AXIS Optimizer

AXIS Optimizer for XProtect®
AXIS Optimizer for Siemens Siveillance™

Manual do Usuário

Índice

AXIS Optimizer 7
Finalidade de uso do AXIS Optimizer 7
Requisitos do sistema 7
Suporte a sistemas federados 7
Suporte a sistemas interconectados 7
Notas de lançamento 7
Instalação ou atualização do AXIS Optimizer 8
Instalação do AXIS Optimizer 8
Que versões estão instaladas em meu sistema? 8
Opções avançadas de instalação 8
Migração do VMS 9
Verificar a integridade da instalação 9
Atualização do AXIS Optimizer 9
Atualização manual 10
Atualizar o sistema automaticamente 10
Ativar a atualização automática 10
Desativar atualização automática 11
Saiba mais 11
Desinstalar o AXIS Optimizer 11
Padrão de fábrica 11
Descomissionamento seguro 11
Privilégios de usuário 12
Acessar as configurações dos dispositivos 13
Assistente de dispositivos 13
Configurar um dispositivo Axis 13
Instalar aplicativos em um dispositivo Axis 13
Configurar aplicativos em um dispositivo Axis 13
Atualizar aplicativos em um dispositivo Axis 13
Reiniciar um dispositivo Axis 14
Copiar o endereço IP de um dispositivo Axis 14
Realize a automação 15
Crie ações para dispositivos Axis 15
Plug-in do servidor de eventos 15
Instalar plug-in do servidor de eventos 15
Secar várias câmeras com um clique 15
Ative o foco automático para várias câmeras com apenas um clique 16
Acionar várias sirenes estroboscópicas com um clique 17
Desativar automaticamente máscaras de privacidade em várias câmeras 18
Ativar uma sirene estroboscópica quando uma câmera detectar movimento 20
Reproduzir clipes de áudio em alto-falantes ou em uma zona de alto-falante quando uma câmera detecta movimento 22
Solucionar problemas em uma regra 23
Gerenciamento centralizado de listas de placas de licença 23
Criar uma lista 23
Configurar permissões de lista 24
Editar uma lista 24
Importar uma lista 25
Exportar uma lista 25
Saiba mais sobre listas 26
Responda a eventos ao vivo 27
Usar controles de dispositivos 27
Controles do operador 27
Acesso aos controles do operador 27

Salvar uma área de foco para uma câmera PTZ 27
Foco automático de uma câmera 28
Ativar secagem rápida ou limpador 28
Medição de temperatura pontual 29
Aplicar zoom e acompanhar automaticamente um objeto em movimento 29
Criar controles do operador personalizados 30
Configurar acesso a controles de operadores 30
Interagir via alto-falantes 30
Gerenciador de alto-falantes 30
Modos 31
Modo AXIS Audio Manager Pro 31
Modo AXIS Audio Manager Edge 33
Modo legado 34
Reprodução de áudio em alto-falantes 35
Reprodução de áudio em alto-falantes na exibição da câmera 35
Reproduzir áudio nos alto-falantes em caso de alarmes 36
Defina a configuração do comportamento visual para a interação com o alto-falante 36
Marcadores de clipes de áudio na exibição da câmera ou alarme 36
Gerencie visitantes 37
Plug-in de intercomunicador 37
Configuração de um intercomunicador 37
Definir permissões para intercomunicador 38
Fazer uma chamada de teste 39
Previna o eco durante as chamadas 39
Controle o interfone via visualização ao vivo 40
Responder a uma chamada da visualização ao vivo 42
Mostrar várias câmeras na janela de chamada 43
Ações de janela de chamada 44
Exibir uma página na janela de chamada 44
Filtrar na extensão da chamada 45
Exibir o histórico de chamadas 45
Desativar o microfone quando não houver uma chamada ativa 46
Receber um alarme se uma porta for forçada para abrir 47
Receber um alarme se uma porta permanecer aberta por muito tempo 47
Impedir que um cliente receba chamadas 47
Visualizar áudio 47
Exibição de microfone 47
Configurar VMS para exibição de microfone 48
Adicionar exibição de microfone ao Smart Client 48
Usar exibição de microfone 48
Ouça vários microfones ao mesmo tempo 49
Detecção de incidentes com áudio 49
Investigue incidentes após eles terem ocorrido 49
Pesquisa forense 50
Pesquisa forense 50
Antes de começar 50
Configurar a pesquisa forense 50
Realizar uma pesquisa 51
Fazer o ajuste preciso de uma pesquisa 52
Limitações 52
Pesquisa de veículos 53
Configurar pesquisa de veículos 55
Procurar um veículo 55
Fazer o ajuste preciso de uma pesquisa 55
Otimizar a velocidade da pesquisa 56
Pesquisa de velocidade na zona 56

Configurar pesquisa de velocidade da zona....56
Pesquisar por eventos de velocidade de zona....57
Fazer o ajuste preciso de uma pesquisa....57
Pesquisa de contêineres....58
Configurar pesquisa de contêineres....58
Procurar um contêiner....58
Fazer o ajuste preciso de uma pesquisa....59
Criar um relatório PDF de alta qualidade....59
Placas de licença da Axis....59
Antes de começar....60
Configurar placas de licença da Axis....60
Procurar uma placa de licença....60
Procurar uma placa de licença em tempo real....60
Fazer o ajuste preciso de uma pesquisa....61
Otimizar a velocidade da pesquisa....61
Exportar uma pesquisa de placa de licença como relatório PDF....61
Exportar uma pesquisa de placa de licença como relatório CSV....62
Percepções da Axis....62
Acesse Axis insights....62
Criar um novo painel....62
Configurar a lista suspensa do painel....63
Exibir insights para uma visualização de câmera específica....63
Configurar percepções de dados Axis....63
Solução de problemas do Axis insights....64
Correção de distorção de vídeo....65
Criar uma exibição de correção de distorção....65
Criar uma exibição de correção de distorção para câmeras panorâmicas multissensor....66
Visão ampla....67
Definir uma posição inicial....67
Permitir que os operadores controlem e editem exibições de correção de distorção....68
Desempenho e solução de problemas....68
Integração a dispositivos de uso corporal....70
Saiba mais....70
Controle de acesso....71
Configuração do controle de acesso....71
Adicionar um controlador de porta em rede Axis ao seu sistema....71
Ativar licenças de porta....72
Configurar o controle de acesso....72
Integração do controle de acesso....72
Portas e zonas....73
Exemplo de portas e zonas....74
Adicione uma porta....74
Configurações da porta....76
Nível de segurança da porta....77
Opções de tempo....78
Adicionar um monitor de porta....79
Adicionar uma porta com monitoramento....79
Adicionar um leitor....80
Adicionar um dispositivo REX....81
Adicionar uma zona....82
Nível de segurança da zona....82
Entradas supervisionadas....83
Ações manuais....84
Formatos de cartão e PIN....84
Configurações de formato de cartão....86
Perfis de identificação....88

Comunicação criptografada 89
OSDP Secure Channel 89
Multisservidor BETA 89
Fluxo de trabalho 90
Gerar o arquivo de configuração do subservidor 90
Importar o arquivo de configuração para o servidor principal 90
Revogar um subservidor 90
Remover um subservidor 90
Gerenciamento de acesso 91
Fluxo de trabalho do gerenciamento de acesso 91
Adicionar um portador de cartão 91
Adicionar credenciais 92
Adicionar um grupo 94
Adicione uma regra de acesso 95
Destravar portas e zonas manualmente 95
Exportar relatórios de configuração do sistema 95
Criar relatórios de atividade de portadores de cartões 96
Configurações de gerenciamento de acesso 97
Importação e exportação 97
Fazer backup e restaurar 99
Gerenciamento de acesso no Smart Client 99
Configurações de funções no AXIS Secure Entry 99
Gerenciamento do sistema e controles de segurança 101
Personalizar acesso a recursos para operadores 101
Configurações da função 101
Configurar opções de funções 101
Gerenciamento de dispositivos 102
AXIS Device Manager Extend 102
Instalar o host de borda 102
Reivindique o host de borda e sincronize os dispositivos 102
Usar o AXIS Device Manager Extend para configurar dispositivos 103
Solução de problemas para adicionar dispositivos ao host de borda 104
Importação do AXIS Site Designer 104
Importar projeto de desenho 104
Configurações importadas 105
Limitações 105
Gerenciamento de contas 106
Conecte-se a dispositivos com conta de serviço XProtect 106
Eventos da Axis 106
Configurar um evento para vários dispositivos 106
Informações sobre eventos 107
Metadados e pesquisas 107
Configurar as opções de metadados 107
Configurar categorias de pesquisa da Axis 108
Cibersegurança 109
Gerenciamento de vulnerabilidades 109
Notificações de segurança 109
Ciclo de vida seguro do produto 109
Guia para aumento do nível de proteção 109
Precisa de mais ajuda? 110
Perguntas Frequentes 110
Solução de problemas 110
Entre em contato com o suporte 110
Dicas e truques 111
Adicionar página da Web em uma exibição do Smart Client 111
Exportar vídeos com funções de pesquisa incorporadas 111

Exportação de vídeos no formato XProtect 111
Desbloquear exportações em computadores receptores..... 111
Reproduzir a visualização corrigida do Axis exportada 111

AXIS Optimizer

O AXIS Optimizer libera recursos da Axis diretamente no XProtect ou Siemens Siveillance Video. O aplicativo otimiza o desempenho dos dispositivos Axis nesses sistemas de gerenciamento de vídeo, o que permite a você poupar tempo e esforço ao configurar um sistema ou durante a operação diária. O aplicativo é gratuito.

Finalidade de uso do AXIS Optimizer

Este produto destina-se ao uso por profissionais que possuam amplo conhecimento na operação de um Sistema de Gerenciamento de Vídeo (VMS).

Requisitos do sistema

O AXIS Optimizer é totalmente compatível com as seguintes plataformas:

- XProtect Essential+
- XProtect Express+
- XProtect Professional+
- XProtect Expert
- XProtect Corporate
- Siemens Siveillance Video Pro
- Siemens Siveillance Video Advanced
- Siemens Siveillance Video Core Plus
- Siemens Siveillance Video Core

Recomendamos usar as versões mais recentes do Management Client e do Smart Client. A versão mais recente do AXIS Optimizer é sempre testada e compatível com a versão mais recente do VMS. Para obter mais informações, leia *Notas de lançamento, on page 7*.

Observação

Plataforma com suporte mínimo

- VMS versão 2019 R3.

Quando fazemos referência ao Smart Client na ajuda, estamos nos referindo ao XProtect Smart Client e ao Video Client em um sistema Siemens.

Suporte a sistemas federados

O AXIS Optimizer é totalmente compatível com sistemas federados.

Suporte a sistemas interconectados

O AXIS Optimizer é totalmente compatível com sistemas interconectados.

Observação

Requisitos

- VMS versão 2022 R3 ou posterior.

Notas de lançamento

Para ver as notas de versão mais recentes, acesse *axis.com/ftp/pub_soft/cam_srv/optimizer_milestone/latest/*/relnote.txt*.

Instalação ou atualização do AXIS Optimizer

Instalação do AXIS Optimizer



Observação

Para atualizar o AXIS Optimizer, você deve ter direitos de administrador.

1. Certifique-se de que você tenha a versão correta do cliente do VMS.
2. Faça login na sua conta MyAxis.
3. Em *axis.com/products/axis-optimizer-for-milestone-xprotect*, baixe o AXIS Optimizer para cada dispositivo que executa o Management Client ou o Smart Client.
4. Execute o arquivo baixado e siga as instruções no guia passo a passo.

Que versões estão instaladas em meu sistema?

Em **System overview (Visão geral do sistema)**, você pode ver quais versões do AXIS Optimizer e AXIS Optimizer Body Worn Extension estão instaladas nos diferentes servidores e clientes em seu sistema.

Observação

Para exibir os clientes ou servidores do seu sistema em **System overview (Visão geral do sistema)**, eles devem ter o AXIS Optimizer versão 3.7.17.0, o AXIS Optimizer Body Worn Extension versão 1.1.11.0 ou versões posteriores.

Para exibir servidores e clientes ativos:

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > System overview (Navegação no site > AXIS Optimizer > Visão geral do sistema)**.

Para atualizar um servidor ou cliente específico:

1. Vá para aquele servidor ou cliente específico e atualize-o localmente.

Opções avançadas de instalação

Para instalar o AXIS Optimizer em vários dispositivos ao mesmo tempo, sem interação com o usuário:

1. Clique com o botão direito do mouse no menu **Start (Iniciar)**.
2. Clique em **Run (Executar)**.
3. Navegue para o arquivo de instalação baixado e clique em **Open (Abrir)**.
4. Adicione um ou mais parâmetros no final do caminho.

Parâmetro	Descrição
`/SILENT`	Durante uma instalação silenciosa, o assistente passo a passo e a janela em segundo plano não são mostrados. No entanto, a janela de progresso da instalação é mostrada.
`/VERYSILENT`	Durante uma instalação muito silenciosa, o assistente passo a passo, a janela em segundo plano e a janela de progresso da instalação não são mostrados.

/FULL	Faça a instalação de todos os componentes, por exemplo, o plug-in opcional do servidor de eventos e o plug-in do Secure Entry. Esta opção é útil quando combinada a /VERYSILENT
/SUPPRESSMSGBOXES	Suprime todas as caixas de mensagens. Geralmente, é combinado com /VERYSILENT
/log=<filename>	Crie um arquivo de log.
/NORESTART	Impede que o computador reinicie durante a instalação.
/EVENTSERVERPLUGIN	Instale o plug-in do servidor de eventos se o computador de destino for o servidor de eventos.
/SECUREENTRY	Instale o serviço de controle de acesso Secure Entry se o computador de destino for o servidor de eventos.

5. Pressione **Enter**.

Exemplo:
Instalação muito silenciosa, registrada em output.txt, sem nenhuma reinicialização do computador

```
.\AxisOptimizerXProtectSetup.exe /VERYSILENT /log=output.txt /NORESTART
```

Migração do VMS

O AXIS Optimizer armazena a maior parte dos dados no banco de dados do VMS e, por isso, as informações são mantidas quando você migra o VMS para outro servidor.

Para migrar seu VMS para outro servidor, consulte *Como transferir uma instalação/versão do XProtect VMS de servidores antigos para novos servidores*.

Verificar a integridade da instalação

Para verificar a integridade do instalador AXIS Optimizer:

1. Clique com o botão direito do mouse no arquivo do instalador e selecione **Properties (Propriedades)**.
2. Vá para **Digital Signatures (Assinaturas digitais)** e clique em **Details (Detalhes)**.
3. Verifique o seguinte:
   - Na seção **Digital Signature Information (Informações sobre a assinatura digital)**, consta: This digital signature is OK (Esta assinatura digital está correta).
   - Em **Signer information (Informações do signatário)** > **Name (Nome)**, consta Axis Communications AB.

Atualização do AXIS Optimizer

Atualizamos regularmente o AXIS Optimizer com novos recursos, melhorias e atualizações de segurança. O AXIS Optimizer oferece apenas uma única linha de versões (a mais recente e avançada), e é somente essa versão mais recente que está disponível para download no site axis.com. Recomendamos que você sempre utilize a versão mais recente do AXIS Optimizer.

O AXIS Optimizer também inclui um recurso que permite atualizar todos os clientes do seu VMS. Para obter mais informações, consulte *Atualizar o sistema automaticamente*.

Observação

Para atualizar o AXIS Optimizer, você deve ter direitos de administrador.

Notificações de atualização

O AXIS Optimizer verifica regularmente se há novas versões e notifica você quando novas atualizações estão disponíveis. Se você tiver uma conexão de rede, receberá notificações de atualização no Smart Client.

Para alterar o tipo das notificações a receber:

1. No Smart Client, vá para **Settings** > **Axis general options** > **Notification preference** (Settings > Axis general options > Notification preference (Configurações > Opções gerais da Axis > Preferência de notificação).
2. Selecione **All (Todas)**, **Major (Principais)** ou **None (Nenhuma)**.

Para realizar a configuração dessas notificações para todos os clientes do seu VMS:

1. Vá para **Management Client** > **Site Navigation** > **AXIS Optimizer** > **System overview** (Management Client > Navegação no site > AXIS Optimizer > Visão geral do sistema).
2. Clique em **System upgrade settings (Configurações de atualização do sistema)**.
3. Ative ou desative **Show upgrade notifications on all clients (Mostrar notificações de atualização em todos os clientes)**.

Atualização manual

Você pode atualizar manualmente o AXIS Optimizer tanto via Management Client quanto pelo Smart Client.

Observação

Para atualizar o AXIS Optimizer, você deve ter direitos de administrador.

No Management Client

1. Vá para **Site Navigation > Basics > AXIS Optimizer (Navegação no site > Fundamentos > AXIS Optimizer)**.
2. Clique em **Atualizar**.

No Smart Client

1. Vá para **Settings > Axis general options (Configurações > Opções gerais da Axis)**.
2. Clique em **Atualizar**.

Atualizar o sistema automaticamente

No servidor de gerenciamento do VMS, você pode publicar uma versão do AXIS Optimizer local para seu sistema. Quando você fizer isso, o AXIS Optimizer será atualizado automaticamente em todas as máquinas clientes. A atualização automática nunca interrompe o trabalho do operador. Instalações silenciosas são realizadas durante a reinicialização do computador ou do cliente VMS. A atualização automática também pode ser feita quando o cliente não está conectado à Internet.

Observação

A atualização automática é compatível com clientes que executam o AXIS Optimizer 4.4 ou posterior.

Ativar a atualização automática



Observação

Requisitos

- Um sistema em que o Management Client é executado no mesmo computador que o servidor de gerenciamento do VMS.
- Direitos de administrador de PC no servidor de gerenciamento do VMS.

Para ativar a atualização automática, é necessário publicar uma versão específica do AXIS Optimizer em seu sistema:

1. No servidor de gerenciamento de VMS, instale a versão do AXIS Optimizer que deseja publicar em todo o sistema.
2. Na máquina do servidor de gerenciamento do VMS, abra o Management Client.
3. Vá para **Site Navigation > AXIS Optimizer > System overview (Navegação no site > AXIS Optimizer > Visão geral do sistema)**.
4. Clique em **System upgrade settings (Configurações de atualização do sistema)**.
5. Certifique-se de que a **Local version (Versão local)** esteja correta e clique em **Publish (Publicar)**.
   Se já houver uma versão publicada do AXIS Optimizer, ela será substituída pela nova versão.

Observação

As máquinas clientes com uma versão do AXIS Optimizer anterior à 4.4 devem ser atualizadas manualmente.

Desativar atualização automática

Para desativar a atualização automática, é necessário redefinir a versão publicada:

1. Na máquina do servidor de gerenciamento do VMS, abra o Management Client.
2. Vá para **Site Navigation > AXIS Optimizer > System overview (Navegação no site > AXIS Optimizer > Visão geral do sistema)**.
3. Clique em **System upgrade settings > Reset published version (Configurações de atualização do sistema > Redefinir versão publicada)**.

Saiba mais

- Smart Clients sem o AXIS Optimizer podem acessar o arquivo do instalador publicado na página da Web do servidor de gerenciamento *http://[endereço do servidor]/installation/*) mesmo se não estiverem conectados à Internet.
- O pacote de instalação do AXIS Optimizer está disponível e pode ser configurado no Gerenciador de downloads do VMS.
- Em sistemas federados ou interconectados, você deve publicar o AXIS Optimizer em cada servidor de gerenciamento.
- Após publicar uma nova versão do AXIS Optimizer, você poderá monitorar quais clientes atualizarão para a versão publicada. As máquinas na página **System overview (Visão geral do sistema)** mostrarão um símbolo de seleção verde quando estiverem executando a versão publicada.
- A atualização automática está desativada em máquinas que executam um servidor de gerenciamento de VMS.

Desinstalar o AXIS Optimizer

Padrão de fábrica

Para redefinir o AXIS Optimizer para sua configuração padrão, desinstale-o do VMS e instale-o novamente.

Descomissionamento seguro

Para remover completamente o AXIS Optimizer e os dados armazenados do VMS, é necessário seguir primeiro as etapas a seguir, quando aplicável, antes de removê-lo do seu computador local.

1. Para remover as listas de placas de licença:

- Abra o Client de Gerenciamento e ir para **AXIS Optimizer** > **Listas de placas de licença**.
- Remova todos os sites da lista.

2. Para desconectar o servidor AXIS Audio Manager Pro:
   - Abra o Management Client e vá para **AXIS Optimizer** > **Speaker manager (Gerenciador de alto-falantes)**.
   - Clique em **Disconnect (Desconectar)**.

Para remover o AXIS Optimizer e os dados armazenados localmente do computador:

1. Clique no **menu Start (Iniciar) > Settings (Configurações)** > **Apps (Aplicativos)** > **Installed apps (Aplicativos instalados)**.
2. Vá para **AXIS Optimizer**.
3. Clique p,255mm,sfx)=″graphics:graphicF514E97847ADD97F4BD7253E4437FE02″ e selecione**Uninstall (Desinstalar)**.

Observação

Após desinstalar o AXIS Optimizer, alguns serviços do VMS podem precisar ser reiniciados.

Privilégios de usuário

O AXIS Optimizer inclui uma função de usuário específica do AXIS Optimizer. O objetivo é simplificar para você fornecer aos usuários os privilégios do Smart Client necessários para usar os recursos e capacidades do AXIS Optimizer.

Se você executa o XProtect 2018 R3 ou anterior, essa função estará disponível somente no XProtect Corporate.

Se você executa o XProtect 2019 R1 ou posterior, essa função estará disponível nas seguintes edições de XProtect:

- Corporativo
- Expert
- Professional+
- Essential+
- Express+

Se você preferir configurar os privilégios manualmente, use essa configuração para permitir que um operador do Smart Client use todos os recursos incluídos no AXIS Optimizer:

- Hardware: comandos de driver
- Câmeras: Comandos AUX

Observação

Para lidar com funções de usuário mais avançadas, consulte *Personalizar acesso a recursos para operadores, on page 101*.

Acessar as configurações dos dispositivos

Assistente de dispositivos

Use o Assistente de dispositivo para fornecer acesso fácil a todas as configurações do dispositivo Axis diretamente no Management Client do VMS. Você pode encontrar e acessar facilmente a página da Web do seu dispositivo Axis no VMS para alterar configurações de dispositivos diferentes. Você também pode configurar aplicativos instalados em seus dispositivos.

Importante

- Para usar o Assistente de dispositivos, o dispositivo Axis deve estar conectado à mesma rede que o Management Client.
- O Assistente de dispositivos não é compatível com redes IPv6.

Configurar um dispositivo Axis

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Device assistant)**.
2. Selecione um dispositivo e vá para **Device settings (Configurações do dispositivo)**. A página da Web do dispositivo será aberta
3. Defina as configurações desejadas.

Instalar aplicativos em um dispositivo Axis

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Device assistant)**.
2. Selecione um dispositivo e vá para **Device settings (Configurações do dispositivo)**. A página da Web do dispositivo será aberta
3. Vá para **Apps (Aplicativos)**. O local em que a funcionalidade **Apps (Aplicativos)** pode ser encontrada depende da versão do software do dispositivo. Para obter mais informações, consulte a ajuda do aplicativo.
4. Instale os aplicativos desejados.

Configurar aplicativos em um dispositivo Axis

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Device assistant)**.
2. Selecione um dispositivo e acesse **Applications (Aplicativos)**. Se algum aplicativo estiver instalado no dispositivo, você os verá aqui.
3. Vá para o aplicativo relevante, por exemplo, o AXIS Object Analytics.
4. Configure o aplicativo de acordo com suas necessidades.

Atualizar aplicativos em um dispositivo Axis

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Device assistant)**.
2. Clique com o botão direito do mouse em um dispositivo e selecione **Show updates (Mostrar atualizações)**. Se algum aplicativo puder ser atualizado, você verá uma lista de atualizações disponíveis.
3. Baixe o arquivo de atualização.
4. Clique em **How to update (Como atualizar)** e siga as instruções.

Reiniciar um dispositivo Axis

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Device assistant)**.
2. Clique com o botão direito do mouse em um dispositivo e selecione **Restart device (Reiniciar dispositivo)**.

Copiar o endereço IP de um dispositivo Axis

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Device assistant)**.
2. Clique com o botão direito do mouse em um dispositivo e selecione **Copy device address (Copiar endereço do dispositivo)**.

Realize a automação

Crie ações para dispositivos Axis

Plug-in do servidor de eventos

O plug-in do servidor de eventos do AXIS Optimizer permite criar ações personalizadas para os dispositivos Axis. Ao usar o mecanismo de regras do XProtect e o plug-in do servidor de eventos, você pode, por exemplo:

- Executar uma ação personalizada quando o operador clicar em um botão no Smart Client. Para obter um exemplo de configuração, consulte *Secar várias câmeras com um clique, on page 15*.
- Executar ações sem interação humana (automação). Para obter um exemplo de configuração, consulte *Desativar automaticamente máscaras de privacidade em várias câmeras, on page 18*.

O plug-in do servidor de eventos consiste em duas partes:

- Um plug-in separado que é executado no servidor de eventos. Ele preenche o mecanismo de regras com novas ações.
- Uma página chamada **Axis actions (Ações da Axis)** no servidor de gerenciamento, na qual você pode criar novas predefinições de ações.

As ações personalizadas para os dispositivos Axis são: Executar o controle do operador, ativar/desativar o radar, iniciar uma chamada no intercomunicador e secar a câmera (secagem rápida/limpador).

O plug-in do servidor de eventos está incluído no AXIS Optimizer. Em um sistema com vários PCs, você deve instalar o AXIS Optimizer tanto no computador do Management Client quanto na máquina do servidor de eventos.

Instalar plug-in do servidor de eventos

O plug-in do servidor de eventos é um componente opcional que está incluído no instalador do AXIS Optimizer. Você só pode instalá-lo em um servidor de eventos de sistema de gerenciamento de vídeo (VMS). Se os requisitos forem atendidos, você receberá uma opção para instalar o plug-in do servidor de eventos ao executar o instalador do AXIS Optimizer.

Observação

O servidor de eventos do VMS exigirá uma reinicialização curta durante a instalação e, às vezes, durante a atualização do AXIS Optimizer. Você será notificado quando esse for o caso.

Secar várias câmeras com um clique

Com o plug-in do servidor de eventos, você pode configurar regras personalizadas para facilitar a vida dos operadores. Neste exemplo, mostraremos como secar todas as câmeras em uma área específica clicando em um botão de sobreposição.



Observação

Requisitos

- AXIS Optimizer versão 4.0 ou posterior no servidor de eventos e no Management Client
- Uma ou várias câmeras compatíveis com secagem rápida ou limpador, por exemplo, AXIS Q86, Q87 ou Q61 Series.

1. Adicionar um evento definido pelo usuário:

1.1. Vá para **Site Navigation > Rules and Events (Navegação no site > Regras e eventos)** e clique com o botão direito em **User-defined Event (Evento definido pelo usuário)**.

1.2. Selecione **Add User-defined Event (Adicionar evento definido pelo usuário)** e insira um nome. Neste exemplo, "Dry all cameras" (Secar todas as câmeras).

2. Crie uma nova regra:

2.1. Vá para **Site Navigation > Rules and Events (Navegação no site > Regras e eventos)** e clique com o botão direito em **Rules (Regras)**.

2.2. Selecione **Add Rule (Adicionar regra)** e insira um nome. Neste exemplo, "Dry all cameras Rule" (Regra para secar todas as câmeras).

2.3. Selecione **Perform an action on <event. (Realizar uma ação em evento)>**.

2.4. No campo **Edit the rule description (Editar a descrição da regra)**, clique em **event (evento)**.

2.5. Vá para **Events > External Events > User-defined Events (Eventos > Eventos externos > Eventos definidos pelo usuário)** e selecione **Dry all cameras (Secar todas as câmeras)**.

2.6. Clique em **Next (Avançar)** até chegar a **Step 3: Actions (Etapa 3: ações)**.

2.7. Selecione a ação: **Axis: Dry <camera> (Secar a câmera)**.

2.8. No campo **Edit the rule description (Editar a descrição da regra)**, clique em **Axis: Dry camera (Secar a câmera)**.

2.9. Na janela **Select Triggering Devices (Selecionar dispositivos de acionamento)**, escolha **Select devices (Selecionar dispositivos)** e clique em **OK**.

2.10. Selecione os dispositivos que deseja que acionem a ação e clique em **OK**. Em seguida , clique em **Finish (Concluir)**.

3. No Smart Client, adicione o evento definido pelo usuário como um botão de sobreposição em uma exibição de mapa ou vídeo.

4. Clique no botão sobreposição e certifique-se de que a regra funcione da forma desejada.

Ative o foco automático para várias câmeras com apenas um clique

Com o plug-in do servidor de eventos, você pode configurar regras personalizadas para facilitar a vida dos operadores. Neste exemplo, mostraremos como ativar o foco automático para todas as câmeras com apenas um clique.

Observação

Requisitos

- AXIS Optimizer versão 4.1 ou posterior no servidor de eventos e no Management Client
- Uma ou várias câmeras que oferecem suporte ao foco automático

1. Adicionar um evento definido pelo usuário:

1.1. Vá para **Site Navigation > Rules and Events (Navegação no site > Regras e eventos)** e clique com o botão direito em **User-defined Event (Evento definido pelo usuário)**.

1.2. Selecione **Add User-defined Event (Adicionar evento definido pelo usuário)** e insira um nome, por exemplo "Autofocus" (Foco automático).

2. Crie uma nova regra:

2.1. Vá para **Site Navigation > Rules and Events (Navegação no site > Regras e eventos)** e clique com o botão direito em **Rules (Regras)**.

2.2. Selecione **Add Rule (Adicionar regra)** e insira um nome, neste exemplo, "Perform autofocus" (Executar foco automático).

2.3. Selecione **Perform an action on <event. (Realizar uma ação em evento)>**.

2.4. No campo **Edit the rule description (Editar a descrição da regra)**, clique em **event (evento)**.

2.5. Vá para **Events > External Events > User-defined Events (Eventos > Eventos externos > Eventos definidos pelo usuário)** e selecione **Autofocus (Foco automático)**. Clique em **OK**.

2.6. Clique em **Next (Avançar)** até chegar a **Step 3: Actions (Etapa 3: ações)**.

2.7. Selecione a ação: **Axis: Run autofocus on <camera>** (Executar foco automático na câmera).

2.8. No campo **Edit the rule description (Editar a descrição da regra)**, clique em **Axis: Run autofocus on camera (Executar foco automático na câmera)**.

2.9. Na janela **Select Triggering Devices (Selecionar dispositivos de acionamento)**, escolha **Select devices (Selecionar dispositivos)** e clique em **OK**.

2.10. Selecione os dispositivos que deseja que acionem a ação e clique em **OK**. Em seguida , clique em **Finish (Concluir)**.

3. No Smart Client, adicione o evento definido pelo usuário "Autofocus" (Foco automático) como um botão de sobreposição em uma exibição de mapa ou vídeo.
4. Clique no botão sobreposição e certifique-se de que a regra funcione da forma desejada.

Acionar várias sirenes estroboscópicas com um clique

Com o plug-in do servidor de eventos, você pode configurar regras personalizadas para facilitar a vida dos operadores. Neste exemplo, mostraremos como ativar várias sirenes estroboscópicas com um clique no Smart Client.

Observação

Requisitos

- AXIS Optimizer versão 4.4 ou posterior no servidor de eventos e no Management Client
- Um ou mais sirenes estroboscópicas Axis
- Saída 1 da sirene estroboscópica Axis ativada e adicionada aos dispositivos de saída no Management Client

1. Crie um evento definido pelo usuário:
   1.1. Vá para **Site Navigation > Rules and Events (Navegação no site > Regras e eventos)** e clique com o botão direito em **User-defined Event (Evento definido pelo usuário)**.
   1.2. Selecione **Add User-defined Event (Adicionar evento definido pelo usuário)** e insira um nome, por exemplo, "Acionar todas as sirenes estroboscópicas".
2. No assistente de dispositivos, crie perfis de sirenes estroboscópicas:
   2.1. Vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Assistente de dispositivos)**.
   2.2. Selecione uma sirene estroboscópica. A página da Web da sirene estroboscópica é aberta.
   2.3. Vá para **Profiles (Perfis)** e clique em **Add profile (Adicionar perfil)**.
   2.4. Configure o que você deseja que a sirene estroboscópica faça quando o operador a acionar no Smart Client.
   2.5. Crie os mesmos perfis nas outras sirenes estroboscópicas. Você deve usar o mesmo nome de perfil em todos os dispositivos
3. Nas ações da Axis, crie uma predefinição de ação:
   3.1. Acesse **Site Navigation > Rules and Events > Axis actions (Navegação no site > Regras e eventos > Ações da Axis)**.
   3.2. Clique em **Add new preset (Adicionar nova predefinição)**.
   3.3. Vá para **Select strobe siren (Selecionar sirene estroboscópica)** e clique em **Strobe siren (Sirene estroboscópica)**.
   3.4. Selecione as sirenes estroboscópicas que deseja usar e clique em **OK**.
   Você verá uma lista de perfis de sirenes estroboscópicas
   3.5. Selecione o perfil de sirene estroboscópica que você criou na etapa anterior. A predefinição de ação será salva automaticamente

3.6. Pressione F5 para atualizar a configuração do servidor. Agora você pode começar a usar a nova predefinição de ação que criou.

4. Crie uma regra:
   4.1. Vá para **Site Navigation > Rules and Events (Navegação no site > Regras e eventos)** e clique com o botão direito em **Rules (Regras)**.
   4.2. Selecione **Add Rule (Adicionar regra)** e insira um nome, por exemplo, "Regra Acionar todas as sirenes estroboscópicas".
   4.3. Selecione **Perform an action on <event. (Realizar uma ação em evento)>**.
   4.4. No campo **Edit the rule description (Editar a descrição da regra)**, clique em **event (evento)**.
   4.5. Vá para **Events > External Events > User-defined Events (Eventos > Eventos externos > Eventos definidos pelo usuário)** e selecione **Trigger all strobe sirens (Acionar todas as sirenes estroboscópicas)**.
   4.6. Clique em **Next (Avançar)** até chegar a **Step 3: Actions (Etapa 3: ações)**.
   4.7. Selecione a ação **Axis: Run a profile on a strobe siren (Axis: Executar um perfil em uma sirene estroboscópica) <preset (predefinido)>**.
   4.8. No campo **Edit the rule description (Editar a descrição da regra)**, clique em **preset (predefinido)**.
   4.9. Selecione a predefinição que deseja usar.
   4.10. Clique em **Next (Avançar)** e em **Finish (Concluir)**.
5. No Smart Client, adicione o evento definido pelo usuário como um botão de sobreposição em uma exibição de mapa ou vídeo.
6. Clique no botão sobreposição e certifique-se de que a regra funcione da forma desejada.

Desativar automaticamente máscaras de privacidade em várias câmeras

Com o plug-in de servidor de eventos, você pode automatizar determinadas ações. Neste exemplo, mostraremos como desativar automaticamente máscaras de privacidade em várias câmeras quando um evento de análise ocorrer. O evento no exemplo é que pessoas ou veículos entram em uma área em que normalmente não deveriam estar. Portanto, queremos desativar automaticamente as máscaras de privacidade para obter uma visão melhor do que está acontecendo.



O fluxo de trabalho é:

1. *Configurar um cenário analítico, on page 19* no AXIS Object Analytics (outro aplicativo de análise à sua escolha)
2. *Adicionar controles do operador às câmeras relevantes, on page 19*
3. *Criar predefinições de ações, on page 19*
4. *Crie uma regra para desativar máscaras de privacidade quando o evento de análise ocorrer, on page 19*
5. *Crie uma regra para ativar as máscaras de privacidade novamente, on page 20*
6. *Testar a regra, on page 20* e se certifique de que tudo funcione da forma desejada.

Observação

Requisitos

- AXIS Optimizer versão 4.0 ou posterior no servidor de eventos e no Management Client
- Câmeras com AXIS OS 7.40 ou posterior
- Câmeras que possam gerar eventos; neste exemplo, uma câmera com AXIS Object Analytics

Configurar um cenário analítico

1. Vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Assistente de dispositivos)** e encontre o dispositivo com a análise que deseja usar.
2. Clique em **Applications (Aplicativos)** e crie um cenário de análise para acionar a ação.
3. Vá para **Devices > Cameras (Dispositivos > Câmeras)** e encontre a câmera em que você criou o cenário de análise.
4. Na janela **Properties (Propriedades)**, clique em **Events > Add (Eventos > Adicionar)**.
5. Selecione um evento acionador, neste exemplo, "Object Analytics: Event test Rising" (Teste de evento de subida) e clique em **OK**.
6. Clique em **Add (Adicionar)** e selecione o evento acionador "Object Analytics: Event test Failing" (Análise de objetos: Falha no teste de evento). Em seguida, clique em **OK**.
7. Clique em **Save (Salvar)**.

Adicionar controles do operador às câmeras relevantes

1. Vá para **AXIS Optimizer > Operator controls (AXIS Optimizer > Controles do operador)** e abra a biblioteca de controles.
2. Na janela **Configuration (Configuração)**, selecione a pasta relevante e ative **Turn off privacy mask (Desativar máscara de privacidade)** e **Turn on privacy mask (Ativar máscara de privacidade)**.

Criar predefinições de ações

1. Vá para **Rules and Events > Axis actions (Regras e eventos > Ações da Axis)** e clique em **Add new preset (Adicionar nova predefinição)**.
2. Clique em **Cameras (Câmeras)** e selecione câmeras relevantes. Neste exemplo: AXIS P1375 e AXIS Q6075-E. Em seguida, selecione o controle **Turn on privacy mask (Ativar máscara de privacidade)**.
3. Clique em **Add new preset > Cameras (Adicionar nova predefinição > Câmeras)** e selecione as câmeras relevantes. Neste exemplo: AXIS P1375 e AXIS Q6075-E. Em seguida, selecione o controle **Turn off privacy mask (Desativar máscara de privacidade)**.

Crie uma regra para desativar máscaras de privacidade quando o evento de análise ocorrer

1. Vá para **Site Navigation > Rules and Events (Navegação no site > Regras e eventos)** e clique com o botão direito em **Rules (Regras)**.
2. Selecione **Add Rule (Adicionar regra)** e insira um nome. Neste exemplo, "Turn off privacy mask on analytics stop" (Desativar máscara de privacidade quando a análise parar).
3. Selecione **Perform an action on <event. (Realizar uma ação em evento)>**.
4. No campo **Edit the rule description (Editar a descrição da regra)**, clique em **event (evento)**. Acesse **Devices (Dispositivos) > Configurable Events (Eventos configuráveis)** e selecione **Object Analytics: Event test Rising (Teste de evento de aumento)**.
5. No campo **Edit the rule description (Editar descrição da regra)**, selecione um dispositivo. Neste exemplo, AXIS P1375.
6. Clique em **Next (Avançar)** até chegar a **Step 3: Actions (Etapa 3: ações)**.
7. Selecione a ação **Axis: Run operator control: <preset> (Executar o controle do operador predefinido)**.

8. No campo **Edit the rule description (Editar a descrição da regra)**, clique em **preset (predefinido)**. Em seguida, adicione **Turn off privacy mask on 2 cameras (Desativar máscara de privacidade em 2 câmeras)** e clique em **OK**.
9. Clique em **Finish (Concluir)**.

Crie uma regra para ativar as máscaras de privacidade novamente

1. Selecione **Add Rule (Adicionar regra)** e insira um nome. Neste exemplo, "Turn on privacy mask on analytics stop" (Ativar máscara de privacidade quando a análise parar).
2. Selecione **Perform an action on <event. (Realizar uma ação em evento)>**.
3. Na seção **Edit the rule description (Editar a descrição da regra)**, clique em **event (evento)**. Acesse **Devices (Dispositivos) > Configurable Events (Eventos configuráveis)** e selecione **Object Analytics: Event test Failing (Teste de evento de diminuição)**.
4. Na seção **Edit the rule description (Editar descrição da regra)**, selecione um dispositivo. Neste exemplo, AXIS P1375.
5. Clique em **Next (Avançar)** até chegar a **Step 3: Actions (Etapa 3: ações)**.
6. Selecione a ação **Axis: Run operator control: <preset> (Executar o controle do operador predefinido)**.
7. Na seção **Edit the rule description (Editar a descrição da regra)**, clique em **preset (predefinido)**. Em seguida, adicione **Turn on privacy mask on 2 cameras (Ativar a máscara de privacidade em 2 câmeras)** e clique em **OK**.
8. Clique em **Finish (Concluir)**.

Testar a regra

1. Vá para **AXIS Optimizer > Device assistant (AXIS Optimizer > Assistente de dispositivos)** e encontre o dispositivo com a análise que você usou para criar a automação. Neste exemplo, a AXIS P1375.
2. Abra o cenário relevante e clique em **Test alarm (Testar alarme)**.

Ativar uma sirene estroboscópica quando uma câmera detectar movimento

Com o plug-in do servidor de eventos, você pode configurar regras personalizadas para automatizar ações. Neste exemplo, mostraremos como ativar sirenes estroboscópicas automaticamente quando uma câmera detectar movimento.

Observação

Requisitos

- AXIS Optimizer versão 4.4 ou posterior no servidor de eventos e no Management Client
- Um ou mais sirenes estroboscópicas Axis
- Saída 1 da sirene estroboscópica Axis ativada e adicionada aos dispositivos de saída no Management Client.
- Para uma versão mais antiga que o VMS versão 2022 R2, as ações da Axis não estão disponíveis como ações de parada. Para versões mais antigas, é necessário criar duas regras separadas para executar e parar a sirene estroboscópica.

1. Crie perfis de sirenes estroboscópicas:
   1.1. Vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Assistente de dispositivos)**.
   1.2. Vá para **Axis output devices (Dispositivos de saída Axis)** e selecione uma sirene estroboscópica. A página da Web da sirene estroboscópica é aberta.
   1.3. Vá para **Profiles (Perfis)** e clique em **Add profile (Adicionar perfil)**.
   1.4. Certifique-se de escolher o mesmo nome de perfil para todas as sirenes.
   1.5. Configure o que você deseja que a sirene estroboscópica faça ao detectar movimento.

2. Criar predefinições de ações para iniciar e parar:
   2.1. Acesse **Site Navigation > Rules and Events > Axis actions (Navegação no site > Regras e eventos > Ações da Axis)**.
   2.2. Para criar uma predefinição de início, vá para **Strobe siren (Sirene estroboscópica)** e clique em **Add new preset (Adicionar nova predefinição)**.
   2.3. Vá para **Select strobe siren (Selecionar sirene estroboscópica)** e clique em **Strobe siren (Sirene estroboscópica)**.
   2.4. Selecione uma ou mais sirenes estroboscópicas na lista.
   2.5. Selecione o perfil de sirene que você criou anteriormente na lista. A predefinição de ação será salva automaticamente
   2.6. Para criar uma predefinição de parada, clique em **Add new preset (Adicionar nova predefinição)**.
   2.7. Vá para **Select strobe siren (Selecionar sirene estroboscópica)** e clique em **Strobe siren (Sirene estroboscópica)**.
   2.8. Selecione as mesma sirenes estroboscópicas na lista que foram escolhidas para a predefinição de início.
   2.9. Vá para **Select action (Selecionar ação)** e selecione **Stop (Parar)**.
   2.10. Selecione o mesmo perfil de sirene que foi criado para a ação de início. A predefinição de ação será salva automaticamente
   2.11. Clique em **click to refresh (clique para atualizar)** ou pressione F5 para atualizar a configuração do servidor.
3. Crie uma regra:
   3.1. Acesse **Site Navigation > Rules and Events > Rules (Navegação no site > Regras e eventos > Regras)**.
   3.2. Clique com o botão direito do mouse em **Rules (Regras)**, selecione **Add Rule (Adicionar regra)** e insira um nome.
   3.3. Em **Edit the rule description (Editar a descrição da regra)**, clique em **event (evento)**.
   3.4. Acesse **Devices > Predefined Events (Dispositivos Eventos predefinidos)** e selecione **Motion Started (Iniciado por movimento)**.
   3.5. Em **Edit the rule description (Editar a descrição da regra)**, clique em **devices/recording_server/ /management_server**.
   3.6. Selecione a câmera que deve acionar as sirenes estroboscópicas.
   3.7. Clique em **Next (Avançar)** até chegar a **Step 3: Actions (Etapa 3: ações)**.
   3.8. Selecione a ação **Axis: Start or stop a profile on a strobe siren (Axis: Iniciar ou parar um perfil em uma sirene estroboscópica): <preset (predefinido)>**.
   3.9. Em **Edit the rule description (Editar a descrição da regra)**, clique em **preset (predefinido)**.
   3.10. Selecione a predefinição de início que você criou anteriormente.
   3.11. Clique em **Next (Avançar)** e selecione **Perform stop action on <event. (Executar ação de parada em evento)>**.
   3.12. Clique em **Next (Avançar)** e selecione **Axis: Start or stop a profile on a strobe siren (Axis: Iniciar ou parar um perfil em uma sirene estroboscópica) <event (evento)>**.
   3.13. Em **Edit the rule description (Editar a descrição da regra)**, clique em **preset (predefinido)**.
   3.14. Selecione a predefinição de parada que você criou anteriormente.
   3.15. Selecione **Finish (Concluir)**.
4. Teste se as sirenes estroboscópicas funcionam corretamente quando há movimento detectado pela câmera.

Reproduzir clipes de áudio em alto-falantes ou em uma zona de alto-falante quando uma câmera detecta movimento



Com o plug-in do servidor de eventos, você pode configurar regras personalizadas para automatizar ações – as predefinições de ações Neste exemplo, mostramos como reproduzir automaticamente um clipe de áudio em um alto-falante de áudio ou em uma zona de alto-falantes quando uma câmera detectar movimento.

Observação

Requisitos

- AXIS Optimizer versão 4.6 ou posterior no servidor de eventos e no Management Client.
- Um ou vários alto-falantes Axis dedicados ou dispositivos Axis com alto-falantes integrados.
- Para reproduzir um clipe de áudio em uma zona de alto-falantes, é necessário um sistema AXIS Audio Manager Edge ou AXIS Audio Manager Pro com a configuração correta. Para obter mais informações sobre como configurar esses sistemas, consulte *Modo de configuração, on page 31*.

1. Para carregar um clipe de áudio:
   1.1. Com o modo AXIS Audio Manager Edge ou modo Legacy (legado) Coloque o clipe de áudio que deseja carregar nos alto-falantes na pasta padrão **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
   No modo AXIS Audio Manager Pro, envie clipes de áudio pela interface web do AXIS Audio Manager Pro.
   1.2. No Management Client, vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navegação no site, Gerenciador de alto-falantes) e selecione um alto-falante, grupo de dispositivos ou zona de alto-falantes da lista.

   Observação

   Para obter mais informações sobre como selecionar um modo de gerenciamento de alto-falantes, consulte *Modo de configuração, on page 31*.

   1.3. Vá para **Audio clips (Clipes de áudio)** e clique em **+** na frente do clipe de áudio que deseja carregar.
   1.4. No modo Legacy, repita as etapas 1.2 a 1.3 para cada alto-falante no qual você deseja reproduzir o clipe de áudio. Certifique-se de carregar o mesmo arquivo de áudio para cada alto--falante.
2. Para criar predefinições de ações para reproduzir um clipe de áudio em um alto-falante ou em uma zona de alto-falantes:
   2.1. Vá para **Site Navigation** > **Rules and Events** > **Axis actions.** (Navegação no site > Regras e Eventos > Ações Axis).
   2.2. Para criar uma predefinição, vá para **Audio clips (Clipes de áudio)** e clique em **Add new preset (Adicionar nova predefinição)**.
   2.3. No modo AXIS Audio Manager Edge ou AXIS Audio Manager Pro, vá para **Select playback destination (Selecionar destino de reprodução)**.
   No modo Legacy, vá para **Select speaker (Selecionar alto-falante)**.
   2.4. Selecione um alto-falante ou uma zona de alto-falantes.
   2.5. Na lista, selecione o clipe de áudio que você enviou na etapa 1. A predefinição de ação será salva automaticamente

2.6. No modo AXIS Audio Manager Pro, vá para **Select visual profile (Selecionar perfil visual)** e configure o perfil visual e o texto.

Observação

Selecione **Default (Padrão)** na lista de perfis visuais para utilizar o comportamento padrão do perfil visual no servidor AXIS Audio Manager Pro quando a ação do clipe de áudio for acionada.

2.7. Clique em **refresh (atualizar)** ou pressione F5 ara atualizar a configuração do servidor.

3. Para criar uma regra:
   3.1. Vá para **Site Navigation** > **Rules and Events** > **Rules** ((Navegação no site > Regras e eventos > Regras).
   3.2. Clique com o botão direito do mouse em **Rules (Regras)**, selecione **Add Rule (Adicionar regra)** e insira um nome.
   3.3. Em **Edit the rule description (Editar a descrição da regra)**, clique em **event (evento)**.
   3.4. Vá para **Devices** > **Predefined Events** (Dispositivos > Eventos predefinidos) e selecione **Motion Started** (Movimento iniciado).
   3.5. Em **Edit the rule description (Editar a descrição da regra)**, clique em **devices/recording_server/ /management_server**.
   3.6. Selecione a câmera que deve acionar a predefinição de ação ou o clipe de áudio.
   3.7. Clique em **Next (Avançar)** até chegar a **Step 3: Actions (Etapa 3: ações)**.
   3.8. Selecione a ação **Axis: Play audio clip: <preset> (Axis: reproduzir clipes de áudio: <predefinido>**.
   3.9. Em **Edit the rule description (Editar a descrição da regra)**, clique em **preset (predefinido)**.
   3.10. Selecione a predefinição que você criou na etapa anterior.
   3.11. Selecione **Finish (Concluir)**.
4. Teste se o clipe de áudio é executado corretamente quando o movimento é detectado pela câmera.

Solucionar problemas em uma regra

Se uma regra não funcionar, verifique primeiro as mensagens do servidor de eventos para ver se o serviço de eventos está em execução.

Você também pode verificar os logs do AXIS Optimizer no servidor de eventos. Se o Management Client ou Smart Client estiverem disponíveis, use-os para ativar e salvar logs.

Gerenciamento centralizado de listas de placas de licença

Ao usar o gerenciador de listas do AXIS Optimizer, você poderá gerenciar de forma centralizada listas de placas de licença para todas as câmeras ao mesmo tempo. Você pode criar e gerenciar listas de permissão, lista de bloqueio e listas personalizadas diretamente do VMS. O sistema oferece suporte a listas combinadas. Isso significa que você pode ter uma lista global que se aplica a todas as câmeras no sistema e listas locais que se aplicam a câmeras específicas.

O gerenciamento centralizado de listas é útil, por exemplo, quando você deseja automatizar a entrada e a saída do estacionamento ou deseja receber um alarme quando o sistema registra uma determinada placa de licença.

Você deve ser um administrador para criar e editar listas. É possível conceder direitos de leitura e edição a outras funções, consulte a seção *Configurar permissões de lista, on page 24*.

Criar uma lista

Observação

Requisitos

- AXIS License Plate Verifier 1.8 ou posterior em execução nas câmeras
- Para criar listas personalizadas, é necessário ter o AXIS License Plate Verifier 2.0 ou posterior

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > License plate lists (Navegação no site > AXIS Optimizer > Listas de placas de licença)**.
2. Selecione as câmeras que deseja enviar para a lista de permitidas, lista de bloqueadas e lista personalizada.
3. (Opcional) Adicionar funções de usuário que podem exibir e editar a lista de permitidas, a lista de bloqueadas e listas personalizadas.
4. Adicione placas de licença à lista de permitidas, lista de bloqueadas e lista personalizada.
   Também é possível importar listas de placas de licença existentes.
   Quando a lista recebe o status **Synchronized (Sincronizada)**, ela foi enviada para as câmeras que você selecionou.

Configurar permissões de lista

Você pode configurar quais funções de usuário podem editar a lista de permissão, a lista de bloqueio e a lista personalizada. Isso é útil, por exemplo, quando o administrador configurou as listas, mas você deseja que o operador adicione visitantes com base em necessidades diárias.

No Management Client

Todas as permissões para exibir e editar listas podem ser escolhidas individualmente para cada lista.

1. Vá para **Security > Roles (Segurança > Funções)** e selecione uma função
2. Vá para a guia **AXIS Optimizer**.
3. Vá para **Role settings** > **AXIS Optimizer** > **License plate lists (Configurações de função > AXIS Optimizer > Listas de placas de licença)**.
4. Selecione **Read (Ler)** no campo **License plate lists (node) (Listas de placas de licença (nó))**.
5. Selecione uma lista em **License plate lists (Listas de placas de licença)** e selecione **Edit license plates (Editar placas de licença)**.
   - Para versões anteriores ao XProtect 2023 R2, vá para **MIP > AXIS Optimizer > AXIS Optimizer Security > License plate lists (MIP > AXIS Optimizer > AXIS Optimizer Security > Listas de placas de licença)** e selecione **Edit license plate lists (Editar listas de placas de licença)**.

Editar uma lista

No Management Client

1. Vá para **Site Navigation > AXIS Optimizer > License plate lists (Navegação no site > AXIS Optimizer > Listas de placas de licença)**.
2. Selecione o site que deseja editar.
3. Atualize **Cameras (Câmeras)** ou **License plates (Placas de licença)** conforme necessário.
   Quando a lista receber o status **Synchronized (Sincronizada)**, suas alterações são enviadas para as câmeras selecionadas.

No Smart Client

1. Vá para *Placas de licença da Axis, on page 59* e clique em **License plate lists (Listas de placas de licença)**.
   Se você não conseguir ver a guia, vá para **Settings > Axis search options (Configurações > Opções de pesquisa da Axis)** e selecione **Show license plate tab (Mostrar guia de placas de licença)**.
2. Selecione o site que deseja editar.
3. Adicione placas de licença à lista de permitidas, lista de bloqueadas e lista personalizada.
   Também é possível importar listas de placas de licença existentes.

Quando a lista recebe o status **Synchronized (Sincronizada)**, ela foi enviada para as câmeras que você selecionou.

Importar uma lista

Você pode importar listas em vários formatos de texto ou CSV.

- Formato de texto permitido: uma placa de licença em cada linha
- Formatos CSV permitidos:
  - Uma placa de licença em cada linha
  - Dois campos: placa de licença e data
  - Três campos: placa de licença, proprietário e comentário
  - Quatro campos: placa de licença, proprietário, comentário e a cadeia de caracteres "Active" (Ativo) ou "Inactive" (Inativo). (O mesmo formato que uma lista exportada.)

No Management Client

1. Vá para **Site Navigation > AXIS Optimizer > License plate lists (Navegação no site > AXIS Optimizer > Listas de placas de licença)**.
2. Selecione o site que deseja editar.
3. Vá para **Allowed (Permitidas)**, **Blocked (Bloqueadas)** ou **Custom (Personalizada)**.
4. Clique em ⋮ e, em seguida, selecione **Import to allow list (Importar para lista de permitidas)**, **Import to block list (Importar para lista de bloqueadas)** ou **Import to custom list (Importar para lista personalizada)**.
5. Na caixa de diálogo **Reset list (Redefinir lista)**:
   - Clique em **Yes (Sim)** para remover todas as placas de licença existentes e adicionar somente as placas de licença recém-importadas à lista.
   - Clique em **No (Não)** para mesclar as placas de licença recém-importadas com as placas de licença existentes na lista.

No Smart Client

1. Vá para *Placas de licença da Axis, on page 59* e clique em **License plate lists (Listas de placas de licença)**.
   Se você não conseguir ver a guia, vá para **Settings > Axis search options (Configurações > Opções de pesquisa da Axis)** e selecione **Show license plate tab (Mostrar guia de placas de licença)**.
2. Selecione o site que deseja editar.
3. Vá para **Allowed (Permitidas)**, **Blocked (Bloqueadas)** ou **Custom (Personalizada)**.
4. Clique em ⋮ e, em seguida, selecione **Import to allow list (Importar para lista de permitidas)**, **Import to block list (Importar para lista de bloqueadas)** ou **Import to custom list (Importar para lista personalizada)**.
5. Na caixa de diálogo **Reset list (Redefinir lista)**:
   - Clique em **Yes (Sim)** para remover todas as placas de licença existentes e adicionar somente as placas de licença recém-importadas à lista.
   - Clique em **No (Não)** para mesclar as placas de licença recém-importadas com as placas de licença existentes na lista.

Exportar uma lista

Observação

Para exportar listas de placas de licença, é necessário ter direitos de administrador.

No Management Client

1. Vá para **Site Navigation > AXIS Optimizer > License plate lists (Navegação no site > AXIS Optimizer > Listas de placas de licença)**.
2. Selecione o site que deseja editar.
3. Vá para **Allowed (Permitidas)**, **Blocked (Bloqueadas)** ou **Custom (Personalizada)**.
4. Clique em ⋮ e, em seguida, selecione **Export allow list (Exportar lista de permitidas)**, **Export block list (Exportar lista de bloqueadas)** ou **Export custom list (Exportar lista personalizada)**.
   A lista será exportada no formato CSV com quatro campos: placa de licença, proprietário, comentário e o status "Active" (Ativa) ou "Inactive" (Inativa).

No Smart Client

1. Vá para *Placas de licença da Axis, on page 59* e clique em **License plate lists (Listas de placas de licença)**.
   Se você não conseguir ver a guia, vá para **Settings > Axis search options (Configurações > Opções de pesquisa da Axis)** e selecione **Show license plate tab (Mostrar guia de placas de licença)**.
2. Selecione o site que deseja editar.
3. Vá para **Allowed (Permitidas)**, **Blocked (Bloqueadas)** ou **Custom (Personalizada)**.
4. Clique em ⋮ e, em seguida, selecione **Export allow list (Exportar lista de permitidas)**, **Export block list (Exportar lista de bloqueadas)** ou **Export custom list (Exportar lista personalizada)**.
   A lista será exportada no formato CSV com quatro campos: placa de licença, proprietário, comentário e o status "Active" (Ativa) ou "Inactive" (Inativa).

Saiba mais sobre listas

- É possível criar vários sites.
- Cada site é associado a uma ou várias câmeras que possuem o AXIS License Plate Verifier instalado.
- Cada site está associado a uma ou várias funções de usuário do VMS. A função de usuário define quem tem permissão para ler e editar as listas de placas de licença.
- Todas as listas são armazenadas no banco de dados do VMS.
- Quando você adiciona a câmera a um site, placas de licença já existentes na câmera são sobrescritas.
- Se a mesma câmera estiver presente em vários sites, a câmera receberá a soma de todas as listas.
- Se a mesma placa de licença estiver presente em várias listas, o "bloqueio" terá a prioridade mais alta, "permitidas" tem prioridade média e "personalizada" tem a menor prioridade.
- Para cada placa de licença, você pode adicionar informações sobre o proprietário do veículo. No entanto, essas informações não são sincronizadas com as câmeras.

Responda a eventos ao vivo

Usar controles de dispositivos

Controles do operador

Os controles do operador permitem a você acessar os recursos específicos de uma câmera Axis diretamente no Smart Client. A quais recursos você terá acesso depende de quais câmeras existem no seu sistema e dos recursos que elas oferecem. Além dos controles do operador pré-instalados, você pode criar itens personalizados. Você também pode configurar a quais controles um operador tem acesso.

Alguns exemplos de controles do operador são:

- Ativar ou desativar o limpador
- Ativar ou desativar aquecedor
- Ativar ou desativar a iluminação~IR
- Recuperação de foco
- Ativar ou desativar o WDR
- Ativar ou desativar a estabilização eletrônica de imagem (EIS).
- Ativar ou desativar máscaras de privacidade.

Para obter informações sobre os controles de operadores específicos da sua câmera, consulte a folha de dados.

Acesso aos controles do operador

Observação

Requisitos

- Dispositivos Axis com AXIS OS 7.10, 7.40 ou posterior. (As versões 7.20 e 7.30 não são compatíveis com controles de operador.)

1. No Smart Client, clique em **Live (Ao vivo)** e vá para sua câmera AXIS.
2. Clique em e selecione a função a ser usada.

Salvar uma área de foco para uma câmera PTZ

A função de recuperação de foco permite a você salvar áreas de foco para as quais a câmera PTZ retorna automaticamente ao se mover para essa área da cena. Isso é especialmente útil em condições de baixa iluminação, onde a câmera teria problemas para encontrar o foco.



1. No Smart Client, mova a câmera para a área na qual deseja focar.

Observação

As condições de iluminação devem ser boas quando você define a área de foco.

2. Focalize a câmera.
3. Selecione **Add Focus Recall Zone (Adicionar zona de recuperação de foco)**.

Posteriormente, ao fazer o pan ou tilt da câmera e mover a exibição para uma área, a câmera recuperará automaticamente o foco predefinido para essa exibição. Mesmo se você aumentar ou diminuir o zoom, a câmera manterá a mesma posição de foco.

Se a zona estiver configurada incorretamente, selecione **Remove Focus Recall Zone (Remover zona de recuperação de foco**.

Foco automático de uma câmera



As câmeras com foco automático podem ajustar a lente de forma mecânica e automática para que a imagem permaneça focalizada na área de interesse quando a exibição mudar.

Definir foco automático em uma câmera PTZ

1. No Smart Client, selecione uma exibição de câmera.
2. Clique em e acesse **Set Focus > AF (Ajustar foco > AF)**.
   O **Focus Control (Controle de foco)** permite a você aproximar ou afastar o ponto de foco:
   - Para passos grandes, clique na barra grande.
   - Para passos pequenos, clique na barra pequena.

Definir foco automático em câmeras box e dome fixas

1. No Smart Client, selecione uma exibição de câmera.
2. Clique em e acesse **Autofocus (Foco automático)**.

Ativar secagem rápida ou limpador



A função de secagem rápida permite que a dome se agite quando está molhada. Quando a dome vibra em alta velocidade, a tensão superficial da água é quebrada e as gotículas são removidas. Isso permite que a câmera produza imagens nítidas até mesmo em condições de chuva.

Para ativar a função de secagem rápida

1. No Smart Client, selecione uma exibição de câmera.
2. Clique em e acesse **PTZ > Speed Dry (PTZ Secagem rápida)**.

Importante

A função de secagem rápida está disponível somente nas câmeras AXIS Q61 Series.

Para ativar a função de limpador

O limpador remove o excesso de água e chuva da lente das câmeras de posicionamento Axis.

1. No Smart Client, selecione uma exibição de câmera.
2. Clique em .

Importante

A função limpador está disponível somente nas câmeras AXIS Q86 Series.

Medição de temperatura pontual



Se houver uma câmera integrada com leitura de temperatura pontual, você poderá medir a temperatura diretamente na exibição da câmera. As câmeras AXIS com leitura de temperatura pontual são a AXIS Q1961-TE, AXIS Q2101-E e AXIS Q2901-E.

1. No Smart Client, abra uma exibição de câmera em uma câmera integrada com a leitura de temperatura pontual.
2. Para medir a temperatura pontual, clique em e selecione:
   - **Measure spot temperature (Medir temperatura pontual)** para a AXIS Q2901-E.
   - **Enable temperature spot meter (Ativar medidor de temperatura pontual)** para AXIS Q1961-TE e AXIS Q2101-E.
3. Clique em qualquer área na exibição para ver a temperatura pontual atual.
   Para os modelos Q1961-TE e AXIS Q2101-E, clique em **Done (Pronto)**.
4. Para a AXIS Q1961-TE e a AXIS Q2101-E, a temperatura pontual permanecerá na imagem até ser desativada:
   - Selecione > **Disable temperature spot meter (Desativar medidor de temperatura pontual)**.

Observação

Se o zoom digital for usado, as medidas de temperatura poderão gerar resultados incorretos.

Aplicar zoom e acompanhar automaticamente um objeto em movimento

Rastreamento automático

Com o rastreamento automático, a câmera aplica zoom automaticamente e rastreia objetos móveis, por exemplo, um veículo ou uma pessoa. Você pode selecionar manualmente um objeto para acompanhamento ou configurar áreas de acionamento e deixar que a câmera detecte objetos em movimento. Quando a câmera não está rastreando um objeto, ela retorna para sua posição inicial após 5 segundos.

- Configure as áreas de acionamento na interface Web da câmera PTZ.
- No Smart Client, você verá:
  - Quadrado vermelho: o objeto rastreado.
  - Zonas azuis: objetos que não estão sendo rastreados, mas que podem ser rastreados se entrarem em uma zona de acionamento ou se você clicar com o botão direito do mouse sobre eles.

Configurar o rastreamento automático

Observação

Requisitos

- AXIS OS 12.0
- Uma ou mais câmeras Axis compatíveis com o Rastreamento automático (Autotracking) 2, por exemplo, AXIS Q6075 PTZ Dome Network Camera

1. Verifique se a câmera e os dispositivos de metadados estão ativados.
2. Selecione Metadata 1 (Metadados 1) para sua câmera e clique em **Settings (Configurações)**.

3. Vá para **Metadata stream > Event data (Stream de metadados > Dados de eventos)** e selecione **Yes (Sim)**.
4. Clique em **Save (Salvar)**.
5. Configure o Rastreamento automático (Autotracking) na interface Web da câmera PTZ.

Ativar ou desativar o rastreamento automático

1. No Smart Client, clique em .
2. Selecione **Turn on autotracking (Ativar rastreamento automático)** ou **Turn off autotracking (Desativar rastreamento automático)**.

Observação

Se houver várias opções para ativar/desativar o rastreamento automático (autotracking), use a última opção da lista.

Iniciar o rastreamento automático manualmente

Se você mover o ponteiro do mouse sobre um objeto, a sobreposição será preenchida. Clique com o botão direito do mouse enquanto move o ponteiro sobre um objeto para definir o objeto como um alvo, e a câmera começará a rastrear esse objeto-alvo. A câmera será redefinida após 5 segundos se o objeto não puder ser mais rastreado.

Clicar com o botão direito do mouse fora das caixas azuis interrompe o rastreamento automático (autotracking).

Criar controles do operador personalizados

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Operator controls (Navegação no site > AXIS Optimizer > Controles do operador)**.
2. Selecione um dispositivo ou um grupo de dispositivos.
3. Clique em **Add new control (Adicionar novo controle)**.
4. Insira um **Name (Nome)** e uma **Description (Descrição)**.
5. Selecione **Administrator (Administrador)** se desejar que o controle do operador esteja disponível somente para usuários com direitos de administrador.
6. Adicione o URL VAPIX para o controle específico.
   Exemplo: para adicionar um controle do operador Defog on (Remoção de névoa ativada), insira este URL: `/axis-cgi/param.cgi?action=update&imageSource.IO.Sensor.Defog=on`
   Para saber mais sobre as APIs de dispositivos de rede da Axis, consulte a .
7. Vá para o Smart Client e teste se o controle do operador funciona conforme o esperado.

Configurar acesso a controles de operadores

Você pode configurar a quais controles de operadores um operador no Smart Client tem acesso.

1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Operator controls (Navegação no site > AXIS Optimizer > Controles do operador)**.
2. Selecione um dispositivo ou um grupo de dispositivos.
3. Selecione a quais controles de operador você deseja que os operadores tenham acesso no Smart Client.

Interagir via alto-falantes

Gerenciador de alto-falantes

O Gerenciador de alto-falantes integra os produtos de áudio Axis ao VMS para oferecer a você toda a funcionalidade dos seus dispositivos Axis.

- Acessar alto-falante relacionado à sua câmera

Conecte câmeras a um alto-falante ou grupos de alto-falantes e acesse os alto-falantes na visualização ao vivo. Não é mais necessário procurar os alto-falantes manualmente.

- Enviar áudio para um grupo de alto-falantes
  Envie áudio para vários alto-falantes com um único clique.
- Gerenciar clipes de áudio
  Você pode facilmente realizar o gerenciamento de seus clipes de áudio.
- Aja imediatamente com os alto-falantes
  Responda rapidamente a um alarme sem sair do Gerenciador de alarmes.
- Sincronizar áudio entre alto-falantes
  Se desejar usar seu sistema de áudio para música ambiente, o Gerenciador de alto-falantes poderá ajudar você a configurar zonas para sincronizar o áudio entre os alto-falantes (somente nos modos AXIS Audio Manager Pro e Edge).

Modos

O gerenciador de alto-falantes oferece três modos diferentes para diversos tipos de configurações de alto--falantes.

- **Pro** para sistemas AXIS Audio Manager Pro
  Uma solução de software abrangente projetada para sistemas de notificação pública de grande escala ou avançados. É compatível com mais de 5.000 alto-falantes e mais de 500 zonas, além de oferecer opções flexíveis de licença e instalação. É recomendado para sistemas de maior porte ou para usuários com necessidades de programação mais avançadas.
- **Edge** para sistemas AXIS Audio Manager Edge
  Uma solução de software simplificada para o gerenciamento de até 200 alto-falantes em 20 zonas. Está incorporado diretamente nos alto-falantes de rede Axis e não requer servidores nem licenças adicionais. Recomendado para sistemas menores sem necessidades de programação avançadas.
- **Legado**
  O modo legado utiliza a integração com alto-falantes nativos para transmitir áudio a um grupo de alto--falantes ou acionar clipes de áudio. Não oferece suporte à transmissão sincronizada. Recomendado para sistemas com alto-falantes individuais e sem necessidade de transmissão sincronizada.

Modo de configuração

Na primeira vez que acessar esta página, será solicitado que selecione um modo, mas você poderá alterá-lo a qualquer momento. As configurações que você define em cada modo são independentes, mas são mantidas ao alternar entre os modos.

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falantes)**.
2. Em **Mode (Modo)**, clique no modo em que você está atualmente e selecione o modo desejado na janela pop-up.
3. Clique em **Switch mode (Alterar modo)**.

Modo AXIS Audio Manager Pro

Para utilizar este modo:

- Instale o software AXIS Audio Manager Pro em um servidor, por exemplo, um servidor de gravação.
- Adquira a licença e configure o AXIS Audio Manager Pro com acesso à API.
- Opcional: configure um certificado de servidor para a interface Web; consulte *Certificados*.
- Altere a porta 443 do servidor AXIS Audio Manager Pro, caso esteja instalado em um servidor VMS.

Este modo não requer a adição ou o licenciamento de alto-falantes no VMS, mas será criado automaticamente um dispositivo de hardware para a conexão com o servidor AXIS Audio Manager Pro (é necessária uma licença

de dispositivo VMS). Para saber mais sobre AXIS Audio Manager Pro, consulte o *Manual do usuário do AXIS Audio Manager Pro*.

Observação

O modo Pro do AXIS Audio Manager Pro está limitado ao suporte em um único site. Arquiteturas com vários sites, federadas e interconectadas estão fora do escopo desta integração.

Conecte-se a um servidor AXIS Audio Manager Pro no modo Pro

1. No Management Client, vá para **Site Navigation** > **AXIS Optimizer**> **Speaker manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falante)**.
2. Clique em **Conectar**.
3. Na caixa de diálogo:
   - Selecione um servidor de gravação ao qual deseja adicionar o hardware do servidor AXIS Audio Manager Pro .
   - Insira o endereço e a porta HTTPS do servidor AXIS Audio Manager Pro.
   - Insira o nome de usuário e a senha da API (o acesso à API deve estar ativado no servidor do AXIS Audio Manager Pro).
   - Clique em **Conectar**.

Você pode ver todos os destinos e zonas disponíveis no AXIS Audio Manager Pro no lado esquerdo. Ao clicar no **servidor AXIS Audio Manager Pro**, a interface web do AXIS Audio Manager Pro é exibida na parte direita.

Observação

Para ter acesso à interface web, é necessária uma conexão direta entre o computador do gerenciamento e o servidor AXIS Audio Manager Pro.

Se você fizer alguma alteração nas zonas, destinos, clipes de áudio ou perfis visuais na interface web do AXIS Audio Manager Pro:

- Vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falantes)**.
- Clique em **Update (Atualização)**

Associar uma câmera a um destino ou uma zona

Você pode associar uma câmera a um destino ou zona específica e utilizá-la diretamente na exibição de câmera do SMART Client.

1. No Management Client, vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, Gerenciador de alto-falantes)** e selecione um destino ou uma zona.
2. Em **Associated cameras (Câmeras associadas)**, clique em **Add cameras... (Adicionar câmeras...)** e selecione as câmeras que deseja associar ao destino ou à zona.

Quando uma câmera é associada a um destino ou zona, a barra de ferramentas da exibição de câmeras do Smart Client mostra .

Criar perfis visuais

- No Management Client, vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navegação no site, AXIS Optimizer, Gerenciador de alto-falante).
- Clique em **Audio Manager Pro server (servidor do Audio Manager Pro)** para acessar a interface web.
- Clique em **Visual profiles (Perfis visuais)** para criar ou editar perfis visuais.

Para saber mais sobre perfis visuais, consulte *o manual do usuário do AXIS Audio Manager Pro*.

Modo AXIS Audio Manager Edge

O AXIS Audio Manager Edge vem pré-instalado na maioria dos alto-falantes Axis e será detectado automaticamente quando você selecionar esse modo. Líderes de sites, dispositivos intermediários para fonte de megafonia e alto-falantes independentes precisam ser adicionados ao VMS para o modo AXIS Audio Manager Edge funcionar corretamente.

Observação

No modo AXIS Audio Manager Edge, não é possível usar saídas de áudio de câmera integradas e outros dispositivos de áudio incompatíveis.

Para saber mais sobre AXIS Audio Manager Edge, consulte o *Manual do usuário do AXIS Audio Manager Edge*.

Configurar alto-falantes e zonas no modo AXIS Audio Manager Edge

Para reproduzir clipes de áudio e falar ao vivo, é necessário ativar primeiro o paging para suas zonas.

1. No Management Client, vá para **Site Navigation** > **Devices** > **Speakers (Navegação no site, Dispositivos, Alto-falantes)** para adicionar grupos de dispositivos ou adicionar e remover alto-falantes de grupos de dispositivos.
2. Vá para **Site Navigation** > **AXIS Optimizer** > **Speaker Manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falantes)** e certifique-se de que o modo **Edge** esteja selecionado.
   O Gerenciador de alto-falantes procurará todos os alto-falantes no sistema VMS e mostrará todos os sites e zonas do AXIS Audio Manager Edge que podem ser usados no Smart Client.
3. Na lista do site, selecione uma região com paging desativado.
4. Selecione **Turn on paging for the zone (Ativar paging para a zona)**.

Se você alterar alguma coisa nas zonas ou nas fontes de megafonia:

5. Vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falantes)**.
6. Clique em **Update (Atualização)**

Observação

Se a configuração falhar, verifique a configuração do AXIS Audio Manager Edge e tente novamente.



Associar uma câmera a um alto-falante ou uma zona

Para usar um alto-falante ou zona específica na exibição de câmeras do Smart Client, é possível associá-los a uma câmera.

1. No Management Client, vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, Gerenciador de alto-falantes)** e selecione um alto-falante ou uma zona.
2. Na janela **Associated cameras (Câmeras associadas)**, clique em **+ Add cameras (Adicionar câmeras)** e selecione as câmeras às quais deseja associar o alto-falante ou zona.

Quando uma câmera é associada a um alto-falante, grupo de dispositivos ou zona, a barra de ferramentas da exibição de câmeras do Smart Client mostra .

Carregar clipes de áudio nos alto-falantes

Para reproduzir clipes de áudio em um alto-falante ou zona a partir do Smart Client, é necessário carregar antes os clipes de áudio no alto-falante com o Management Client.

1. Coloque os clipes de áudio que deseja carregar nos alto-falantes na pasta padrão **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
2. No Management Client, vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, Gerenciador de alto-falantes)** e selecione um alto-falante ou uma zona.
3. Vá para **Audio clips (Clipes de áudio)** e clique em **+** na frente dos clipes que deseja carregar nos alto-falantes.

Modo legado

O modo Legacy amplia a funcionalidade nativa das suas caixas de som Axis e de outros dispositivos Axis com capacidade de áudio que tenham sido adicionados ao VMS. Ao contrário dos outros modos, o modo Legacy não oferece suporte à transmissão sincronizada para vários alto-falantes.

Configurar alto-falantes no modo legado

1. No Management Client, vá para **Site Navigation** > **Devices** > **Speakers (Navegação no site, Dispositivos, Alto-falantes)** para adicionar grupos de dispositivos ou adicionar e remover alto-falantes de grupos de dispositivos.
2. Vá para **Site Navigation** > **AXIS Optimizer** > **Speaker Manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falantes)** e certifique-se de que o modo compatível com versões anteriores esteja selecionado.
3. Clique em .
   3.1. Na janela **Manage Side Panel (Gerenciar painel lateral)**, selecione os alto-falantes que deseja mostrar no Smart Client.
   3.2. Clique em **Add (Adicionar)** e em **OK**.
   Os alto-falantes no painel **Visible (Visíveis)** agora são mostrados no Smart Client para todos os usuários que têm acesso ao alto-falante.
4. Para remover alto-falantes:
   4.1. Vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falantes)** e clique em .
   4.2. Na janela **Manage Side Panel (Gerenciar painel lateral)**, selecione os alto-falantes que deseja remover.
   4.3. Clique em **Remove (Remover)** e em **OK**.

Associar uma câmera a um alto-falante ou grupo de alto-falantes

Você pode associar uma câmera a um destino ou zona específica e utilizá-la diretamente na exibição de câmera do SMART Client.

1. No Management Client, vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falantes)** e selecione um alto-falante ou grupo de alto-falantes.
2. Em **Associated cameras (Câmeras associadas)**, clique em **Add cameras... (Adicionar câmeras...)** e selecione as câmeras que deseja associar ao alto-falante ou ao grupo de alto-falantes.

Quando uma câmera é associada a um alto-falante ou grupo de alto-falantes, a barra de ferramentas da exibição de câmeras do Smart Client mostra .

Carregar clipes de áudio nos alto-falantes

Para reproduzir clipes de áudio em um alto-falante ou zona a partir do Smart Client, é necessário carregar antes os clipes de áudio no alto-falante com o Management Client.

1. Coloque os clipes de áudio que deseja carregar nos alto-falantes na pasta padrão **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
2. No Management Client, vá para **Site Navigation** > **AXIS Optimizer** > **Speaker manager (Navegação no site, AXIS Optimizer, Gerenciador de alto-falantes)** e selecione um alto-falante ou grupo de alto-falantes.
3. Vá para **Audio clips (Clipes de áudio)** e clique em **+** na frente dos clipes que deseja carregar nos alto-falantes.



Alterar o volume

Para alterar o volume dos alto-falantes:

1. No Management Client, vá para **Site Navigation > Speaker manager (Navegação no site, Gerenciador de alto-falantes)** e selecione um alto-falante ou grupo de alto-falantes.
2. Vá para **Volume** e ajuste o volume desejado.



Reprodução de áudio em alto-falantes

1. No Smart Client, vá para **Live** > **MIP plug-ins** > **Axis speaker control (Ao vivo, Plug-ins MIP, Controle de alto-falantes Axis)** e selecione um alto-falante ou zona na lista suspensa.
2. Para permitir que seu microfone envie áudio para o alto-falante:
   2.1. Pressione e mantenha pressionado enquanto fala.
   Certifique-se de que o medidor de nível do microfone esteja mostrando a atividade de voz.
3. Reproduza um clipe de áudio no alto-falante:
   3.1. Vá para **Media clip (Clipe de mídia)** e selecione um clipe de áudio na lista suspensa.
   3.2. Para iniciar a reprodução do clipe de áudio no alto-falante selecionado, clique em executar.

Reprodução de áudio em alto-falantes na exibição da câmera

1. No Smart Client, vá para uma exibição de câmera.
2. Se houver uma associação feita a um alto-falante, grupo de dispositivos ou zona, ela estará visível na barra de ferramentas.
3. Clique em para abrir a janela **Axis speaker control (Controle de alto-falantes Axis)**.

4. Para permitir que seu microfone envie áudio para o alto-falante:

   4.1. Pressione e mantenha pressionado enquanto fala.
   Certifique-se de que o medidor de nível do microfone esteja mostrando a atividade de voz.

5. Reproduza um clipe de áudio no alto-falante:

   5.1. Vá para **Media clip (Clipe de mídia)** e selecione um clipe de áudio na lista suspensa.

   5.2. Para iniciar a reprodução do clipe de áudio no alto-falante selecionado, clique em executar.

Reproduzir áudio nos alto-falantes em caso de alarmes

1. No Smart Client, vá para **Alarms (Alarmes)**.
2. Selecione um alarme cuja fonte seja uma câmera.
   Se houver uma associação a um alto-falante ou zona, os controles do alto-falante ficarão visíveis.
3. Para permitir que seu microfone envie áudio para o alto-falante:

   – Pressione e mantenha pressionado enquanto fala.
   Certifique-se de que o medidor de nível do microfone esteja mostrando a atividade de voz.

4. Reproduza um clipe de áudio no alto-falante:

   – Vá para **Media clip (Clipe de mídia)** e selecione um clipe de áudio na lista suspensa.

   – Para iniciar a reprodução do clipe de áudio no alto-falante selecionado, clique em executar.

Defina a configuração do comportamento visual para a interação com o alto-falante

No Smart Client, você pode realizar a configuração do comportamento visual do seu dispositivo no controle de alto-falantes da Axis, diretamente na visualização da câmera ou no Gerenciador de alarmes.

Observação

Os perfis visuais são compatíveis apenas no modo AXIS Audio Manager Pro.

- No painel lateral do **controle do alto-falante da Axis**:

  – Clique em .

  – Selecione um perfil visual na lista suspensa.

  – Digite na caixa de texto se desejar substituir os textos atuais associados ao perfil visual selecionado.

- Na visualização da câmera:

  – Vá para uma visualização específica da câmera.

  – Se houver uma associação feita a um alto-falante, grupo de dispositivos ou zona, ela estará visível na barra de ferramentas.

  – Clique em para abrir a janela **Axis speaker control (Controle de alto-falantes Axis)**.

  – Clique em .

- No **Gerenciador de alarmes**:

  – Selecione um evento, vá para a visualização da câmera e clique em .

Marcadores de clipes de áudio na exibição da câmera ou alarme

Quando você reproduz um clipe de áudio a partir dos controles do alto-falante em uma exibição da câmera ou nos Alarmes, , é criado um marcador com informações sobre quem reproduziu e em qual dispositivo o clipe de áudio foi reproduzido.

Para pesquisar os marcadores de clipes de áudio:

1. No Smart Client, vá para **Search (Pesquisar)**.
2. Selecione um intervalo de tempo e uma ou várias câmeras.
3. Clique em **Search for (Pesquisar)** > **Bookmarks (Marcadores)** > **New search (Nova pesquisa)**.

Gerencie visitantes

Plug-in de intercomunicador

Os intercomunicadores de rede Axis combinam comunicação, videomonitoramento e controle de entrada remoto em um único dispositivo. O AXIS Optimizer facilita a configuração e o uso de intercomunicadores Axis com o VMS. Por exemplo, você pode receber chamadas e abrir portas.

Configuração de um intercomunicador



A fechadura da porta deve, normalmente, ser conectada ao primeiro relé no intercomunicador. O AXIS Optimizer determina qual porta de saída será usada com base nas informações de **Usage** (Uso). Ele usará a primeira porta com **Usage = Door (Utilização = Porta)** (RELAY1, por padrão).

Observação

Requisitos

- Um intercomunicador Axis
- Um microfone instalado no PC que recebe as chamadas
- Smart Client ativo e em funcionamento

Observação

A partir da versão 5.0.X.X, o AXIS Optimizer configura os intercomunicadores no VMS usando um método de configuração diferente daquele nas versões anteriores. O dispositivo de metadados pode ser usado para detecção de chamadas, em vez de se utilizar a Input (Entrada 1). Ainda oferecemos suporte ao método de configuração antigo, mas recomendamos o novo método de configuração para novas instalações.

1. Instale a versão mais recente do AXIS Optimizer em cada cliente em que deseja receber chamadas e controlar a porta.
2. Faça login no Management Client.
3. Adicione o intercomunicador Axis ao servidor de gravação.
4. No Management Client, ative todos os dispositivos desejados. Para poder receber chamadas no Smart Client, você precisa de:
   - Câmera 1
   - Microfone
   - Alto-falante
   - Metadados
   - Entrada 2 (opcional se você tiver um relé de segurança conectado ao intercomunicador na porta 2).
   - Saída conectada à porta. Se você souber qual saída está conectada à porta, selecione-a. Caso contrário, selecione todas as saídas.

5. Vá para **Site Navigation > Devices > Metadata (Navegação no site > Dispositivos > Metadados)** e selecione o dispositivo de metadados para o intercomunicador que você está instalando.
6. Clique em **Settings (Configurações)**.
7. Defina **Event data (Dados de eventos)** como **Yes (Sim)**.
8. Clique em **Save (Salvar)**.
9. Se você habilitou a Entrada 2, também será necessário configurá-la.
   9.1. Vá para**Site Navigation > Devices > Input (Navegação no site > Dispositivos > Entrada)** e selecione Entrada 2.
   9.2. Clique em **Events (Eventos)** e, em seguida, em **Add (Adicionar)**.
   9.3. Selecione **Input Falling event (Evento de queda da entrada)** e adicione-o às entradas ativadas. Repita para **Input Rising event (Evento de subida da entrada)**.
   9.4. Clique em **Save (Salvar)**.
10. Para configurar permissões para funções específicas, consulte *Definir permissões para intercomunicador, on page 38*.
11. *Fazer uma chamada de teste, on page 39*.

Definir permissões para intercomunicador

Para lidar com uma chamada, antes é necessário ativar as permissões.

1. Vá para **Site Navigation > Security > Roles (Navegação no site > Segurança > Funções)**.
2. Escolha uma função.
3. Vá para **Overall Security (Segurança geral)**.
4. Confirme se as permissões necessárias para cada grupo de segurança estão definidas. Vá para **Hardware** e selecione **Driver commands (Comandos do driver)**.
5. Para definir permissões em nível de sistema, vá para **Overall Security (Segurança geral)**.
   Para definir permissões em nível de dispositivo, acesse **Device (Dispositivo)**.
6. Defina permissões para os grupos de segurança:
   6.1. Vá para **Cameras (Câmeras)**. Selecione **Read (Ler)** e **View live (Exibição ao vivo)**.
   6.2. Vá para **Microphones (Microfones)**. Selecione **Read (Ler)** e **Listen (Escutar)**.
   6.3. Em **Overall Security (Segurança geral)**, vá para **Speakers (Alto-falantes)**. Selecione **Read (Ler)** e **Speak (Falar)**.
   Em **Device (Dispositivo)**, vá para **Speakers (Alto-falantes)** e selecione **Read (Ler)**. Em seguida, vá para a guia **Speech (Fala)** e selecione **Speak (Falar)**.
   6.4. Vá para **Metadata (Metadados)**. Selecione **Read (Ler)** e **Live (Ao vivo)**.
   6.5. Vá para **Input (Entrada)**. Selecione **Read (Ler)**.
   6.6. Vá para **Output (Saída)**. Selecione **Read (Ler)** e **Activate (Ativar)**.

Para atribuir permissões para controlar quais operadores lidam com as chamadas de um determinado intercomunicador:

1. Selecione a permissão **Read (Ler)** para o dispositivo de entrada 1 do intercomunicador específico.
2. Desmarque essa permissão para todas as outras funções. Usuários que não têm permissão não poderão receber chamadas.

Para exibir o histórico de chamadas, você precisará de permissões adicionais.

1. Para definir permissões em nível de sistema, vá para **Overall Security (Segurança geral)**.
   Para definir permissões em nível de dispositivo, acesse **Device (Dispositivo)**.
2. Selecione estas permissões para os grupos de segurança:

2.1. Vá para **Cameras (Câmeras)**. Selecione **Playback (Reproduzir)** e **Read sequences (Ler sequências)**.

2.2. Vá para **Microphones (Microfones)**. Selecione **Playback (Reproduzir)** e **Read sequences (Ler sequências)**.

2.3. Vá para **Speakers (Alto-falantes)**. Selecione **Listen (Escutar)**, **Playback (Reproduzir)** e **Read sequences (Ler sequências)**.

Fazer uma chamada de teste

1. No Smart Client, vá para **Settings > Axis intercom options (Configurações > Opções do intercomunicador Axis)**.
2. Clique **Test call** (Chamada de teste).
3. Selecione um interfone e clique em **Make call (Fazer chamada)**.

Previna o eco durante as chamadas

Com o recurso de pressionar para falar, você pode enviar áudio em apenas uma direção de cada vez pelo interfone. E você pode ativar o recurso de pressionar para falar quando há um eco em uma chamada.

Para ativar **Push-to-talk (Pressionar para falar)**:

- No Smart Client, vá para **Settings (Configurações)** > **Axis intercom options (Opções do intercomunicador Axis)**.
- Vá para **Call (Chamar)** e selecione **Push-to-talk (Pressionar para falar)**.

Controle o interfone via visualização ao vivo

Para cada exibição de intercomunicador, clique em



para controlar rapidamente o dispositivo.

Como eu faço?	Instruções	Comentários
Abrir a fechadura	Clique em  > **Access (Acesso)** ou **Extended access (Acesso estendido)**.	Quando a fechadura estiver destravada, você não poderá clicar em **Access (Acesso)** ou **Extended access (Acesso estendido)**.
Saber se uma porta está travada ou destravada	Clique em  e leia o status na parte inferior do menu.	-

Como eu faço?	Instruções	Comentários
Conversar com uma pessoa na frente do intercomunicador	Clique em  > **Start call (Iniciar chamada)**.	A janela de chamada abre e inicia a comunicação bidirecional com o intercomunicador.
Descobrir quem chamou ontem	Clique em  > **Call history (Histórico de chamadas)**.	Você verá uma lista de chamadas feitas com o intercomunicador atual.

Responder a uma chamada da visualização ao vivo

Quando um visitante pressiona o botão de chamada no intercomunicador, uma janela de chamada é exibida em cada um dos Smart Clients em execução. A janela de chamada seleciona automaticamente a exibição de câmera apropriada quando você redimensiona a janela, como corredor ou paisagem, por exemplo.

Como eu faço?	Instruções	Comentários
Atender à chamada	Clique em **Aceitar**	Um canal de áudio bidirecional entre o operador e a pessoa no intercomunicador é aberto.
Enviar a chamada para outro operador porque estou ocupado	Feche a janela clicando em **X**	Quando você descartar uma chamada, um operador diferente poderá atender à chamada em outro cliente O intercomunicador continuará a tocar e piscar até que alguém atenda à chamada. Se ninguém responder, a chamada receberá o status de perdida no histórico de chamadas.
Recusar a chamada porque eu já abri a porta com base na	Clique em **Decline (Recusar)**	Quando você recusa uma chamada, as janelas de chamadas são fechadas automaticamente

Como eu faço?	Instruções	Comentários
confirmação visual e não preciso falar com a pessoa Recusar a chamada porque não desejo falar com visitantes indesejados		nos outros clientes. Nenhum outro operador pode aceitar a chamada. O intercomunicador para de tocar e piscar. Em seguida, a janela de chamada é fechada. A chamada recebe o status atendida no histórico de chamadas.
Abrir a porta	Clique em **Access (Acesso)**.	A trava do intercomunicador permanece aberta por 7 segundos. Para configurar o tempo em que a porta permanecerá aberta: 1. No Smart Client, vá para **Settings > Axis intercom options > Door access (Configurações > Opções do intercomunicador Axis > Acesso à porta)**. 2. Altere o valor de **Access time (Tempo de acesso)**.
Interrompe temporariamente o áudio do operador para o intercomunicador.	Clique em **Mute (Mudo)**	-
Fale com o visitante quando o recurso de pressionar para falar estiver ativado.	Clique em **Talk (Falar)**	Solte o botão de falar para ouvir o visitante quando ele falar.
Encerra a chamada.	Clique em **Hang up (Desligar)**	A configuração padrão de fechamento automático é fechar a janela de chamada quando uma chamada é recusada ou encerrada. Para alterar o comportamento padrão da janela de chamada: 1. No Smart Client, vá para **Settings > Axis intercom options > Call (Configurações > Opções do intercomunicador Axis > Chamada)**. 2. Desmarque a opção **Auto-close window (Fechar janela automaticamente)**.

Mostrar várias câmeras na janela de chamada

Você pode mostrar até três câmeras ao mesmo tempo na janela de chamada. Isso significa que você pode ver o fluxo de vídeo do intercomunicador e os fluxos de vídeo de duas outras câmeras na mesma janela de chamada. Isso é útil, por exemplo, quando você deseja ver a pessoa que está fazendo a entrega e a área ao redor da porta de entrega ao mesmo tempo.

Para configurar várias câmeras na janela de chamada:

1. No Smart Client, vá para **Settings > Axis intercom options (Configurações > Opções do intercomunicador Axis)**. Vá para **Call > Intercom settings (Chamada > Configurações do intercomunicador)**.
2. Vá para **Selected device (Dispositivo selecionado)** e selecione qual dispositivo você deseja configurar.
3. Vá para **Multiple cameras (Várias câmeras)**. Selecione qual intercomunicador deseja ver como **camera 1 (câmera 1)** na janela de chamada.
4. Selecione quais câmeras associadas você deseja ver como **camera 2 (câmera 2)** e **camera 3 (câmera 3)** na janela da chamada quando o intercomunicador ligar.
5. Feche a janela **Intercom settings (Configurações do intercomunicador)**.

Ações de janela de chamada

Com ações de janela de chamada, você pode configurar eventos definidos pelo usuário que estão vinculados a regras no mecanismo de regras do XProtect. Quais eventos você pode configurar e usar dependem da sua função.

Para configurar ações de janela de chamada:

1. No Smart Client, vá para **Settings > Axis intercom options (Configurações > Opções do intercomunicador Axis)**.
2. Vá para **Call > Intercom settings (Chamada > Configurações do intercomunicador)**.
3. Vá para **Selected device (Dispositivo selecionado)** e selecione qual dispositivo você deseja configurar.
4. Vá para **Call window actions (Ações de janela de chamada)** para selecionar as ações da janela de chamada que você deseja usar.

Existem dois tipos de ações da janela de chamada:

- **Access button action (Ação do botão de acesso)**: Ao configurar uma ação de botão de acesso, você substitui a ação padrão do botão **Access (Acesso)**. Por exemplo, você pode configurar a abertura de um conjunto de portas com o botão **Access (Acesso)**.
- **Custom action (Ação personalizada)**: Quando você configura uma ação personalizada, um botão é mostrado na janela da chamada. Você pode acionar a ação personalizada clicando neste botão. Uma ação personalizada é uma ação que não está necessariamente relacionada ao acesso à porta, por exemplo, enviar e-mails, disparar alarmes ou iniciar gravações contínuas.

Exibir uma página na janela de chamada

É possível exibir páginas na janela de chamada ao utilizar o AXIS I8307-VE Network Intercom. Isso é útil para exibir informações para a pessoa que está usando o intercomunicador, por exemplo, um mapa ou o horário de funcionamento.

Primeiro, configure essas páginas na interface Web do seu intercomunicador; consulte *AXIS I8307-VE Network Intercom*.

Quando há uma chamada recebida do intercomunicador:

1. Clique em **Show page (Exibir página)** para visualizar uma caixa de diálogo com todas as páginas configuradas no seu dispositivo.
2. Clique em **Load previews (Carregar visualizações)** para visualizar todas as páginas.
   Para visualizar uma página configurada, passe o cursor sobre a página e clique no ícone da imagem.
3. Clique em uma página configurada para exibir no intercomunicador.

É possível configurar a janela de chamada para exibir tanto a imagem da câmera do intercomunicador quanto a página utilizando diferentes câmeras associadas, ou seja, a câmera 1 para a imagem da câmera e a câmera 2 para a exibição da página. Consulte *Mostrar várias câmeras na janela de chamada, on page 43*.

Observe que a página será fechada quando a chamada terminar. Repita as etapas acima para exibir uma página para uma nova chamada.

Filtrar na extensão da chamada

Por padrão, todos os PCs conectados a um intercomunicador recebem as chamadas. Ao adicionar extensões de chamadas e filtragem delas no VMS, você pode configurar os intercomunicadores para rotear chamadas para determinados Smart Clients em seu sistema VMS. Você pode configurar agendamentos para a roteamento de chamadas e adicionar contatos de fallback. Você também pode rotear as chamadas para contatos baseados em SIP e adicioná-las como contatos de fallback.

Na interface Web do intercomunicador

1. Vá para **Communication** > **SIP (Comunicação > SIP)**.
2. Selecione **Enable SIP (Ativar SIP)**.
3. Clique em **Save (Salvar)**.
4. Vá para **Communication** > **VMS Calls (Comunicação > Chamadas de VMS)**.
5. Certifique-se de que **Allow calls in the video management system (VMS) (Permitir chamadas no sistema de gerenciamento de vídeo (VMS))** esteja ativado.
6. Vá para **Communication** > **Contact list (Comunicação > Lista de contatos)**.
7. Em **Recipients (Destinatários)**, clique em + clique em + para adicionar um novo contato. Insira as informações do novo contato e clique em **Save (Salvar)**. Você pode adicionar vários contatos.
   - Em **SIP address (Endereço SIP)** insira `VMS_CALL:<extension>`. Substitua `<extension>` pelo nome de extensão da chamada para seu contato, por exemplo `ReceptionA`.
   - Se desejar configurar um agendamento para o contato, escolha a **Availability (Disponibilidade)** do contato.
   - Você poderá adicionar um contato de fallback que receberá a chamada se nenhum dos contatos originais responder, por exemplo, `ReceptionB`.
8. Vá para **Communication** > **Calls (Comunicação > Chamadas)**.
9. Para dispositivos com AXIS OS anteriores à versão 11.6, desative **Make calls in the video management system (VMS) (Fazer chamadas no sistema de gerenciamento de vídeo (VMS))**.
10. Em **Recipients (Destinatários)**, remova o contato **VMS** e adicione o novo contato que você criou.

No Management Client

Recomendamos configurar os intercomunicadores no VMS para usar um dispositivo de metadados para detecção de chamadas. Consulte *Configuração de um intercomunicador, on page 37*.

No Smart Client

Configure uma extensão de chamada para cada usuário que deve receber as chamadas. A configuração é armazenada no nível de usuário. Isso significa que o usuário receberá as chamadas independentemente de qual PC é usado.

1. Faça login no Smart Client como o usuário que deve receber as chamadas.
2. Vá para **Settings > Axis intercom options (Configurações > Opções do intercomunicador Axis)**.
3. Em **Call > Call extension (Chamada > Extensão de chamada)**, insira o nome de extensão da chamada do contato. Por exemplo `ReceptionA`. O usuário agora só receberá chamadas se a extensão da chamada corresponder ao valor do filtro.
   Se desejar adicionar vários nomes de extensão de chamadas, separe-os com um ponto e vírgula, por exemplo, `ReceptionA;ReceptionC`.

Exibir o histórico de chamadas

No histórico de chamadas, você pode exibir chamadas respondidas e perdidas e se a porta foi destrancada. É possível selecionar entre as chamadas e exibir o vídeo de reprodução correspondente, se disponível.

1. No Smart Client, vá para a exibição do intercomunicador.

2. Clique em



> **Call history (Histórico de chamadas)**.

Observação

O histórico de chamadas está limitado a 39 chamadas e 1000 registros de log de acesso. O número limitado de chamadas poderá ser menor se você silenciar a conversa com frequência.

Para registrar quando uma porta foi destrancada, é necessário definir o tempo de retenção (dias) para o intercomunicador Axis:

1. No Management Client, vá para **Tools > Options > Alarm and Events > Event retention (Ferramentas > Opções > Alarme e eventos > Retenção de eventos)**.
2. Defina as horas para **Output Activated (Saída ativada)** e **Output Deactivated (Saída desativada)**.

Desativar o microfone quando não houver uma chamada ativa

É possível desativar o microfone quando não houver chamadas entrando no intercomunicador Axis. O microfone será ativado quando houver uma chamada ativa.

Observação

- Você precisa de direitos de administrador para desativar o microfone.
- Isso não é suportado na arquitetura federada ou quando você usa contatos alternativos.

1. No Smart Client, vá para **Settings (Configurações)** > **Axis intercom options (Opções do intercomunicador Axis)**.

2. Selecione **Turn off intercom microphone when no active call (Desativar microfone do intercomunicador quando não houver chamada ativa)**.

Receber um alarme se uma porta for forçada para abrir

Se uma porta tiver um relé de segurança (Entrada 2), a sobreposição da porta na janela de chamada do Smart Client mostrará quando a porta for aberta ou fechada. Isso significa que, se alguém forçar a porta para abri-la enquanto a porta estiver trancada, você poderá receber um alarme.

Observação

Para receber um alarme, pelo menos um Smart Client deverá estar em execução.

Para configurar o alarme:

1. No Smart Client, vá para **Settings > Axis intercom options > Administrator options (Configurações > Opções do intercomunicador Axis > Opções do administrador)**.
2. Selecione **Trigger an alarm when a door has been forced open (Acionar um alarme quando uma porta for forçada para abrir)**.

Receber um alarme se uma porta permanecer aberta por muito tempo

Se uma porta tiver um relé de segurança (Entrada 2), a sobreposição da porta na janela de chamada do Smart Client mostrará quando a porta for aberta ou fechada. Isso significa que, se alguém abrir a porta e a porta permanecer aberta por muito tempo, você poderá receber um alarme.

Observação

Para receber um alarme, pelo menos um Smart Client deverá estar em execução.

Para configurar o alarme:

1. No Smart Client, vá para **Settings > Axis intercom options > Administrator options (Configurações > Opções do intercomunicador Axis > Opções do administrador)**.
2. Selecione **Trigger an alarm when a door has been open longer than (s) (Acionar um alarme quando uma porta estiver aberta por mais de (s))**.
3. Insira por quanto tempo a porta poderá permanecer aberta antes que o alarme seja acionado.

Impedir que um cliente receba chamadas

Você pode configurar um cliente para não receber chamadas. Isso significa que, quando uma pessoa faz uma chamada, nenhuma janela de chamada é aberta no cliente específico.

1. No Smart Client, vá para **Settings > Axis intercom options > Call (Configurações > Opções do intercomunicador Axis > Chamada)**.
2. Desmarque **Receive calls on this client (Receber chamadas neste cliente)**.

Visualizar áudio

Exibição de microfone

Você pode visualizar o áudio em seu sistema adicionando um ou mais modos de exibição de microfone ao Smart Client. Em seguida, você pode monitorar o áudio na visualização ao vivo e na reprodução. Você também pode ver quando os níveis de áudio ultrapassam um determinado nível usando a detecção de áudio integrada em seu dispositivo Axis. Os casos de uso típicos são:

- *Ouça vários microfones ao mesmo tempo, on page 49*
- *Detecção de incidentes com áudio, on page 49*
- *Investigue incidentes após eles terem ocorrido, on page 49*

Observação

Requisitos

- VMS Smart Client 2020 R2 ou posterior.

Configurar VMS para exibição de microfone

1. Defina os níveis de detecção:
   1.1. No Management Client, vá para **Site Navigation > AXIS Optimizer > Device assistant (Navegação no site > AXIS Optimizer > Device assistant)** e selecione seu dispositivo.
   1.2. Abra as configurações de **Detectors (Detectores)**. A forma como você abrirá essas configurações dependerá da versão do software do dispositivo.
   1.3. Vá para **Audio detection (Detecção de áudio)** e modifique o valor de **Input 1 sound level (Nível de som da entrada 1)** para atender às suas necessidades.
2. Obtenha eventos da câmera no VMS:
   2.1. No Management Client, vá para **Site Navigation > Devices > Microphones (Navegação no site > Dispositivos > Microfones)**.
   2.2. Clique no microfone e, em seguida, clique em **Events (Eventos)**.
   2.3. Adicione os eventos **Audio Falling (Áudio diminuindo)** e **Audio Rising (Áudio aumentando)**.
3. Configure por quanto tempo o sistema mantém metadados sobre o áudio detectado:
   3.1. Vá para **Tools > Options > Alarm and Events > Device events (Ferramentas > Opções > Alarme e eventos > Eventos do dispositivo)**.
   3.2. Encontre **Audio Falling (Áudio diminuindo)** e defina o tempo de retenção.
   3.3. Encontre **Audio Raising (Áudio aumentando)** e defina o tempo de retenção.
4. Verifique se você configurou a gravação de áudio. Você pode, por exemplo, gravar áudio o tempo todo ou criar uma regra de gravação com base em eventos de áudio aumentando ou diminuindo.
5. Para cada microfone que deseja usar com a exibição de microfone, repita as etapas acima.
6. No Smart Client, vá para **Settings > Timeline > Additional data (Configurações > Linha do tempo > Dados adicionais)** e selecione **Show (Mostrar)**.

Adicionar exibição de microfone ao Smart Client

1. Abra o Smart Client e clique em **Setup (Configuração)**.
2. Vá para **Views (Exibições)**.
3. Clique em **Create new view (Criar nova exibição)** e selecione um formato.
4. Vá para **System overview > AXIS Optimizer (Visão geral > AXIS Optimizer)**.
5. Clique em **Microphone view (Exibição de microfone)** e arraste-a para a exibição.
6. Selecione um microfone.
7. Clique em **Setup (Configuração)**.

Usar exibição de microfone

- Visualização ao vivo
  - Os níveis de áudio são exibidos como um gráfico de barras com o nível atual para a direita e até 60 segundos de histórico de áudio movendo-se para a esquerda.
  - Clique na exibição para ouvir o áudio do microfone.
  - Em cada exibição de microfone há um ícone de fone de ouvido. Clique no ícone para ativar ou desativar o áudio de cada exibição sem precisar selecionar a exibição propriamente dita. Isso permite ouvir vários microfones ao mesmo tempo.

- Reprodução
  - Um ícone realçará quando o áudio detectado estiver disponível para o microfone.
  - As barras amarelas indicam que o áudio foi detectado de acordo com os níveis de detecção que você definiu no dispositivo.
  - Clique na exibição para ouvir o áudio do microfone.
  - Em cada exibição de microfone há um ícone de fone de ouvido. Clique no ícone para ativar ou desativar o áudio de cada exibição sem precisar selecionar a exibição propriamente dita. Isso permite ouvir vários microfones ao mesmo tempo.

Ouça vários microfones ao mesmo tempo

A exibição de microfone permite que você ouça vários microfones ao mesmo tempo, tanto na visualização ao vivo quanto na reprodução.

1. *Configurar VMS para exibição de microfone, on page 48*.
2. Abra o Smart Client e clique em **Setup (Configuração)**.
3. Vá para **Views (Exibições)**.
4. Clique em **Create new view (Criar nova exibição)** e selecione uma exibição dividida.
5. Vá para **System overview > AXIS Optimizer (Visão geral > AXIS Optimizer)**.
6. Para cada microfone que você deseja ouvir:
   6.1. Clique em **Microphone view (Exibição de microfone)** e arraste-a para a exibição.
   6.2. Selecione um microfone.
7. Clique em **Setup (Configuração)**.
8. Para cada microfone, decida se deseja ativar ou desativar o áudio clicando no ícone de fone de ouvido em cada exibição de microfone. Agora você pode escutar todos os microfones sem áudio ao mesmo tempo.

Detecção de incidentes com áudio

Talvez você queira monitorar ações de áreas em que você não tem permissão para instalar câmeras, por exemplo, toaletes. Na exibição de microfone, você pode ver rapidamente quando um incidente ocorre ou não quando o nível de som excede os níveis de detecção.

1. *Configurar VMS para exibição de microfone, on page 48*. Lembre-se de definir níveis de detecção relevantes para o dispositivo e a área que deseja monitorar.
2. Adicione uma exibição de microfone com a visualização ao vivo do dispositivo no Smart Client. Consulte *Adicionar exibição de microfone ao Smart Client, on page 48*.

Investigue incidentes após eles terem ocorrido

Após um incidente ocorrer, você poderá identificar rapidamente os períodos na linha do tempo de reprodução quando o áudio for detectado por seus microfones.

1. *Configurar VMS para exibição de microfone, on page 48*.
2. Adicione um ou mais modos de exibição de microfone com os dispositivos relevantes para reprodução no Smart Client, consulte *Adicionar exibição de microfone ao Smart Client, on page 48*.

Pesquisa forense

O AXIS Optimizer oferece quatro categorias de pesquisa para dispositivos Axis na pesquisa centralizada:

- *Pesquisa forense, on page 50* (pesquisa de objetos)
- *Pesquisa de veículos, on page 53*
- *Pesquisa de velocidade na zona, on page 56*
- *Pesquisa de contêineres, on page 58*

Você também pode adicionar uma guia de pesquisa de placas de licença separada ao Smart Client, consulte *Placas de licença da Axis, on page 59*.

Você pode configurar essas categorias de pesquisa em um painel centralizado, consulte *Configurar categorias de pesquisa da Axis, on page 108*.

Pesquisa forense

As câmeras Axis com AXIS OS 9.50 ou posterior geram metadados que descrevem todos os objetos atualmente em movimento no campo de visão de uma câmera. O VMS pode gravar esses dados junto com o vídeo e o áudio correspondentes. A função de pesquisa forense no AXIS Optimizer permite a você analisar e pesquisar esses dados. Use a pesquisa forense para obter uma visão geral de toda a atividade na cena ou encontrar rapidamente um objeto ou evento de interesse específico.

Antes de começar

1. Certifique-se de que a câmera tenha a versão do AXIS OS mais recente.
2. Certifique-se de que seu VMS tenha uma versão correta:
   - Corporate 2019 R3 ou posterior, ou Expert 2019 R3 ou posterior
   - Professional+ 2022 R3 ou posterior, ou Express + 2022 R3 ou posterior
3. A hora da câmera deve ser sincronizada com NTP.
4. Para filtrar os tipos de objetos **Human (Pessoa)**, **Vehicle (Veículo)**, **Bike (Bicicleta)**, **Bus (Ônibus)**, **Car (Carro)** ou **Truck (Caminhão)** como filtros:
   4.1. Use um dispositivo Axis compatível com AXIS Object Analytics. Consulte filtro Analytics (Analíticos) no *Product selector (Seletor de produtos)*.
   4.2. Vá para **System > Analytics Metadata (Sistema > Metadados de analíticos)** e ative **Analytics Scene Description (Descrição de cena com analíticos)** na página web da câmera.
5. Para filtrar por **Vehicle color (Cor do veículo)**, **Upper body clothing color (Cor da peça de roupa superior)** ou **Lower body clothing color (Cor da peça de roupa inferior)**:
   5.1. Use um dispositivo Axis compatível com AXIS Object Analytics. Consulte filtro Analytics (Analíticos) no *Product selector (Seletor de produtos)*.
   5.2. Use um dispositivo Axis com ARTPEC-8 ou CV25. Consulte o filtro System on chip (Sistema em chip) no *Seletor de produtos*.

Configurar a pesquisa forense



1. No Management Client, certifique-se de que o dispositivo de metadados esteja ativado para as câmeras.

2. Certifique-se de que o dispositivo de metadados esteja relacionado à câmera:
   - Vá para **Devices** > **Camera** (Dispositivos > Câmera) e selecione o dispositivo.
   - Acesse a guia **Client (Cliente)** e certifique-se de que o dispositivo de metadados da câmera esteja selecionado em **Related metadata (Metadados relacionados)**.
3. Vá para **Site Navigation > Devices > Metadata (Navegação no site > Dispositivos > Metadados)**.
4. Selecione seu dispositivo e clique em **Record (Gravar)**. Certifique-se de que a opção **Recording (Gravação)** esteja ativada.
   Por padrão, os metadados são gravados somente quando o VMS detecta movimento em uma cena. Portanto, recomendamos ajustar o limite de movimento para seu ambiente para que você não perca nenhum movimento de objeto.
5. Clique em **Settings (Configurações)** e certifique-se de que a opção **Analytics data (Dados de analíticos)** esteja ativada.
6. Abra a visualização ao vivo do Smart Client e verifique se você vê caixas delimitadoras de objetos e se as caixas são exibidas corretamente.
   Pode demorar um pouco para que o relógio se adapte à hora NTP.
7. Aguarde pelo menos 15 min para permitir que o sistema grave vídeo e metadados. Decorrido esse tempo, você poderá iniciar a pesquisa, consulte *Realizar uma pesquisa, on page 51*.
8. Ative **Consolidated metadata (Metadados consolidados)** para aprimorar a velocidade de pesquisa em dispositivos com AXIS OS 11.10 ou superior. Consulte *Metadados e pesquisas, on page 107*.

Realizar uma pesquisa



Observação

Antes de usar essa função de pesquisa, você precisa configurá-la no Management Client. Para saber como fazer isso, consulte *Configurar a pesquisa forense, on page 50*.

1. No Smart Client, vá para **Search (Pesquisar)**.
2. Selecione um intervalo de tempo e uma ou várias câmeras.
3. Clique em **Search for > Forensic search > New search (Pesquisar > Pesquisa forense > Nova pesquisa)**.
   Para cada resultado de pesquisa, você verá o objeto e o caminho de deslocamento do objeto na miniatura.
   - A miniatura mostra o quadro de vídeo quando o objeto foi o mais visível.
   - O ponto verde marca a localização na qual a câmera detectou o objeto pela primeira vez.
   - O ponto vermelho marca a localização na qual a câmera detectou o objeto pela última vez.
   - Para ver a sequência de vídeo completa para um resultado de pesquisa, selecione-a e clique em **Play forward (Reproduzir)** no painel de visualização.
   - Para ocultar as sobreposições gráficas, vá para **Bounding boxes (Caixas delimitadoras)** e selecione **Hide (Ocultar)**.

   Observação

   Os aplicativos de analíticos executados na câmera, como o AXIS Object Analytics e o AXIS Loitering Guard, também podem gravar sobreposições no vídeo. Para remover essas sobreposições, acesse a página de configuração da web do aplicativo.
4. Selecione filtros de pesquisa para restringir o número de resultados de pesquisa.

Para saber mais sobre como usar os diferentes filtros, consulte *Fazer o ajuste preciso de uma pesquisa, on page 52*.

5. Selecione os resultados da pesquisa que deseja examinar melhor. Você pode, por exemplo, marcá-los ou *Criar um relatório PDF de alta qualidade, on page 59*.

Fazer o ajuste preciso de uma pesquisa

Para restringir os resultados da pesquisa, você pode usar um ou vários filtros de pesquisa.

- **Region of interest (Região de interesse)**
  Detecte objetos que foram movidos em uma área específica.
- **Object direction (Direção do objeto)**
  Detecte objetos que se moveram ao longo de uma rota específica em uma cena: à esquerda, à direita, para baixo ou para cima.
- **Tipo do objeto**
  Detecte objetos de um determinado tipo: pessoas, veículos, bicicletas, ônibus, carros ou caminhões.

Observação

- Velocidade (km/h ou mph) e placa de licença só são compatíveis com a AXIS Q1686–DLE Radar-Video Fusion Camera.
- Você precisa ativar as funções de velocidade (km/h ou mph) e placa de licença antes de usá-las. Para isso, consulte *Configurar categorias de pesquisa da Axis, on page 108*.
- **Speed (Velocidade) (em km/h ou mph)**
  Detecte veículos que se movem em uma determinada velocidade.
- **Placa de licença**
  Detecte veículos com uma placa de licença específica. Também pode ser usado para procurar placas de licença que incluem determinados alfabetos ou números.
- **Cor do veículo**
  Detecte veículos da cor escolhida.
- **Cor da peça de roupa superior**
  Detecte roupas da cor escolhida na parte superior do corpo de uma pessoa.
- **Lower body clothing color (Cor da peça de roupa inferior)**
  Detecte roupas da cor escolhida na parte inferior do corpo de uma pessoa.
- **Time-of-day (Hora do dia)**
  Detecte objetos que foram detectados durante uma parte específica do dia. Esse filtro é útil quando você pesquisa vários dias, mas está interessado somente em objetos em um horário específico de cada dia, como durante a tarde, por exemplo.
- **Minimum time in scene (s) (Tempo mínimo na cena (s))**
  Detecte objetos que foram detectados e rastreados por um número mínimo de segundos. Esse filtro elimina objetos que não sejam de interesse, como objetos muito distantes e objetos falsos (efeitos de iluminação), por exemplo. O valor padrão é 1 segundo. Isso significa que, quando o filtro não é definido, ele exclui objetos com duração inferior a 1 segundo.
- **Swaying objects (% of image) (Objetos balançando (% da imagem))**
  Exclua objetos que se movem somente em uma área restringida, por exemplo, um sinalizador ou uma árvore que se move no vento. O valor padrão é 5 – 100%. Isso significa que, quando o filtro não é definido, ele exclui objetos que não se moveram por mais de 5% da área da imagem.

Limitações

- Para obter as sequências de vídeo corretas para os resultados da pesquisa, é importante ter o relógio sincronizado corretamente.
- Os dados analisados na pesquisa forense não levam em consideração a perspectiva da cena. Isso significa que o tamanho e a velocidade de um objeto variam dependendo da proximidade em relação à câmera.

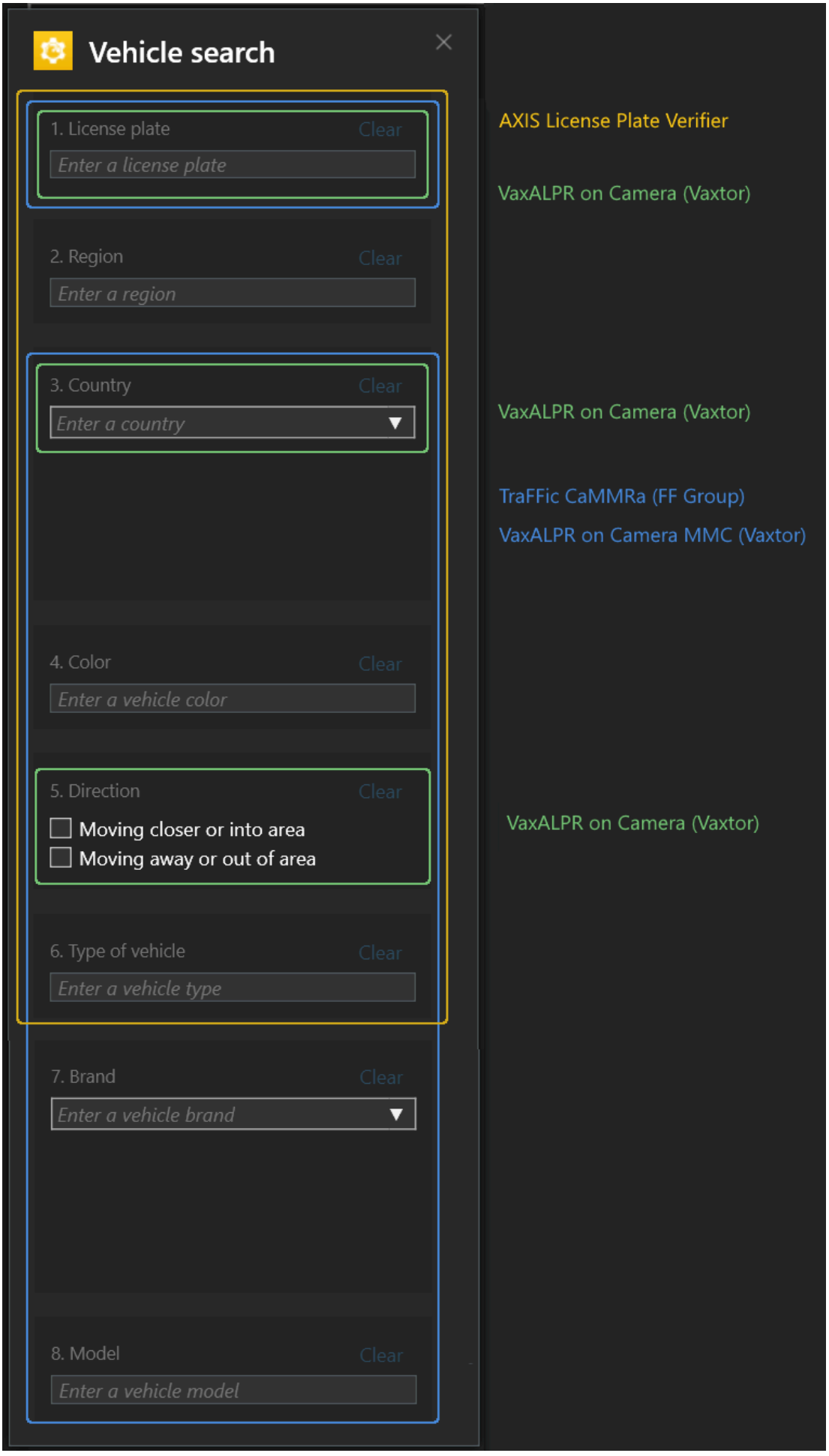
- Condições climáticas, como chuva pesada ou neve, podem afetar a precisão da detecção.
- Se houver um bom contraste do objeto em cenas de iluminação baixa, a análise se tornará mais precisa.
- Um único objeto pode, em algumas circunstâncias, gerar vários resultados. Por exemplo, quando o rastreamento é perdido quando um objeto é temporariamente obscurecido por outro objeto.
- As sobreposições podem ser diferentes dependendo da versão do XProtect. Por exemplo: sobreposições na visualização de vídeo exigem o XProtect 2020 R3 e as cores de sobreposição necessitam do XProtect 2020 R2.
- Para que a pesquisa forense funcione em streams de vídeo que foram girados 180 graus, você deve:
  - usar o AXIS OS 10.6 ou posterior nas câmeras ou
  - usar o Device Pack 11.0 ou posterior no servidor de gravação
- A configuração de balanço de branco na câmera deve ser precisa para obter uma boa detecção de cores

Pesquisa de veículos

Ao usar o AXIS Optimizer junto com certos aplicativos instalados na câmera, você pode pesquisar, identificar e compartilhar evidências de vídeo sobre veículos. A pesquisa de veículos suporta dados de placas de licença dos seguintes aplicativos:

- *AXIS License Plate Verifier* pela AXIS communications
- *CAMMRA AI* do FF Group (versão 1.3 ou superior necessária)
- *VaxALPR On Camera* pela Vaxtor Recognition Technologies
- *VaxALPR On Camera MMC* pela Vaxtor Recognition Technologies

Os filtros de pesquisa que podem ser usados dependem de qual aplicativo você instalou nas câmeras, consulte *Fazer o ajuste preciso de uma pesquisa, on page 55*


Vehicle search
1. License plate
Clear
Enter a license plate
2. Region
Clear
Enter a region
3. Country
Clear
Enter a country
4. Color
Clear
Enter a vehicle color
5. Direction
Clear
Moving closer or into area
Moving away or out of area
6. Type of vehicle
Clear
Enter a vehicle type
7. Brand
Clear
Enter a vehicle brand
8. Model
Clear
Enter a vehicle model
AXIS License Plate Verifier
VaxALPR on Camera (Vaxtor)
VaxALPR on Camera (Vaxtor)
TraFFic CaMMRa (FF Group)
VaxALPR on Camera MMC (Vaxtor)
VaxALPR on Camera (Vaxtor)

Configurar pesquisa de veículos

Observação

Requisitos

- Sistema VMS:
  - Corporate ou Expert 2019 R3 ou posterior
  - Professional+ ou Express+ 2022 R3 ou posterior
- Hora da câmera sincronizada com NTP
- Um dos aplicativos listados na

1. No Management Client, adicione a câmera que executa o aplicativo escolhido.
2. Ative todos os dispositivos desejados. Para poder usar o AXIS License Plate Verifier, Camera 1 e Metadata 1 são necessários.
3. Certifique-se de que o dispositivo de metadados esteja relacionado à câmera:
   - Vá para **Devices** > **Camera** (Dispositivos > Câmera) e selecione o dispositivo.
   - Acesse a guia **Client (Cliente)** e certifique-se de que o dispositivo de metadados da câmera esteja selecionado em **Related metadata (Metadados relacionados)**.
4. Configurar metadados:
   4.1. Vá para **Site Navigation > Recording Server (Navegação no site > Servidor de gravação)** e encontre o dispositivo.
   4.2. Selecione Metadata 1 (Metadados 1) e clique em **Settings (Configurações)**.
   4.3. Vá para **Metadata stream > Event data (Stream de metadados > Dados de eventos)** e selecione **Yes (Sim)**.
5. Vá para a guia **Record settings (Configurações da gravação)** e verifique se a gravação está ativada para metadados.
6. Clique em **Save (Salvar)**.
7. Configure o aplicativo de modo que ele funcione para um usuário padrão:
   7.1. Adicione direitos de leitura e reprodução à câmera e ao usuário específicos.
   7.2. Adicione os direitos de leitura e reprodução nos metadados para a câmera e o usuário específicos.

Procurar um veículo

1. No Smart Client, vá para **Search (Pesquisar)**.
2. Selecione um intervalo de tempo e uma ou várias câmeras.
3. Clique em **Search for > Vehicle search > New search (Pesquisar > Pesquisa de veículos > Nova pesquisa)**.
4. Selecione filtros de pesquisa para restringir o número de resultados de pesquisa.
   Para saber mais sobre os diferentes filtros, consulte *Fazer o ajuste preciso de uma pesquisa, on page 55*.
5. Selecione os resultados da pesquisa que deseja examinar melhor. Você pode, por exemplo, marcá-los ou *Criar um relatório PDF de alta qualidade, on page 59*.

Fazer o ajuste preciso de uma pesquisa

Para restringir os resultados da pesquisa, você pode usar um ou vários filtros de pesquisa. Aplicativos diferentes fornecem opções de filtro diferentes.

- **Placa de licença**
  Encontre um número de placa de licença específico.
  Aplicativo: AXIS License Plate Verifier, VaxALPR On Camera, CAMMRA AI ou VaxALPR On Camera MMC.

- **Região**
  Encontre veículos de uma região específica.
  Aplicativo: AXIS License Plate Verifier 2.9.19.

Observação

Defina o local da câmera nas configurações do AXIS License Plate Verifier para obter o reconhecimento da região ideal.

- **País**
  Encontre veículos de um país específico.
  Aplicativo: AXIS License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI ou VaxALPR On Camera MMC.
- **Cor**
  Encontre veículos de uma cor específica.
  Aplicativo: AXIS License Plate Verifier 2.9.19, CAMMRA AI ou VaxALPR On Camera MMC.
- **Direção**
  Encontre os veículos que se movem em uma direção específica.
  Aplicativo: AXIS License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI ou VaxALPR On Camera MMC.
- **Type of vehicle (Tipo de veículo)**
  Encontre um tipo de veículo específico.
  Aplicativo: AXIS License Plate Verifier 2.9.19, CAMMRA AI ou VaxALPR On Camera MMC.
- **Marca**
  Encontre uma marca de veículo específica.
  Aplicativo: CAMMRA AI ou VaxALPR On Camera MMC.
- **Modelo**
  Encontre um modelo de veículo específico.
  Aplicativo: CAMMRA AI ou VaxALPR On Camera MMC.

Otimizar a velocidade da pesquisa

Você pode aumentar a velocidade da pesquisa controlando os dados que o sistema armazena no dispositivo de metadados do VMS.

- Desative os dados analíticos se você não precisar deles.
  - Vá para **Devices** > **Metadata** (Dispositivos > Metadados) e selecione seu dispositivo.
  - Clique em **Configurações** e desative **Dados analíticos**.
- Se você precisar de dados analíticos, poderá usar metadados consolidados, se estiverem disponíveis. Consulte *Metadados e pesquisas, on page 107*.
- Desative os eventos que você não precisa no AXIS License Plate Verifier. Você só precisa do evento **Lost** (Perdido) para que o AXIS Optimizer funcione. Consulte *AXIS License Plate Verifier*.
- Certifique-se de usar o AXIS OS 12.8 ou posterior.

Pesquisa de velocidade na zona

No AXIS Optimizer, é possível usar a pesquisa de velocidade na zona para procurar veículos em alta velocidade que foram detectados ao entrar em uma zona predeterminada na visão de uma câmera. A pesquisa de velocidade na zona funciona em conjunto com o *AXIS Speed Monitor* para mostrar a velocidade dos veículos em uma zona de detecção de radar na visão ao vivo da câmera. Com o AXIS Zone Speed Search, é possível configurar filtros específicos para reduzir sua pesquisa e exportar e compartilhar evidências de vídeo durante as investigações.

Configurar pesquisa de velocidade da zona

Observação

Requisitos

- Sistema VMS:
  - Corporate ou Expert 2019 R3 ou posterior
  - Professional+ ou Express+ 2022 R3 ou posterior
- Hora da câmera sincronizada com NTP

1. No Management Client, adicione a câmera que executa o aplicativo escolhido.
2. Ative todos os dispositivos desejados. Para poder usar o AXIS Zone Speed Search, Camera 1 e Metadata 1 são necessários.
3. Certifique-se de que o dispositivo de metadados esteja relacionado à câmera:
   - Vá para **Devices** > **Camera** (Dispositivos > Câmera) e selecione o dispositivo.
   - Acesse a guia **Client (Cliente)** e certifique-se de que o dispositivo de metadados da câmera esteja selecionado em **Related metadata (Metadados relacionados)**.
4. Para configurar metadados:
   4.1. Vá para **Site Navigation > Recording Server (Navegação no site > Servidor de gravação)** e encontre o dispositivo.
   4.2. Selecione Metadata 1 (Metadados 1) e clique em **Settings (Configurações)**.
   4.3. Vá para **Metadata stream > Event data (Stream de metadados > Dados de eventos)** e selecione **Yes (Sim)**.
5. Vá para a guia **Record settings (Configurações da gravação)** e verifique se a gravação está ativada para metadados.
6. Clique em **Save (Salvar)**.
7. Para configurar o aplicativo de modo que ele funcione para um usuário padrão:
   7.1. Adicione direitos de leitura e reprodução à câmera e ao usuário específicos.
   7.2. Adicione os direitos de leitura e reprodução nos metadados para a câmera e o usuário específicos.

Pesquisar por eventos de velocidade de zona



1. No Smart Client, vá para **Search (Pesquisar)**.
2. Selecione um intervalo de tempo e uma ou várias câmeras.
3. Clique em **Search for > Zone speed search > New search (Pesquisar > Pesquisa de velocidade na zona > Nova pesquisa)**.
4. Selecione filtros de pesquisa para restringir o número de resultados de pesquisa.
   Para saber mais sobre os diferentes filtros, consulte *Fazer o ajuste preciso de uma pesquisa, on page 57*.
5. Selecione os resultados da pesquisa que deseja examinar melhor. Você pode, por exemplo, marcá-los ou *Criar um relatório PDF de alta qualidade, on page 59*.

Fazer o ajuste preciso de uma pesquisa

Para restringir os resultados da pesquisa de eventos de excesso de velocidade, você pode usar um ou vários filtros de pesquisa.

- **Velocidade máxima**

Filtre a velocidade máxima de qualquer objeto na zona pela duração do evento. Você pode definir um limite inferior e superior para a velocidade máxima.

- **Tipo do objeto**
  Se **Vehicle (Veículo)** for selecionado, a pesquisa só mostrará eventos de excesso de velocidade onde o objeto mais rápido da região foi classificado como um veículo.
- **Nome da zona**
  Pesquise e filtre zonas por nome.

Pesquisa de contêineres

Ao usar o AXIS Optimizer junto com determinados aplicativos, você pode pesquisar, identificar e compartilhar evidências de vídeo sobre contêineres. A pesquisa de contêineres suporta dados do seguinte aplicativo:

- *VaxOCR Containers* da Vaxtor Recognition Technologies

Configurar pesquisa de contêineres

Observação

Requisitos

- Sistema VMS:
  - Corporate ou Expert 2019 R3 ou posterior
  - Professional+ ou Express+ 2022 R3 ou posterior
- Hora da câmera sincronizada com NTP
- O aplicativo listado em

1. No Management Client, adicione a câmera que executa o aplicativo escolhido.
2. Ative todos os dispositivos desejados.
3. Certifique-se de que o dispositivo de metadados esteja relacionado à câmera:
   - Vá para **Devices** > **Camera** (Dispositivos > Câmera) e selecione o dispositivo.
   - Acesse a guia **Client (Cliente)** e certifique-se de que o dispositivo de metadados da câmera esteja selecionado em **Related metadata (Metadados relacionados)**.
4. Configurar metadados:
   4.1. Vá para **Site Navigation > Recording Server (Navegação no site > Servidor de gravação)** e encontre o dispositivo.
   4.2. Selecione Metadata 1 (Metadados 1) e clique em **Settings (Configurações)**.
   4.3. Vá para **Metadata stream > Event data (Stream de metadados > Dados de eventos)** e selecione **Yes (Sim)**.
5. Vá para a guia **Record settings (Configurações da gravação)** e verifique se a gravação está ativada para metadados.
6. Clique em **Save (Salvar)**.
7. Configure o aplicativo de modo que ele funcione para um usuário padrão:
   7.1. Adicione direitos de leitura e reprodução à câmera e ao usuário específicos.
   7.2. Adicione os direitos de leitura e reprodução nos metadados para a câmera e o usuário específicos.

Procurar um contêiner

1. No Smart Client, vá para **Search (Pesquisar)**.
2. Selecione um intervalo de tempo e uma ou várias câmeras.
3. Clique em **Search for > Container search > New search (Pesquisar > Pesquisa de contêiner > Nova pesquisa)**.

4. Selecione filtros de pesquisa para restringir o número de resultados de pesquisa.
   Para saber mais sobre os diferentes filtros, consulte *Fazer o ajuste preciso de uma pesquisa, on page 59*.
5. Selecione os resultados da pesquisa que deseja examinar melhor. Você pode, por exemplo, marcá-los ou *Criar um relatório PDF de alta qualidade, on page 59*.

Fazer o ajuste preciso de uma pesquisa

Para restringir os resultados da pesquisa, você pode usar um ou vários filtros de pesquisa. Todas as opções de filtro são provenientes do aplicativo VaxOCR Containers.

- **Código do contêiner**
  Encontre um código de contêiner específico.
- **Proprietário**
  Encontre contêineres pertencentes a um determinado proprietário.
- **Owner code (Código do proprietário)**
  Encontre contêineres pertencentes a um determinado proprietário.
- **Tamanho**
  Encontre contêineres de um determinado tamanho e tipo.
- **Size code (Código do tamanho)**
  Encontre contêineres de um determinado tamanho e tipo.
- **City or country (Cidade ou país)**
  Encontre contêineres de uma determinada cidade ou país.
- **Validação**
  Encontre contêineres que já foram validados por meio do código do proprietário ou dígito de controle.

Criar um relatório PDF de alta qualidade



Crie um relatório com base nos resultados de sua pesquisa. É possível usar essa função para incluir imagens de alta resolução no resultado.

1. No Smart Client, faça uma pesquisa.
2. Selecione os resultados de pesquisa que deseja incluir no relatório.
3. Clique em p,255mm,sfx)=″graphics:graphicF514E97847ADD97F4BD7253E4437FE02″ **> Create high quality PDF report (Criar relatório PDF de alta qualidade)**.
4. (Opcional) Insira o **Report name (Nome do relatório)**, **Report destination (Destino do relatório)** e **Notes (Anotações)**.
5. Para cada resultado de pesquisa, selecione o quadro que deseja incluir no relatório. Para ampliar uma imagem, clique duas vezes.
6. Clique em **Create (Criar)**. Quando o relatório estiver pronto, você receberá uma notificação.

Placas de licença da Axis

Você pode adicionar uma guia separada para pesquisa e gerenciamento de placas de licença no Smart Client. Essa guia centraliza todas as tarefas do operador relacionadas ao gerenciamento, pesquisa e exportação da placa de licença com base nas informações fornecidas por suas câmeras Axis habilitadas para LPR.



Antes de começar

- Certifique-se de ter VMS versão 2018 R3 ou posterior
- Certifique-se de ter o VMS Device Pack 10.1 ou posterior
- A hora da câmera deve ser sincronizada com NTP
- Use um dos aplicativos listados em

Configurar placas de licença da Axis

1. No Management Client, adicione a câmera que executa o aplicativo escolhido.
2. Ative todos os dispositivos desejados. Para poder usar o AXIS License Plate Verifier, Camera 1 e Metadata 1 são necessários.
3. Certifique-se de que o dispositivo de metadados esteja relacionado à câmera:
   - Vá para **Devices** > **Camera** (Dispositivos > Câmera) e selecione o dispositivo.
   - Acesse a guia **Client (Cliente)** e certifique-se de que o dispositivo de metadados da câmera esteja selecionado em **Related metadata (Metadados relacionados)**.
4. Configurar metadados:
   4.1. Vá para **Site Navigation > Recording Server (Navegação no site > Servidor de gravação)** e encontre o dispositivo.
   4.2. Selecione Metadata 1 (Metadados 1) e clique em **Settings (Configurações)**.
   4.3. Vá para **Metadata stream > Event data (Stream de metadados > Dados de eventos)** e selecione **Yes (Sim)**.
5. Vá para a guia **Record settings (Configurações da gravação)** e verifique se a gravação está ativada para metadados.
6. Clique em **Save (Salvar)**.

Procurar uma placa de licença

1. No Smart Client, vá para **Axis license plates (Placas de licença da Axis)**.
   Se você não conseguir ver a guia, vá para **Settings > Axis search options (Configurações > Opções de pesquisa da Axis)** e selecione **Show license plate tab (Mostrar guia de placas de licença)**.
2. Clique em **Add camera... (Adicionar câmera)**, selecione as câmeras relevantes e clique em **Close (Fechar)**.
   É necessário ser um administrador para adicionar câmeras ao sistema. Quando as placas de licença forem detectadas pela câmera, elas aparecerão em tempo real na lista, incluindo imagens cortadas das placas capturadas pela câmera. O resultado da pesquisa não exibirá mais de 5000 resultados.
3. Insira uma placa de licença e um **Time interval (Intervalo de tempo)** para filtrar o resultado da pesquisa.
   - Insira um **Intervalo de tempo** personalizado entre duas datas escolhidas para filtrar o resultado da pesquisa.

Procurar uma placa de licença em tempo real

1. No Smart Client, vá para **Axis license plates (Placas de licença da Axis)**.

Se você não conseguir ver a guia, vá para **Settings > Axis search options (Configurações > Opções de pesquisa da Axis)** e selecione **Show license plate tab (Mostrar guia de placas de licença)**.

2. Clique em **Add camera... (Adicionar câmera)**, selecione as câmeras relevantes e clique em **Close (Fechar)**.
É necessário ser um administrador para adicionar câmeras ao sistema. Quando as placas de licença forem detectadas pela câmera, elas aparecerão em tempo real na lista, incluindo imagens cortadas das placas capturadas pela câmera. O resultado da pesquisa não exibirá mais de 5000 resultados.
3. Insira uma placa de licença e selecione **Time interval (Intervalo de tempo)** > **Live (Tempo real)** para filtrar o resultado da pesquisa.

Fazer o ajuste preciso de uma pesquisa

Para restringir os resultados da pesquisa, você pode usar um ou vários filtros de pesquisa.

- **Intervalo de tempo**
Filtrar por acertos da pesquisa em um determinado período.
- **Placa de licença**
Filtre um texto de placa de licença parcial ou completo.
- **Câmeras**
Filtrar por acertos de pesquisa detectados por câmeras específicas.
- **Direção**
Filtrar por veículos que se movem em uma determinada direção.
- **Lists (Listas)**
Filtrar por acertos de pesquisas em determinados sites e filtrar por acertos de pesquisas em listas de permissões, bloqueio e personalizadas. Para obter mais informações sobre como configurar listas, consulte *Gerenciamento centralizado de listas de placas de licença, on page 23*.

Otimizar a velocidade da pesquisa

Você pode aumentar a velocidade da pesquisa controlando os dados que o sistema armazena no dispositivo de metadados do VMS.

- Desative os dados analíticos se você não precisar deles.
  - Vá para **Devices** > **Metadata** (Dispositivos > Metadados) e selecione seu dispositivo.
  - Clique em **Configurações** e desative **Dados analíticos**.
- Se você precisar de dados analíticos, poderá usar metadados consolidados, se estiverem disponíveis. Consulte *Metadados e pesquisas, on page 107*.
- Desative os eventos que você não precisa no AXIS License Plate Verifier. Você só precisa do evento **Lost** (Perdido) para que o AXIS Optimizer funcione. Consulte *AXIS License Plate Verifier*.
- Certifique-se de usar o AXIS OS 12.8 ou posterior.

Exportar uma pesquisa de placa de licença como relatório PDF

Use essa função para compilar seus resultados de pesquisa de interesse como um relatório em PDF com imagens de alta qualidade.

1. Clique em **Export... (Exportar...)**.
2. Selecione **PDF...**.
3. (Opcional) Insira o **Report name (Nome do relatório)**, **Report destination (Destino do relatório)** e **Notes (Anotações)**.
4. Para cada resultado de pesquisa, selecione o quadro que deseja incluir no relatório. Para ampliar uma imagem, clique duas vezes nela
5. Clique em **Create (Criar)**. Quando o relatório estiver pronto, você receberá uma notificação.

Exportar uma pesquisa de placa de licença como relatório CSV

Use esta função para compilar um grande número de resultados de pesquisa como um relatório CSV.

1. Clique em **Export... (Exportar...)**.
2. Selecione **CSV...**.
3. Escolha um destino para o arquivo a ser exportado.

Percepções da Axis

As percepções da Axis proporcionam uma visão geral dos dados de seus dispositivos em gráficos e painéis. Assim, você pode exibir metadados de todos os seus dispositivos. Você pode exibir dados sobre objetos detectados, veículos identificados e alarmes. Você também pode criar novos painéis e compartilhá-los com outros usuários.

As percepções da Axis estão disponíveis nas visualizações padrão do administrador e do operador. A visualização padrão do administrador no Axis insights está disponível apenas para usuários com direitos de administrador, enquanto a visualização padrão do operador está disponível para todos os operadores com as permissões apropriadas. Consulte *Configurar opções de funções, on page 101*. A visualização do operador fornece dados específicos de visualizações de câmeras selecionadas, enquanto a visualização do administrador fornece uma visão geral de todo o sistema.

Acesse Axis insights

- Acesse **Smart Client** e clique em **Axis insights**.
- **Dashboard (Painel)**: Selecione um painel na lista suspensa.
- **Camera view (Visualização de câmera)**: Selecione uma visualização de câmera específica para obter uma visão geral dos dados.
- **Time range (Intervalo de tempo)**: Selecione um intervalo de tempo específico.
- **Auto update (Atualização automática)**: Ative para atualizar os dados automaticamente.

••• O menu de contexto contém:

- **Edit dashboard (Editar painel de controle)**: Editar, compartilhar ou remover o painel.
- **Add chart (Adicionar gráfico)**: Crie um novo gráfico no painel.
- **About Axist insights (Sobre Axis insights)**: Leia sobre Axis insights.

••• O menu de contexto em cada gráfico contém:

- **Maximize chart (Maximizar gráfico)**: Clique para ampliar o gráfico.
- **Copy as image (Copiar como imagem)**: Clique para copiar o gráfico para sua área de transferência.
- **Export (Exportar)**: Clique para exportar o gráfico como PNG ou CSV.
- **Edit chart (Editar gráfico)**: Clique para editar o gráfico.
- **Remove chart (Remover gráfico)**: Clique para remover o gráfico.

Observação

- Você pode clicar na figura em alguns gráficos para ver informações adicionais.
- : Mostra as seleções específicas que se aplicam a cada gráfico em seu painel.

Criar um novo painel

1. **Dashboard (Painel)**: Selecione **Add dashboard (Adicionar painel)** na lista suspensa.
2. Clique em **Empty** (Vazio) para criar um novo painel ou clique em **From existing dashboard** (Do painel existente) para criar um painel semelhante a um disponível no sistema.

3. **Nome**: Insira um nome para seu painel.
4. **Allow other users to view this dashboard (Permitir que outros usuários visualizem este painel)**: Clique para compartilhar seu painel com outros usuários no modo somente leitura.
5. Clique em **Aplicar**.
6. **Add chart (Adicionar gráfico)**: Clique para adicionar um novo gráfico.
   - **Select chart type (Selecione o tipo de gráfico)**: Selecione o tipo de gráfico que deseja e clique em **Next (Avançar)**. Você pode pesquisar um tipo de gráfico usando tags ou títulos de gráficos, como analíticos de vídeo, veículos, gráficos de linha e assim por diante.
   - **Modify data selections (Modifique as seleções de dados)**: Selecione os filtros aplicáveis em cada categoria.
   - **Adjust appearance (Ajuste a aparência)**: Edite os textos e selecione o tamanho do gráfico.

Configurar a lista suspensa do painel

Observação

- Por padrão, você só pode ver os painéis que criou.

Para visualizar os painéis compartilhados por outros usuários na lista suspensa no **Dashboard** (Painel):

1. Acesse **Shared dashboards** (Painéis compartilhados).
2. Ative o botão de alternância para cada painel compartilhado que deseja adicionar à lista suspensa.

Exibir insights para uma visualização de câmera específica

Ao visualizar vídeos ao vivo e de reprodução em uma visualização de câmera, é possível abrir os insights da Axis com a visualização de câmera ativa pré-selecionada.

Para abrir as percepções da Axis para uma exibição de câmera específica:

1. Vá para **Smart Client (Cliente inteligente)** e abra uma exibição.
2. Clique em **Show insights (Mostrar percepções)**.

Configurar percepções de dados Axis

1. Verifique se a câmera é compatível com o AXIS Object Analytics. Consulte os analíticos no *seletor de produtos Axis*.
2. Verifique se a data e a hora da câmera estão definidas corretamente.
3. No Management Client, certifique-se de que o dispositivo de metadados esteja ativado para as câmeras.
4. Certifique-se de que o dispositivo de metadados esteja relacionado à câmera:
   - Vá para **Devices** > **Camera** (Dispositivos > Câmera) e selecione o dispositivo.
   - Acesse a guia **Client (Cliente)** e certifique-se de que o dispositivo de metadados da câmera esteja selecionado em **Related metadata (Metadados relacionados)**.
5. Para visualizar todos os dados disponíveis nos insights da Axis, ative a análise de cena na sua câmera usando *AXIS Scene Metadata*:
   5.1. Vá para **Devices** > **Metadata** (Dispositivos > Metadados) e selecione seu dispositivo.
      - Clique em **Record (Gravar)** e confirme se a opção **Recording (Gravando)** está ativada.
      - Clique em **Settings (Configurações)** e certifique-se de que a opção **Analytics data (Dados de analíticos)** esteja ativada.

   5.1. Ative **os metadados** consolidados para proporcionar um tempo de carregamento mais rápido se disponível. Consulte *Metadados e pesquisas, on page 107*.
6. Para ativar dados para tipos de gráficos usando *AXIS Object Analytics*, *AXIS Image Health Analytics* ou *Sensores ambientais*:

- Vá para **Devices** > **Metadata** (Dispositivos > Metadados) e selecione seu dispositivo.
- Clique em **Record (Gravar)** e confirme se a opção **Recording (Gravando)** está ativada.
- Clique em **Settings (Configurações)** e certifique-se de que a opção **Event data (Dados de eventos)** esteja ativada.
- Recomendamos que crie uma regra no VMS para sempre realizar a gravação de metadados deste dispositivo.

7. Defina permissões para os grupos de segurança:
   7.1. Vá para **Site Navigation** > **Security** > **Roles** (Navegação no site > Segurança > Funções).
   7.2. Selecione uma função.
   7.3. Vá para **Cameras (Câmeras)**. Selecione **Read (Ler)**.
   7.4. Vá para **Metadata (Metadados)**. Selecione **Read (Ler)**, **Live (Ao vivo)** e **Playback (Reprodução)**.
8. Para adicionar metadados de placas de licença às percepções da Axis, consulte *Configurar placas de licença da Axis, on page 60*

Solução de problemas do Axis insights

Problema	Solução
Os gráficos mostram "no data" (sem dados).	Você precisa configurar as percepções da Axis. Consulte *Configurar percepções de dados Axis, on page 63*.
A exibição do operador demora muito tempo para ser carregada.	• Reduza o intervalo de tempo. • Crie e use uma exibição que tenha menos câmeras com análise de cena. • Ative os metadados consolidados, consulte *Metadados e pesquisas, on page 107*.

Correção de distorção de vídeo

A correção de distorção planifica e corrige a perspectiva de uma imagem distorcida geométrica causada por uma lente grande angular ou fisheye. A correção de distorção da Axis no VMS pode ser usada com qualquer câmera panorâmica Axis 360°. A correção de distorção é feita diretamente na câmera ou no Smart Client.

Mais detalhes sobre a correção de distorção:

- Ao usar a correção de distorção no lado do cliente, você obterá uma correção suave em vídeos ao vivo e gravados.
- Ao voltar para uma exibição, você será direcionado automaticamente para o local da correção mais recente.
- A correção de distorção é incluída quando você exporta vídeos.
- É possível salvar uma posição inicial, consulte *Definir uma posição inicial, on page 67*.
- Você pode configurar se os operadores poderão controlar e editar as exibições de correção de distorção, consulte *Permitir que os operadores controlem e editem exibições de correção de distorção, on page 68*.

Criar uma exibição de correção de distorção

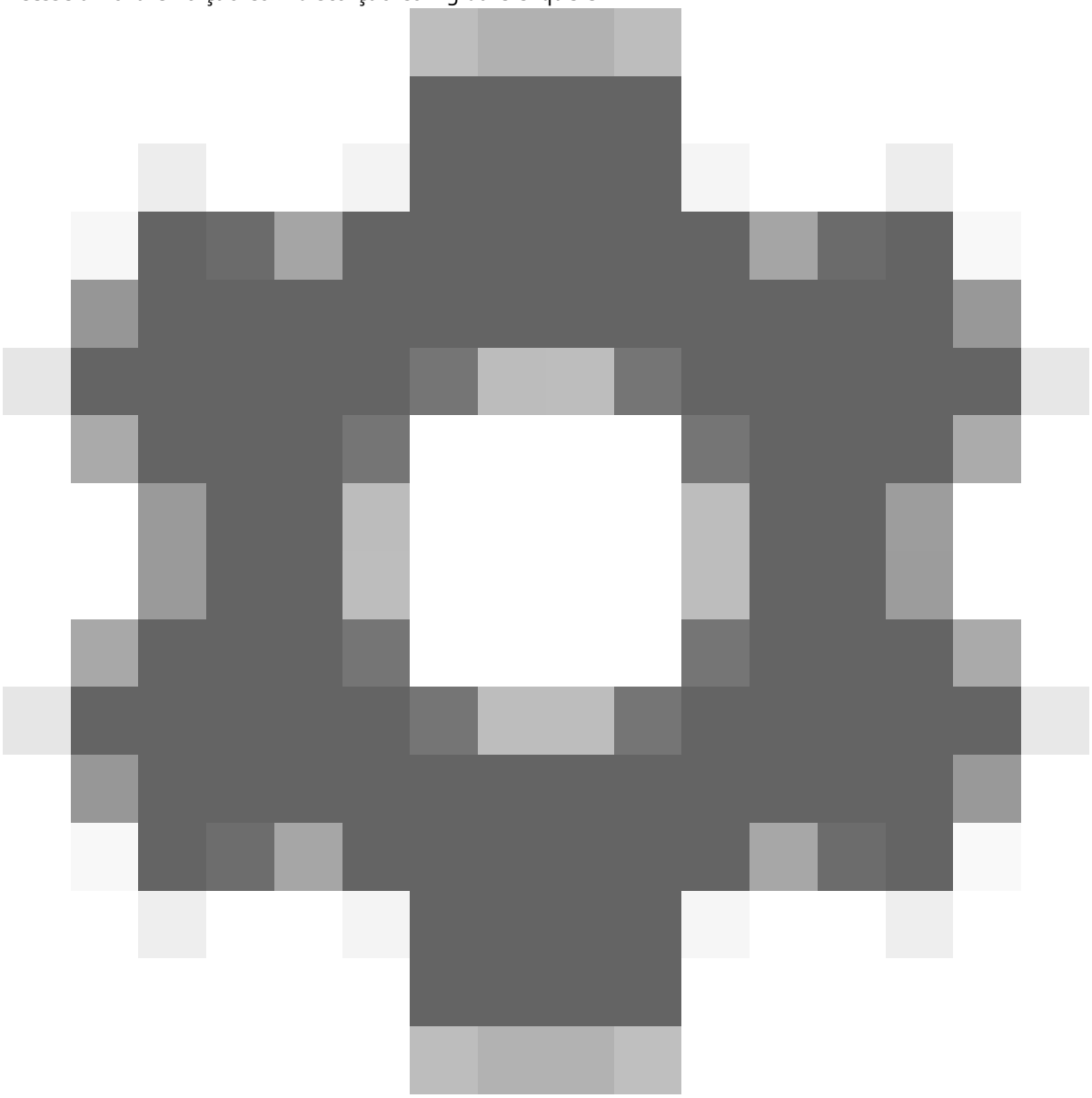


Observação

Para otimizar o fluxo para a correção de distorção, selecione a resolução máxima disponível para **Video Stream 1 (Fluxo de vídeo 1)** da **Camera 1 (Câmera 1)** no Management Client. Para obter mais informações, consulte *Desempenho e solução de problemas, on page 68*.

1. Abra o Smart Client e clique em **Setup (Configuração)**.
2. Vá para **Views (Exibições)**.
3. Clique em **Create new view (Criar nova exibição)** e selecione um formato.
4. Vá para **System overview > AXIS Optimizer (Visão geral > AXIS Optimizer)**.
5. Clique em **Dewarping view (Exibição com distorção corrigida)** e arraste-a para a exibição.
6. Selecione uma câmera e a posição de montagem atual da câmera.
7. Clique em **Setup (Configuração)**.

8. Acesse a nova exibição com distorção corrigida e clique em



.

9. Clique em **Set view type (Definir tipo de exibição)** e selecione uma opção. Dependendo de como a câmera está montada, você pode selecionar **Quad**, **Normal**, **Normal with overview (Normal com visão geral)** ou **Panorama**.

Observação

Recomendamos usar 100% de DPI. Se a resolução for diferente de 100%, a deformação da Axis na segunda tela poderá não estar totalmente visível.

Se você usar outras configurações de DPI, as janelas de correção de distorção poderão estar parcialmente visíveis. Siga as instruções nestas artigos externos para resolver esse problema:

- *Problemas com o XProtect em monitores de alta resolução (4K e acima)*
- *Dimensionamento da GUI do cliente em visores com DPI alto*

Criar uma exibição de correção de distorção para câmeras panorâmicas multissensor

Você pode usar exibições com distorção corrigida para câmeras panorâmicas multissensor, por exemplo AXIS P3807-PVE Network Camera e AXIS Q3819-PVE Panoramic Camera.

- Costura no lado do cliente. Se a câmera estiver configurada no modo de captura com correção de distorção no cliente, o AXIS Optimizer costurará as quatro imagens em um panorama simples (somente AXIS P3807-PVE).
- Ajuste do horizonte. É possível ajustar o horizonte do panorama. Isso poderá ser necessário se a câmera for inclinada para o chão e o horizonte mundial estiver curvo. Isso também tornará o controle de PTZ virtual mais intuitivo.
- Controle de PTZ. Permite aumentar o zoom e percorrer a imagem como se fosse uma câmera PTZ.



Observação

Requisitos

- Usuários com um dos seguintes direitos de usuário:
  - Função de otimizador
  - Hardware > Comandos do driver = Permitir
- Uma câmera panorâmica multissensor Axis

1. Se aplicável, defina o modo de captura como **Client Dewarp (Correção de distorção no cliente)** durante a configuração inicial do dispositivo.
2. Abra o Smart Client e clique em **Setup (Configuração)**.
3. Vá para **Views (Exibições)**.
4. Clique em **Create new view (Criar nova exibição)** e selecione um formato.
5. Vá para **System overview > AXIS Optimizer (Visão geral > AXIS Optimizer)**.
6. Clique em **Dewarping view (Exibição com distorção corrigida)** e arraste-a para a exibição.
7. Selecione uma câmera panorâmica multissensor.
   Na primeira vez que você adicionar a câmera panorâmica multissensor a uma exibição com distorção corrigida, uma janela de calibração de horizonte será mostrada acima da exibição.
8. Clique nas setas para alinhar a linha vermelha ao horizonte mundial.
9. Clique em **Done (Concluído)** para salvar suas configurações e sair do modo de calibração.

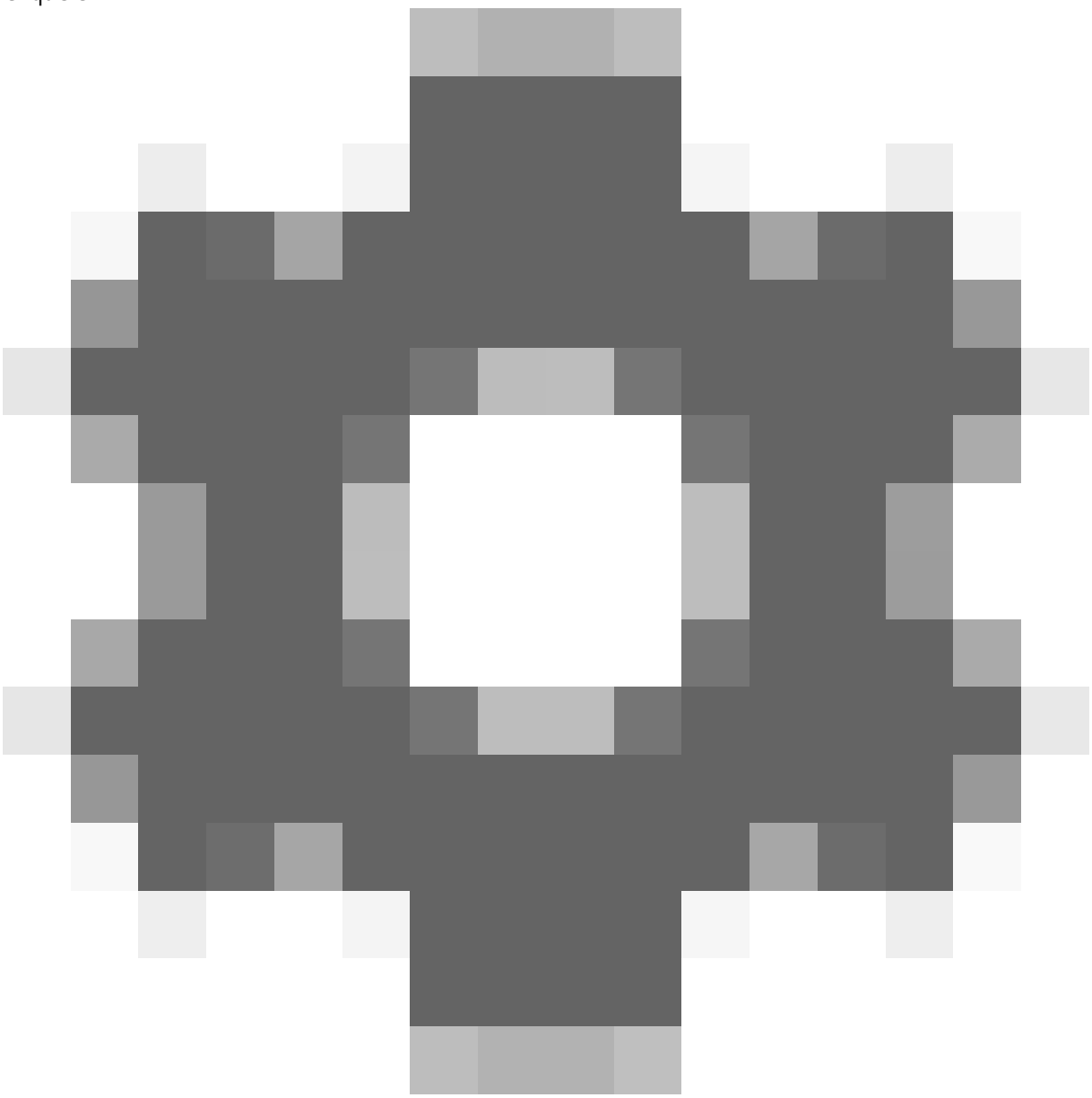
Visão ampla

A visão ampla é um tipo de visualização para câmeras panorâmicas multissensor. Ative a **wide view (visão ampla)** se o campo de visão normal de 120° não for suficiente. Com a visão ampla, a imagem sempre terá a distorção corrigida Desative a **wide view (visão ampla)** para obter uma transição para a visualização normal quando o zoom for totalmente reduzido.

Definir uma posição inicial

1. No Smart Client, abra uma exibição com distorção corrigida.
2. Vá para a posição que deseja salvar como posição inicial.

3. Clique em



e, em seguida, em **Set home position (Definir posição inicial)**.

Permitir que os operadores controlem e editem exibições de correção de distorção

Você pode configurar se os operadores têm permissão para controlar e editar as exibições de correção de distorção, consulte *Personalizar acesso a recursos para operadores, on page 101*.

Desempenho e solução de problemas

Considerações sobre desempenho

- A correção de distorção de vídeo Axis é executada na GPU, quando possível, mas ela também deposita carga sobre a CPU.
- Para impedir que a taxa de quadros caia em uma exibição grande com muitas exibições com distorção corrigida, considere o seguinte:
  - Resolução da câmera. Uma alta resolução de câmera, por exemplo, 2880 x 2880, requer alta capacidade de computação quando comparada, por exemplo, à resolução 1920 x 1920.
  - Taxa de quadros da câmera. Se você não precisar de uma taxa de quadros alta, uma taxa de quadros menor poderá impedir falhas na exibição com distorção corrigida e outras exibições.

– Resolução do monitor. Monitores de alta resolução, por exemplo, 4K, necessitam de muitos recursos para mostrar o vídeo. Se você não precisar da resolução mais alta, uma resolução de monitor inferior possibilitará a execução de mais exibições sem falhas com a distorção corrigida.

Resolução dinâmica

- O fluxo de vídeo será automaticamente reduzido em escala, se possível, sem prejuízos à qualidade do vídeo. Isso pode melhorar o desempenho das exibições com distorção corrigida.
- Se você observar um cintilação ao aplicar zoom na visão geral, desativar a resolução dinâmica poderá ajudar.
- Para ativar ou desativar a resolução dinâmica: no Smart Client, acesse **Settings (Configurações) > Axis dewarping options (Opções de correção de distorção em barri) > Rendering options (Opções de renderização)** e selecione ou limpe **Dynamic resolution (Resolução dinâmica)**.
- A **Dynamic resolution (Resolução dinâmica)** é ativada por padrão.

Renderização de compatibilidade

- Se houver qualquer erro visual na imagem com distorção corrigida, por exemplo, uma imagem preta, ou se o desempenho parecer pior do que o esperado, ative a renderização de compatibilidade. Observe que um efeito negativo de renderização de compatibilidade é que a transição entre as exibições e a varredura durante a reprodução pode cintilar.
- Para ativar ou desativar a renderização de compatibilidade: abra o Smart Client e acesse **Settings (Configurações) > Axis dewarping options (Opções de correção de distorção em barri) > Rendering options (Opções de renderização)** e selecione ou limpe **Use compatibility rendering (Usar renderização de compatibilidade)**.
- A opção **Use compatibility rendering (Usar renderização de compatibilidade)** é desativada por padrão.

O que esperar

Em um sistema de referência com um Intel i7 8700 NVIDIA GeFore 1050 GTX e três monitores 1920 x 1080, você pode esperar que:

- 7 exibições com distorção corrigida na resolução 1920 x 1920 e 25 fps podem ser executadas sem perda de quadros, ou
- 4 exibições com distorção corrigida na resolução 2880 x 2880 e 25 fps

Se um dos três monitores operar na resolução 4K em vez de 1920 x 1080, você poderá esperar que:

- 5 exibições com distorção corrigida na resolução 1920 x 1920 e 25 fps podem ser executadas sem perda de quadros, ou
- 3 exibições com distorção corrigida na resolução 2880 x 2880 e 25 fps. Uma exibição com distorção corrigida em cada monitor.

A taxa de quadros e as escalas de resolução são lineares. Um computador capaz de executar 5 exibições com distorção removida com 30 fps poderá executar 10 visualizações se você reduzir a taxa de quadros para 15 fps.

Integração a dispositivos de uso corporal

O AXIS Optimizer Body Worn Extension permite que os usuários de câmeras em campo gravem, rotulem e compartilhem vídeos com investigadores baseados na central, que podem procurar e gerenciar provas em vídeo usando o VMS. O serviço proporciona de forma segura a conexão e a transferência entre o sistema de uso corporal Axis e o VMS. O AXIS Body Worn Extension é um serviço gratuito e autônomo que você deve instalar no servidor de gravação.

Observação

As versões compatíveis são:

- VMS versão 2020 R1 Corporate ou versões mais recentes
- VMS versão 2020 R1 Professional+ ou versões mais recentes
- VMS versão 2020 R1 Expert ou versões mais recentes

Use sempre os hotfixes e instaladores de patches cumulativos mais recentes do VMS.

Saiba mais

- Para baixar o serviço em si ou ler o guia de integração e a nota da solução, vá para *axis.com*.
- Para ler o manual do usuário, vá para *axis.help.com*.

Controle de acesso

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

Observação

Requisitos

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

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

Para utilizar portas no AXIS Secure Entry, é necessário adquirir uma licença por porta; consulte *Ativar licenças de porta, on page 72*.

Configuração do controle de acesso

Observação

Antes de começar, faça o seguinte:

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

Versão do AXIS Optimizer	Versão mínima do AXIS OS	Versão recomendada do AXIS OS
6.0	12.6.94.1	12.10.73.4
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

Adicionar um controlador de porta em rede Axis ao seu sistema

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

Observação

- Você verá os controladores adicionados na guia **Management (Gerenciamento)**.
- Para adicionar manualmente um controlador ao sistema, clique em **+ Add (+ Adicionar)** na guia **Management (Gerenciamento)**.
- Para integrar sua atualização ao VMS sempre que você adicionar, remover ou editar o nome de um controlador de porta:
  - Vá para **Site Navigation** > **Access control(Navegação no site > Controle de acesso)** e clique na integração do controle de acesso.
  - Clique em **Refresh Configuration (Atualizar configuração)** na guia **General settings (Configurações gerais)**.

Ativar licenças de porta

Antes de poder adicionar portas, é necessário ativar as licenças que você possui no seu sistema.

1. Em **Site Navigation (Navegação no site)**, vá para **License Information (Informaçõe da licença)**.
2. Clique em **Activate License Manually (Ativar licença manualmente)** e selecione **Online** ou **Offline**.
3. Para ativar licenças de porta online:
   – Insira seu nome de usuário e senha.
4. Para ativar licenças de porta offline, consulte *ativar licenças offline*.

Caso precise ajustar o número de licenças de porta a serem ativadas:

1. Vá para **AXIS Optimizer** > **Access control (Controle de acesso)**.
2. Em **Configuration (Configuração)**, selecione **Devices (Dispositivos)**.
3. Vá para **Allocated door licenses (Licenças de porta alocadas)** > **Custom license allocation (Alocação personalizada de licenças)** e insira o número de licenças de porta que deseja utilizar.
4. Clique em **Aplicar**.
5. Vá para **License Information (Informações sobre licenças)** e reative suas licenças.

Configurar o controle de acesso

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control (Navegação no site, AXIS Optimizer, Controle de acesso)**.
2. Para editar os perfis de identificação predefinidos ou criar um novo perfil de identificação, consulte *Perfis de identificação, on page 88*.
3. Para usar uma configuração personalizada para formatos de cartões e tamanhos de PIN, consulte *Formatos de cartão e PIN, on page 84*.
4. Adicione uma porta e aplique um perfil de identificação à porta. Consulte *Adicione uma porta, on page 74*.
5. Adicione uma zona e adicione portas à zona. Consulte *Adicionar uma zona, on page 82*.

Compatibilidade do software do dispositivo para controladores de porta

Importante

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

- **Supported AXIS OS versions (Versões compatíveis do AXIS OS):** As versões do AXIS OS compatíveis listadas acima só se aplicam quando se atualiza a partir da versão do VMS original recomendada e quando o sistema tem uma porta. Se o sistema não atender a essas condições, você deverá atualizar para a versão do AXIS OS recomendada para a versão específica do VMS.
- **Minimum supported AXIS OS version (Versão mínima compatível d AXIS OS:** A versão mais antiga do AXIS OS instalada no sistema determina a versão mínima suportada do AXIS OS, com um limite de duas versões anteriores. Suponha que você esteja usando o AXIS Optimizer versão 6.0 e atualize todos os dispositivos para a versão recomendada AXIS OS, 12.10.73.4. Assim, a versão 12.6.94.1 do AXIS OS passa a ser a versão mínima compatível com o seu sistema.
- **Atualização para uma versão do AXIS OS superior à recomendada:** Suponha que você atualize para uma versão do AXIS OS superior à recomendada para uma determinada versão do VMS. Você sempre poderá fazer downgrade e retornar para a versão recomendada do AXIS OS sem nenhum problema, desde que esteja dentro dos limites de suporte definidos para a versão do VMS.
- **Futuras recomendações do AXIS OS:** Siga sempre a versão do AXIS OS recomendada para a respectiva versão do VMS, a fim de garantir a estabilidade do sistema e total compatibilidade.

Integração do controle de acesso

Para integrar o controle de acesso ao VMS:

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

Observação

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

Portas e zonas

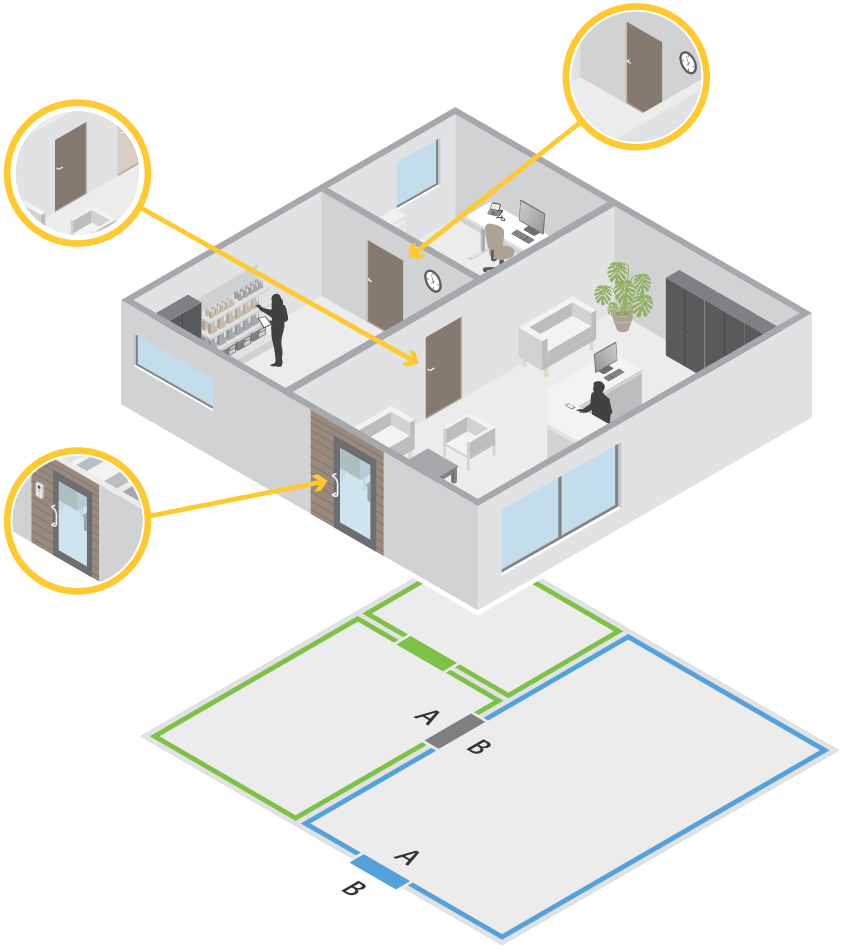
Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones (Navegação no site, AXIS Optimizer, Controle de acesso, Portas e zonas)** para obter uma visão geral e configurar portas e zonas.

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

Portas	
Nome	O nome da porta.
Controle de porta	O controlador de porta conectado à porta.
Lado A	A zona na qual o lado A da porta está localizado.
Lado B	A zona na qual o lado B da porta está localizado.
Identification profile: (Perfil de identificação:	O perfil de identificação aplicado à porta.
Formatos de cartão e PIN	Mostra o tipo de formatos de cartões ou comprimento do PIN.
Status	Estado da porta. • **Online:** A porta está online e funciona corretamente. • **Reader offline (Leitor offline):** O leitor na configuração da porta está offline.

	• **Reader error (Erro no leitor):** O leitor na configuração da porta não suporta canal seguro ou o canal seguro foi desativado para esse leitor.
Zonas	
Nome	O nome da zona.
Número de portas	O número de portas incluídas na zona.

Exemplo de portas e zonas



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

Adicione uma porta

Observação

- Você pode configurar um controlador de porta com uma porta com duas fechaduras ou duas portas com uma trava cada.
- Se um controlador de porta não tiver portas e você estiver usando uma nova versão do AXIS Optimizer com um software mais antigo no controlador, o sistema impedirá que você adicione uma porta. No

entanto, o sistema permite novas portas em controladores de sistema com software mais antigo se já houver uma porta existente.

Criar uma configuração de porta para adicionar uma porta:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas)**.
2. Clique em **Add door (Adicionar porta)**.
3. Insira um nome de porta.
4. No menu suspenso **Controller (Controlador)**, selecione um controlador de porta. O controlador fica cinza quando não é possível adicionar outra porta quando está offline ou o HTTPS não está ativo.
5. No menu suspenso **Door type (Tipo de porta)**, selecione o tipo de porta que deseja criar.
6. Clique **Next (Avançar)** para ir para a página configuração da porta.
7. Selecione uma porta de relé no menu suspenso **Primary lock (Trava principal)**.
8. Para configurar duas travas na porta, selecione uma porta de relé no menu suspenso **Secondary lock (Trava secundária)**.
9. Selecione um perfil de identificação. Consulte *Perfis de identificação, on page 88*.
10. Configure as opções da porta. Consulte *Configurações da porta, on page 76*.
11. Configure uma porta com monitoramento. Consulte *Adicionar uma porta com monitoramento, on page 79*.
12. Clique em **Save (Salvar)**.

Copie uma configuração de porta existente para adicionar uma porta:

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

Para editar uma porta:

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

Para remover uma porta:

1. Vá para **Site Navigation** > **AXIS Optimizer**> **Access control** > **Doors and zones** > **Doors (Navegação no site, AXIS Optimizer , Controle de acesso, Portas e zonas, Portas)**.
2. Selecione uma porta na lista.

3. Clique em **Remove (Remover)**.
4. Clique em **Sim**.

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

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

Configurações da porta

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

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

Nível de segurança da porta

Você pode adicionar os seguintes recursos de segurança à porta:

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

Dupla passagem – A dupla passagem permite que um titular de cartão substitua o estado atual de uma porta. Por exemplo, ele pode usá-la para travar ou destravar uma porta fora da programação regular, o que é mais conveniente do que entrar no sistema para destravar a porta. A dupla passagem não afeta uma programação existente. Por exemplo, se uma porta estiver programada para travar na hora do fechamento e um funcionário sair para o intervalo de almoço, a porta ainda será travada de acordo com a programação.

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

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

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

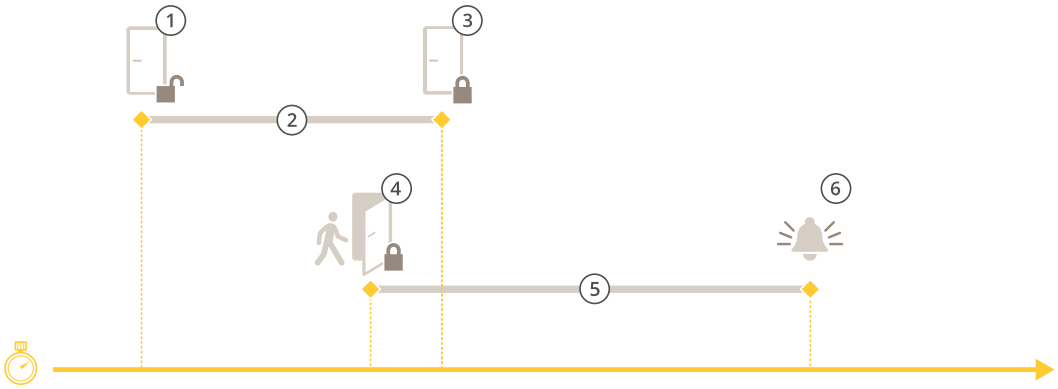
Regra das duas pessoas	
Laterais A e **B**	Selecione em quais lados da porta a regra será usada.
Programações	Selecione quando a regra estiver ativa.
Tempo limite (segundos)	O tempo limite é o tempo máximo permitido entre as passagens do cartão ou outro tipo de credencial válida.

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

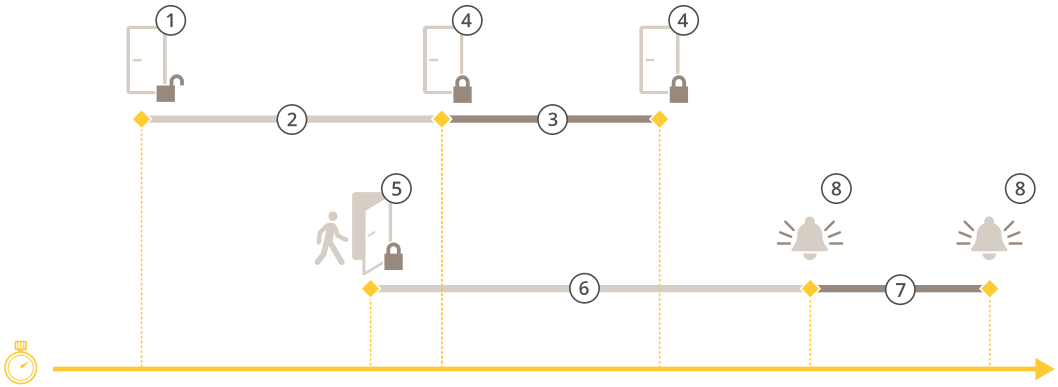
1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas)**.
2. Selecione a porta para a qual deseja configurar um nível de segurança.
3. Clique em **Edit (Editar)**.
4. Clique em **Nível de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

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

Opções de tempo



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



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

Adicionar um monitor de porta

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

1. Vá para a página de configuração de porta. Consulte *Adicione uma porta, on page 74*
2. Em **Sensores**, clique em **Adicionar**.
3. Selecione **Door position sensor (Sensor de posição de porta)**.
4. Selecione a porta de E/S à qual deseja conectar o monitor de porta.
5. Em **Door open if (Porta aberta se)**, selecione como os circuitos do monitor de porta serão conectados.
6. Para ignorar as alterações de estado da entrada digital antes de entrar em um novo estado estável, defina um horário **Debounce time (Tempo de debounce)**.
7. Para acionar um evento quando ocorre uma interrupção na conexão entre o controlador de porta e o monitor de porta, ative **Supervised input (Entrada supervisionada)**. Consulte *Entradas supervisionadas, on page 83*.

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

Adicionar uma porta com monitoramento

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

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

Observação

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

Para configurar uma porta com monitoramento:

1. Faça a instalação do AXIS A9210 e atualize-o com a versão mais recente do AXIS OS.
2. Instale os sensores de posição da porta.
3. No VMS, vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones (Navegação no site > AXIS Optimizer > Controle de acesso > Portas e zonas)**.
4. Clique em **Add door (Adicionar porta)**.
5. Insira um nome.
6. Em **Type (Tipo)**, selecione **Monitoring door (Porta com monitoramento)**.

7. Em **Device (Dispositivo)**, selecione o seu módulo de relé de E/S em rede.
8. Clique em **Next** (Próximo).
9. Em **Sensors (Sensores)**, clique em **+ Add (+ Adicionar)** e selecione **Door position sensor (Sensor de posição da porta)**.
10. Selecione a E/S conectada ao sensor de posição da porta.
11. Clique em **Adicionar**.

Adicionar um leitor

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

Se você aplicar uma configuração personalizada dos formatos de cartões ou um tamanho de PIN a um leitor, será possível vê-la em **Card formats (Formatos de cartões)** em **Configuration > Access control > Doors and zones (Configuração > Controle de acesso > Portas e zonas)**. Consulte *Portas e zonas, on page 73*.

1. Vá para a página de configuração de porta. Consulte *Adicione uma porta, on page 74*.
2. Em um lado da porta, clique em **Add (Adicionar)**.
3. Selecione **Card reader (Leitor de cartões)**.
4. Selecione o **Reader type (Tipo de leitor)**.
5. Para usar uma configuração personalizada de comprimento de PIN para este leitor.
   5.1. Clique em **Advanced (Avançado)**.
   5.2. Ative **Custom PIN length (Tamanho do PIN personalizado)**.
   5.3. Defina os valores de **Min PIN length (Tamanho mínimo do PIN)**, **Max PIN length (Tamanho máximo do PIN)** e **End of PIN character (Caractere de fim de PIN)**.
6. Para usar um formato de cartão personalizado para este leitor.
   6.1. Clique em **Advanced (Avançado)**.
   6.2. Ative **Custom card formats (Formatos de cartões personalizados)**.
   6.3. Selecione os formatos de cartões que deseja usar para o leitor. Se um formato de cartão com o mesmo comprimento de bits já estiver em uso, você deverá desativá-lo primeiro. Um ícone de aviso é exibido no cliente quando a configuração do formato de cartão é diferente da configuração do sistema configurada.
7. Clique em **Adicionar**.
8. Para adicionar um leitor ao outro lado da porta, faça esse procedimento novamente.

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

Wiegand	
Controle LED	Selecione **Single wire (Fio único)** ou **Dual wire (R/G) (Fio duplo (R/G))**. Leitores com controle de LED duplo usam fios diferentes para os LEDs vermelhos e verdes.
Alerta de adulteração	Selecione quando a entrada de violação do leitor estiver ativo.

	• **Open circuit (Circuito aberto)**: O leitor envia para a porta o sinal de violação quando o circuito está aberto. • **Closed circuit (Circuito fechado)**: O leitor envia para a porta o sinal de violação quando o circuito está fechado.
Tempo de debounce de violação	Para ignorar as alterações de estado da entrada de violação do leitor antes de entrar em um novo estado estável, defina um horário **Tamper debounce time (Tempo de debounce de violação)**.
Entrada supervisionada	Ative para acionar um evento quando houver uma interrupção na conexão entre o controlador de porta e o leitor. Consulte *Entradas supervisionadas, on page 83*.

Adicionar um dispositivo REX

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

1. Vá para a página de configuração de porta. Consulte *Adicione uma porta, on page 74*.
2. Em um lado da porta, clique em **Add (Adicionar)**.
3. Selecionar **REX device (Dispositivo REX)**.
4. Selecione a porta de E/S à qual deseja conectar o dispositivo REX. Se houver apenas uma porta disponível, ela será selecionada automaticamente.
5. Selecione qual **Action (Ação)** que será acionada quando a porta receber o sinal do REX.
6. Em **REX active (REX ativo)**, selecione a conexão dos circuitos do monitor de porta.
7. Para ignorar as alterações de estado da entrada digital antes de entrar em um novo estado estável, defina um horário **Debounce time (ms) (Tempo de debounce (ms))**.
8. Para acionar um evento quando uma interrupção na conexão entre o controlador de porta e o dispositivo REX ocorrer, ative **Supervised input (Entrada supervisionada)**. Consulte *Entradas supervisionadas, on page 83*.

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

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

Adicionar uma zona

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

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

Observação

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

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

Para editar uma zona:

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

Para remover uma zona:

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

Nível de segurança da zona

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

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

Observação

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

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

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

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

Entradas supervisionadas

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

- Conexão entre o controlador de porta e o monitor de porta. Consulte *Adicionar um monitor de porta, on page 79*.
- Conexão entre o controlador de porta e o leitor que usa os protocolos Wiegand. Consulte *Adicionar um leitor, on page 80*.
- Conexão entre o controlador de porta e o dispositivo REX. Consulte *Adicionar um dispositivo REX, on page 81*.

Para usar entradas supervisionadas:

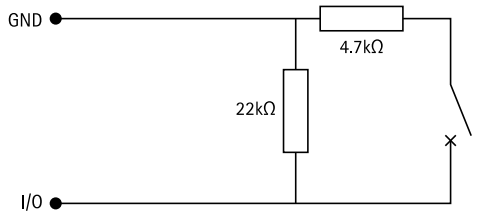
1. Instale os resistores de fim de linha próximos ao dispositivo periférico conforme o possível segundo o diagrama de conexão.
2. Vá para a página de configuração de um leitor, um monitor de porta ou um dispositivo REX, ative **Supervised input (Entrada supervisionada)**.

3. Se você seguiu o diagrama de conexão paralela primeiro, selecione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Conexão paralela primeiro com um resistor paralelo de 22 KΩ e um resistor serial de 4,7 KΩ)**.
4. Se você tiver seguido o diagrama de conexão serial primeiro, selecione **Serial first connection (Conexão serial primeiro)** e selecione um valor de resistor no menu suspenso **Resistor values (Valores de resistor)**.

Diagramas de conexão

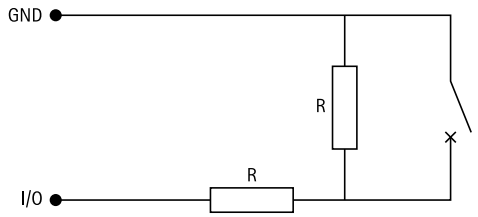
Conexão paralela primeiro

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



Conexão serial primeiro

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



Ações manuais

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

Redefinir – Retorna às regras configuradas do sistema.

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

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

Lock (Bloquear) – Mantém a porta travada até que o sistema conceda acesso ao portador de um cartão.

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

Para realizar uma ação manual:

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

Observação

A porta permanecerá no estado de operação manual, também conhecido como modo de override manual, até que você a redefina para seu cronograma normal.

Formatos de cartão e PIN

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

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

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

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

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

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

Para criar um formato de cartão:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN (Navegação no site > AXIS Optimizer > Controle de acesso > Formatos de cartão e PIN)**.
2. Clique em **Add card format (Adicionar formato de cartão)**.
3. Insira um nome de formato de cartão.
4. No campo **Bit length (Comprimento de bits)**, insira um comprimento de bits entre 1 e 256.
5. Selecione **Invert bit order (Inverter ordem de bits)** se desejar inverter a ordem dos bits de dados recebidos do leitor de cartões.
6. Selecione **Invert byte order (Inverter ordem de bytes)** se desejar inverter a ordem dos bytes dos dados recebidos do leitor de cartões. Essa opção está disponível somente quando você especifica um comprimento de bits que pode ser dividido por oito.
7. Selecione e configure os campos de dados como ativos no formato do cartão. O **Card number (Número do cartão)** ou o **Facility code (Código da instalação)** devem estar ativos no formato do cartão.
8. Clique em **OK**.
9. Para ativar o formato do cartão, marque a caixa de seleção na frente do nome do formato do cartão.

Observação

- Dois formatos de cartão com o mesmo tamanho em bits não podem estar ativos ao mesmo tempo. Por exemplo, se você definiu dois formatos de cartão de 32 bits, somente um deles poderá estar ativo. Desativar o formato do cartão para ativar o outro.
- Você só pode ativar e desativar os formatos de cartão se o controlador de porta foi configurado com pelo menos um leitor.

ⓘ	Clique em ⓘ para ver um exemplo da saída após inverter a ordem de bits.
Alcance	Defina o intervalo de bits dos dados para o campo de dados. O intervalo deve estar dentro do que você especificou para **Bit length (Comprimento de bits)**.

Formato da saída	Selecione o formato de saída dos dados para o campo de dados. **Decimal**: Também conhecido como sistema numérico de posição de base 10, consiste nos números de 0 a 9. **Hexadecimal**: também conhecido como sistema numérico posicional de base 16, consiste em 16 símbolos exclusivos: os números 0 – 9 e as letras a – f.
Ordem de bits do subintervalo	Selecione a ordem de bits. **Little endian**: O primeiro bit é a menor (menos significativa). **Big endian**: O primeiro bit é a maior (mais significativa).

Para editar um formato de cartão:

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

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

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

Para redefinir um formato de cartão predefinido:

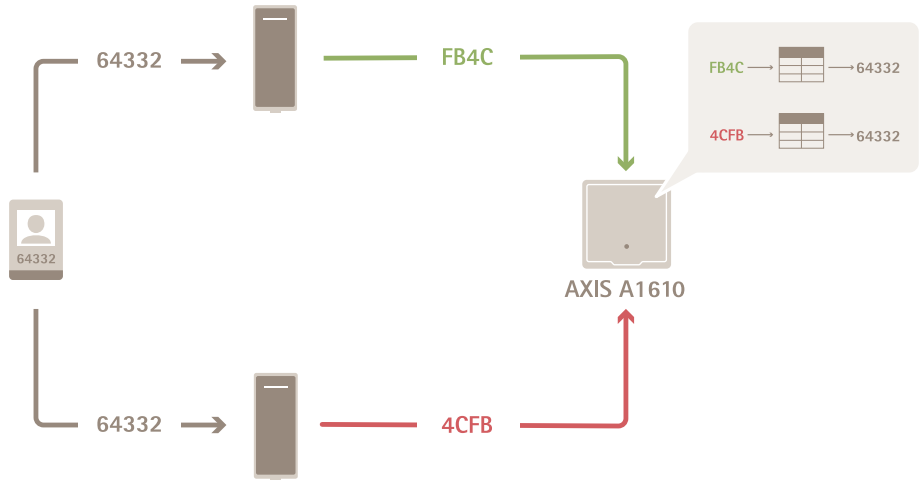
1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN (Navegação no site > AXIS Optimizer > Controle de acesso > Formatos de cartão e PIN)**.
2. Clique em para redefinir um formato de cartão para o mapa de campos padrão.

Para configurar o tamanho do PIN:

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

Configurações de formato de cartão

Visão geral



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

Inverter ordem de bits

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



Inverter ordem de bytes

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



Formato de cartão Wiegand padrão de 26 bits



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

4 Paridade final

Perfis de identificação

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

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

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

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

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

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

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

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

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

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

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

Para criar um perfil de identificação:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles (Navegação no site > AXIS Optimizer > Controle de acesso > Perfis de identificação)**.
2. Clique em **Create identification profile (Criar perfil de identificação)**.
3. Digite um nome para o perfil de identificação.
4. Selecione **Include facility code for card validation (Incluir código da instalação para validação do cartão)** para usar o código da instalação como um dos campos de validação da credencial. Este campo estará disponível somente se você tiver ativado **Facility code (Código da instalação)** em **Access management > Settings (Gerenciamento de acesso > Configurações)**.
5. Configure o perfil de identificação para um lado da porta.
6. No outro lado da porta, repita as etapas anteriores.
7. Clique em **OK**.

Para editar um perfil de identificação:

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

Para remover um perfil de identificação:

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

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

Comunicação criptografada

OSDP Secure Channel

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

Para ativar o OSDP Secure Channel para todo um sistema:

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Encrypted communication (Navegação no site > AXIS Optimizer > Controle de acesso > Comunicação criptografada)**.
2. Insira sua chave de criptografia principal e clique em **OK**.
3. Ative o **OSDP Secure Channel**. Essa opção está disponível somente após você inserir a chave de criptografia principal.
4. Por padrão, a chave de criptografia principal gera uma chave do OSDP Secure Channel. Para definir manualmente a chave do OSDP Secure Channel:
   4.1. Em **OSDP Secure Channel**, clique em .
   4.2. Desmarque a opção **Use main encryption key to generate OSDP Secure Channel key (Usar a chave de criptografia principal para gerar a chave OSDP Secure Channel)**.
   4.3. Insira a chave do OSDP Secure Channel e clique em **OK**.

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

Multisservidor BETA

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

Observação

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

Fluxo de trabalho

1. Configure um servidor como um subservidor e gere o arquivo de configuração. Consulte *Gerar o arquivo de configuração do subservidor, on page 90*.
2. Configure um servidor como um servidor principal e importe o arquivo de configuração dos subservidores. Consulte *Importar o arquivo de configuração para o servidor principal, on page 90*.
3. Configure os portadores e grupos de portadores de cartões globais no servidor principal. Consulte *Adicionar um portador de cartão, on page 91* e *Adicionar um grupo, on page 94*.
4. Exiba e monitore portadores e grupos de portadores globais do subservidor. Consulte *Gerenciamento de acesso, on page 91*.

Gerar o arquivo de configuração do subservidor

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

Importar o arquivo de configuração para o servidor principal

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

Revogar um subservidor

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

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

Remover um subservidor

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

Para remover um subservidor:

1. No servidor principal:
   1.1. Vá para **Access management** > **Dashboard (Gerenciamento de acesso > Painel)**.

1.2. Altere os titulares e grupos de cartões globais para portadores de cartões locais e grupos.

1.3. Vá para **AXIS Optimizer** > **Access control** > **Multi server (AXIS Optimizer > Controle de acesso > Multisservidor)**.

1.4. Clique em **Main server (Servidor principal)** para mostrar a lista de subservidores.

1.5. Selecione o subservidor e clique em **Delete (Excluir)**.

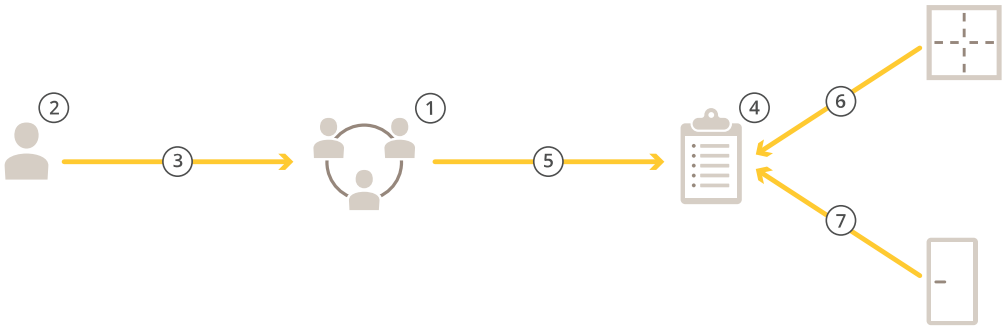
2. No subservidor:
   - Vá para **AXIS Optimizer** > **Access control** > **Multi server (AXIS Optimizer > Controle de acesso > Multisservidor)**.
   - Clique em **Sub server (Subservidor)**e **Revoke server (Revogar servidor)**.

Gerenciamento de acesso

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

Fluxo de trabalho do gerenciamento de acesso

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



1. Adicione grupos. Consulte *Adicionar um grupo, on page 94*.
2. Adicione portadores de cartões. Consulte *Adicionar um portador de cartão, on page 91*.
3. Adicione portadores de cartões a grupos.
4. Adicione regras de acesso. Consulte *Adicione uma regra de acesso, on page 95*.
5. Aplique grupos a regras de acesso.
6. Aplique zonas a regras de acesso.
7. Aplique portas a regras de acesso.

Adicionar um portador de cartão

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

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management (Navegação no site > AXIS Optimizer > Controle de acesso > Gerenciamento de portadores de cartões)**.
2. Vá para **Cardholders (Portadores de cartões)** e clique em **+ Add (+ Adicionar)**.
3. Insira o nome e o sobrenome do portador do cartão e clique em **Next (Avançar)**.
4. Opcionalmente, clique em **Advanced (Avançado)** e selecione as opções desejadas.
5. Adicione uma credencial ao portador do cartão. Consulte *Adicionar credenciais, on page 92*

6. Clique em **Save (Salvar)**.
7. Adicionar o portador do cartão a um grupo.
   7.1. Em **Groups (Grupos)**, selecione o grupo ao qual deseja adicionar o portador do cartão e clique em **Edit (Editar)**.
   7.2. Clique em **+ Add (+ Adicionar)** e selecione o portador do cartão que deseja adicionar ao grupo. Você pode selecionar vários portadores de cartões.
   7.3. Clique em **Adicionar**.
   7.4. Clique em **Save (Salvar)**.

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

Adicionar credenciais

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

- PIN
- Cartão
- Placa de licença
- Telefone celular

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

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

Veja um exemplo em *Usar o número de placa de licença como credencial, on page 93*.

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

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

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

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

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

Observação

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

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

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

Válido até	
Sem data de término	A credencial nunca expira.
Data	Defina uma data e hora em que a credencial expira.
Desde o primeiro uso	Selecione em quanto tempo a credencial expira após o primeiro uso. Selecione os dias, os meses, os anos ou o número de vezes após o primeiro uso.
Desde o último uso	Selecione em quanto tempo a credencial expira após o último uso. Selecione dias, meses ou anos após o último uso.

Usar o número de placa de licença como credencial

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

1. Adicione o controlador de porta e a câmera ao AXIS Optimizer.
2. Defina a data e a hora para os novos dispositivos com a opção **Synchronize with server computer time (Sincronizar com a data/hora do computador servidor)**.
3. Atualize o software nos novos dispositivos para a versão mais recente disponível.
4. Adicione uma nova porta conectada ao seu controlador de porta. Consulte *Adicione uma porta, on page 74*.
   4.1. Adicione um leitor em **Side A (Lado A)**. Consulte *Adicionar um leitor, on page 80*.
   4.2. Em **Door settings (Configurações da porta)**, selecione **AXIS License Plate Verifier** como **Reader type (Tipo de leitor)** e insira um nome para o leitor.
   4.3. Opcionalmente, adicione um dispositivo leitor ou REX em **Side B (Lado B)**.
   4.4. Clique em **OK**.
5. Instale e ative o AXIS License Plate Verifier em sua câmera. Consulte o *Manual do usuário do AXIS License Plate Verifier*.
6. Inicie o AXIS License Plate Verifier.
7. Configure o AXIS License Plate Verifier.
   7.1. Vá para **Configuration > Access control > Encrypted communication (Configuração > Controle de acesso > Comunicação criptografada)**.
   7.2. Em **External Peripheral Authentication Key (Chave de autenticação de periférico externo)**, clique em **Show authentication key (Mostrar chave de autenticação)** e em **Copy key (Copiar chave)**.
   7.3. Abra o AXIS License Plate Verifier na interface Web da câmera.
   7.4. Não faça a configuração.
   7.5. Vá para **Settings (Configurações)**.
   7.6. Em **Access control (Controle de acesso)**, selecione **Secure Entry** como **Type (Tipo)**.
   7.7. Em **IP address (Endereço IP)**, insira o endereço do controlador de porta.
   7.8. Em **Authentication key (Chave de autenticação)**, cole a chave de autenticação que você copiou antes.
   7.9. Clique em **Conectar**.
   7.10. Em **Door controller name (Nome do controlador de porta)**, selecione seu controlador de porta.
   7.11. Em **Reader name (Nome do leitor)**, selecione o leitor que você adicionou anteriormente.
   7.12. Ative a integração.
8. Adicione o portador de cartão ao qual você deseja conceder acesso. Consulte *Adicionar um portador de cartão, on page 91*.
9. Adicione as credenciais da placa de licença ao novo titular do cartão. Consulte *Adicionar credenciais, on page 92*.
10. Adicione uma regra de acesso. Consulte *Adicione uma regra de acesso, on page 95*.
    10.1. Adicionar um cronograma.
    10.2. Adicione o portador de cartão ao qual você deseja conceder acesso à placa de licença.
    10.3. Adicione a porta com o leitor do AXIS License Plate Verifier.

Adicionar um grupo

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

1. Vá para **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management (Navegação no site > AXIS Optimizer > Controle de acesso > Gerenciamento de portadores de cartões)**.
2. Vá para **Groups (Grupos)** e clique em **+ Add (+ Adicionar)**.

3. Insira um nome e, opcionalmente, as iniciais do grupo.
4. Selecione **Global group (Grupo global)** para permitir a visualização e o monitoramento do titular do cartão nos subservidores. Essa opção está disponível somente para portadores de cartões criados no servidor principal. Consulte *Multisservidor BETA, on page 89*.
5. Adicione portadores de cartões ao grupo:
   5.1. Clique em **+ Adicionar**.
   5.2. Selecione os portadores de cartões que deseja adicionar e clique em **Add (Adicionar)**.
6. Clique em **Save (Salvar)**.

Adicione uma regra de acesso

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

Uma regra de acesso consiste em:

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

Portas e zonas – onde o acesso se aplica.

Programações – quando conceder acesso.

Para adicionar uma regra de acesso:

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

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

Destravar portas e zonas manualmente

Para obter informações sobre ações manuais, como destravar manualmente uma porta, consulte *Ações manuais, on page 84*.

Para obter informações sobre ações manuais, como destravar manualmente uma zona, consulte *Ações manuais, on page 84*.

Exportar relatórios de configuração do sistema

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

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

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

Criar relatórios de atividade de portadores de cartões

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

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

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

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

1. Vá para **Reports** > **Cardholder activity (Relatórios > Atividade do portador do cartão)**.
2. Clique em **+ Add (+ Adicionar)** e selecione **Roll call / Mustering (Lista de presença/conferência)**.
3. Insira um nome para o relatório.
4. Selecione quais zonas incluir no relatório.
5. Selecione os grupos que deseja incluir no relatório.
6. Se desejar um relatório de conferência, selecione **Mustering point (Ponto de conferência)** e um leitor para o ponto de conferência.
7. Selecione um período de tempo para o relatório.
8. Clique em **Save (Salvar)**.

9. Selecione o relatório e clique em **Run (Executar)**.

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

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

Configurações de gerenciamento de acesso

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

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

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

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

Observação

Você também deve selecionar **Include facility code for card validation (Incluir código da instalação para validação de cartões** ao configurar perfis de identificação. Consulte .

Importação e exportação

Importar portadores de cartões

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

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

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

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

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

Exportar portadores de cartões

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

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

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

Desfazer importação

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

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

Fazer backup e restaurar

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

1. Mova o arquivo de backup para C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry \restore.
2. Reinicie o AXIS Secure Entry usando um destes métodos:
   - Inicie o programa MSC (Serviços), localize o "AXIS Optimizer Secure Entry Service" e reinicie.
   - Reinicie o computador.
3. Execute novamente a instalação do AXIS Optimizer na máquina do servidor de eventos.

Gerenciamento de acesso no Smart Client

Por meio do Smart Client, os operadores podem realizar operações relacionadas ao seu sistema de controle de acesso. A maioria das funções do controle de acesso, como o controle manual de portas, está disponível no Smart Client. Para obter mais informações sobre esses recursos, consulte *Utilização do controle de acesso no Smart Client*.

Você também pode realizar o gerenciamento do acesso diretamente no Smart Client. Os recursos a seguir, presentes no Management Client, também estão disponíveis no Smart Client:

- Gerenciamento de portadores de cartões
- Configurações gerais
- Campos personalizados do portador do cartão
- Código da instalação
- Modelos de email
- Modelos de crachás BETA

Para exibir a guia Axis access management (Gerenciamento de acesso da Axis) no Smart Client:

1. Instale o AXIS Optimizer na máquina do Smart Client.
2. Ative a licença para uma porta, caso nenhuma tenha sido ativada. Para ativar a licença de uma porta, consulte *Ativar licenças de porta, on page 72*.
3. Certifique-se de que o usuário que está entrando tem as permissões de gerenciamento de acesso, consulte *Configurações de funções no AXIS Secure Entry, on page 99*.

Configurações de funções no AXIS Secure Entry

1. No Management Client, vá para **Site Navigation (Navegação no site)** > **Security (Segurança)** > **Roles (Funções)**.
2. Selecione uma função específica no sistema.
3. Selecione **AXIS Optimizer**.

4. Expanda a lista e clique em **Access control (Controle de acesso)**.
5. Selecione **Read (Ler)** para as configurações de Controle de acesso.
6. Clique no recurso para o qual a função deve ter permissão e selecione **Grant (Conceder)**.
   - **Access control configuration (Configuração de controle de acesso):** Isso concede à função de operador a permissão para todas as funções na guia Configuration (Configuração).
   - **Access management (Gerenciamento de acesso):** Isso concede à função de operador a permissão para todas as funções na guia Access Management (Gerenciamento de acesso).

Gerenciamento do sistema e controles de segurança

Personalizar acesso a recursos para operadores

Configurações da função

Por padrão, um operador terá acesso a todos os recursos do AXIS Optimizer no Smart Client se ele também tiver acesso ao dispositivo no VMS. No entanto, no Management Client, é possível configurar a quais recursos um operador tem acesso via Role settings (Configurações de função).

Configurar opções de funções

Ative as **Role settings (Configurações de funções)**:

1. No Management Client, vá para **Site Navigation > Security > AXIS Optimizer Security (Navegação no site > Segurança > Segurança do AXIS Optimizer)**.

Observação

Não é possível desativar as configurações de função após ativá-las. A configuração é permanente.

2. Selecione **Turn on role settings (Ativar configurações de função)**.
3. Reinicie o Management Client.

Configure as **Role settings (Configurações de funções)**:

1. No Management Client, vá para **Site Navigation > Security > Roles (Navegação no site > Segurança > Funções)**.
2. Selecione uma função e vá para a **Overall security (Segurança geral)**.
3. Clique em **AXIS Optimizer Security**.
4. Selecione a quais recursos a função deve ter acesso ou não.
   - **Controle total**Concede à função de operador acesso total a todos os recursos do AXIS Optimizer.
   - **Edit (not applicable) (Editar (não aplicável))**Uma função do VMS que não é aplicável às configurações de função do AXIS Optimizer.
   - **Acessar o AXIS Optimizer no Management Client.**A função de operador pode usar todos os recursos de administração do AXIS Optimizer no Management Client.
   - **Gerenciar a segurança do AXIS Optimizer.**A função de operador pode alterar as configurações em **Site Navigation > Security >AXIS Optimizer Security**.
   - **Controles dinâmicos de câmera do operador.**A função de operador tem acesso a todas as funções pré-instaladas que o sistema encontra em um dispositivo.
   - **Controle de foco remoto do operador.**A função de operador pode definir o foco remoto em câmeras dome fixas.
   - **Controles PTZ do operador**A função de operador recebe acesso a controles de PTZ de operador específicos: controle de foco, predefinições de PTZ, controles do operador para Autotracking 2, lavador e botão de secagem rápida/limpador.
   - **Controle de medição de temperatura pontual.**A função de operador pode medir a temperatura pontual na AXIS Q2901-E.
   - **Controle de alto-falante do operador.**A função de operador tem acesso a todos os recursos do gerenciador de alto-falantes no Smart Client.
   - **Acessar o gerenciamento de visitantes**A função de operador recebe acesso a tudo relacionado ao gerenciamento de visitantes, por exemplo, atender a uma chamada e abrir uma porta na visualização ao vivo.
   - **Acessar o histórico de chamadas.**A função de operador pode acessar o histórico de chamadas de um intercomunicador. Você deve permitir que o **Access visitor management (Gerenciamento de acesso de visitantes)** use essa configuração.

- **Funções de pesquisa estendidas.**Se você selecionar **Deny**, a guia do AXIS License Plate Verifier será ocultada no Smart Client. Além disso, você não pode usar a pesquisa de veículos e contêineres na pesquisa centralizada.
- **Controlar a exibição de correção de distorção**A função de operador pode navegar pelas exibições de correção de distorção.
- **Editar a posição inicial de uma exibição de correção de distorção**A função de operador pode editar a posição inicial de uma câmera.
- **Página web**A função de operador pode criar uma exibição usando um navegador da Web.
- **Painel de percepções de dados Axis**
  A função de operador tem acesso ao painel de percepções de dados Axis.

5. Clique em **Save (Salvar)**.
6. Reinicie todos os Smart Clients em execução em seu sistema.

Gerenciamento de dispositivos

AXIS Device Manager Extend

No AXIS Optimizer, é possível usar o AXIS Device Manager Extend para gerenciar dispositivos de vários sites. Ao configurar hosts de borda em servidores de gravação, o AXIS Device Manager Extend pode se conectar aos seus dispositivos no sistema VMS. Isso facilita a revisão de informações de garantia e a realização de atualizações de software em vários dispositivos e sites por meio de uma única interface de usuário.

Para obter mais informações sobre o AXIS Device Manager Extend, consulte o *manual do usuário*.

Observação

Requisitos

- Faça login na sua *conta MyAxis*.
- Os servidores de gravação devem ter acesso à Internet.
- Compatível somente com dispositivos com AXIS OS 6.50 em execução. Para saber quais dispositivos são compatíveis, consulte as *Perguntas frequentes*.

Instalar o host de borda

O host de borda é um serviço de gerenciamento local que permite ao AXIS Device Manager Extend se comunicar com seus dispositivos locais no sistema VMS.

O host de borda e o cliente de área de trabalho precisam ser instalados para usar AXIS Device Manager Extend no VMS. O host de borda e o cliente de área de trabalho estão incluídos no instalador do AXIS Device Manager Extend.

1. Baixe o *instalador* do AXIS Device Manager Extend.
   O host de borda deve ser instalado nos servidores de gravação do VMS.
2. Execute o instalador no servidor de gravação e selecione somente para instalar o host de borda.

Consulte o *Manual do Usuário do AXIS Device Manager Extend* para obter mais informações sobre portas de rede abertas e outros requisitos.

Reivindique o host de borda e sincronize os dispositivos



1. Abra o Management Client.
2. Vá para **Site Navigation > AXIS Optimizer > System overview (Navegação no site > AXIS Optimizer > Visão geral do sistema)**.
3. Selecione e faça login no MyAxis.
4. Clique em um bloco de servidor de gravação com um host de borda instalado pronto para ser reivindicado.
5. Na barra lateral, crie uma nova organização ou selecione uma organização criada anteriormente.
6. Clique e reivindique o host de borda.
7. Aguarde até que a página seja recarregada e, em seguida, clique em **Synchronize (Sincronizar)**. Agora, todos os dispositivos Axis no servidor de gravação serão adicionados ao host de borda e pertencerão à organização selecionada

Observação

O AXIS Device Manager Extend deve ser capaz de acessar o hardware Axis no VMS. Para obter mais informações sobre dispositivos compatíveis, consulte *Solução de problemas para adicionar dispositivos ao host de borda, on page 104*.

8. Se você adicionar novos dispositivos a um servidor de gravação ou alterar as informações de algum dispositivo, será necessário executar a etapa 7 novamente para sincronizar as alterações com o sistema AXIS Device Manager Extend.
9. Repita as etapas 4-7 para todos os servidores de gravação com dispositivos que deseja adicionar ao AXIS Device Manager Extend.

Status do host de borda

Em cada servidor de gravação em **System overview (Visão geral do sistema)**, você pode ver se o host de borda foi instalado ou reivindicado. Você pode ativar **Show machines that need edge host action (Mostrar máquinas que necessitam de ação do host de borda)** para filtrar a exibição.

- – Nenhum host de borda foi detectado no servidor de gravação.
  - Se nenhum host de borda tiver sido instalado, baixe e instale o host de borda no servidor de gravação. Consulte *Instalar o host de borda, on page 102*.
  - Se o host de borda estiver instalado, isso significa que você precisará fazer login na conta MyAxis para detectá-lo.
- – O host de borda está instalado, mas não foi reivindicado. Reivindique o host de borda criando uma nova organização ou selecione uma organização criada anteriormente. Consulte *Reivindique o host de borda e sincronize os dispositivos, on page 102*.
- – O host de borda está instalado e foi reivindicado, mas está inacessível. Verifique se o servidor de gravação tem acesso à Internet.
- – O host de borda está sincronizado.
- – O host de borda precisa de sincronização. É possível que haja novos dispositivos no VMS que podem ser adicionados ao host de borda ou informações de dispositivos atualizadas que precisam ser sincronizadas.

Usar o AXIS Device Manager Extend para configurar dispositivos

Após os dispositivos terem sido sincronizados com host de borda, é possível configurar os dispositivos no AXIS Device Manager Extend. Você pode fazer isso em qualquer PC conectado à internet.

Observação

Se você também quiser gerenciar dispositivos por meio de uma conexão remota, será necessário ativar o *acesso remoto em cada host de borda*.

1. Instale e abra o *aplicativo de área de trabalho AXIS Device Manager Extend*.
2. Selecione a organização que foi usada para reivindicar o host de borda.
3. Os dispositivos sincronizados podem ser encontrados em um site com o mesmo nome do servidor de gravação do VMS.

Solução de problemas para adicionar dispositivos ao host de borda

Em caso de problemas ao adicionar dispositivos ao host de borda, certifique-se de fazer o seguinte:

- O AXIS Optimizer adicionará somente hardware ativado ao VMS.
- Certifique-se de que a conexão com o hardware não esteja quebrada no VMS.
- Certifique-se de que o dispositivo tenha o AXIS OS 6.50 ou superior.
- Certifique-se de que o dispositivo esteja configurado para autenticação digest. Por padrão, o AXIS Device Management não oferece suporte à autenticação básica.
- Experimente adicionar dispositivos diretamente no aplicativo AXIS Device Manager Extend.
- Reúna logs de AXIS Device Manager Extend e entre em contato com o suporte da AXIS.
  1. No aplicativo AXIS Device Manager Extend, acesse o site específico no servidor de gravação em que a câmera está instalada.
  2. Vá para **Settings (Configurações)** e clique em **Download sitelog (Baixar sitelog)**.

Importação do AXIS Site Designer

No AXIS Optimizer, você pode importar seu projeto de design do AXIS Site Designer e aplicar a configuração ao VMS em um processo de importação fácil. Use o *AXIS Site Designer* para projetar e configurar seu sistema. Após o término do projeto, você pode importar configurações para todas as câmeras e outros dispositivos do AXIS Site Designer para o Management Client usando o AXIS Optimizer.

Para obter mais informações sobre o AXIS Site Designer, consulte o *manual do usuário*.

Observação

Requisitos

- VMS versão 2020 R2 ou posterior

Importar projeto de desenho



No AXIS Site Designer

1. Crie um projeto e configure os dispositivos.
2. Após terminar seu projeto, gere um código ou baixe o arquivo de configurações.

Observação

Se você fizer alguma atualização do seu projeto de design, será necessário gerar um novo código ou baixar um novo arquivo de configurações.

No Management Client

1. Certifique-se de que os dispositivos relevantes sejam adicionados ao VMS.
2. Vá para **Site Navigation > AXIS Optimizer > Import design project (Navegação no site > AXIS Optimizer > Importar projeto de design)**.
3. Um guia passo a passo é aberto. Selecione o projeto que deseja importar inserindo o código de acesso ou selecionando o arquivo de configurações do projeto. Clique em **Next** (Próximo).
4. Em **Project overview (Visão geral do projeto)**, é possível ver informações sobre quantos dispositivos são encontrados no projeto do AXIS Site Designer e quantos dispositivos estão no VMS. Clique em **Next** (Próximo).
5. Na próxima etapa, os dispositivos no VMS são combinados a dispositivos no projeto de design do AXIS Site Designer. Dispositivos com apenas uma correspondência possível são selecionados automaticamente. Somente os dispositivos com correspondências serão importados. Ao concluir a correspondência, clique em **Next (Avançar)**.
6. As configurações para todos os dispositivos combinados são importadas e aplicadas ao seu VMS. Isso pode levar vários minutos dependendo do tamanho do projeto. Clique em **Next** (Próximo).
7. Em **Results of import (Resultados de importação)**, você pode encontrar detalhes sobre as diferentes etapas do processo de importação. Se algumas configurações não puderam ser importadas, corrija os problemas e execute a importação novamente. Clique em **Export... (Exportar...)** se desejar salvar a lista de resultados como um arquivo. Clique **Done (Pronto)** para fechar o guia passo a passo.

Configurações importadas

Somente dispositivos compatíveis entre o VMS e o projeto de design fazem parte da importação. As seguintes configurações são importadas e aplicadas ao VMS para todos os tipos de dispositivos:

- Nome do dispositivo usado no projeto de design
- Descrição do dispositivo usado no projeto de design
- Configurações de geolocalização, se o dispositivo for colocado em um mapa

Se o dispositivo for um dispositivo com vídeo, as seguintes configurações também serão aplicadas:

- Um ou dois streams de vídeo configurados no VMS (opções de resolução, taxa de quadros, codec, compactação e Zipstream)
  - O fluxo de vídeo 1 está configurado para visualização e gravação ao vivo.
  - O fluxo de vídeo 2 está configurado para gravação se as configurações de fluxo no projeto de design diferirem entre a visualização ao vivo e a gravação.
- As regras para detecção de movimento ou gravação contínua são configuradas de acordo com o projeto de design. A detecção de movimento integrada do VMS é usada, perfis de hora para as regras são criados e perfis de armazenamento para diferentes tempos de retenção são criados nos servidores de gravação.
- O microfone é ativado ou desativado de acordo com as configurações de áudio do projeto de design.

Limitações

Há limitações no VMS no que diz respeito à importação de projetos de design do AXIS Site Designer.

- A regra de gravação de movimento padrão no VMS pode substituir as regras de gravação criadas pela importação. Desative quaisquer regras conflitantes ou exclua os dispositivos afetados das regras.
- As estimativas de gravação podem ser imprecisas para as gravações acionadas por movimento do VMS.
- Não há suporte a plantas na versão atual.
- Se tanto gravações acionadas por movimento quanto gravações contínuas forem configuradas simultaneamente no projeto de design, somente configurações de stream das configurações de gravação acionadas por movimento serão usadas.
- Não é possível configurar a taxa de quadros mínima para Zipstream no VMS.

Gerenciamento de contas

O gerenciamento de contas ajuda a gerenciar contas e senhas em todos os dispositivos Axis usados pelo XProtect.

De acordo com as diretrizes da Axis, você não deve usar uma conta root para se conectar a dispositivos. Com o gerenciamento de contas, você pode criar uma conta de serviço XProtect. Senhas exclusivas de 16 caracteres são criadas para cada dispositivo. Dispositivos que já possuem a conta XProtect ganham novas senhas.

Conecte-se a dispositivos com conta de serviço XProtect

1. Vá para **Site Navigation > AXIS Optimizer > Account management (Navegação no site > AXIS Optimizer > Gerenciamento de contas)**.
   O gráfico mostra quantos dispositivos estão online, quantos deles possuem a conta do serviço XProtect e quantos não possuem a conta do serviço XProtect.
2. Clique **Show device details (Mostrar detalhes do dispositivo)** para ver mais informações sobre os dispositivos. Os dispositivos que estão online são mostrados no topo da lista. Você pode selecionar dispositivos específicos para os quais gerar senhas. Se nenhum for selecionado, todos os dispositivos on--line receberão novas senhas. Clique em **OK**.

Observação

As senhas serão enviadas em texto simples entre o servidor de gravação e o dispositivo Axis se você selecionar HTTP na configuração do hardware. Recomendamos que você configure o HTTPS para proteger a comunicação entre o VMS e seu dispositivo.

3. Clique **Generate passwords (Gerar senhas)**. A senha gerada inclui um texto aleatório de 16 caracteres ASCII que variam de 32 a 126.
   Clique em **Show device details (Mostrar detalhes do dispositivo)** para ver atualizações de status ao vivo do processo. Durante o processo, você verá uma breve interrupção nas visualizações ao vivo ativas e nas gravações pendentes.
4. Os dispositivos que estiverem on-line obterão a conta do serviço XProtect e novas senhas; Dispositivos que estão online e já possuem a conta do serviço XProtect recebem apenas novas senhas.

Eventos da Axis

O recurso de eventos da Axis fornece uma visão geral dos eventos disponíveis para dispositivos Axis em seu VMS. Você pode testar eventos em um dispositivo específico, exibir detalhes sobre os eventos e adicionar eventos a vários dispositivos.

Em **Site Navigation (Navegação no site)**, acesse **Rules and Events > Axis actions (Regras e eventos > Ações da Axis)**. Uma lista de todos os eventos disponíveis é mostrada na janela **Configuração**. Você pode ver quais eventos estão ativos em seu sistema e quais eventos não estão ativos.

Para cada evento, é possível ver o nome do dispositivo dos dispositivos aos qual o evento foi adicionado. Você também pode ver o nome de exibição do evento, o estado do evento e a última vez que o evento foi acionado.

Observação

Requisitos

- VMS versão 2023 R2 ou posterior.

Configurar um evento para vários dispositivos

1. Vá para **Configuração** e selecione um evento.
2. Clique em **Add devices (Adicionar dispositivos)**.
3. A janela **Adicionar dispositivos** mostra uma lista de dispositivos aos quais o evento pode ser adicionado. Selecione um ou mais dispositivos e clique em **Adicionar dispositivos**.

Para remover um evento de um dispositivo, clique em **Remover**.

Informações sobre eventos

Em eventos da Axis, você pode exibir a última ocorrência conhecida, o estado dos eventos e as atualizações em tempo real na interface do usuário. Para fazer isso, você precisa definir o tempo de retenção no Cliente de gerenciamento.

1. Vá para **Tools > Options > Alarm and Events > Event retention (Ferramentas > Opções > Alarme e eventos > Retenção de eventos)**.
2. Defina o tempo de retenção para todo o grupo de eventos do dispositivo ou eventos específicos dentro do grupo.

Metadados e pesquisas

Metadados e pesquisas oferecem uma visão geral de todos os dispositivos adicionados ao VMS, recursos de metadados e categorias de pesquisa Axis visíveis para seus operadores.

Metadados e pesquisas permitem que você ative recursos específicos para esses dispositivos, ou seja, você pode ativar dados de eventos, dados de análise e dados consolidados para vários dispositivos, além de exibir os recursos de analíticos compatíveis com seus dispositivos. Com as categorias de pesquisa Axis, você pode controlar as opções de todos os operadores para refletir os recursos de análise disponíveis no VMS. O suporte a categorias de pesquisa e filtros varia de acordo com os modelos de câmeras e os aplicativos de análise instalados.

Configurar as opções de metadados

1. Vá para **Management Client** > **Site Navigation** > **AXIS Optimizer** > **Metadata and search** (Management Client > Navegação no site > AXIS Optimizer > Metadados e pesquisas).
   - **Dados de eventos**: Ative para que seu VMS recupere dados de eventos do dispositivo. Você precisa disso para vários recursos do AXIS Optimizer.
   - **Analytics data** (Dados de analíticos): Ative-o para usar o recurso de pesquisa forense e mostre caixas delimitadoras na visualização ao vivo e na reprodução.
   - **Analytics features (Recursos de analíticos)**: Exponha os recursos de análise de vídeo que seu dispositivo suporta atualmente, como tipo de objeto (humanos, carros) e cor de objetos. Atualizar o software de dispositivo pode fornecer mais recursos de análise.
   - **Consolidated metadata (Metadados consolidados)**: Ative para agilizar a pesquisa forense e reduzir o tempo de carregamento das percepções da Axis.

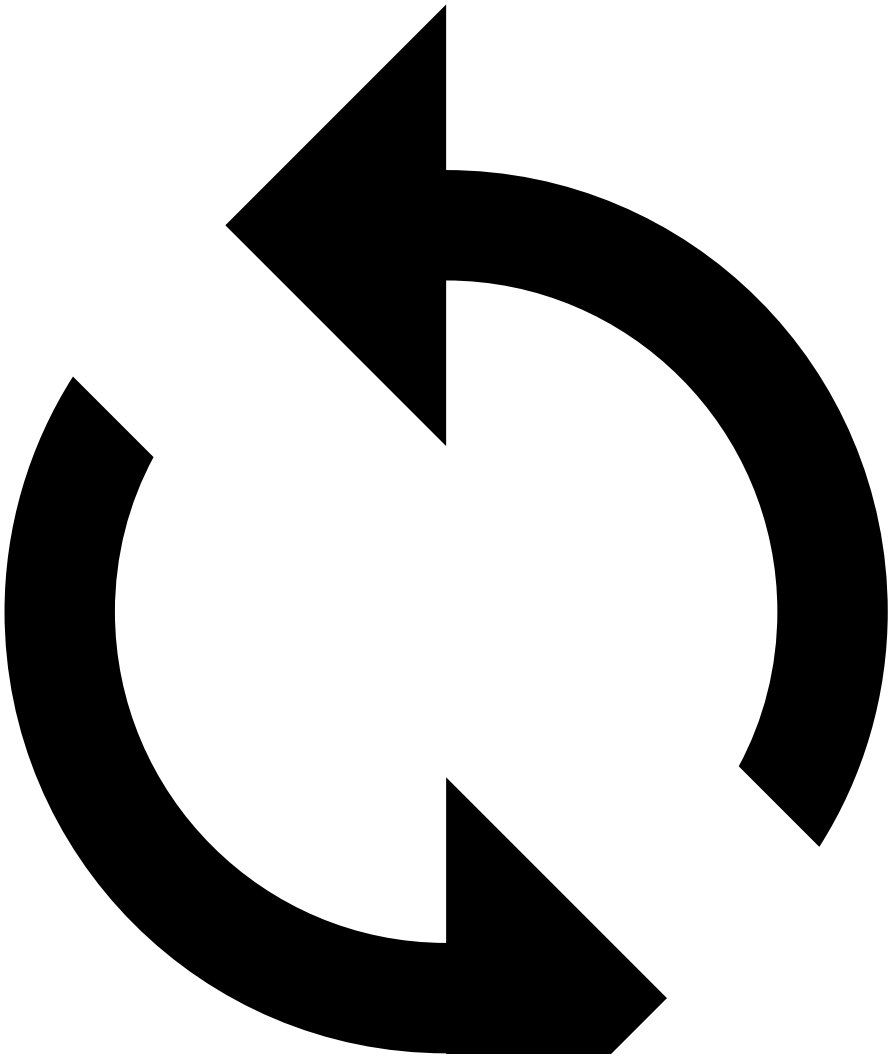
Observação

Requisitos de metadados consolidados

- Dispositivos Axis com AXIS OS 11.10 ou versões posteriores.

Limitações de metadados consolidados

- Caixas delimitadoras na visualização ao vivo e na gravação, e as opções de pesquisa integradas ao VMS não estão disponíveis.

– 
: Clique para recarregar quando fizer alterações na configuração do dispositivo.

Configurar categorias de pesquisa da Axis

1. Vá para **Management Client** > **Site Navigation** > **AXIS Optimizer** > **Metadata and search** (Management Client > Navegação no site > AXIS Optimizer > Metadados e pesquisas).
2. Ative as categorias de pesquisa que deseja usar na caixa de diálogo **Axis search categories (Categorias de pesquisa Axis)**:
   - Pesquisa forense
   - Pesquisa de veículos
   - Pesquisa de velocidade na zona
   - Pesquisa de contêineres
3. Selecione os filtros aplicáveis em cada categoria de pesquisa.

Observação

Requisitos das categorias de pesquisa Axis

- AXIS Optimizer versão 5.3 ou posterior no Smart Client.

Cibersegurança

A segurança cibernética oferece suporte a um ciclo de vida de produto bem-sucedido com riscos minimizados. Você pode encontrar informações detalhadas e documentação sobre nossa abordagem à segurança cibernética em *axis.com/about-axis/cybersecurity*. Siga as diretrizes de segurança cibernética abaixo para receber notificações de segurança da Axis sobre o produto e para realizar a configuração do produto, de modo a garantir um ciclo de vida e um descomissionamento seguros.

No *Axis Trust Center*, você pode encontrar informações sobre como a Axis implementa a conformidade de segurança, a transparência, a proteção de dados e a privacidade.

Gerenciamento de vulnerabilidades

A Axis é uma *Autoridade de numeração de vulnerabilidades e exposições comuns (CVE) (CNA)*. Para minimizar seu risco de exposição, seguimos os padrões do setor ao identificar e resolver vulnerabilidades em nossos dispositivos, software e serviços. Consulte *axis.com/vulnerability-management* para obter informações sobre nossa política de gerenciamento de vulnerabilidades ou para relatar uma vulnerabilidade.

Notificações de segurança

Inscreva-se para receber emails de notificação de segurança da Axis em *axis.com/security-notification-service*. Enviaremos a você informações sobre vulnerabilidades, alertas de segurança correspondentes e outros assuntos relacionados à segurança do seu produto Axis.

Ciclo de vida seguro do produto

A Axis minimiza os riscos durante toda a vida útil de nossos produtos por meio do gerenciamento seguro do ciclo de vida. Use nossos guias para aumento do nível de proteção em *help.axis.com* para configurar e operar com mais segurança seus produtos Axis e para encontrar informações sobre:

Uso seguro desde o primeiro uso – Os produtos Axis são pré-configurados com alta proteção padrão para permitir a inicialização segura e a comunicação criptografada desde o início.

Uso pretendido e erros comuns de configuração – Nossos guias fornecem informações sobre o uso pretendido dos produtos Axis, incluindo erros comuns de configuração e usos indevidos relevantes para a segurança que devem ser evitados.

Gerenciamento de vulnerabilidades e transparência da cadeia de suprimentos – Uma lista de materiais de software (SBOM) é publicada com cada versão de software em *axis.com* para divulgar vulnerabilidades e aumentar a transparência da cadeia de suprimentos.

Descomissionamento e exclusão segura de dados – Para desativar um produto com segurança quando ele chegar ao fim de seu ciclo de vida, redefina-o para as configurações padrão de fábrica. Isso apaga suas configurações, dados armazenados e informações confidenciais.

Guia para aumento do nível de proteção

Como parte integrante da sua infraestrutura VMS, o AXIS Optimizer requer configurações específicas para manter um ambiente seguro. Seguir essas configurações recomendadas é essencial para proteger as senhas dos dispositivos, proteger informações privadas e impedir o acesso não autorizado ao seu sistema.

- Use HTTPS ao adicionar dispositivos Axis ao VMS.
- Ative a criptografia entre os clientes e os servidores do VMS.
- Ative o armazenamento de dados criptografados no VMS.
- Analise todas as funções do VMS e certifique-se de que elas não estejam utilizando mais permissões do que o necessário.

Precisa de mais ajuda?

Perguntas Frequentes

Pergunta	Resposta
Como posso atualizar o AXIS Optimizer quando o PC cliente não tem acesso à Internet?	Publique a nova versão no servidor de gerenciamento de VMS, consulte *Atualizar o sistema automaticamente, on page 10*.
Preciso fazer backup das configurações antes de atualizar para uma versão mais nova doo AXIS Optimizer?	Não é necessário fazer backup. Nada mudará quando você atualizar para uma versão mais nova.
Se eu tiver mais de 30 PCs clientes com o AXIS Optimizer, precisarei atualizá-los um por um?	Você pode atualizar os clientes individualmente. Você também pode enviar a atualização automaticamente publicando uma versão do AXIS Optimizer local para o seu sistema. Consulte *Atualizar o sistema automaticamente, on page 10*.
Posso ativar ou desativar cada plug-in no AXIS Optimizer separadamente?	Não, mas eles não consomem nenhum recurso quando não são usados ativamente.
Que portas são usadas pelo AXIS Optimizer?	As portas 80 e 443 são necessárias para se comunicar com a axis.com, portanto seu sistema pode obter informações sobre novas versões e baixar atualizações. As portas 53459 e 53461 são abertas para tráfego de entrada (TCP) durante a instalação do AXIS Optimizer através do AXIS Secure Entry.

Solução de problemas

Em caso de problemas técnicos, ative o log de depuração, reproduza o problema e compartilhe esses logs com o suporte da Axis. É possível ativar o log de depuração no Management Client ou no Smart Client.

No Management Client:

1. Vá para **Site Navigation** > **Basics** > **AXIS Optimizer (Navegação no site > Fundamentos > AXIS Optimizer)**.
2. Selecione **Turn on debug logging (Ativar log de depuração)**.
3. Clique em **Save report (Salvar relatório)** para salvar os logs no seu dispositivo.

No Smart Client:

1. Vá para **Settings** > **Axis general options (Configurações > Opções gerais da Axis)**.
2. Selecione **Turn on debug logging (Ativar log de depuração)**.
3. Clique em **Save report (Salvar relatório)** para salvar os logs no seu dispositivo.

Entre em contato com o suporte

Se precisar de ajuda adicional, acesse *axis.com/support*.

Dicas e truques

Adicionar página da Web em uma exibição do Smart Client

O AXIS Optimizer permite a você exibir quase todas as páginas da Web diretamente no Smart Client, e não apenas em páginas HTML. Essa exibição da Web é alimentada por um mecanismo de navegador moderno e compatível com a maioria das páginas da Web. Isso é útil, por exemplo, quando você deseja acessar o AXIS Body Worn Manager via Smart Client ou mostrar um painel do AXIS Store Reporter ao lado de suas exibições ao vivo.

1. No Smart Client, clique em **Setup (Configuração)**.
2. Vá para **Views (Exibições)**.
3. Crie uma exibição ou selecione uma exibição existente.
4. Vá para **System overview > AXIS Optimizer (Visão geral > AXIS Optimizer)**.
5. Clique em **Web view (Exibição da Web)** e arraste-a para a exibição.
6. Insira um endereço e clique em **OK**.
7. Clique em **Setup (Configuração)**.

Exportar vídeos com funções de pesquisa incorporadas

Exportação de vídeos no formato XProtect

Para visualizar vídeos com funções de busca do AXIS Optimizer incorporadas e/ou recursos de correção de distorção da Axis, certifique-se de exportar os vídeos no formato XProtect. Isso pode ser útil, por exemplo, para fins de demonstração.

Observação

Comece a partir da etapa 3 para o AXIS Optimizer versão 5.3 ou versões posteriores.

1. No Smart Client, vá para **Settings (Configurações)** > **Axis search options (Opções de pesquisa da Axis)**.
2. Ative a opção **Include search plugins in exports (Incluir plug-ins de pesquisa na exportação)**.
3. Selecione **XProtect format (Formato XProtect)** ao criar a exportação no Smart Client.

Desbloquear exportações em computadores receptores

Para usar a exportação com êxito em outro computador, certifique-se de desbloquear o arquivo de exportação.

1. No computador receptor, clique com o botão direito do mouse no arquivo de exportação (zip) e selecione **Properties (Propriedades)**.
2. Em **General (Geral)**, clique em **Unblock (Desbloquear)** > **OK**.
3. Extraia a exportação e abra o arquivo "SmartClient-Player. exe".

Reproduzir a visualização corrigida do Axis exportada

1. Abra o projeto exportado.
2. Selecione a visualização que inclui a visualização com correção de distorção do Axis.

T10134385_pt

2026-09 (M61.2)

© 2021 – 2026 Axis Communications AB