independentes de acesso à mídia.

Certificados

Quando configurado sem um certificado de CA, a validação do certificado do servidor é desativada e o dispositivo tenta se autenticar independentemente da rede à qual está conectado.

Ao usar um certificado, na implementação da Axis, o dispositivo e o servidor de autenticação se autenticam com certificados digitais usando EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Para permitir que o dispositivo acesse uma rede protegida por certificados, é necessário instalar um certificado de cliente assinado no dispositivo.

Authentication method (Método de autenticação): Selecione um tipo de EAP usado para autenticação.

Client certificate (Certificado de cliente): Selecione um certificado de cliente para usar o IEEE 802.1x. O servidor de autenticação usa o certificado para validar a identidade do cliente.

CA certificates (Certificados CA): Selecione certificados CA para validar identidade do servidor de autenticação. Quando nenhum certificado é selecionado, o dispositivo tenta se autenticar independentemente da rede à qual está conectado.

EAP identity (Identidade EAP): Insira a identidade do usuário associada ao seu certificado de cliente.

EAPOL version (Versão EAPOL): Selecione a versão EAPOL que é usada no switch de rede.

Use IEEE 802.1x (Usar IEEE 802.1x): Selecione para usar o protocolo IEEE 802.1 x.

Essas configurações só estarão disponíveis se você usar **IEEE 802.1x PEAP-MSCHAPv2** como método de autenticação:

- **Senha**: Insira a senha para sua identidade de usuário.
- **Peap version (Versão do Peap)**: Selecione a versão do Peap que é usada no switch de rede.
- **Label (Rótulo)**: Selecione 1 para usar a criptografia EAP do cliente; selecione 2 para usar a criptografia PEAP do cliente. Selecione o rótulo que o switch de rede usa ao utilizar a versão 1 do Peap.

Essas configurações só estarão disponíveis se você usar o **IEEE 802.1ae MACsec (CAK estático/chave pré-compartilhada)** como método de autenticação:

- **Nome da chave de associação de conectividade do acordo de chaves**: Insira o nome da associação de conectividade (CKN). Deve ter de 2 a 64 (divisível por 2) caracteres hexadecimais. O CKN deve ser configurado manualmente na associação de conectividade e deve corresponder em ambas as extremidades do link para ativar inicialmente o MACsec.
- **Chave de associação de conectividade do acordo de chaves**: Insira a chave da associação de conectividade (CAK). Ela deve ter 32 ou 64 caracteres hexadecimais. O CAK deve ser configurado manualmente na associação de conectividade e deve corresponder em ambas as extremidades do link para ativar inicialmente o MACsec.

Impedir ataques de força bruta

Blocking (Bloqueio): Ative para bloquear ataques de força bruta. Um ataque de força bruta usa tentativa e erro para adivinhar informações de login ou chaves de criptografia.

Blocking period (Período de bloqueio): Insira o número de segundos para bloquear um ataque de força bruta.

Blocking conditions (Condições de bloqueio): Insira o número de falhas de autenticação permitidas por segundo antes do início do bloco. Você pode definir o número de falhas permitidas em nível de página ou em nível de dispositivo.

Firewall

Firewall: Ative para ativar o firewall.

Default Policy (Política padrão): Selecione como deseja que o firewall trate as solicitações de conexão não cobertas por regras.

- **ACCEPT (ACEITAR):** Permite todas as conexões com o dispositivo. Essa opção é definida por padrão.
- **DROP (DESCARTAR):** Bloqueia todas as conexões com o dispositivo.

Para criar exceções à política padrão, você pode criar regras que permitem ou bloqueiam conexões com o dispositivo a partir de endereços, protocolos e portas específicos.

+ New rule (+ Nova regra): clique para criar uma regra.

Rule type (Tipo de regra):

- **FILTER (FILTRAR)**: Selecione para permitir ou bloquear conexões de dispositivos que correspondam aos critérios definidos na regra.
  - **Policy (Política)**: Selecione **Accept (Aceitar)** ou **Drop (Descartar)** a regra de firewall.
  - **IP range (Faixa IP)**: Selecione para especificar uma faixa de endereços a serem permitidos ou bloqueados. Use IPv4/IPv6 em **Start (Início)** e **End (Fim)**.
  - **Endereço IP**: Digite um endereço que você deseja permitir ou bloquear. Use o formato IPv4/ /IPv6 ou CIDR.
  - **Protocol (Protocolo)**: Selecione um protocolo de rede (TCP, UDP ou ambos) para permitir ou bloquear. Se você selecionar um protocolo, também deverá especificar uma porta.
  - **MAC**: Digite o endereço MAC de um dispositivo que você deseja permitir ou bloquear.
  - **Port range (Faixa de portas)**: Selecione para especificar a faixa de portas a serem permitidas ou bloqueadas. Adicione-as a **Start (Início)** e **End (Fim)**.
  - **Porta**: Insira um número de porta que você deseje permitir ou bloquear. Os números de portas devem estar entre 1 e 65535.
  - **Traffic type (Tipo de tráfego)**: Selecione o tipo de tráfego que você deseja permitir ou bloquear.
    - **UNICAST**: Tráfego de um único remetente para um único destinatário.
    - **BROADCAST**: Tráfego de um único remetente para todos os dispositivos na rede.
    - **MULTICAST**: Tráfego de um ou mais remetentes para um ou mais destinatários.
- **LIMIT (LIMITAR)**: Selecione para aceitar conexões de dispositivos que correspondam aos critérios definidos na regra, mas aplique limites para reduzir o tráfego excessivo.
  - **IP range (Faixa IP)**: Selecione para especificar uma faixa de endereços a serem permitidos ou bloqueados. Use IPv4/IPv6 em **Start (Início)** e **End (Fim)**.
  - **Endereço IP**: Digite um endereço que você deseja permitir ou bloquear. Use o formato IPv4/ /IPv6 ou CIDR.
  - **Protocol (Protocolo)**: Selecione um protocolo de rede (TCP, UDP ou ambos) para permitir ou bloquear. Se você selecionar um protocolo, também deverá especificar uma porta.
  - **MAC**: Digite o endereço MAC de um dispositivo que você deseja permitir ou bloquear.
  - **Port range (Faixa de portas)**: Selecione para especificar a faixa de portas a serem permitidas ou bloqueadas. Adicione-as a **Start (Início)** e **End (Fim)**.
  - **Porta**: Insira um número de porta que você deseje permitir ou bloquear. Os números de portas devem estar entre 1 e 65535.
  - **Unit (Unidade)**: Selecione o tipo de conexão a ser permitida ou bloqueada.
  - **Period (Período)**: Selecione o período de tempo relacionado a **Amount (Quantidade)**.
  - **Amount (Quantidade)**: Defina o número máximo de vezes que um dispositivo tem permissão para se conectar dentro do período definido em **Period (Período)**. O valor máximo é 65535.

- **Burst (Surto)**: Insira o número de conexões que podem exceder o valor definido em **Amount (Quantidade)** uma vez durante o período definido em **Period (Período)**. Quando o número for atingido, somente a quantidade definida durante o período definido será permitida.
- **Traffic type (Tipo de tráfego)**: Selecione o tipo de tráfego que você deseja permitir ou bloquear.
  - **UNICAST**: Tráfego de um único remetente para um único destinatário.
  - **BROADCAST**: Tráfego de um único remetente para todos os dispositivos na rede.
  - **MULTICAST**: Tráfego de um ou mais remetentes para um ou mais destinatários.

Test rules (Testar regras): Clique para testar as regras que você definiu.

- **Test time in seconds (Tempo de teste em segundos)**: Defina um limite de tempo para testar as regras.
- **Roll back (Reverter)**: Clique para reverter o firewall ao seu estado anterior, antes de testar as regras.
- **Apply rules (Aplicar regras)**: Clique para ativar as regras sem testar. Não recomendamos fazer isso.

Certificado do AXIS OS com assinatura personalizada

Para instalar o software de teste ou outro software personalizado da Axis no dispositivo, certificado do AXIS OS com assinatura personalizada é necessário. O certificado verifica se o software é aprovado pelo proprietário do dispositivo e pela Axis. O software só pode ser executado em um dispositivo específico identificado por seu número de série e ID de chip exclusivos. Somente a Axis pode criar certificados do AXIS OS com assinatura personalizada, pois é a Axis que possui a chave para assiná-los.

Install (Instalar): Clique para instalar o certificado. É necessário instalar o certificado antes de instalar o software.

O menu de contexto contém:

- **Delete certificate (Excluir certificado)**: Exclua o certificado.

Contas

Contas

Adicionar conta: Clique para adicionar uma nova conta. É possível adicionar até 100 contas.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Privileges (Privilégios):

- **Administrator (Administrador)**: Tem acesso irrestrito a todas as configurações. Os administradores também podem adicionar, atualizar e remover outras contas.
- **Operator (Operador)**: Tem acesso a todas as configurações, exceto:
  - Todas as configurações do **System (Sistema)**.
- **Viewer (Visualizador)**: Não tem acesso para alterar as configurações.

O menu de contexto contém:

Update account (Atualizar conta): Edite as propriedades da conta.

Delete account (Excluir conta): Exclua a conta. Não é possível excluir a conta root.

MQTT

O MQTT (Message Queuing Telemetry Transport) é um protocolo de troca de mensagens padrão para a Internet das Coisas (IoT). Ele foi desenvolvido para integração simplificada com a IoT e é usado em uma ampla variedade de setores para conectar dispositivos remotos com o mínimo de código e largura de banda de rede. O cliente MQTT no software do dispositivo Axis pode simplificar a integração de dados e eventos produzidos no dispositivo a sistemas que não são software de gerenciamento de vídeo (VMS).

Configure o dispositivo como um cliente MQTT. A comunicação MQTT baseia-se em duas entidades, os clientes e o broker. Os clientes podem enviar e receber mensagens. O broker é responsável por rotear mensagens entre os clientes.

Saiba mais sobre MQTT na *Base de conhecimento do AXIS OS*.

ALPN

O ALPN é uma extensão do TLS/SSL que permite a seleção de um protocolo de aplicação durante a fase de handshake da conexão entre o cliente e o servidor. Isso é usado para permitir o tráfego MQTT na mesma porta que é utilizada para outros protocolos, como o HTTP. Em alguns casos, pode não haver uma porta dedicada aberta para a comunicação MQTT. Uma solução nesses casos é usar o ALPN para negociar o uso do MQTT como protocolo de aplicação em uma porta padrão permitida pelos firewalls.

Cliente MQTT

Connect (Conectar): Ative ou desative o cliente MQTT.

Status: Mostra o status atual do cliente MQTT.

Broker

Host: Insira o nome de host ou endereço IP do servidor MQTT.

Protocol (Protocolo): Selecione o protocolo que será usado.

Porta: Insira o número da porta.

- 1883 é o valor padrão para **MQTT sobre TCP**
- 8883 é o valor padrão para **MQTT sobre SSL**
- 80 é o valor padrão para **MQTT sobre WebSocket**
- 443 é o valor padrão para **MQTT sobre WebSocket Secure**

Protocol ALPN: Insira o nome do protocolo ALPN fornecido pelo seu provedor de broker de MQTT. Isso se aplica apenas com MQTT sobre SSL e MQTT sobre o WebSocket Secure.

Username (Nome de usuário): Insira o nome de usuário que será usado pelo cliente para acessar o servidor.

Senha: Insira uma senha para o nome de usuário.

Client ID (ID do cliente): Insira um ID de cliente. O identificador do cliente é enviado para o servidor quando o cliente se conecta a ele.

Clean session (Limpar sessão): Controla o comportamento na conexão e na desconexão. Quando selecionada, as informações de estado são descartadas na conexão e desconexão.

HTTP proxy (Proxy HTTP): Um URL com comprimento máximo de 255 bytes. Deixe o campo vazio se não quiser usar um proxy HTTP.

HTTPS proxy (Proxy HTTPS): Um URL com comprimento máximo de 255 bytes. Deixe o campo vazio se não quiser usar um proxy HTTPS.

Keep alive interval (Intervalo de Keep Alive): Permite que o cliente detecte quando o servidor não está mais disponível sem que seja necessário aguardar o longo tempo limite de TCP/IP.

Timeout (Tempo limite): O intervalo de tempo em segundos para permitir que uma conexão seja concluída. Valor padrão: 60

Device topic prefix (Prefixo do tópico do dispositivo): Usado nos valores padrão para o tópico na mensagem de conexão e na mensagem de LWT na guia **MQTT client (Cliente MQTT)** e nas condições de publicação na guia **MQTT publication (Publicação MQTT)**.

Reconnect automatically (Reconectar automaticamente): Especifica se o cliente deve se reconectar automaticamente após uma desconexão.

Mensagem de conexão

Especifica se uma mensagem deve ser enviada quando uma conexão é estabelecida.

Send message (Enviar mensagem): ative para enviar mensagens.

Use default (Usar padrão): Desative para inserir sua própria mensagem padrão.

Topic (Tópico): insira o tópico para a mensagem padrão.

Payload (Carga): insira o conteúdo para a mensagem padrão.

Retain (Reter): selecione para manter o estado do cliente neste **Topic (Tópico)**

QoS: Altere a camada de QoS para o fluxo do pacote.

Mensagem de Último desejo e testamento

A opção Last Will Testament (LWT) permite que um cliente forneça uma prova juntamente com suas credenciais ao conectar ao broker. Se o cliente se desconectar abruptamente em algum momento mais tarde (talvez porque sua fonte de energia seja interrompida), ele pode permitir que o broker envie uma mensagem para outros clientes. Essa mensagem de LWT tem o mesmo formato que uma mensagem comum e é roteada através da mesma mecânica.

Send message (Enviar mensagem): ative para enviar mensagens.

Use default (Usar padrão): Desative para inserir sua própria mensagem padrão.

Topic (Tópico): insira o tópico para a mensagem padrão.

Payload (Carga): insira o conteúdo para a mensagem padrão.

Retain (Reter): selecione para manter o estado do cliente neste **Topic (Tópico)**

QoS: Altere a camada de QoS para o fluxo do pacote.

Publicação MQTT

Use default topic prefix (Usar prefixo de tópico padrão): selecione para usar o prefixo de tópico padrão, o qual é definido com o uso do prefixo de tópico de dispositivo na guia **MQTT client (Cliente MQTT)**.

Incluir condição: selecione para incluir o tópico que descreve a condição no tópico MQTT.

Incluir espaços de nome: selecione para incluir espaços para nome de tópico ONVIF no tópico MQTT.

Include serial number (Incluir número de série): selecione para incluir o número de série do dispositivo na carga MQTT.

Adicionar condição: clique para adicionar uma condição.

Retain (Reter): define quais mensagens MQTT são enviadas como retidas.

- **None (Nenhuma)**: envia todas as mensagens como não retidas.
- **Property (Propriedade)**: envia somente mensagens stateful como retidas.
- **All (Todas)**: envie mensagens stateful e stateless como retidas.

QoS: selecione o nível desejado para a publicação MQTT.

Assinaturas MQTT

Adicionar assinatura: clique para adicionar uma nova assinatura MQTT.

Subscription filter (Filtro de assinatura): insira o tópico MQTT no qual deseja se inscrever.

Use device topic prefix (Usar prefixo de tópico do dispositivo): adicione o filtro de assinatura como prefixo ao tópico MQTT.

Subscription type (Tipo de assinatura):

- **Stateless**: selecione para converter mensagens MQTT em mensagens stateless.
- **Stateful**: selecione para converter mensagens MQTT em condições. A carga é usada como estado.

QoS: selecione o nível desejado para a assinatura MQTT.

Acessórios

Portas de E/S

Use a entrada digital para conectar dispositivos externos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas ou janelas e detectores de quebra de vidros.

Use a saída digital para conectar dispositivos externos, como relés e LEDs. Você pode ativar dispositivos conectados via interface de programação de aplicativos VAPIX® ou na interface Web.

Detecção automática

Nome: Edite o texto para renomear a porta.

Direção:  indica que a porta é uma porta de entrada.  indica que é uma porta de saída. Se a porta for configurável, você poderá clicar nos ícones para alternar entre entrada e saída.

Normal state (Estado normal): Clique em  para circuito aberto e  para circuito fechado.

Current state (Estado atual): Mostra o estado atual da porta. A entrada ou saída é ativada quando o estado atual é diferente do estado normal. Uma entrada no dispositivo tem um circuito aberto quando desconectada ou quando há uma tensão acima de 1 VCC.

Observação

Durante a reinicialização, o circuito de saída é aberto. Quando a reinicialização é concluída, o circuito retorna para a posição normal. Se você alterar qualquer configuração nesta página, os circuitos de saída voltarão para suas posições normais, independentemente de quaisquer acionadores ativos.

Supervisionado  : Ative para possibilitar a detecção e o acionamento de ações se alguém manipular a conexão com dispositivos de E/S digitais. Além de detectar se uma entrada está aberta ou fechada, você também pode detectar se alguém a manipulou (ou seja, cortada ou em curto). Supervisionar a conexão requer hardware adicional (resistores de fim de linha) no loop de E/S externo.

Logs

Relatórios e logs

Relatórios

- **View the device server report (Exibir o relatório do servidor de dispositivos)**: Exiba informações sobre o status do produto em uma janela pop-up. O Log de acesso é incluído automaticamente no Relatório do servidor.
- **Download the device server report (Baixar o relatório do servidor de dispositivos)**: Ele cria um arquivo .zip que contém um arquivo de texto do relatório completo do servidor no formato UTF-8, bem como um instantâneo da imagem da visualização ao vivo atual. Inclua sempre o arquivo. zip do relatório do servidor ao entrar em contato com o suporte.
- **Download the crash report (Baixar o relatório de falhas inesperadas)**: Baixe um arquivo com informações detalhadas sobre o status do servidor. O relatório de panes contém informações que fazem parte do relatório do servidor, além de informações de depuração detalhadas. Esse relatório pode conter informações sensíveis, como rastreamentos de rede. A geração do relatório poderá demorar vários minutos.

Logs

- **View the system log (Exibir o log do sistema)**: Clique para mostrar informações sobre eventos do sistema, como inicialização de dispositivos, avisos e mensagens críticas.
- **View the access log (Exibir o log de acesso)**: clique para mostrar todas as tentativas de acessar o dispositivo que falharam, por exemplo, quando uma senha de login incorreta é usada.
- **View the audit log (Exibir o log de auditoria)**: Clique para exibir informações sobre as atividades do usuário e do sistema, por exemplo, autenticações e configurações bem-sucedidas ou com falha.

Rastreamento de rede

Importante

Um arquivo de rastreamento de rede pode conter informações confidenciais, por exemplo, certificados ou senhas.

Um arquivo de trace de rede pode ajudar a solucionar problemas gravando as atividades na rede.

Trace time (Tempo de trace): Selecione a duração do trace em segundos ou minutos e clique em **Download (Baixar)**.

Acesse o sistema remotamente

O syslog é um padrão para o registro de mensagens. Ele permite a separação do software que gera mensagens, o sistema que as armazena e o software que as relata e analisa. Cada mensagem é rotulada com um código da instalação que indica o tipo de software que gerou a mensagem e recebe um nível de gravidade.

Servidor: Clique para adicionar um novo servidor.

Host: Insira o nome de host ou endereço IP do servidor.

Format (Formatar): Selecione o formato de mensagem do syslog que será usado.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocolo): Selecione o protocolo que a ser usado:

- UDP (a porta padrão é 514)
- TCP (a porta padrão é 601)
- TLS (a porta padrão é 6514)

Porta: Edite o número da porta para usar uma porta diferente.

Severity (Severidade): Selecione quais mensagens serão enviadas após o acionamento.

Tipo: Selecione os tipos de registros que deseja enviar.

Test server setup (Testar configuração do servidor): Envie uma mensagem de teste para todos os servidores antes de salvar as configurações.

CA certificate set (Certificado CA definido): Consulte as configurações atuais ou adicione um certificado.

Manutenção

Restart (Reiniciar): Reinicie o dispositivo. Isso não afeta nenhuma das configurações atuais. Os aplicativos em execução reiniciam automaticamente.

Restore (Restaurar): Devolve a maioria das configurações para os valores padrão de fábrica. Posteriormente, você deverá reconfigurar o dispositivo e os aplicativos, reinstalar quaisquer apps que não vieram pré-instalados e recriar quaisquer eventos e predefinições.

Importante

As únicas configurações que permanecem salvas após a restauração são:

- Protocolo de inicialização (DHCP ou estático)
- Endereço IP estático
- Roteador padrão
- Máscara de sub-rede
- Configurações 802.1X
- Configurações de O3C
- Endereço IP do servidor DNS

Factory default (Padrão de fábrica): Retorna todas as configurações para os valores padrão de fábrica. Em seguida, você deverá redefinir o endereço IP para tornar o dispositivo acessível.

Observação

Todo software de dispositivo Axis é digitalmente assinado para garantir que somente software verificado seja instalado em seu dispositivo. Esse procedimento aprimora ainda mais o nível de segurança cibernética mínimo dos dispositivos Axis. Para obter mais informações, consulte o white paper "Axis Edge Vault" em *axis.com*.

Atualização do AXIS OS: atualize para uma nova versão do AXIS OS. As novas versões podem conter funcionalidades aprimoradas, correções de falhas ou ainda recursos inteiramente novos. Recomendamos sempre utilizar a versão mais recente do AXIS OS. Para baixar a versão mais recente, vá para *axis.com/support*.

Ao atualizar, é possível escolher entre três opções:

- **Standard upgrade (Atualização padrão)**: atualize para a nova versão do AXIS OS.
- **Factory default (Padrão de fábrica)**: Atualize e retorne todas as configurações para os valores padrão de fábrica. Ao escolher essa opção, você não poderá reverter para a versão anterior do AXIS OS após a atualização.
- **Automatic rollback (Reversão automática)**: Atualize e confirme a atualização dentro do período definido. Se você não confirmar, o dispositivo reverterá para a versão anterior do AXIS OS.

AXIS OS rollback (Reversão do AXIS OS): reverta para a versão anteriormente instalada do AXIS OS.

T10125657_pt

2025-11 (M14.3)