MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2023 R3

Manual do administrador

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

Índice

Copyright, marcas comerciais e limitação de responsabilidade

Marcas comerciais

XProtect é uma marca registrada de Milestone Systems A/S.

Microsoft e Windows são marcas comerciais registradas da Microsoft Corporation. App Store é uma marca de serviço da Apple Inc. Android é uma marca comercial da Google Inc.

Todas as outras marcas comerciais mencionadas neste documento pertencem a seus respectivos proprietários.

Limitação de responsabilidade

Este texto destina-se apenas a fins de informação geral, e os devidos cuidados foram tomados em seu preparo.

Qualquer risco decorrente do uso destas informações é de responsabilidade do destinatário e nenhuma parte deste documento deve ser interpretada como alguma espécie de garantia.

Milestone Systems A/S reserva-se o direito de fazer ajustes sem notificação prévia.

Todos os nomes de pessoas e organizações utilizados nos exemplos deste texto são fictícios. Qualquer semelhança com organizações ou pessoas reais, vivas ou falecidas, é mera coincidência e não é intencional.

Este produto pode fazer uso de software de terceiros, para os quais termos e condições específicos podem se aplicar. Quando isso ocorrer, mais informações poderão ser encontradas no arquivo `3rd_party_software_terms_and_conditions.txt` localizado em sua pasta de instalação do sistema Milestone.

Visão Geral

O que há de novo?

No Management Client 2023 R3

XProtect Management Client

Agora, é possível usar o Azure Active Directory para autenticação. Durante a instalação, você pode escolher entre a **Autenticação do Windows** e o **Azure Active Directory Integrated** para proporcionar segurança integrada.

Para obter mais informações sobre como instalar o XProtect com segurança integrada do Azure, consulte Instale o seu sistema – opção Personalizado na página 163.

XProtect Management Client

Agora, a opção (não confiar no certificado do servidor) está disponível para a autenticação do Windows e para o Azure Active Directory Integrated. Essa opção é obrigatória para o Azure Active Directory Integrated. A opção (não confiar no certificado do servidor) garante que os certificados do servidor sejam validados e verificados antes da instalação.

XProtect Management Client:

Lançamos uma nova permissão de usuário **Editar configurações de alarme** para alarmes que permite aos administradores editar definições de alarme, estados de alarme, categorias de alarme, sons de alarme, retenção de alarme e retenção de eventos. As permissões de edição correspondentes para definições de alarme foram removidas da permissão de usuário **Gerenciar** existente, e os administradores precisarão de ambas as permissões de usuário (**Editar configurações de alarme** e **Gerenciar**) para gerenciar as configurações de alarme.

A nova permissão de usuário **Editar configurações de alarme** não é aplicada aos usuários existentes e deve ser atribuída manualmente a usuários que precisem de acesso de nível de administrador para configurar alarmes após a instalação ou atualização.

Para obter informações sobre a instalação personalizada, consulte Funões (nó Segurança) na página 525

No Management Client 2023 R2

XProtect Management Client:

Agora, é possível configurar o fluxo adaptável para uso no modo de reprodução. Esse método é conhecido como reprodução adaptável. Para obter mais informações, consulte Reprodução adaptável (explicação) na página 240.

XProtect Management Client:

Ao instalar os componentes do XProtect, agora você pode optar por usar uma base de dados pré-criada como parte de uma instalação personalizada. Para obter informações sobre a instalação personalizada, consulte Instale o seu sistema – opção Personalizado na página 163

XProtect Management Client:

Lançamos novas permissões de usuário para restrições de vídeo que permitem aos administradores configurar e atribuir direitos de criação, visualização, edição e exclusão aos usuários. Para obter mais informações, consulte Funões (nó Segurança) na página 525

No Management Client 2023 R1

XProtect Incident Manager:

- Para cumprir o GDPR ou outras leis aplicáveis relativas a dados pessoais, os administradores do XProtect Management Client podem agora definir um tempo de retenção para projetos de incidente.

No Management Client 2022 R3

XProtect Incident Manager:

- Agora, a extensão XProtect Incident Manager também é compatível com o XProtect Expert, XProtect Professional+, XProtect Express+ versão 2022 R3 ou posterior.
- O XProtect Incident Manager agora pode mostrar mais de 10.000 projetos de incidente.

No Management Client 2022 R2

XProtect Incident Manager:

- A primeira versão dessa extensão.
- A extensão XProtect Incident Manager é compatível com o XProtect Corporate versão 2022 R2 e posterior e com i XProtect Smart Client versão 2022 R2 e posterior.

XProtect LPR:

- Os estilos de placa de veículo, que são parte dos módulos de país, agora estão listados em um único lugar.
- Para facilitar o gerenciamento dos estilos de placa de veículo, você pode agrupá-los em apelidos de acordo com suas necessidades de reconhecimento de placa.
- As listas de correspondências agora são compatíveis com apelidos.

No Management Client 2022 R1

Criptografia do servidor de eventos:

- Você pode criptografar a conexão bidirecional entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos , incluindo o LPR Server.

  Para obter mais informações, consulte Ativar criptografia do servidor de eventos na página 314.

Como fazer login por meio de um IDP externo:

- Agora você pode fazer login no Milestone XProtect VMS usando um IDP externo. Fazer login por meio de um IDP externo é uma alternativa a fazer login como usuário do Active Directory ou como usuário básico. Com o método de login por IDP externo, você pode ignorar os requisitos de configuração de um usuário básico e ainda ser autorizado a acessar os componentes e dispositivos em XProtect.

  Para mais informações, consulte External IDP (explicado).

Atualizar dados do hardware

- Agora você pode ver a versão atual do firmware para o dispositivo de hardware detectado pelo sistema no Management Client.

  Para obter mais informações, consulte Atualize os dados do seu hardware na página 358.

XProtect Management Server Failover

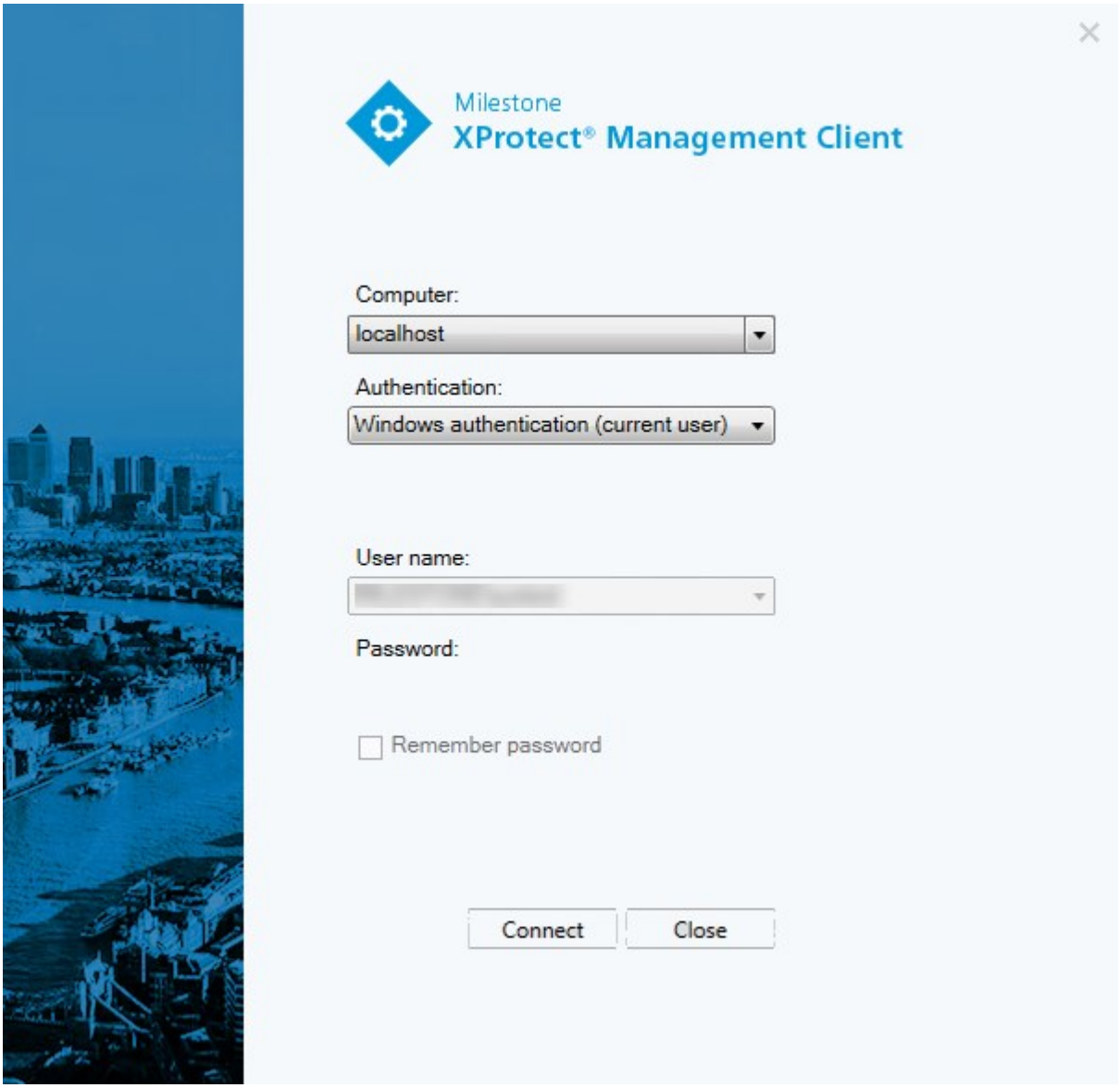
- Agora você pode obter alta disponibilidade de seu sistema configurando um servidor de gerenciamento de failover entre dois computadores redundantes. Se o computador que executa o servidor de gerenciamento falhar, o segundo assume. A replicação de dados em tempo real garante que os bancos de dados do servidor de gerenciamento, do servidor de registros e do servidor de eventos são idênticos em ambos os computadores.

  Para obter mais informações, consulte XProtect Management Server Failover na página 38.

Efetuando login (explicado)

Ao iniciar o Management Client, você deve primeiro digitar suas informações de login para se conectar a um sistema.

Com XProtect Corporate 2016 ou XProtect Expert 2016 ou uma versão mais recente instalada, você pode efetuar o login em sistemas que executam versões mais antigas do produto após a instalação de uma atualização. As versões compatíveis são XProtect Corporate 2013 e XProtect Expert 2013 ou mais recentes.



Autorização de login (explicado)

O sistema permite que os administradores configurem usuários para que só possam fazer login em um sistema, se um segundo usuário com permissões suficientes autorize este login. Neste caso, o XProtect Smart Client ou o Management Client pedirá a segunda autorização durante o login.

Um usuário associado com a função de **Administradores** incorporado sempre tem permissão para autorizar e não lhe é solicitado um segundo login, a menos que o usuário esteja associado a outra função que requeira um segundo login.

Os usuários que fazem login por meio de um IDP externo não podem ser configurados com uma exigência de autorização por um segundo usuário.

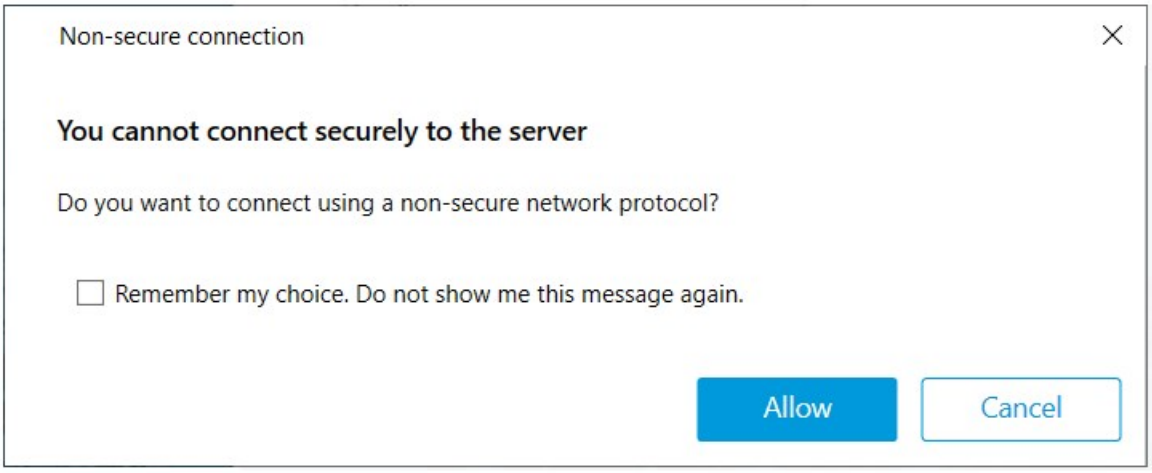
Para associar as autorizações de login a uma função:

- Configure **Autorização de login necessária** na função selecionada na guia **Informações** (consulte Configurações de funções) em **Funções** para que seja solicitada autorização adicional ao usuário durante o login.
- Configure **Autorizar usuários** na função selecionada na guia **Segurança geral** (consulte Configurações de funções) em **Funções** para que o usuário possa autorizar o login de outros usuários.

É possível escolher as duas opções para o mesmo usuário. Isto significa que é solicitada autorização adicional ao usuário durante o login e que ele também pode autorizar logins de outros usuários, exceto o seu próprio.

Faça login usando uma conexão não segura

Quando faz login no Management Client, você pode ser questionado se deseja fazer login usando um protocolo de rede não seguro.



- Clique em **Permitir** para fazer login desconsiderando a notificação. Para evitar receber esta notificação no futuro, selecione **Lembrar minha escolha. Não me mostre esta mensagem novamente** ou clique em **Ferramentas** > **Opções** e selecione **Permitir conexão não segura com o servidor (é necessário reiniciar o Management Client)**.

Para obter informações sobre comunicação segura, consulte Comunicação segura (explicado) na página 151.

Alterar sua senha de usuário básica

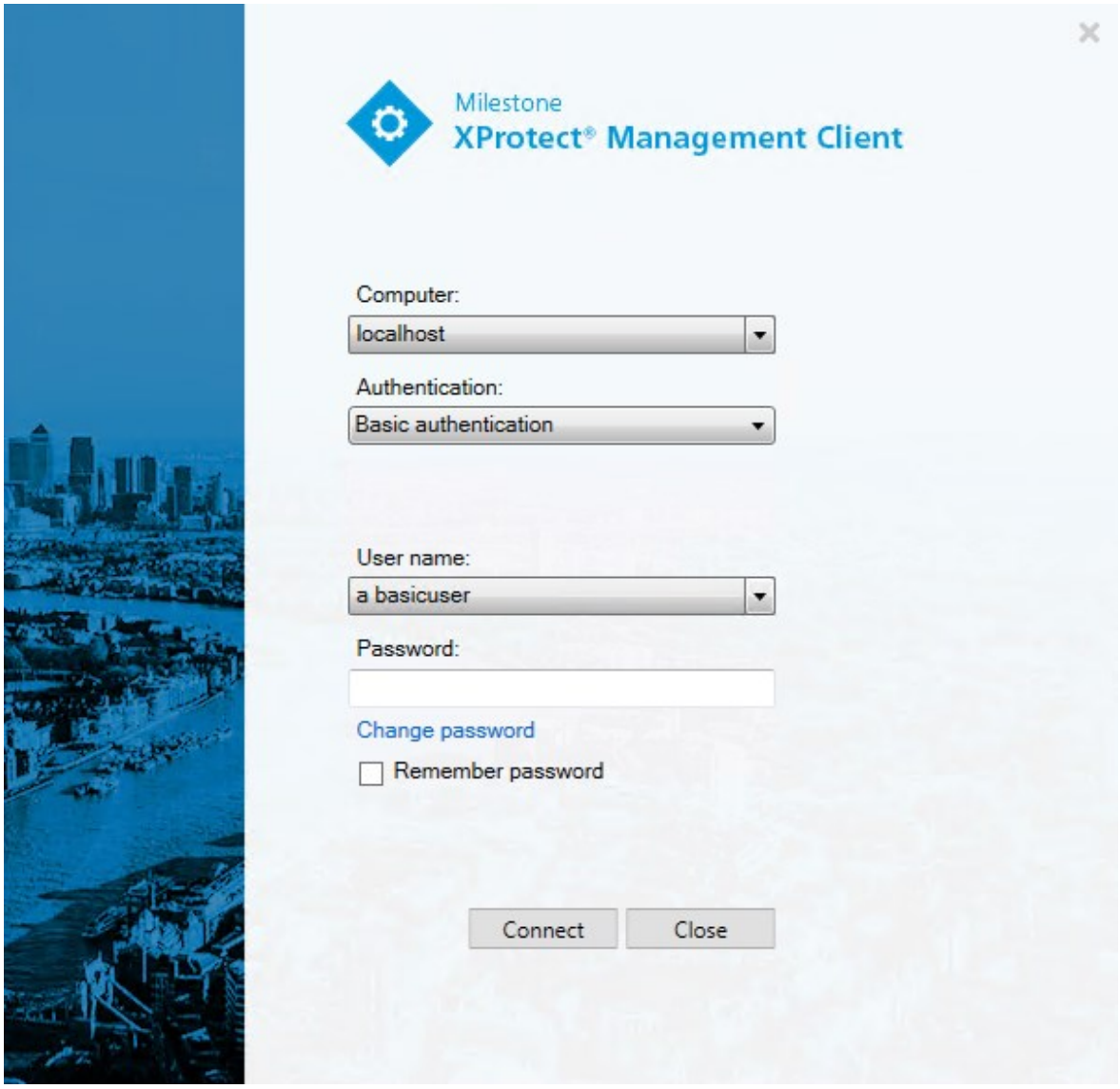
Se você fizer o login como **Usuário básico**, você poderá alterar a sua senha. Se você escolher um método de autenticação diferentes, somente o administrador do sistema pode alterar a sua senha. A alteração frequente da sua senha aumenta a segurança do seu sistema VMS XProtect.

Requisitos

A versão do seu sistema VMS XProtect deve ser 2021 R1 ou posterior.

Etapas:

1. Iniciar Management Client. A janela de login é aberta.
2. Especifique suas informações de login. Na lista **Autenticação**, selecione **Autenticação básica**. Um link com o texto **Alterar senha** aparece.



3. Clique no link. Uma janela do navegador abre.
4. Siga as instruções e salve suas alterações.
5. Agora você pode fazer o login no Management Client usando a sua nova senha.

Visão geral do produto

Os produtos XProtect VMS são sistemas de gerenciamento de vídeo (VMS) feitos para instalações de todas as formas e tamanhos. Se quiser proteger a sua loja de vandalismo ou gerenciar uma instalação de alta segurança em vários locais, XProtect torna isso possível. As soluções oferecem gerenciamento centralizado de

todos os dispositivos, servidores e usuários, e permite um sistema de regras extremamente flexível acionado por programações e eventos.

O seu sistema consiste nos seguintes componentes principais:

- O **servidor de gerenciamento** é o centro da instalação, sendo composto por vários servidores
- Um ou mais **servidores de gravação**.
- Um ou mais instalações do **XProtect Management Client**
- **XProtect Download Manager**
- Um ou mais instalações do **XProtect® Smart Client**
- Um ou mais usos de **XProtect Web Client** e/ou instalações do cliente **XProtect Mobile** se necessário

Seu sistema também inclui uma funcionalidade Matrix totalmente integrada para visualização distribuída de vídeo de qualquer câmera no seu sistema de monitoramento para qualquer computador com um XProtect Smart Client instalado.

Você pode instalar seu sistema em servidores virtualizados ou em vários servidores físicos em uma configuração distribuída. Consulte também Configuração de sistema na página 93.

O sistema também oferece a possibilidade de incluir XProtect® Smart Client – Player autônomo quando exportar evidência de vídeo do XProtect Smart Client. XProtect Smart Client – Player permite que os destinatários de evidência de vídeo (tais como policiais, investigadores internos ou externos, etc.) naveguem pelas gravações exportadas e as reproduzam sem que precisem instalar qualquer software de vigilância em seus computadores.

Com os produtos mais ricos em recursos instalados (consulte Comparação de produto na página 118), seu sistema pode lidar com um número irrestrito de câmeras, servidores e usuários em vários locais, se necessário. Seu sistema é capaz de usar IPv4 bem como IPv6.

Componentes do sistema

Servidor de gerenciamento (explicado)

O servidor de gerenciamento é o componente central do sistema VMS. Ele armazena a configuração do sistema de monitoramento em um banco de dados do SQL Server, seja no SQL Server do próprio computador do servidor de gerenciamento ou em um SQL Server distinto na rede. Também processa a autenticação de usuários, permissões de usuários, sistema de regras etc. Para melhorar o desempenho do sistema, é possível executar vários servidores de gerenciamento como um Milestone Federated Architecture™. O servidor de gerenciamento é executado como um serviço e geralmente é instalado em um servidor dedicado.

Os usuários se conectam ao servidor de gerenciamento para a autenticação inicial e em seguida de forma transparente, aos servidores de gravação, para acesso a gravações de vídeo etc.

SQL Server instalações e bancos de dados (explicado)

O servidor de gerenciamento, o servidor de eventos e o servidor de registros armazenam, por exemplo, a configuração do sistema, alarmes, eventos e mensagens de registros em bancos de dados SQL Server em uma ou mais instalações do SQL Server. O servidor de gerenciamento e o servidor de eventos compartilham o mesmo banco de dados SQL Server, enquanto o servidor de registros , XProtect Incident Manager, e o Identity Provider têm cada um seu próprio banco de dados SQL Server. Para obter mais informações sobre o Identity Provider, consulteIdentity Provider (explicado) na página 68. Para obter mais informações sobre o banco de dados e o registro do XProtect Incident Manager, consulte o manual do administrador exclusivo para o XProtect Incident Manager.

O instalador do sistema inclui o Microsoft SQL Server Express, que é uma edição gratuita do SQL Server.

Para sistemas muito grandes ou com muitas transações para e do banco de dados SQL Server, a Milestone recomenda que você use a edição Microsoft® SQL Server® Standard ou Microsoft® SQL Server® Enterprise do SQL Server em um computador dedicado na rede e em uma unidade de disco rígido não utilizada para outros fins. Instalar o SQL Server em sua própria unidade melhorará o desempenho de todo o sistema.

Servidor de gravação (explicado)

O servidor de gravação é responsável pela comunicação com as câmeras e codificadores de vídeo da rede, gravação de áudio e vídeo recuperado, bem como por proporcionar o acesso do cliente a áudio e vídeo ao vivo e gravado. O servidor de gravação também é responsável pela comunicação com outros produtos Milestone conectados pela tecnologia Milestone Interconnect.

Drivers de dispositivo

- A comunicação com as câmeras e codificadores de vídeo da rede é feita através de um driver de dispositivo desenvolvido especificamente para dispositivos individuais ou para uma série de dispositivos semelhantes do mesmo fabricante
- A partir da versão 2018 R1, os drivers de dispositivos estão divididos em dois pacotes: o pacote de dispositivos regular, com drivers mais recentes, e um pacote de dispositivos herdados com drivers mais antigos
- O pacote de dispositivos regular é instalado automaticamente quando você instala o servidor de gravação. Mais tarde, você pode atualizar os drivers fazendo o download e instalando uma versão mais recente do pacote de dispositivos
- O pacote de dispositivos herdados só pode ser instalado se o sistema tiver um pacote de dispositivos regular instalado. Os drivers do pacote de dispositivos herdados são instalados automaticamente se uma versão anterior já estiver instalada em seu sistema. Está disponível para download e instalação manual na página de download do software (https://www.milestonesys.com/downloads/)

Banco de dados de mídia:

- O servidor de gravação armazena os dados de áudio e vídeo recuperados no banco de dados de mídia feito sob medida para alto desempenho na gravação e armazenamento de dados de áudio e vídeo
- O banco de dados de mídia suporta várias características exclusivas, tais como arquivamento em múltiplos estágios, grooming de vídeo, criptografia e inclusão de assinatura digital às gravações

O sistema usa servidores de gravação para gravação de feeds de vídeo e para comunicação com câmeras e outros dispositivos. Um sistema de monitoramento é tipicamente constituído por vários servidores de gravação.

Os servidores de gravação são computadores em que você instalou o software Recording Server e o configurou para se comunicar com o servidor de gerenciamento. É possível ver os servidores de gravação do seu sistema no painel **Visão geral** quando você expande a pasta **Servidores** e seleciona **Servidores de Gravação**.

A compatibilidade com versões de servidores de gravação anteriores à versão atual do servidor de gerenciamento é limitada. Você ainda pode acessar gravações nesses servidores de gravação com versões mais antigas, mas se desejar alterar a sua configuração, certifique-se de que eles tenham a mesma versão do servidor de gerenciamento. A Milestone recomenda que você atualize todos os servidores de gravação no seu sistema para a mesma versão que o seu servidor de gerenciamento.

O servidor de gravação suporta criptografia de fluxos de dados para clientes e serviços:

- Ative a criptografia para cliente e serviços na página 316
- Visualizar status de criptografia para clientes na página 300

O servidor de gravação também suporta a criptografia da conexão com o servidor de gerenciamento:

- Ativar criptografia para e do servidor de gerenciamento na página 311

Existem várias opções relacionadas ao gerenciamento de seus servidores de gravação:

- Adicionar hardware na página 221
- Mover hardware na página 351
- Excluir todos o hardware em um servidor de gravação na página 370
- Remover um servidor de gravação na página 370

Quando o Recording Server serviço estiver funcionado, é muito importante que o Windows Explorer ou outros programas não acessem os arquivos do Banco de dados de Mídia ou pastas associadas com a configuração do sistema. Caso contrário, o servidor de gravação não poderá renomear ou mover arquivos de mídia importantes. Isto pode levar o servidor de gravação a uma parada. Para reinicializar um servidor de gravação parado, pare o Recording Server serviço, feche o programa acessando o(s) arquivo(s) de mídia ou pasta(s) importante(s) e reinicie o Recording Server serviço.

Servidor móvel (explicado)

O servidor móvel é responsável por dar ao cliente XProtect Mobile e aos usuários XProtect Web Client acesso ao sistema.

Além de atuar como um sistema de gateway para os dois clientes, o servidor móvel pode transcodificar o vídeo, já que o fluxo de vídeo da câmera original em muitos casos é grande demais para caber na largura de banda disponível para os usuários do cliente.

Se você estiver executando uma instalação **Distribuída** ou **Personalizada**, Milestone recomenda que você instale o servidor móvel em um servidor dedicado.

Servidor de eventos (explicado)

O servidor de eventos lida com várias tarefas relacionadas a eventos, alarmes e mapas e talvez também integrações de terceiros através do MIP SDK.

Eventos

- Todos os eventos do sistema são consolidados no servidor de eventos de forma que há um lugar e uma interface para que parceiros façam integrações que usem eventos do sistema
- Além disso, o servidor de eventos oferece acesso a terceiros para o envio de eventos para o sistema através das interfaces de eventos Genéricos ou Analíticos

Alarmes

- O servidor de eventos aloja a função de alarme, a lógica alarme, o estado de alarme, bem como opera o banco de dados de alarmes. O banco de dados de alarme é armazenado no mesmo banco de dados SQL Server usado pelo servidor de gerenciamento

Mensagens

- A comunicação por mensagens é processada pelo servidor de eventos, permitindo que plug-ins enviem mensagens em tempo real entre ambientes, como XProtect Smart Client, Management Client, servidor de eventos e serviços autônomos.

Mapas

- O servidor de eventos também hospeda os mapas que são configurados e usados no XProtect Smart Client

MIP SDK

- Finalmente, plug-ins desenvolvidos por terceiros podem ser instalados no servidor de eventos e usar o acesso a eventos do sistema

Servidor de registro (explicado)

O servidor de registros armazena todas as mensagens de registro para todo o sistema em um banco de dados do SQL Server. Esse banco de dados de mensagens de registro pode existir no mesmo SQL Server do banco de dados de configuração do sistema do servidor de gerenciamento ou em um SQL Server distinto. Normalmente, o servidor de registros é instalado no mesmo servidor que o servidor de gerenciamento, mas ele pode ser instalado em um servidor separado para maior desempenho dos servidores de gerenciamento e de registros.

API Gateway (explicado)

O MIP VMS API fornece uma API RESTful unificada, baseada em protocolos padrão do setor, como OpenAPI, para acessar funcionalidades XProtect VMS, simplificar projetos de integração e servir como base para comunicação conectada à nuvem.

O XProtect VMS API Gateway é compatível com essas opções de integração por meio do Milestone Integration Platform VMS API (MIP VMS API).

O API Gateway é instalado com serviços no local e destina-se a servir como um front-end e ponto de entrada comum para serviços de API RESTful e WebSocket Messaging API em todos os componentes atuais do servidor VMS (servidor de gerenciamento, servidor de eventos, servidores de gravação, servidor de registros etc.). Um serviço API Gateway pode ser instalado no mesmo host que o servidor de gerenciamento ou separadamente, e mais de um pode ser instalado (cada um em seu próprio host).

A API RESTful é implementada em parte por cada componente específico do servidor VMS e o API Gateway pode simplesmente passar por essas solicitações e respostas, enquanto que, para outras solicitações, o API Gateway converterá solicitações e respostas conforme apropriado.

Atualmente, a API de configuração, hospedada pelo servidor de gerenciamento, está disponível como API RESTful. A API RESTful Events, a Websockets Messaging API e a API RESTful Alarms, hospedadas pelo servidor de eventos, também estão disponíveis.

Para obter mais informações, consulte o manual do administrador API Gateway e a Milestone Integration Platform VMS APIdocumentação de referência .

Recuperação de falha

XProtect Management Server Failover

Se um computador independente executando o serviço Management Server ou SQL Server tiver uma falha de hardware, isso não afetará as gravações ou o servidor de gravação. No entanto, essas falhas de hardware podem resultar em tempo de inatividade para operadores e administradores que ainda não estejam

conectados aos clientes.

O XProtect Management Server Failover fornece alta disponibilidade e recuperação de desastres para o servidor de gerenciamento. Se o servidor de gerenciamento ficar indisponível em um computador, o outro assumirá as tarefas de execução dos componentes do sistema.

Você pode usar a replicação segura em tempo real dos bancos de dados do SQL Server para garantir que não haja perda de dados em caso de falhas de hardware.

O XProtect Management Server Failover pode ajudar você a reduzir o tempo de inatividade do sistema. Você pode se beneficiar de um cluster de failover quando:

- Um servidor falha – você pode executar o serviço Management Server e SQL Server de outro computador enquanto resolve os problemas.
- Você precisa aplicar atualizações do sistema e patches de segurança – A aplicação de patches de segurança em um servidor de gerenciamento autônomo pode ser demorada, resultando em longos períodos de inatividade. Quando você tem um cluster de failover, pode aplicar atualizações do sistema e patches de segurança com tempo de inatividade mínimo.
- Você precisa de uma conexão perfeita – os usuários têm acesso contínuo ao vídeo ao vivo e de reprodução, e à configuração do sistema em todos os momentos.

Você configura XProtect Management Server Failover entre dois computadores. Para fazer a recuperação de falha funcionar, você precisa instalar em cada computador:

- XProtect Management Server
- Serviço XProtect Event Server
- Serviço XProtect Log Server
- Microsoft SQL Server (recomendado)

Servidor de gerenciamento de failover (explicado)

O suporte a failover no servidor de gestão é feito instalando-se o servidor de gestão em um Microsoft Windows Cluster. O cluster, então, garantirá que um outro servidor assuma a função de servidor de gerenciamento em caso de falha do primeiro servidor.

Servidor do sistema de gravação ininterrupta (explicado)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Um servidor do sistema de gravação ininterrupta (failover) é um servidor de gravação extra que retoma a partir do servidor de gravação padrão se este se torna indisponível. Você pode configurar um servidor do sistema de gravação ininterrupta (failover) em dois modos, como um **servidor em cold standby** ou como um **servidor em hot standby**.

Você instala servidores do sistema de gravação ininterrupta (consulte Instale um servidor do sistema de gravação ininterrupta através do Download Manager na página 175). Depois de ter instalado os servidores de gravação ininterrupta (failover), eles são visíveis no Management Client. Milestone recomenda que você instale todos os servidores do sistema de gravação ininterrupta (failover) em computadores separados. Não deixe de configurar servidores do sistema de gravação ininterrupta com o endereço IP/nome do host do servidor de gerenciamento. As permissões de usuário para a conta de usuário sob a qual o serviço Failover Server é executado são fornecidas durante o processo de instalação. São eles:

- Permissões Iniciar/Parar para iniciar ou parar o servidor do sistema de gravação ininterrupta
- Permissões de acesso a gravação e leitura para ler ou gravar o arquivo RecorderConfig.xml

Se um certificado estiver selecionado para criptografia, o administrador deve conceder permissão de acesso ao usuário de failover na chave privada do certificado selecionado.

Se o servidor do sistema de gravação ininterrupta assumir a partir de um servidor de gravação que usa criptografia, o Milestone recomenda que você também prepare o servidor do sistema de gravação ininterrupta para o uso de criptografia. Para obter mais informações, consulte Comunicação segura (explicado) na página 151 e Instale um servidor do sistema de gravação ininterrupta através do Download Manager na página 175.

Você pode especificar que tipo de suporte de failover você quer no nível de dispositivo. Para cada dispositivo em um servidor de gravação, selecione completo, apenas ao vivo ou nenhum suporte de failover. Isso ajuda você a priorizar seus recursos de failover e, por exemplo, apenas configurar failover para vídeo e não para áudio, ou só ter failover em câmeras essenciais, e não em câmeras menos importantes.

Enquanto seu sistema estiver no modo de recuperação de falhas, não é possível substituir ou mover o hardware, atualizar o servidor de gravação ou alterar configurações do dispositivo, como configurações de armazenamento ou configurações de fluxo de vídeo.

Servidores de gravação de failover em cold standby

Em uma configuração do servidor do sistema de gravação ininterrupta (failover) em cold standby, você agrupa diversos servidores de gravação de failover em um grupo de failover. Todo o grupo de emergência é dedicado para assumir a partir de qualquer um dos diversos servidores de gravação pré-selecionados, se um destes se tornar indisponível. Você pode criar quantos grupos deseja (consulte Servidores de gravação de failover do grupo para cold standby na página 218).

Agrupamento tem um benefício claro: quando você posteriormente especifica quais os servidores do sistema de gravação ininterrupta (failover) devem assumir o controle de um servidor de gravação, você seleciona um grupo de servidores do sistema de gravação ininterrupta (ailover). Se o grupo selecionado contiver mais de um servidor do sistema de gravação ininterrupta (failover), isto lhe dará a segurança de ter mais do que um servidor do sistema de gravação ininterrupta (failover) pronto para assumir o controle caso um servidor de gravação fique indisponível. Você pode especificar um grupo de servidor de failover secundário que assume a partir do grupo primário se todos os servidores de gravação no grupo primário estiverem ocupados. Um servidor do sistema de gravação ininterrupta (failover) só pode ser membro de um grupo de cada vez.

Os servidores de gravação de failover em um grupo de failover são ordenados em uma sequência. A sequência determina a ordem em que os servidores de gravação de failover assumirão a partir de um servidor de gravação. Por padrão, a sequência reflete a ordem na qual você tem incorporado os servidores de gravação de failover no grupo de failover: o primeiro a entrar é o primeiro na sequência. Você pode mudar isso, caso precise.

Servidores de gravação de failover de espera ativa

Em uma configuração do servidor do sistema de gravação ininterrupta (failover) em hot standby, você dedica um servidor do sistema de gravação ininterrupta (failover) para assumir a partir de apenas **um** servidor de gravação. Por isso, o sistema pode manter este servidor do sistema de gravação ininterrupta (failover) em um modo de "espera", o que significa que ele é sincronizado com a configuração correta/atual que o servidor de gravação é dedicado e pode assumir muito mais rápido do que um servidor do sistema de gravação ininterrupta (failover) em cold standby. Conforme mencionado, você atribui servidores em espera ativa para apenas um servidor de gravação e não pode agrupá-lo. Você não pode atribuir os servidores de failover que já fazem parte de um grupo de failover como servidores de gravação em hot standby.

Validação do servidor do sistema de gravação ininterrupta

Para validar uma fusão de dados de vídeo do servidor de emergência para o servidor de gravação, você deve tornar o servidor de gravação indisponível, parando o serviço do servidor de gravação ou desligando o computador do servidor de gravação.

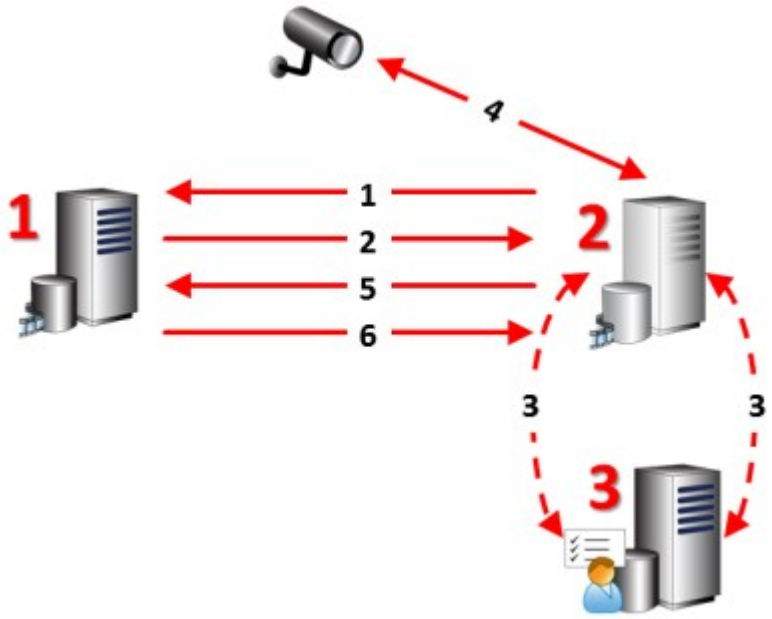
Qualquer interrupção manual da rede que você possa causar removendo o cabo de rede ou bloqueando a rede usando uma ferramenta de teste não é um método válido.

Funcionalidade do servidor do sistema de gravação ininterrupta (explicado)

- Um servidor do sistema de gravação ininterrupta (failover) verifica o estado dos servidores de gravação relevantes a cada 0,5 segundo. Se um servidor de gravação não responde dentro de 2 segundos, o servidor de gravação é considerado indisponível e o servidor do sistema de gravação ininterrupta (failover) assume o controle
- Um servidor do sistema de gravação ininterrupta (failover) em cold standby assume o servidor de gravação que se tornou indisponível após cinco segundos mais o tempo que o serviço Recording Server do servidor do sistema de gravação ininterrupta (failover) leva para iniciar e o tempo que leva para conectar-se as câmeras. Por outro lado, um servidor do sistema de gravação ininterrupta (failover) em hot standby assume mais rápido porque o serviço Recording Server já está em execução com a configuração correta e precisa apenas iniciar suas câmeras para fornecer feeds. Durante o período de inicialização, você não pode armazenar as gravações nem visualizar o vídeo ao vivo das câmeras afetadas
- Quando um servidor de gravação torna-se disponível novamente, ele assume automaticamente a partir do servidor do sistema de gravação ininterrupta (failover). As gravações armazenadas pelo servidor do sistema de gravação ininterrupta (failover) são mescladas automaticamente nos bancos de dados do servidor de gravação padrão. O tempo que leva para mesclar, depende da quantidade de gravações, da capacidade da rede e muito mais. Durante o processo de mesclagem, você não pode pesquisar gravações do período durante o qual o servidor do sistema de gravação ininterrupta (failover) assumiu
- Se um servidor do sistema de gravação ininterrupta (failover) deve assumir o controle de um outro servidor de gravação durante o processo de fusão, ele adia o processo de fusão com o servidor de gravação A e assume a gravação do servidor B. Quando o servidor de gravação B tornar-se disponível novamente, o servidor de gravação de failover assume o processo de fusão e permite que o servidor de gravação A e o servidor de gravação B mesclem as gravações simultaneamente.
- Em uma configuração em hot standby, um servidor em hot standby não pode assumir um outro servidor de gravação porque ele só pode ser hot standby para um único servidor de gravação. Mas se esse servidor de gravação falhar novamente, a espera ativa assume novamente e também mantém as gravações do período anterior. O servidor de gravação mantém as gravações até que sejam fundidas ao gravador primário ou até que o servidor do sistema de gravação ininterrupta (failover) fique sem espaço em disco
- Uma solução de failover não fornece redundância completa. Isso só pode servir como uma maneira segura de minimizar o tempo de inatividade. Se um servidor de gravação se torna disponível novamente, o serviço Failover Server certifica que o servidor de gravação está pronto para armazenar as gravações novamente. Somente então a responsabilidade de armazenar gravações é voltada para o servidor de gravação normal. Assim, uma perda de gravações neste estágio do processo é muito improvável

- Os usuários do cliente dificilmente percebem que um servidor do sistema de gravação ininterrupta (failover) está assumindo o controle. Uma pequena pausa ocorre, normalmente, apenas por alguns segundos, quando o servidor do sistema de gravação ininterrupta (failover) assume o controle. Durante esta pausa, os usuários não podem acessar vídeo do servidor de gravação afetado. Os usuários do cliente podem continuar a visualizar vídeo ao vivo assim que o servidor do sistema de gravação ininterrupta (failover) assumir o controle. Visto que as gravações recentes são armazenadas no servidor do sistema de gravação ininterrupta (failover), ele pode reproduzir gravações depois que o servidor do sistema de gravação ininterrupta (failover) assumiu o controle. Os clientes não podem reproduzir gravações antigas armazenadas somente no servidor de gravação afetado até que o servidor de gravação esteja funcionando novamente, e tenha assumido o servidor do sistema de gravação ininterrupta (failover). Você não pode acessar gravações arquivadas. Quando o servidor de gravação está funcionando de novo, um processo de fusão ocorre durante o qual as gravações de failover são fundidas de volta no banco de dados do servidor de gravação. Durante este processo, você não pode reproduzir gravações do período durante o qual o servidor do sistema de gravação ininterrupta (failover) assumiu o controle
- Em uma configuração em cold standby, a configuração de um servidor do sistema de gravação ininterrupta (failover) como backup para outro servidor do sistema de gravação ininterrupta (failover) não é necessária. Isto porque você distribui grupos de emergência e não distribui servidores do sistema de gravação ininterrupta para assumir servidores de gravação normal. Um grupo de failover precisa conter pelo menos um servidor do sistema de gravação ininterrupta (failover), mas você pode adicionar quantos servidores de gravação de failover você desejar. Se um grupo de emergência contiver mais que um servidor do sistema de gravação ininterrupta, mais do que um servidor do sistema de gravação ininterrupta pode de assumir o controle.
- Em uma configuração em hot standby, você não pode configurar servidores do sistema de gravação ininterrupta ou servidores em hot standby como emergência para um servidor em hot standby.

Etapas da emergência (explicado)



Descrição
Servidores envolvidos (números em vermelho): 1. Recording Server 2. Failover Recording Server 3. Management Server
Etapas de Failover para as configurações em **Cold standby**: 1. Para verificar se está executando ou não, um servidor do sistema de gravação ininterrupta (failover) tem uma conexão TCP ininterrupta com um servidor de gravação. 2. Esta conexão está interrompida. 3. O servidor do sistema de gravação ininterrupta (failover) solicita a configuração atual do servidor de gravação do servidor de gerenciamento. O servidor de gerenciamento envia a configuração solicitada, o servidor do sistema de gravação ininterrupta (failover) recebe a configuração, inicializa, e inicia a gravação em nome do servidor de gravação. 4. O servidor do sistema de gravação ininterrupta (failover) e a(s) câmera(s) trocam dados de vídeo.

Descrição
5. O servidor do sistema de gravação ininterrupta (failover) tenta continuamente restabelecer a conexão com o servidor de gravação. 6. Quando a conexão com o servidor de gravação é restabelecida, o servidor do sistema de failover fecha e o servidor de gravação busca dados de vídeo (se houver) gravados durante o tempo de inatividade e os dados de vídeo são reunidos no banco de dados do servidor de gravação.
Etapas de Failover para as configurações em **Hot standby**: 1. Para verificar se está executando ou não, um servidor em hot standby tem uma conexão TCP ininterrupta com um servidor de gravação atribuído. 2. Esta conexão está interrompida. 3. A partir do servidor de gerenciamento, o servidor em espera ativa já sabe a configuração atual de seu servidor de gravação atribuído e começa a gravar em seu nome. 4. O servidor em espera ativa e a(s) câmera(s) trocam dados de vídeo. 5. O servidor em espera tenta continuamente restabelecer a conexão com o servidor de gravação. 6. Quando a conexão com o servidor de gravação é restabelecida, o servidor em espera ativa volta ao modo de espera ativa, o servidor de gravação busca dados de vídeo (se houver) gravados durante o período de inatividade e os dados de vídeo são reunidos no banco de dados do servidor de gravação.

Serviços dos servidores do sistema de gravação ininterrupta (explicado)

Um servidor do sistema de gravação ininterrupta (failover) tem dois serviços instalados:

- Um serviço Failover Server, que manipula os processos de assumir o lugar do servidor de gravação. Esse serviço está sempre sendo executado e verifica constantemente o estado de servidores de gravação relevantes

- Um serviço Failover Recording Server, que ativa o servidor do sistema de gravação ininterrupta para agir como um servidor de gravação.

  Em uma configuração em cold standby, este serviço somente é iniciado quando necessário, que é quando o servidor do sistema de gravação ininterrupta (failover) em cold standby assume a partir do servidor de gravação. Iniciar este serviço normalmente leva alguns segundos mas pode durar mais dependendo das configurações de segurança local, e muito mais.
  Em uma configuração hot standby, esse serviço está sempre em execução, permitindo que o servidor em hot standby assuma o controle mais rapidamente do que o servidor do sistema de gravação ininterrupta em cold standby.

Clientes

Management Client (explicado)

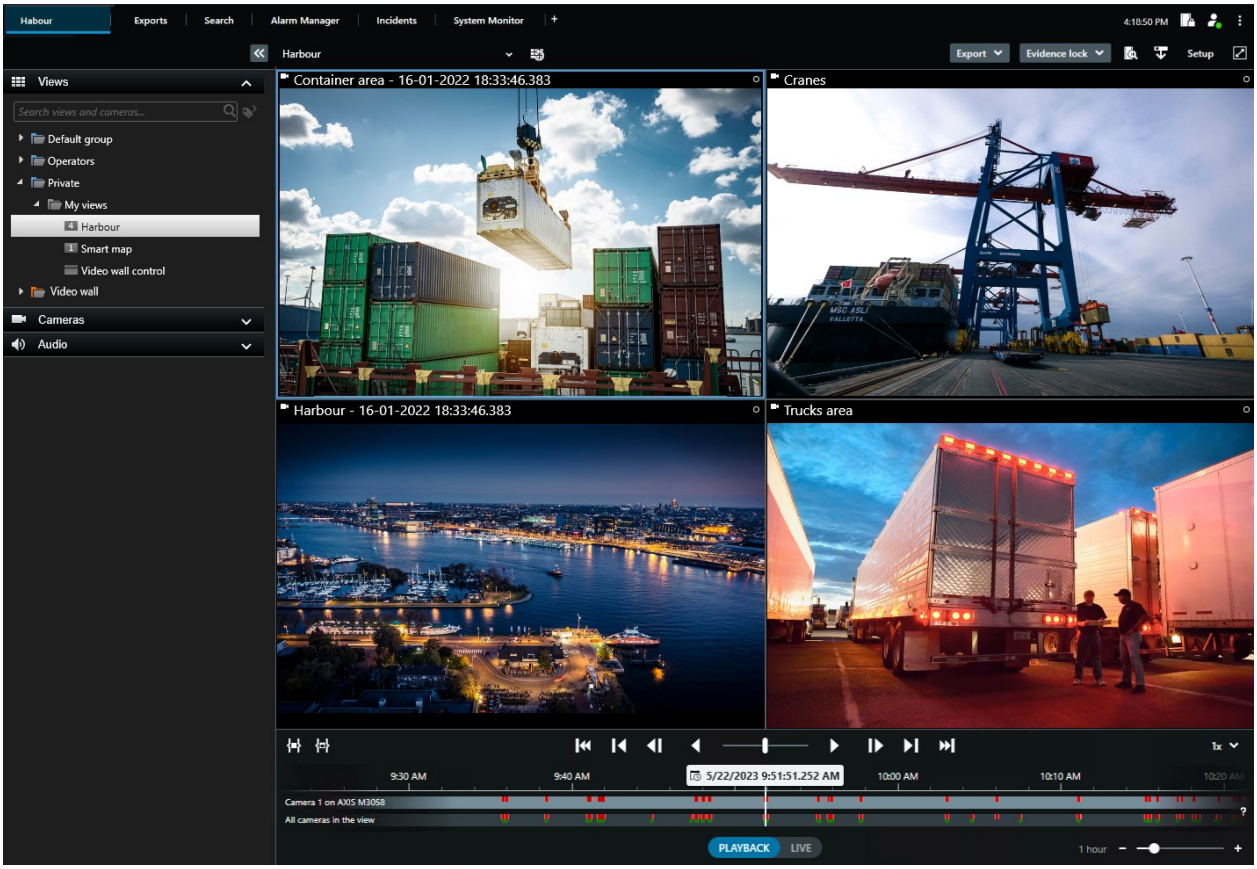
O Management Client é um cliente de administração rico em recursos para configuração e gerenciamento diário do sistema. Disponível em diversos idiomas.

O software do Cliente de Gerenciamento geralmente é instalado na estação de trabalho do administrador do sistema de monitoramento ou semelhante.

XProtect Smart Client (explicado)

XProtect Smart Client é um aplicativo de desktop projetado para ajudá-lo a gerenciar suas câmeras de vigilância . Ele fornece controle intuitivo sobre as instalações de segurança, dando aos usuários acesso a vídeos ao vivo e gravados, controle instantâneo de câmeras e dispositivos de segurança conectados e a capacidade de fazer pesquisas avançadas para gravações e metadados.

Disponível em diversos idiomas, o XProtect Smart Client possui uma interface de usuário adaptável que pode ser otimizada para tarefas individuais dos operadores e ajustada de acordo com as habilidades específicas e os níveis de autoridade.



Ao selecionar um tema claro ou escuro, a interface permite que você personalize sua experiência de visualização para ambientes de trabalho específicos. Ele também possui guias otimizadas para trabalho e uma linha do tempo principal para facilitar a operação de monitoramento.

Usando o MIP SDK, os usuários podem integrar diferentes tipos de sistemas de segurança e de negócios e aplicativos de análise de vídeo, que você gerencia através do XProtect Smart Client.

XProtect Smart Client deve ser instalado em computadores de operadores. Os administradores do sistema de monitoramento gerenciam o acesso ao sistema de segurança por meio do Management Client. As gravações visualizadas por clientes são fornecidas pelo serviço Image Server do seu sistema XProtect. O serviço executa em segundo plano no servidor do sistema de monitoramento. Não é necessário hardware separado.

XProtect Mobile Cliente (explicado)

O cliente XProtect Mobile é uma solução de vigilância móvel integrada com o restante do seu sistema XProtect. Ele é executado em seu tablet ou smartphone Android ou em seu tablet, smartphone ou reprodutor de música portátil da Apple® e proporciona acesso a câmeras, visualizações e outras funcionalidades configuradas nas estações de gerenciamento.

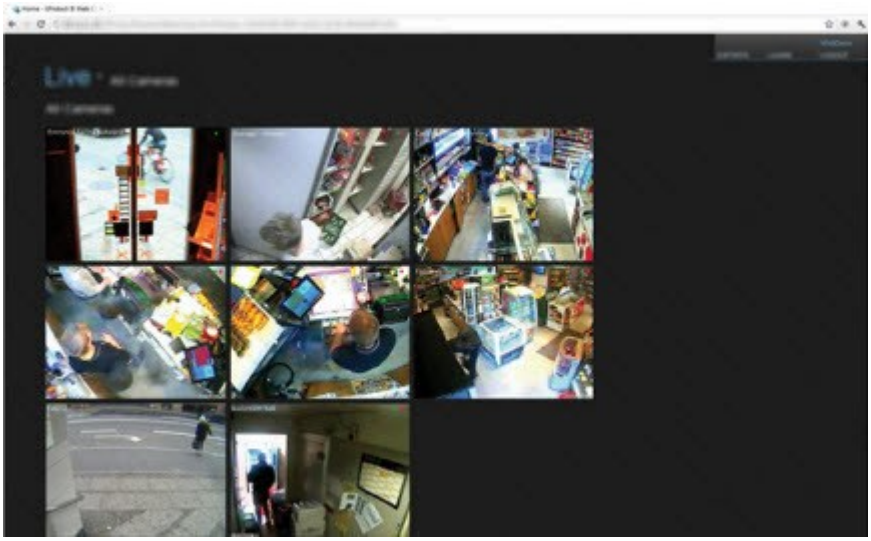
Use o cliente XProtect Mobile para visualizar e reproduzir vídeo ao vivo e gravado a partir de uma ou várias câmeras, controlar a rotação horizontal, vertical e zoom (PTZ), ativar saída e eventos e usar a funcionalidade push de vídeo para enviar vídeo a partir de seu dispositivo para o sistema XProtect.

Se você deseja usar o cliente XProtect Mobile com seu sistema, você deve ter um servidor móvel XProtect Mobile para estabelecer a conexão entre o cliente XProtect Mobile e seu sistema. Depois que o servidor XProtect Mobile estiver configurado, baixe o cliente XProtect Mobile gratuitamente no Google Play ou na App Store para começar a usar o XProtect Mobile.

Você precisa de uma licença de dispositivo por dispositivo que permita push de vídeo no seu sistema XProtect.

XProtect Web Client (explicado)

XProtect Web Client é um aplicativo on-line do cliente para visualização, reprodução e compartilhamento de vídeo. Ele fornece acesso instantâneo às funções de vigilância mais comumente utilizadas, tais como a visualização de vídeo ao vivo, a reprodução de vídeos gravados, a impressão e a exportação de provas. O acesso aos recursos depende de permissões de usuários individuais que são configuradas no Management Client.



Para permitir o acesso ao XProtect Web Client, você deve ter um servidor XProtect Mobile para estabelecer a conexão entre o XProtect Web Client e seu sistema. O XProtect Web Client em si não necessita de qualquer instalação e funciona com a maioria dos navegadores. Depois de configurar o servidor do XProtect Mobile, você pode monitorar seu sistema XProtect de qualquer lugar a partir de qualquer computador ou tablet com acesso à Internet (desde que você saiba o endereço externo/Internet correto, nome de usuário e senha).

Extensões do XProtect

XProtect Access (explicado)

A Milestone desenvolveu várias extensões. Extensões são produtos que ampliam a funcionalidade dos produtos de VMS da XProtect com recursos especializadas adicionais. Seu arquivo de licença do XProtect controla o acesso às extensões.

O uso de XProtect Access requer que você tenha adquirido uma licença básica que lhe permita acessar este recurso no seu sistema XProtect. Também é preciso uma licença de porta de controle de acesso para cada porta que deseja controlar.

É possível usar XProtect Access com sistemas de controle de acesso de terceiros para os quais exista um plug-in específico do fornecedor para XProtect Access.

O recurso de integração de controle de acesso apresenta um novo recurso que facilita a integração dos sistemas de controle de acesso dos clientes com XProtect. Você obtém:

- Uma interface de usuário de operador comum para vários sistemas de controle de acesso em XProtect Smart Client
- Integração mais rápida e mais poderosa dos sistemas de controle de acesso
- Mais funcionalidade para o operador (veja abaixo)

Em XProtect Smart Client, o operador obtém:

- Monitoramento ao vivo de eventos nos pontos de acesso
- Passagem auxiliada por operador para solicitações de acesso
- Integração de mapa
- Definições de alarme para eventos de controle de acesso
- Investigação de eventos nos pontos de acesso
- Visão geral e controle do estado das portas centralizados
- Informações e gerenciamento do titular do cartão

O **Registro de auditoria** registra os comandos que cada usuário realiza no sistema de controle de acesso do XProtect Smart Client.

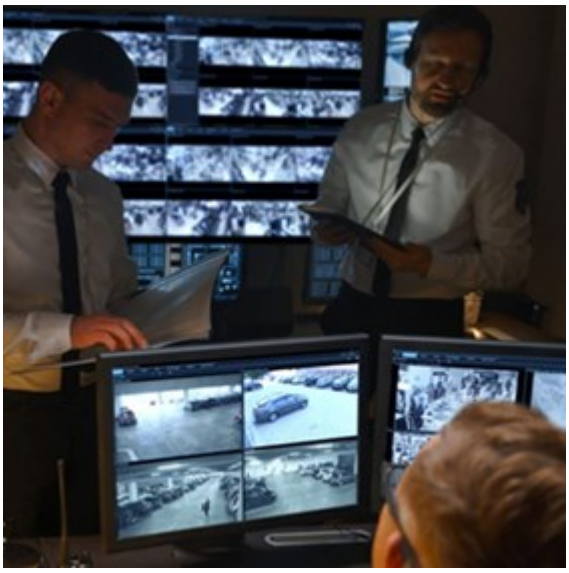
Além de uma licença básica de XProtect Access você precisa de um plug-in de integração específico do fornecedor instalado no servidor de eventos antes de poder iniciar uma integração.

XProtect Incident Manager

A Milestone desenvolveu várias extensões. Extensões são produtos que ampliam a funcionalidade dos produtos de VMS da XProtect com recursos especializadas adicionais. Seu arquivo de licença do XProtect controla o acesso às extensões.

> As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

O XProtect Incident Manager é uma extensão que permite que as organizações documentem incidentes e os combinem com evidência de sequência (vídeo e possivelmente áudio) do VMS da XProtect.



Os usuários do XProtect Incident Manager podem salvar todas as informações de incidentes em projetos de incidentes. A partir dos projetos de incidentes, é possível rastrear o status e as atividades de cada incidente. Dessa forma, os usuários podem gerenciar incidentes de forma eficaz e facilmente compartilhar fortes evidências de incidentes, tanto internamente com colegas quanto externamente com as autoridades.

XProtect Incident Manager ajuda as organizações a obter a visão geral e a compreensão dos incidentes que acontecem nas áreas que inspecionam. Esse conhecimento permite que as organizações implementem medidas para minimizar a chance de incidentes semelhantes acontecerem no futuro.

No XProtect Management Client, os administradores do XProtect VMS de uma organização podem definir as propriedades disponíveis do incidente no XProtect Incident Manager para as necessidades das organizações. Os operadores do XProtect Smart Client iniciam, salvam e gerenciam projetos de incidentes e adicionam várias informações aos projetos de incidentes. Isso inclui texto livre, propriedades de incidentes que os administradores definiram e sequências do VMS XProtect. Para total rastreabilidade, o VMS XProtectregistra quando os administradores definem e editam as propriedades do incidente e quando os operadores criam e atualizam os projetos de incidente.

XProtect LPR (explicado)

A Milestone desenvolveu várias extensões. Extensões são produtos que ampliam a funcionalidade dos produtos de VMS da XProtect com recursos especializadas adicionais. Seu arquivo de licença do XProtect controla o acesso às extensões.

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

O XProtect LPR oferece análise com base em conteúdo de vídeo (VCA) e reconhecimento de placas de veículos que interagem com o sistema de monitoramento e com o seu XProtect Smart Client.

Para ler os caracteres em uma placa, o XProtect LPR usa reconhecimento óptico de caracteres em imagens, auxiliado por configurações especializadas da câmera.

Você pode combinar LPR (reconhecimento de placa) com outros recursos de monitoramento, como a gravação e ativação baseada em eventos de saídas.

Exemplos de eventos em XProtect LPR:

- Disparar registros do sistema de monitoramento em uma situação específica
- Ativar alarmes
- Compare com listas de correspondências positivas e negativas
- Abrir portões
- Acender luzes
- Trazer o vídeo de incidentes para as telas do computador de membros da equipe de segurança determinados
- Enviar mensagens por telefone celular

Com um evento, é possível ativar alarmes no XProtect Smart Client.

XProtect Smart Wall (explicado)

Consulte também o manual do XProtect Smart Wall.

A Milestone desenvolveu várias extensões. Extensões são produtos que ampliam a funcionalidade dos produtos de VMS da XProtect com recursos especializadas adicionais. Seu arquivo de licença do XProtect controla o acesso às extensões.

O XProtect Smart Wall é uma extensão avançada que permite que as organizações criem murais de vídeo que atendam às suas demandas específicas de segurança. O XProtect Smart Wall fornece uma visão geral de todos os dados de vídeo no sistema VMS[1] XProtect e é compatível com qualquer quantidade ou combinação de monitores.

XProtect Smart Wall permite que os operadores vejam videowalls estáticos conforme definido pelo administrador do sistema com um conjunto fixo de câmeras e layout de monitor. No entanto, o videowall também é controlado pelo operador, no sentido de que os operadores podem controlar o que está sendo exibido. Isso inclui:

- Enviar câmeras e outros tipos de conteúdo para o videowall, como, por exemplo, imagens, textos, alarmes e mapa inteligente
- Enviar visualizações inteiras para os monitores
- No decorrer de certos eventos, aplicando predefinições[2] alternativas

---

[1]Abreviação de "Sistema de Gerenciamento de Vídeo".
[2]Layout predefinido para um ou mais monitores Smart Wall no XProtect Smart Client. As predefinições determinam quais câmeras são exibidas e como o conteúdo é estruturado em cada monitor no videowall.

Finalmente, as mudanças nas exibições podem ser controladas por regras que mudam automaticamente com base em eventos ou programações de hora específicos.

XProtect Transact (explicado)

A Milestone desenvolveu várias extensões. Extensões são produtos que ampliam a funcionalidade dos produtos de VMS da XProtect com recursos especializadas adicionais. Seu arquivo de licença do XProtect controla o acesso às extensões.

> As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

O XProtect Transact é uma extensão para as soluções de vigilância por vídeo IP da Milestone.

XProtect Transact é uma ferramenta para a observação de transações em curso e para investigação de transações no passado. As operações estão relacionadas com a vigilância digital de vídeos monitorando transações, por exemplo, para ajudar a provar fraudes ou fornecer evidências contra um agressor. Há uma relação de 1 para 1 entre linhas de transação e imagens de vídeo.

Os dados da transação podem ser originados de diferentes tipos de fontes de transação, geralmente sistemas de ponto de vendas (PoS) ou caixas eletrônicos.

Milestone Open Network Bridge (explicado)

A Milestone desenvolveu várias extensões. Extensões são produtos que ampliam a funcionalidade dos produtos de VMS da XProtect com recursos especializadas adicionais. Seu arquivo de licença do XProtect controla o acesso às extensões.

Milestone Open Network Bridge é uma interface compatível com ONVIF aberta para compartilhamento de vídeo padronizado de sistemas XProtect VMS para outros sistemas de segurança baseados em IP. Isso permite que as autoridades policiais, os centros de vigilância ou organizações semelhantes (referidas como clientes ONVIF) acessem fluxos de vídeo ao vivo e gravados do sistema XProtect VMS para as soluções de monitoramento central. Os fluxos de vídeo são enviados como fluxos RTSP pela Internet.

Os principais benefícios são:

- Permite a verdadeira interoperabilidade e liberdade de escolha para implantações de segurança de vários fornecedores em larga escala e integração de vídeo público-privado perfeita
- Fornece acesso externo a fluxos de vídeo H.264 e H.265 no sistema XProtect VMS, tanto de vídeo ao vivo quanto de reprodução
- Oferece interfaces padronizadas que fornecem uma maneira fácil e sem problemas de integrar soluções XProtect VMS com centrais de alarme e estações de monitoramento

Este documento fornece o seguinte:

- Informações sobre o padrão ONVIF e links para materiais de referência
- Instruções para instalar e configurar o Milestone Open Network Bridge no seu produto XProtect VMS
- Exemplos de como ativar diversos tipos de clientes ONVIF para transmitir vídeos ao vivo e gravados de produtos XProtect VMS

XProtect DLNA Server (explicado)

> Esse produto já não tem suporte do Milestone.

A Milestone desenvolveu várias extensões. Extensões são produtos que ampliam a funcionalidade dos produtos de VMS da XProtect com recursos especializadas adicionais. Seu arquivo de licença do XProtect controla o acesso às extensões.

DLNA (Digital Living Network Alliance) é um padrão de conexão de dispositivos multimídia. Os fabricantes de produtos eletrônicos certificam seus produtos pelo DLNA para assegurar a interoperabilidade entre diferentes fornecedores e dispositivos, habilitando-os, assim, a distribuir conteúdo de vídeo.

Monitores e TVs públicos frequentemente têm certificação DLNA e estão conectados a uma rede. Eles podem verificar a rede em busca de conteúdo de mídia, conectar-se ao dispositivo e solicitar um fluxo de mídia para seu reprodutor de mídia incorporado. O XProtect DLNA Server pode ser descoberto por certos dispositivos certificados para DLNA e fornecer fluxos de vídeo ao vivo de câmeras selecionadas a dispositivos certificados para DLNA com um reprodutor de mídia.

> Os dispositivos DLNA têm um atraso do vídeo ao vivo de 1 a 10 segundos. Isso é causado por diferentes tamanhos de armazenamento em buffer nos dispositivos.

O XProtect DLNA Server deve estar conectado à mesma rede que o sistema XProtect e o dispositivo DLNA deve estar conectado à mesma rede que o XProtect DLNA Server.

Dispositivos

Hardware (explicado)

Hardware representa:

- A unidade física que se conecta diretamente ao servidor de gravação do sistema de monitoramento via IP, por exemplo, uma câmera, um codificador de vídeo, um módulo de I/O
- Um servidor de gravação em uma base remota em uma configuração Milestone Interconnect

Você tem várias opções para adicionar hardware para cada servidor de gravação em seu sistema.

> Se seu hardware está localizado atrás de um roteador ou um firewall habilitado para NAT, você pode precisar especificar um número de porta diferente e configurar o roteador/firewall para que ele mapeie a porta e os endereços IP que o hardware utiliza.

O assistente **Adicionar hardware** ajuda você detectar hardware como câmeras e codificadores de vídeo na sua rede e adicioná-los ao servidor de gravações no seu sistema. O assistente também ajuda a adicionar servidores de gravação remotos para configurações Milestone Interconnect. Só adicione hardware para **um servidor de gravação** de cada vez.

Pré-configuração de hardware (explicado)

Alguns fabricantes exigem que as credenciais sejam definidas no hardware pronto para uso antes de adicionar o hardware a um sistema VMS pela primeira vez. Isso é conhecido como pré-configuração de hardware e é feito através do assistente **Pré-configurar dispositivos de hardware** que aparece quando tal hardware é detectado pelo assistente Adicionar hardware na página 221.

Algumas informações importantes sobre o assistente **Pré-configuração de dispositivos de hardware**:

- Hardware que requer credenciais iniciais antes de ser adicionado a um sistema VMS não pode ser adicionado usando as credenciais padrão típicas e deve ser configurado através do assistente ou conectando-se diretamente ao hardware
- Você só pode aplicar credenciais (nome de usuário ou senha) aos campos marcados como **não definidos**
- Depois que o **status** do hardware é definido como **configurado**, não é possível alterar as credenciais (nome de usuário ou senha)
- A pré-configuração se aplica ao hardware pronto para uso e precisa ser feita apenas uma vez. Uma vez pré-configurado, o hardware pode ser gerenciado como qualquer outro hardware em Management Client
- Depois de fechar o assistente de **Pré-configuração de dispositivos de hardware**, o hardware pré-configurado aparecerá no assistente de Adicionar hardware na página 221 e agora pode ser adicionado ao seu sistema

> É altamente recomendável que você adicione o hardware pré-configurado ao seu site concluindo o assistente Adicionar hardware na página 221 após fechar o assistente **Pré-configuração de dispositivos de hardware**. Management Client não reterá as credenciais pré-configuradas se você não adicionar o hardware ao seu sistema.

Dispositivos (explicado)

Há uma série de dispositivos de hardware que podem ser gerenciados individualmente, p. ex.:

- Uma câmera física tem dispositivos, anexados e/ou embutidos, relativos à parte da câmera (lentes), bem como microfones, alto-falantes, metadados, entrada e saída
- Um codificador de vídeo tem várias câmeras analógicas conectadas, mostradas em uma lista de dispositivos, anexados e/ou embutidos, relativos à parte da câmera (lentes), bem como microfones, alto-falantes, metadados, entrada e saída
- Um módulo de I/O tem dispositivos referentes aos canais de entrada e saída para, p. ex., luzes
- Um módulo de áudio dedicado tem dispositivos referentes microfones e entradas e saídas de alto-falante
- Numa configuração Milestone Interconnect, o sistema remoto aparece como hardware com todos os dispositivos relacionados em uma lista

O sistema acrescenta automaticamente todos os dispositivos do hardware quando você adiciona hardware.

Para obter informações sobre o hardware suportado, consulte a página hardware compatível no site da Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

As seções a seguir descrevem cada um dos tipos de dispositivo que você pode adicionar.

Câmeras

Os dispositivos de câmera enviam transmissões de vídeo ao sistema que os usuários do cliente podem usar para assistir ao vivo ou que o sistema pode gravar para reprodução posterior pelos usuários do cliente. Funções determinam a permissão dos usuários para assistir a vídeos.

Microfones

Em muitos dispositivos, você pode conectar microfones externos. Alguns dispositivos têm microfones embutidos.

Os dispositivos de microfone enviam transmissões de áudio ao sistema que os usuários do cliente podem usar para ouvir ao vivo ou que o sistema pode gravar para reprodução posterior pelos usuários do cliente. Você pode configurar o sistema para receber eventos específicos de microfone que desencadearão ações.

As funções determinam a permissão dos usuários para ouvir os microfones. Você não pode ouvir microfones do Management Client.

Alto-falantes

Em muitos dispositivos, você pode conectar alto-falantes externos. Alguns dispositivos têm alto-falantes embutidos.

O sistema envia um fluxo de áudio para os alto-falantes quando um usuário pressiona o botão de fala no XProtect Smart Client Você também pode usar esse recurso de XProtect Web Client e XProtect® Mobile. O áudio do alto-falante só é registrado quando há fala de um usuário. Funções determinam a permissão dos usuários para falar através dos alto-falantes. Você não pode falar através dos alto-falantes do Management Client.

Se dois usuários quiserem falar ao mesmo tempo, as funções determinam a permissões para usuários falarem pelos alto-falantes. Como parte das definições de funções é possível especificar uma prioridade para o alto-falante de muito alta até muito baixa. Se dois usuários querem falar ao mesmo tempo, o usuário cuja função tem maior prioridade ganhará a capacidade de falar. Se dois usuários com a mesma função quiserem falar ao mesmo tempo, o princípio de quem chegar primeiro se aplica.

Metadados

Dispositivos de metadados transferem fluxos de dados para o sistema que os usuários do cliente podem usar para saber informações sobre os dados, por exemplo, dados que descrevem a imagem de vídeo, o conteúdo ou objetos na imagem, ou o local onde a imagem foi gravada. Os metadados podem ser ligados a câmeras, microfones ou alto-falantes.

Os metadados podem ser gerados por:

- O próprio dispositivo entregando os dados, por exemplo, uma câmera entregando vídeo
- Um sistema de terceiros ou integração através de um driver genérico de metadados

Os metadados gerados pelo dispositivo são automaticamente ligados a um ou mais dispositivos do mesmo hardware.

Funções determinam a permissão dos usuários para ver metadados.

Entradas

Em muitos dispositivos, você pode anexar unidades externas a portas de entrada do dispositivo. Unidades de entrada são geralmente sensores externos. Tais sensores podem ser usados, p.ex., para detectar se portas, janelas ou portões são abertos. A entrada de tais unidades externas é tratada como eventos pelo sistema.

Você pode usar esses eventos em regras. P. ex., você pode criar uma regra especificando que a câmera deve começar a gravação quando uma entrada é ativada e parar a gravação 30 segundos depois que a entrada for desativada.

Saídas

Em muitos dispositivos, você pode anexar unidades externas a portas de saídas do dispositivo. Isso permite a você ativar/desativar luzes, sirenes etc. através do sistema.

Você pode usar saídas ao criar regras. Você pode criar regras que ativam ou desativam automaticamente saídas e regras que desencadeiam ações quando o estado de uma saída é alterado.

Grupos de dispositivos (explicado)

O agrupamento de dispositivos em grupos de dispositivos faz parte do Assistente **Adicionar hardware**, mas você pode sempre modificar os grupos e adicionar mais grupos, caso necessário.

Você pode se beneficiar de agrupar diferentes tipos de dispositivos (câmeras, microfones, alto-falantes, metadados, entradas e saídas) no seu sistema:

- Grupos de dispositivos ajudam a manter uma visão geral intuitiva de dispositivos no seu sistema.
- Os dispositivos podem existir em vários grupos
- Você pode criar subgrupos e subgrupos em subgrupos
- Você pode especificar as propriedades comuns a todos os dispositivos dentro de um grupo de dispositivos de uma só vez
- As propriedades dos dispositivos definidas através do grupo não são armazenadas para o grupo, mas nos dispositivos individuais
- Ao lidar com funções, você pode especificar as configurações de segurança comuns para todos os dispositivos dentro de um grupo de dispositivos de uma só vez
- Ao lidar com regras, você pode aplicar uma regra a todos os dispositivos dentro de um grupo de dispositivos de uma só vez

Você pode adicionar tantos grupos de dispositivos quantos necessários, mas não pode misturar diferentes tipos de dispositivos (por exemplo, câmeras e alto-falantes) em um grupo de dispositivos.

Crie grupos de dispositivos com **menos** que 400 dispositivos para que você possa visualizar e editar todas as propriedades.

Se você excluir um grupo de dispositivos, só poderá excluir o próprio grupo de dispositivos. Se você desejar excluir um dispositivo, por exemplo, uma câmera, a partir de seu sistema, faça isso no nível do servidor de gravação.

Os exemplos que se seguem são baseados no agrupamento de câmeras em grupos de dispositivos, mas os princípios aplicam-se a todos os dispositivos

Adicionar um grupo de dispositivos

Especificar quais dispositivos incluir em um grupo de dispositivos

Especificar as propriedades comuns para todos os dispositivos em um grupo de dispositivos

Armazenamento de mídia

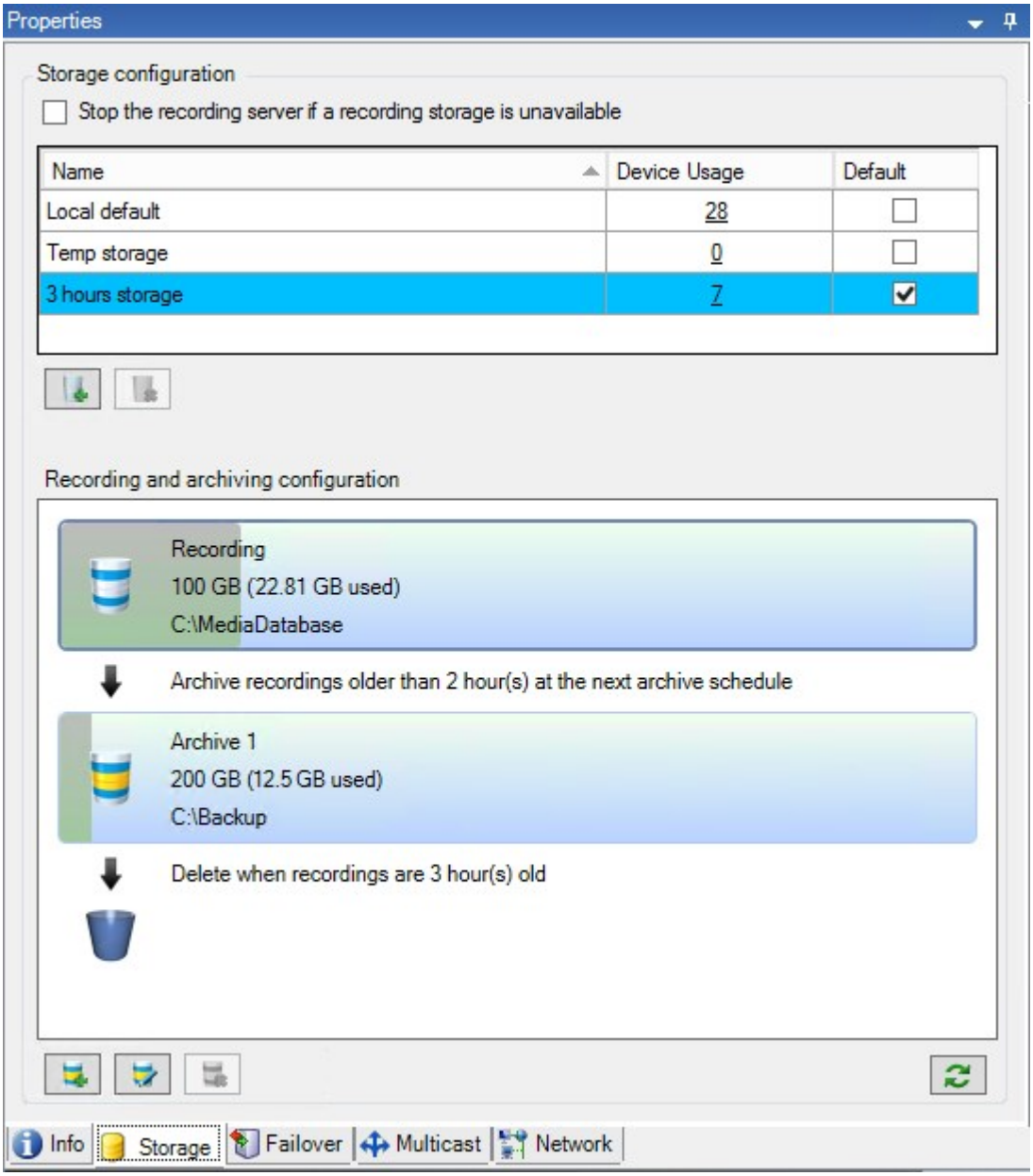
Armazenamento e arquivamento (explicado)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Na guia **Armazenamento**, você pode configurar, gerenciar e visualizar armazenamentos para os servidores de gravação selecionados.

Para armazenamento e arquivos de gravação, a barra horizontal mostra a quantidade atual de espaço livre. Você pode especificar o comportamento do servidor de gravação no caso de armazenamento de gravações ficar disponível. Isso é principalmente relevante se seu sistema inclui servidores de emergência.

Se estiver usando a **Proteção de evidências**, haverá uma linha vermelha vertical mostrando o espaço usado para filmagens de proteção de evidências.



Quando uma câmera grava um vídeo ou um áudio, todas as gravações especificadas ficam guardadas, por padrão, no armazenamento definido para o dispositivo. Cada armazenamento consiste em um armazenamento de gravação que salva gravações no banco de dados de **Gravação**. Um armazenamento não tem arquivo(s) padrão, mas você pode criá-los.

Para evitar que o banco de dados de gravação fique cheio, você pode criar armazenamentos adicionais (consulte Adicionar um novo armazenamento na página 206). Você também pode criar arquivos (consulte Criar um arquivo dentro de um armazenamento na página 206) dentro de cada armazenamento e iniciar um processo de arquivamento para armazenar dados.

Arquivamento é a transferência automática de gravações do, por exemplo, banco de dados de gravação de uma câmera para uma outra localização. Deste modo, a quantidade de gravações que você pode armazenar não é limitada pelo tamanho do banco de dados de gravação. Com o arquivamento, você também pode fazer backup de suas gravações em outra mídia.

Você configura o armazenamento e o arquivamento em cada servidor de gravação.

Contanto que você armazene gravações arquivadas localmente ou em unidades de rede acessíveis, você pode usar XProtect Smart Client para visualizá-las.

Se uma unidade de disco quebrar e o armazenamento de gravação tornar-se indisponível, a barra horizontal fica vermelha. Ainda é possível visualizar o vídeo ao vivo em XProtect Smart Client, mas a gravação e o arquivamento param até que o disco do driver seja restaurado. Se o seu sistema estiver configurado com servidores do sistema de gravação ininterrupta, você pode especificar que o servidor de gravação interrompa a execução para que os servidores failover assumam (consulte Especifique o comportamento quando não houver armazenamento de gravação disponível. na página 204).

A seguir, mencionam-se principalmente câmeras e vídeos, mas alto-falantes, microfones, áudio e som também se aplicam.

A Milestone recomenda que você use uma unidade de disco rígido dedicada para gravar o banco de dados do servidor para evitar um desempenho fraco do disco. Ao formatar o disco rígido, é importante alterar a configuração do seu **Tamanho da unidade de alocação** de 4 para 64 kilobytes. Esse procedimento irá melhorar significativamente o desempenho de gravação do disco rígido. Você pode ler mais sobre tamanhos de unidades de alocação e encontrar ajuda no site da Microsoft (https://support.microsoft.com/en-us/topic/default-cluster-size-for-ntfs-fat-and-exfat-9772e6f1-e31a-00d7-e18f-73169155af95).

Os dados mais antigos no banco de dados sempre são auto-arquivados (ou excluídos se nenhum arquivamento seguinte for definido) quando houver menos de 5GB de espaço livre. Se houver menos de 1GB de espaço livre, os dados são excluídos. Um banco de dados sempre requer 250MB de espaço livre. Se você atingir esse limite porque os dados não são excluídos com rapidez suficiente, as tentativas de gravação no banco de dados podem falhar e, nesse caso, nenhum outro dado é gravado no banco de dados até que você libere espaço suficiente. O tamanho máximo real do banco de dados é a quantidade de gigabytes que você especificar menos 5GB.

Para sistemas compatíveis com FIPS 140-2, com exportações e bancos de dados de mídia arquivados de versões anteriores à 2017 R1 do XProtect VMS que são criptografados com cifras não compatíveis com FIPS, é necessário arquivar os dados em um local onde ainda possam ser acessados após a ativação do FIPS. Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

Conexão de dispositivos de armazenamento

Uma vez que você tenha definido as configurações de armazenamento e arquivamento para um servidor de gravação, você poderá habilitar arquivamento para câmeras individuais ou um grupo de câmeras. Você faz isso a partir dos dispositivos individuais ou do grupo de dispositivos. Consulte Anexar um dispositivo ou um grupo de dispositivos a um armazenamento na página 206.

Arquivamento efetivo

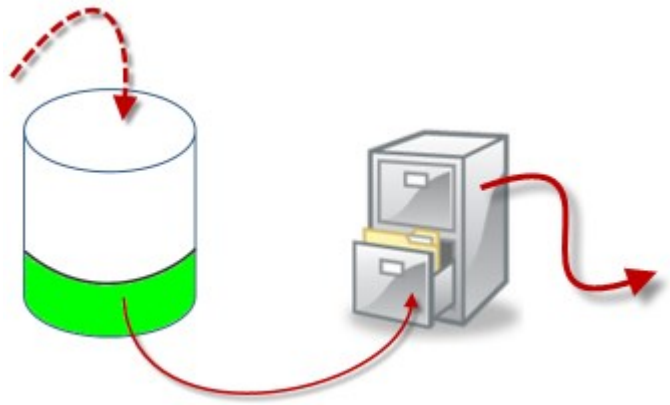
Quando você habilita o arquivamento para uma câmera ou grupo de câmeras, o conteúdo do armazenamento de gravação é automaticamente movido para um arquivo, em intervalos que você define.

Dependendo de seus requisitos, você pode configurar um ou mais arquivos para cada um de seus armazenamentos. Os arquivos podem ser localizados tanto no próprio computador do servidor de gravação, ou em qualquer outro local, o que pode ser alcançado pelo sistema, por exemplo, em uma unidade de rede.

Ao definir o seu arquivamento de uma maneira eficaz, você pode otimizar necessidades de armazenamento. Muitas vezes, você deseja que as gravações arquivadas ocupem o mínimo de espaço possível, especialmente a longo prazo, onde talvez seja possível diminuir um pouco a qualidade da imagem. Você lida com todo o armazenamento eficaz a partir da guia **Armazenamento** de um servidor de gravação, ajustando várias configurações interdependentes:

- Retenção de armazenamento de gravação
- Tamanho do armazenamento de gravação
- Retenção de arquivo
- Tamanho do arquivo
- Agenda do arquivo
- Criptografia
- Quadros por segundo (FPS).

O tamanho dos campos define o tamanho do armazenamento de gravação da câmera, exemplificado pelo cilindro e seu(s) arquivo(s) respectivamente:



Para fins de configuração de retenção de tempo e tamanho para o armazenamento de gravação, exemplificada pela área branca do cilindro, você define o quão antigas as gravações devem ser antes que sejam arquivadas. No nosso exemplo ilustrado, você arquiva as gravações quando elas forem antigas o suficiente para serem arquivadas.

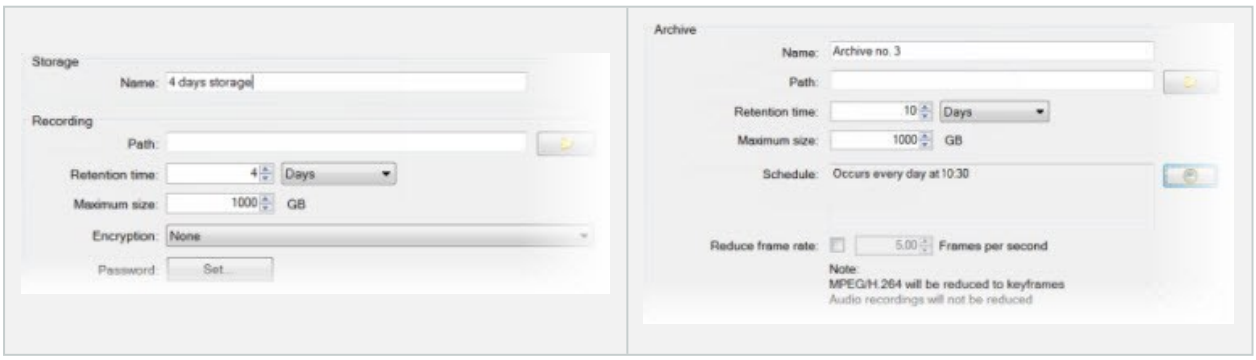
O tempo de retenção e definição de tamanho para arquivos define quanto tempo as gravações permanecem no arquivo. As gravações permanecem no arquivo durante o tempo especificado, ou até que o arquivo tenha atingido o limite de tamanho especificado. Quando essas configurações forem satisfeitas, o sistema começa a substituir gravações antigas no arquivo.

A agenda de arquivamento define com que frequência e quando o arquivamento acontece.

FPS determina o tamanho dos dados nos bancos de dados.

Para arquivar suas gravações, você deve definir todos estes parâmetros de acordo com cada um deles. Isso significa que o período de retenção para o próximo arquivo deve sempre ser maior que o período de retenção de um arquivo ou banco de dados de gravação atuais. Isso é porque o número de dias de retenção indicados por um arquivo inclui todas as retenções em processos anteriores. O arquivamento deve também acontecer com mais frequência do que o período de retenção, senão, você corre o risco de perder dados. Se você tem um tempo de retenção de 24 horas, qualquer dado mais antigo que 24 horas é apagado. Portanto, para ter seu banco de dados movido com segurança para o próximo arquivo é importante executar um arquivamento com uma frequência maior do que 24 horas.

Exemplo: Esses armazenamentos (imagem à esquerda) têm um tempo de retenção de 4 dias e o arquivo seguinte (imagem à direita) um tempo de retenção de 10 dias. O arquivamento é definido para ocorrer todos os dias às 10:30, garantindo um arquivamento muito mais frequente do que o tempo de retenção.



Você também pode controlar o arquivamento por meio do uso de regras e eventos.

Estrutura de arquivo (explicado)

Quando você arquiva gravações, elas são armazenadas em uma certa estrutura de sub-diretório dentro do arquivo.

> Durante todo o uso regular do seu sistema, a estrutura de sub-diretório é completamente transparente aos usuários do sistema, à medida que eles navegam por todas as gravações com o XProtect Smart Client, independentemente de se as gravações estão arquivadas ou não. Conhecer a estrutura de sub-diretório é principalmente interessante se você quiser fazer backup de suas gravações arquivadas.

Em cada um dos diretórios de arquivos do servidor de gravação, o sistema cria automaticamente sub-diretórios separados. Esses sub-diretórios são nomeados depois do nome do dispositivo e do banco de dados do arquivo.

Visto que você pode armazenar gravações de diferentes câmeras no mesmo arquivo e desde que o arquivamento de cada câmera possa ser realizada em intervalos regulares, mais diretórios são automaticamente adicionados.

Esses sub-diretórios representam aproximadamente uma hora de gravações cada. A divisão de uma hora torna possível remover apenas pequenas partes relativamente de um dado do arquivo se você atinge o tamanho máximo do arquivo.

Os sub-diretórios são nomeados de acordo com o dispositivo, seguido por uma indicação de onde as gravações vêm (armazenagem no dispositivo u via SMTP), **mais** a data e a hora do registro mais recente no banco de dados contido no subdiretório.

Estrutura de nomes

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most
recent recording]\
```

Se veio do armazenagem no dispositivo:

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of
most recent recording]\
```

Se partir da SMTP:

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of
most recent recording]\
```

Exemplo da vida real

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

Subdiretórios

Mesmo mais tarde sub-diretórios são adicionados automaticamente. A quantidade e natureza desses sub-diretórios dependem da natureza das gravações atuais. Por exemplo, vários sub-diretórios diferentes serão adicionados, se as gravações forem tecnicamente divididas em sequências. Este é frequentemente o caso, se você tiver usado a detecção de movimento para disparar gravações.

- **Mídia (Media)**: Esta pasta contém a mídia existente que pode ser vídeo ou áudio (não ambos)
- **Nível de movimento (MotionLevel)**: Esta pasta contém grades de nível de movimento geradas a partir dos dados de vídeo usando nosso algoritmo de detecção de movimento. Estes dados permitem que o recurso de pesquisa inteligente em XProtect Smart Client faça pesquisas muito rápidas.
- **Movimento (Motion)**: Nesta pasta, o sistema armazena sequências de gravação. Uma sequência de movimento é uma fatia de tempo para a qual o movimento foi detectado nos dados de vídeo. Esta informação é, por exemplo, usada na linha do tempo em XProtect Smart Client
- **Gravando**: Nesta pasta, o sistema armazena sequências de gravação. Uma sequência de gravação é uma fatia de tempo para a qual existem gravações coerentes de dados de mídia. Esta informação é, por exemplo, usada para traçar a linha do tempo em XProtect Smart Client.
- **Assinatura**: Esta pasta detém as assinaturas geradas para os dados de mídia (na pasta Mídia). Com essa informação, você pode verificar que os dados de mídia não foram adulterados desde ela foi gravada

Se quiser fazer backup de seus arquivos, você pode direcionar seus backups se souber o básico da estrutura do sub-diretório.

Exemplos de backup

Para fazer um backup do conteúdo de um arquivo inteiro, faça um backup do diretório do arquivo solicitado e todos os seu conteúdos. Por exemplo tudo em:

```
...F:\OurArchive\
```

Para fazer um backup de gravações de uma câmera particular para um período de tempo particular, faça o backup apenas de conteúdos de sub-diretórios relevantes. Por exemplo tudo em:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

Pré-buffer e armazenamento de gravações (explicado)

Pré-buffering é a capacidade de gravar áudio e vídeo antes do evento desencadeante real ocorrer. Isto é útil quando você quer gravar o áudio ou vídeo que leva até um evento que aciona a gravação, por exemplo, abrir uma porta.

Pré-buffer é possível porque o sistema recebe continuamente os fluxos de áudio e vídeo a partir de dispositivos conectados e armazena-os temporariamente para o período de pré-buffer definido.

- Se uma regra de gravação é acionada, as gravações temporárias se tornam permanentes pelo tempo de pré-gravação configurado da regra
- Se nenhuma regra de gravação é disparada, as gravações temporárias no pré-buffer são apagadas automaticamente após o tempo de pré-buffer definido

Armazenamento das gravações temporárias de pré-buffer

Você pode escolher o local de armazenamento das gravações temporárias do pré-buffer:

- Na memória; o período pré-buffer é limitado a 15 segundos.
- No disco (no banco de dados de mídia); você pode escolher todos os valores.

O armazenamento na memória em vez de no disco melhora o desempenho do sistema, mas só é possível por períodos mais curtos de pré-buffer.

Quando as gravações são armazenadas na memória e você transforma algumas das gravações temporárias em permanentes, as restantes gravações temporárias são eliminadas e não podem ser recuperadas. Se você precisa ser capaz de manter as gravações restantes, armazene as gravações no disco.

Autenticação

Active Directory (explicado)

O Active Directory é um serviço de diretório distribuído implementado pela Microsoft para redes de domínio Windows. É parte integrante da maioria dos Sistemas operacionais Windows Server. Sua função é identificar recursos em uma rede para que os usuários ou aplicativos os acessem.

Com o Diretório Ativo (Active Directory) instalado você pode adicionar usuários Windows do Diretório Ativo, mas também é permitido adicionar usuários sem o Active Directory. Há certas limitações do sistema relacionadas aos usuários básicos.

Usuários (explicado)

O termo **usuários** se refere primariamente a usuários que se conectam ao sistema de monitoramento por meio de clientes. Você pode configurar tais usuários de duas formas:

- Como **Usuários básicos**, autenticados por uma combinação de nome de usuário/senha
- Como **Usuários do Windows** autenticados com base no login do Windows.

Usuários do Windows

Usuários do Windows podem ser adicionados através do Active Directory. O Active Directory (Diretório Ativo, AD) é um serviço de diretório distribuído implementado pela Microsoft para redes de domínio Windows. É parte integrante da maioria dos Sistemas operacionais Windows Server. Sua função é identificar recursos em uma rede para que os usuários ou aplicativos os acessem. O Active Directory usa os conceitos de usuários e grupos.

Usuários são objetos do Active Directory representando indivíduos com uma conta de usuário. Exemplo:

Grupos são objetos do Active Directory capazes de conter vários usuários. Neste exemplo, o grupo de gerenciamento tem três membros:

Os grupos podem conter qualquer número de usuários. Ao adicionar um grupo ao sistema, você adiciona todos os seus membros de uma só vez. Após adicionar o grupo ao sistema, as alterações feitas ao grupo no Active Directory (tais como novos membros adicionados ou antigos membros removidos) em uma fase posterior são imediatamente refletidas no sistema. Um usuário pode ser membro de mais de um grupo ao mesmo tempo.

Você pode usar o Active Directory para adicionar informações de usuários e grupos existentes ao sistema com algumas vantagens:

- Usuários e grupos são especificados de forma central no Active Directory, assim você não precisará criar qualquer conta de usuário a partir do zero
- Isso também significa não é necessário configurar qualquer tipo de autenticação de usuários no sistema, posto que o Active Directory cuide da autenticação

Antes de adicionar usuários e grupos através do serviço do Active Directory é necessário ter um servidor com Active Directory instalado na rede.

Usuários básicos

Se o seu sistema não possui acesso ao Active Directory, você deve criar um usuário básico. Para obter informações sobre como configurar usuários básicos, consulte Criação de usuários básicos na página 298.

Identity Provider (explicado)

Identity Provider app pool (IDP) é uma entidade do sistema que cria, mantém e gerencia informações de identidade para usuários básicos.

Identity Provider também fornece serviços de autenticação e registro para aplicativos ou serviços confiáveis, neste caso: Servidor de gravação, servidor de gerenciamento, Data Collector e servidor de relatório.

Quando você efetua login em clientes e serviços XProtect como usuário básico, sua solicitação vai para o Identity Provider. Quando autenticado, o usuário pode chamar o servidor de gerenciamento.

O Identity Provider é executado no IIS como parte do servidor de gerenciamento usando o mesmo SQL Server com um banco de dados distinto, sendo responsável por criar e processar tokens de comunicação OAuth que os serviços usam durante a comunicação (Surveillance_IDP).

Registros Identity Provider podem ser encontrdos em: `\\ProgramData\Milestone\IDP\Logs`.

IDP externo (explicação)

IDP é a sigla de Identity Provider. Um IDP externo é um serviço e aplicativo externo em que é possível armazenar e gerenciar informações de identidade de usuário e fornecer serviços de autenticação de usuário para outros sistemas. Você pode associar um IDP externo ao VMS XProtect.

XProtect VMS suporta IDPs externos que são compatíveis com o Connect (OIDC) OpenID.

Reivindicações (explicado)

Alegações formam o vínculo entre o IDP externo e o VMS XProtect.

Uma reivindicação é uma declaração que uma entidade, como um usuário ou um aplicativo, faz sobre si mesma. No VMS XProtect, uma reivindicação pode ser associada a uma função que determina as permissões do XProtect dos usuários.

A reivindicação consistem em um nome de reivindicação e um valor de reivindicação. Por exemplo, o nome da reivindicação pode ser um nome padrão que descreve o conteúdo do valor da reivindicação, e o valor da reivindicação pode ser o nome de um grupo. Veja mais exemplos de alegações de um IDP externo: Exemplo de reivindicações de um IDP externo.

Ativar usuários para fazer login no VMS XProtect a partir de um IDP externo

- A partir do IDP externo, crie os usuários. Além disso, é preciso identificar o VMS XProtect e a interação entre XProtect e o IDP externo. Finalmente, crie as alegações para identificar usuários como usuários de IDP externo no VMS XProtect.

- A partir do VMS XProtect, crie uma configuração que permita que o Identity Provider entre em contato com o IDP externo. Para mais informações sobre como criar uma configuração para um IDP externo, consulte Adicionar e configurar um IDP externo.
- Do VMS XProtect, estabeleça a autenticação de usuários mapeando as alegação do usuário do IDP externo às funções XProtect. Para obter mais informações sobre como mapear alegações para funções, consulte Mapear alegações de um IDP externo para funções em XProtect.

URIs redirecionados

O URI redirecionado especifica a página à qual o usuário é enviado após uma autenticação bem-sucedida. No seu IDP externo, você tem que adicionar o endereço do servidor de gerenciamento seguido pelo **caminho de retorno de chamada** que definiu no XProtect Management Client. Por exemplo, o https://management-server-computer.company.com/idp/signin-oidc

Nomes de usuário exclusivos para usuários de IDP externo

Nomes de usuários são criados automaticamente para usuários que fazem login no Milestone XProtect por meio de um IDP externo.

O IDP externo fornece um conjunto de alegações para criar automaticamente um nome para o usuário em XProtect e em XProtect um algoritmo é usado para escolher um nome a partir de um IDP externo que seja exclusivo no banco de dados de VMS.

Exemplo de alegações de um IDP externo

As reivindicações consistem em um nome de reivindicação e um valor de reivindicação. Por exemplo:

Nome da reivindicação	Valor da reivindicação
nome	Raz Van
e-mail	123@domain.com
amr	pwd
idp	00o2ghkgazGgi9BIE5d7
preferred_ username	321@domain.com

Nome da reivindicação	Valor da reivindicação
vmsRole	Operador
locale	en-US
given_name	Raz
family_name	Lindberg
zoneinfo	América/Los_Angeles
email_verified	Verdadeiro

Usando o número de sequência da reivindicação para criar nomes de usuário em XProtect

No XProtect, a prioridade de busca para criar um usuário no VMS XProtect pelo número de sequência das reivindicações na tabela abaixo. O primeiro nome de reivindicação disponível será usado no VMS XProtect:

Nome da reivindicação	Número sequencial	Descrição
UserNameClaimType	1	Mapeamento configurado com uma declaração para definir o nome de usuário. A alegação é definida no campo **Alegação a ser usada para criar nome de usuário** na guia **IDP externo** em **Ferramentas** > **Opções**.
preferred_username	2	Alegação que pode vir do IDP externo. Uma alegação padrão que é normalmente usada para isso em Oidc (OpenID Connect).
nome	3	
given_name family_ name	4	Nome e sobrenome em uma combinação como Bob Johnson.

Nome da reivindicação	Número sequencial	Descrição
e-mail	5	
Primeira reivindicação disponível + #(primeiro número disponível)	6	Por exemplo, Bob# 1

Definindo reivindicações específicas para criar nomes de usuário no XProtect

Os administradores do XProtect podem definir uma alegação específica a partir do IDP externo que deve ser usada para criar um nome de usuário no VMS XProtect. Quando um administrador define uma alegação a ser usada para a criação do nome de usuário no VMS XProtect, o nome da alegação deve ser escrito exatamente como o nome da alegação que vem do IDP externo.

- A alegação a ser usada para o nome de usuário pode ser definida no campo **Alegação a ser usada para criar nome de usuário** na guia **IDP externo** em **Ferramentas** > **Opções**.

Excluindo usuários do IDP externo

Os usuários criados em XProtect por um login em IDP externo são excluídos da mesma forma que um usuário básico e o usuário pode ser excluído a qualquer momento depois que o usuário é criado.

Se um usuário for excluído no XProtect e o usuário fizer login novamente a partir de um IDP externo, um novo usuário será criado em XProtect. No entanto, os dados associados ao usuário no XProtect, como exibições e funções privadas, são perdidos e essas informações precisam ser criadas novamente para o usuário no XProtect.

Se um IDP externo for excluído no Management Client, quaisquer usuários conectados ao VMS via IDP externo também serão excluídos.

Segurança

Funções e permissões de uma função (explicado)

Todos os usuários em Milestone XProtect VMS pertencem a uma função.

A função define as permissões dos usuários, incluindo os dispositivos que os usuários podem acessar. As funções também determinam as permissões de segurança e acesso no sistema de gerenciamento de vídeo.

O sistema vem com uma função **Administradores** padrão, a qual tem acesso total a todas as funcionalidades do sistema; contudo, na maioria dos casos, você precisa ter mais de mais de uma função em seu sistema para diferenciar entre usuários e o acesso que eles deveriam ter. Você pode adicionar quantas funções forem necessárias. Consulte Atribuir/remover usuários e grupos para/de funções na página 297.

Por exemplo, talvez você precise configurar tipos diferentes de funções para usuários de XProtect Smart Client, dependendo dos dispositivos aos quais quer que eles tenham acesso, ou tipos semelhantes de restrições que precisem de diferenciação entre usuários.

Para criar uma diferenciação entre usuários, você precisa:

- Criar e configurar as funções de que você precisa para suprir as necessidades de negócios da sua organização
- Adicionar usuários e grupos de usuários que você atribua às funções às quais eles pertencem
- Criar perfis no Smart Client e perfis no Management Client para definir o que os usuários podem ver no XProtect Smart Client e na interface de usuário do Management Client.

  As funções controlam somente suas permissões de acesso, não o que os usuários podem ver em sua interface de usuário no XProtect Smart Client ou no Management Client. Você não precisa criar um perfil específico no Management Client para usuários que nunca usarão o Management Client.

Para garantir a melhor experiência de usuário possível aos usuários do XProtect Smart Client e do Management Client com acesso limitado a funcionalidades do Management Client, você tem que garantir que haja consistência entre as permissões fornecidas pela função e os elementos da interface de usuário fornecidos pelo perfil do Smart Client ou Management Client.

> Para ter acesso ao Management Server, é importante que todas as funções tenham a permissão de segurança **Conectar** ativada. A permissão é encontrada em **Configurações de função** > **Management Server** > Guia Segurança Geral (funções) na página 528.

Para configurar as funções no sistema, expanda **Segurança** > **Funções**.

Permissões de uma função

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Ao criar uma função em seu sistema, você pode atribuir essa função a uma série de permissões para os componentes ou recursos do sistema que a função relevante pode acessar e usar.

Por exemplo, você pode querer criar funções que tenham permissões apenas para acessar funcionalidades no XProtect Smart Client ou outros clientes de visualização do Milestone, com permissões para visualizar apenas determinadas câmeras. Se você criar essas funções, essas funções não devem ter permissões para acessar e usar o Management Client, mas apenas ter acesso a algumas ou todas as funcionalidades encontradas no XProtect Smart Client ou em outros clientes.

Para resolver essa necessidade de diferenciação, você configura uma função que tenha algumas ou as permissões mais comuns de administrador, por exemplo, as permissões para adicionar e remover câmeras, servidores e funcionalidades semelhantes. Você pode criar funções que tenham algumas ou a maioria das

permissões de um administrador do sistema. Isto pode ser importante, p. ex., se a sua organização quiser separar pessoas que podem administrar um subconjunto do sistema das pessoas que podem administrar todo o sistema.

Funções dão a você a possibilidade de fornecer permissões de administradores diferenciadas para acessar, editar ou alterar uma ampla variedade de funções do sistema. Por exemplo: a permissão de editar as configurações de servidores ou câmeras no seu sistema. Você especifica essas permissões na guia **Segurança geral** (consulte Guia Segurança Geral (funções) na página 528). Para permitir que o administrador do sistema diferenciado possa iniciar o Management Client, você tem que conceder permissões de leitura para a função no servidor de gerenciamento.

> Para ter acesso ao Management Server, é importante que todas as funções tenham a permissão de segurança **Conectar** ativada. A permissão é encontrada em **Configurações de função** > **Management Server** > Guia Segurança Geral (funções) na página 528.

Também se pode fazer refletir as mesmas limitações na interface do usuário do Management Client para cada função, associando-a um perfil do Management Client do qual tenham sido removidas as funções do sistema correspondentes da interface do usuário. Consulte Perfis Management Client (explicado) na página 76 para obter mais informaões.

Para conceder a uma função tais permissões de administrador diferenciadas, a pessoa com a função de administrador completo padrão deve configurar a função em **Segurança** > **Funções > guia Informações > Adicionar novo**. Após configurar a nova função, você pode, então, associar a função aos seus próprios perfis de forma semelhante a quando cria qualquer outra função no sistema ou utilizar perfis padrão do sistema. Para obter mais informações, consulte Adicionar uma função de gerenciamento na página 296.

Depois de especificar a quais perfis você deseja associar a função, vá para a guia **Segurança geral** para especificar as permissões da função.

> As permissões que você pode definir para uma função são diferentes entre seus produtos. Você só pode conceder todas as permissões disponíveis para uma função em XProtect Corporate.

Máscara de privacidade (explicada)

Máscara de privacidade (explicado)

Com a máscara de privacidade, você pode definir as áreas do vídeo de uma câmera que você deseja cobrir com máscaras de privacidade quando mostradas nos clientes. Por exemplo, se uma câmera de vigilância cobre uma rua, você pode cobrir certas áreas de um edifício (isso poderiam ser janelas e portas) com máscaras de privacidade, a fim de proteger a privacidade dos moradores. Em alguns países, este é um requisito legal.

Você pode especificar máscaras de privacidade como sólidas ou desfocadas. As máscaras cobrem vídeo ao vivo, gravado e exportado.

As máscaras de privacidade são aplicadas e bloqueadas em uma área da imagem da câmera, de modo que a área coberta não siga os movimentos pan-tilt-zoom, mas cubram constantemente a mesma área da imagem da câmera. Em algumas câmeras PTZ, você pode ativar a máscara de privacidade baseada em posição na própria câmera.

Existem dois tipos de máscaras de privacidade:

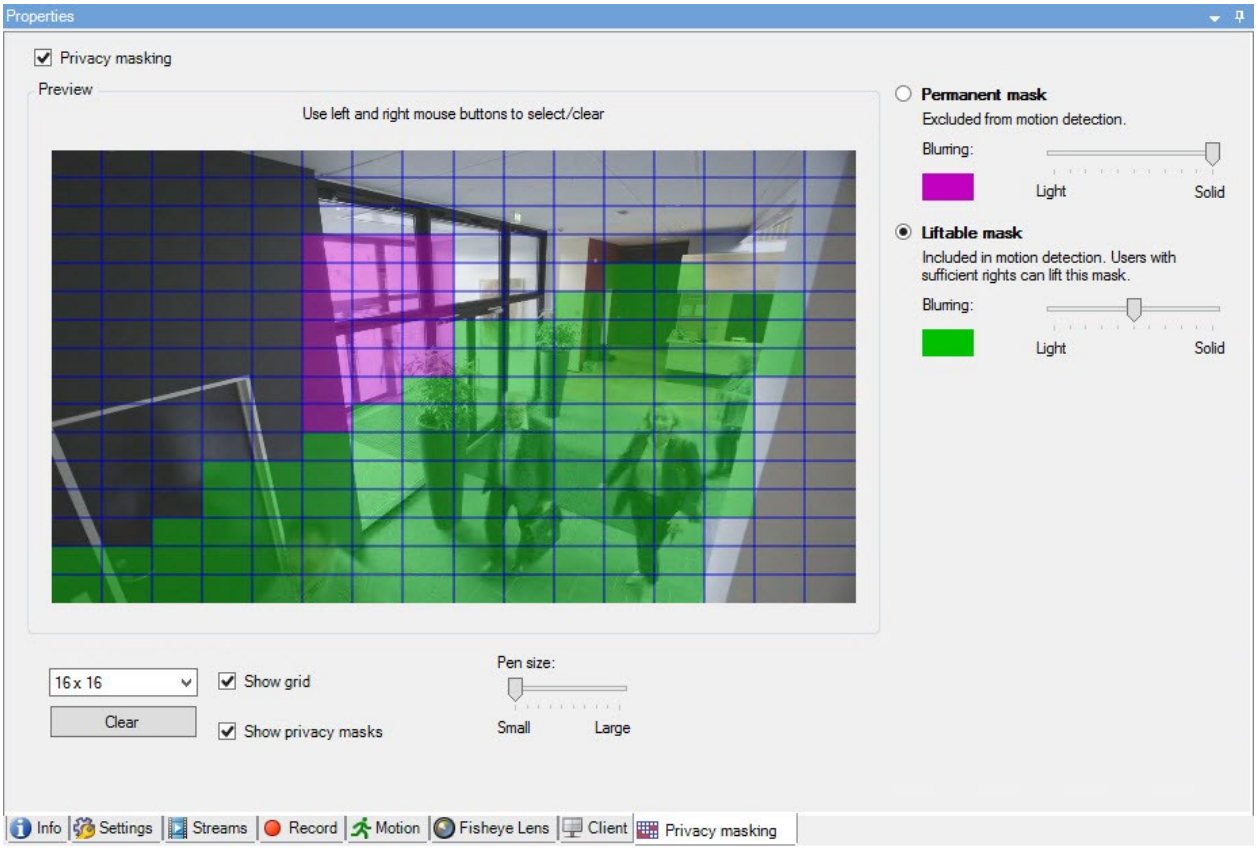
- **Máscara de privacidade permanente**: Áreas com este tipo de máscara estão sempre cobertas nos clientes. Pode ser usada para cobrir áreas do vídeo que nunca requerem vigilância, como áreas públicas ou áreas onde a vigilância não é permitida. A detecção de movimento é excluída de áreas com máscaras de privacidade permanentes
- **Máscara de privacidade removível**: Áreas com este tipo de máscara podem ser temporariamente descobertas no XProtect Smart Client por usuários com permissão para remover máscaras de privacidade. Se o usuário XProtect Smart Client logado não tiver permissão para levantar máscaras de privacidade, o sistema solicitará que um usuário com permissão autorize o levantamento. Máscaras de privacidade são removidas até o tempo limite ou até que o usuário as reaplique. Esteja ciente de que máscaras de privacidade são removidas no vídeo de todas as câmeras às quais o usuário tem acesso

Se você atualizar de um sistema 2017 R3 ou mais antigo com máscaras de privacidade aplicadas, as máscaras serão convertidas em máscaras removíveis.

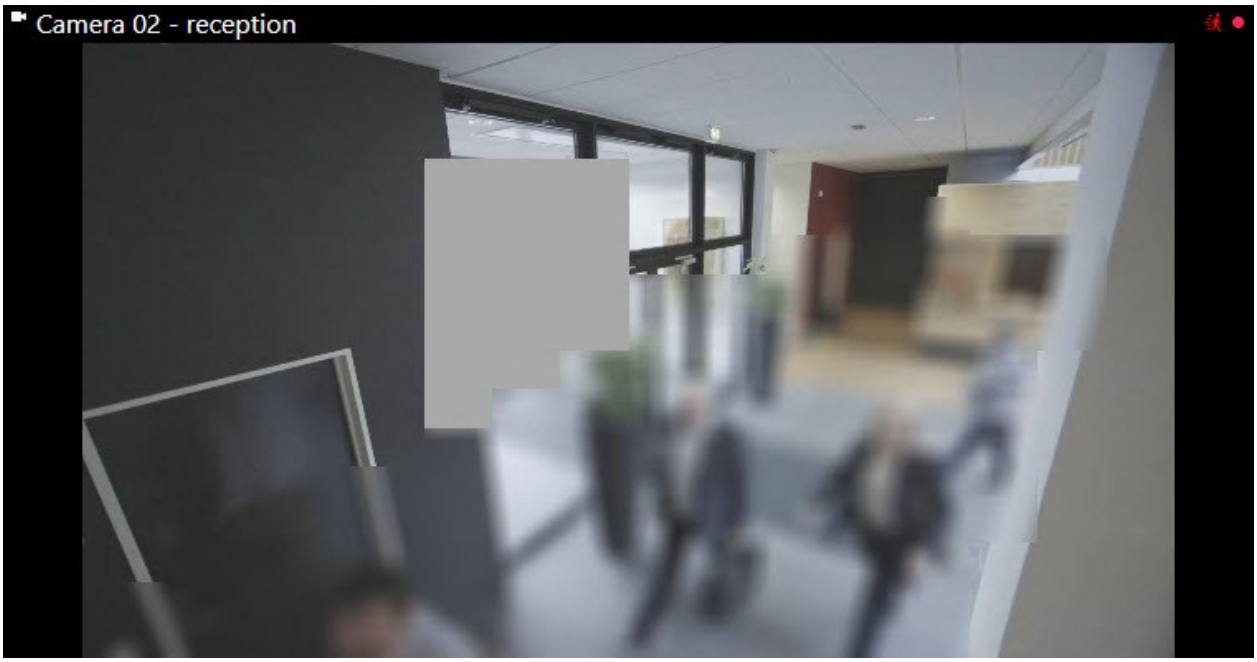
Quando um usuário exporta ou reproduz vídeos gravados de um cliente, o vídeo inclui as máscaras de privacidade configuradas no momento da gravação, mesmo que você tenha alterado ou removido as máscaras de privacidade mais tarde. Se a proteção de privacidade for removida ao exportar, o vídeo exportado **não** inclui as máscaras de privacidade removíveis.

Se você alterar as configurações de máscara de privacidade com muita frequência, por exemplo, uma vez por semana, seu sistema pode ficar sobrecarregado.

Exemplo da guia **Máscara de privacidade** com máscaras de privacidade configuradas:



É assim que elas aparecem nos clientes:



Você pode informar os usuários do cliente sobre as configurações de máscaras de privacidade permanentes e removíveis.

Perfis Management Client (explicado)

Perfis do Management Client permitem que os administradores modifiquem a interface do usuário do Management Client de outros usuários. Faça associação de perfis do Management Client com funções para limitar a interface do usuário a apresentar apenas as funcionalidades disponíveis para cada função de administrador.

Perfis Management Client apenas tratam a representação visual da funcionalidade do sistema e não o real acesso a ele. O acesso geral à funcionalidade do sistema é concedido através da função à qual os usuários estão associados. Para obter informações sobre como gerencial o acesso geral à funcionalidade do sistema para uma função, consulte Gerenciar a visibilidade da funcionalidade para um perfil do Management Client.

Você pode alterar as configurações de visibilidade de todos os elementos do Management Client. Por padrão, o perfil do Management Client pode ver todas as funcionalidades no Management Client.

Perfis Smart Client (explicado)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Todos os usuários de Milestone XProtect VMS pertencem a uma função que tem um perfil do Smart Client conectado a ela.

As funções definem as permissões dos usuários e os perfis do Smart Client definem o que os usuários podem ver na interface de usuário do XProtect Smart Client.

Todas as instalações do Milestone XProtect VMS incluem um perfil Smart Client padrão configurado com uma definição padrão para mostrar a maior parte da configuração que está disponível no sistema da sua organização. Algumas configurações sempre são desativadas por padrão.

Caso haja diversas funções diferentes em uma organização, você pode desativar funcionalidades às quais uma função específica não tenha/não deveria ter acesso em XProtect Smart Client.

Por exemplo, você pode ter uma função cujo trabalho diário não envolve a reprodução de nenhum vídeo. Para essa finalidade, você pode criar um novo perfil do Smart Client para essa função, na qual desative o Modo de **reprodução**. Ao desativar essa configuração no perfil do Smart Client, usuários do XProtect Smart Client com uma função que use esse perfil do Smart Client não poderão mais ver o Modo de **reprodução** em sua interface de usuário do XProtect Smart Client.

É importante observar que perfis do Smart Client têm quase todo o controle sobre o que os usuários podem ver na interface de usuário do XProtect Smart Client, e não sobre as permissões de acesso da função em si. Essas permissões de acesso, como acesso à leitura, modificação e exclusão, são controladas pelas configurações internas da função. Portanto, usuários do XProtect Smart Client podem ter permissões para acessar funcionalidades através de sua função – que eles não podem ver em sua interface de usuário, pois ela está desativada no perfil do Smart Client.

Para garantir a melhor experiência de usuário possível aos usuários do XProtect Smart Client, você precisa garantir que haja consistência entre as permissões fornecidas pela função e os elementos da interface de usuário fornecidos pelo perfil do Smart Client.

Para criar ou editar perfis Smart Client, expanda **Cliente** e selecione **Smart ClientPerfis**.

Você também pode aprender sobre a relação entre perfis do Smart Client, funções e perfis de tempo e como usá-los juntos (consulte Criar e configurar perfis do Smart Client, perfis de funções e de tempo na página 272).

Sobre proteção de evidências

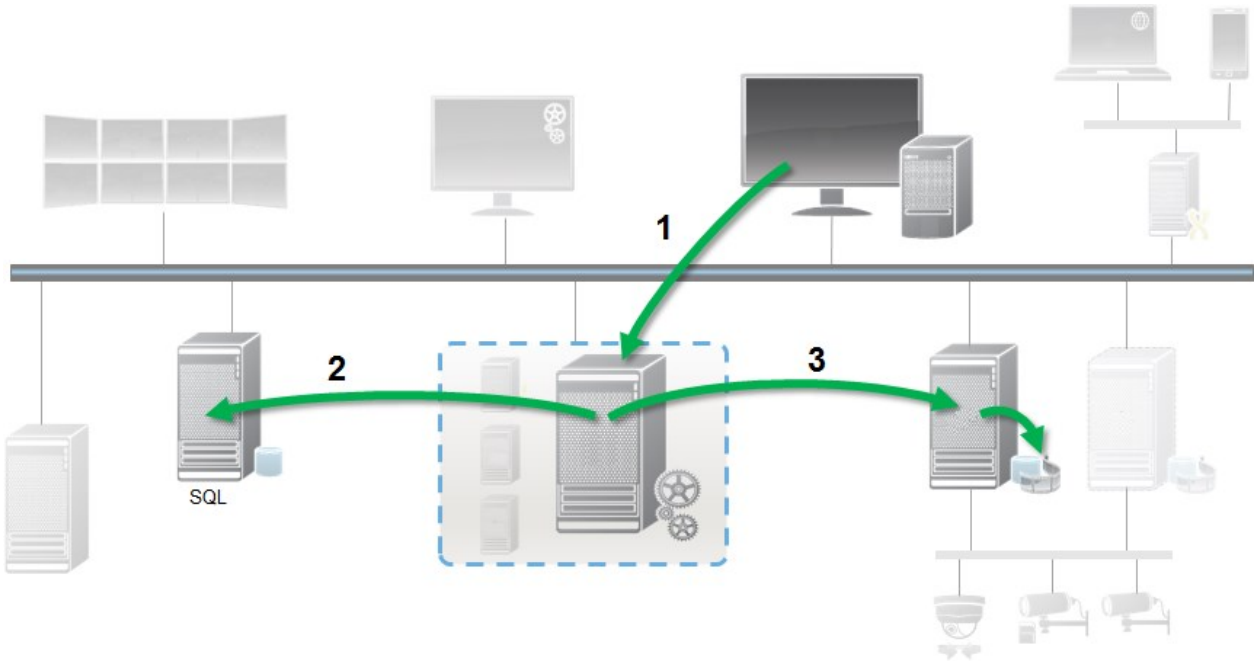
As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

A partir da versão 2020 R2 do XProtect VMS, quando você atualiza o servidor de gerenciamento de uma versão anterior, não será possível criar ou modificar proteções de evidências em servidores de gravação da versão 2020 R1 ou anterior, até que esses servidores de gravação sejam atualizados.
Isto também significa que, se o hardware tiver sido movido de um servidor de gravação (da versão 2020 R1 ou anterior) para outro servidor de gravação, e ainda houver gravações nele, as proteções de evidência não poderão ser criadas ou modificadas.

A funcionalidade de proteção de evidências permite que os operadores do cliente protejam de exclusão sequências de vídeo, inclusive áudio e outros dados, se necessário, por exemplo, enquanto uma investigação ou julgamento está em curso. Para obter mais informações, consulte o manual de usuário do XProtect Smart Client.

Dados protegidos não podem ser apagados, seja automaticamente pelo sistema após o tempo de retenção padrão do sistema ou outras situações, seja manualmente pelos usuários do cliente. Nem o sistema nem um usuário podem apagar os dados até que um usuário com permissões de usuário suficientes desproteja as evidências.

Diagrama de fluxo do sistema de proteção de evidências:



1. Um usuário XProtect Smart Client cria uma proteção de evidência. As informações são enviadas para o Servidor de Gerenciamento.
2. O Management Server armazena informações sobre a proteção de evidências no banco de dados SQL Server.
3. O Servidor de Gerenciamento informa ao Servidor de Gravação que armazene e proteja o registro protegido no banco de dados.

Quando o operador cria uma proteção de evidências, os dados protegidos permanecem no armazenamento de gravação em que foi gravado e é movido para discos de arquivamento, juntamente com dados não protegidos, mas os dados protegidos:

- Seguem o tempo de retenção configurado para a proteção de evidências. Potencialmente, por prazo infinito
- Mantém a qualidade original das gravações, mesmo se a preparação foi configurada para dados não protegidos

Quando um operador cria proteções, o tamanho mínimo de uma sequência é o período em que o banco de dados divide arquivos gravados, cujo padrão é de sequências de uma hora. Isso pode ser alterado, mas exigirá que você personalize o arquivo RecorderConfig.xml no servidor de gravação. Se uma pequena sequência abrange dois períodos de uma hora, o sistema bloqueia as gravações de ambos os períodos.

No registro de auditoria no Management Client, você pode ver quando um usuário cria, edita ou exclui proteções de evidências.

Quando um disco fica sem espaço, isso não afeta os dados protegidos. Somente dados não protegidos mais antigos serão eliminados. Se não houver mais dados não protegidos para apagar, o sistema interrompe a gravação. É possível criar regras e alarmes acionados por eventos de disco cheio para que você seja automaticamente notificado.

Com exceção do armazenamento de mais dados por um período mais longo, o que poderia vir a afetar o armazenamento em disco, o recurso de proteção de evidências, como tal, não influencia o desempenho do sistema.

Se você mover hardware (consulte Mover hardware na página 351) para outro servidor de gravação:

- Gravações protegidas com proteção de evidências permanecem no servidor de gravação antigo, obedecendo o tempo de retenção definido para a proteção de evidências quando ela foi criada
- O usuário do XProtect Smart Client pode ainda proteger os dados com proteção de evidências nas gravações que foram feitas em uma câmera antes de ter sido transferida para outro servidor de gravação. Mesmo que a câmera seja movida várias vezes e as gravações estejam armazenadas em vários servidores de gravação

Por padrão, todos os operadores de clientes têm o perfil padrão de proteção de evidências, mas não têm as permissões de acesso ao recurso. Para especificar as permissões de proteção de evidências de uma função, consulte Guia dispositivo (funções) para as configurações da função. Para especificar o perfil da proteção de evidências de uma função (consulte a guia Informações (funções) para as configurações da função.

No Management Client, é possível editar as propriedades do perfil de proteção de evidências padrão e criar perfis adicionais, atribuindo-os às funções.

Regras e eventos

Regras (explicadas)

As regras especificam ações para levar a cabo em condições especiais. Exemplo: Quando um movimento é detectado (condição), uma câmera começa a gravar (ação).

A seguir são **exemplos** do que você pode fazer com as regras:

- Iniciar e parar a gravação
- Definir a taxa de quadros ao vivo fora do padrão
- Definir taxa de quadros fora do padrão
- Iniciar e parar o patrulha PTZ
- Pausar e continuar o patrulha PTZ
- Mover as câmeras PTZ para posições específicas
- Definir a saída para o estado ativado/desativado
- Enviar notificações por e-mail
- Gerar entradas de log
- Gerar eventos
- Aplicar novas configurações de dispositivo; por exemplo, uma resolução diferente em uma câmera

- Fazer o vídeo aparecer em destinatários do Matrix
- Iniciar e parar plug-ins
- Iniciar e parar feeds dos dispositivos

Parar um dispositivo significa que o vídeo não é transferido do dispositivo para o sistema, nesse caso, você não pode ver o vídeo ao vivo ou gravar vídeos. Em contraste, um dispositivo em que você parou a alimentação ainda pode se comunicar com o servidor de gravação, e você pode começar a alimentação do dispositivo automaticamente através de uma regra, ao contrário de quando o dispositivo está desativado manualmente no Management Client.

> Alguns conteúdos de regra pode exigir que determinados recursos estejam ativados para os dispositivos relevantes. Por exemplo, uma regra especificando que a câmera deve gravar não funciona conforme pretendido se a gravação não estiver ativada para a câmera em questão. Antes de criar uma regra, a Milestone recomenda que você verifique se os dispositivos envolvidos podem funcionar conforme pretendido.

Complexidade de regras

O número exato de opções depende do tipo de regra que você deseja criar e do número de dispositivos disponíveis em seu sistema. As regras fornecem um alto grau de flexibilidade: você pode combinar condições de evento e tempo, especificar várias ações em uma única regra e muitas vezes criar regras que abrangem vários ou todos os dispositivos em seu sistema.

Você pode fazer suas regras simples ou complexas como solicitado. Por exemplo, você pode criar muitas regras simples baseadas em horas:

Exemplo	Explicação
Regras muitos simples baseadas no tempo	Às segundas-feiras, entre as 08h30 e 11h30 (condição de tempo), Câmera 1 e Câmera 2 devem começar a gravar (ação) quando o período de tempo começa, e parar a gravação (interromper a ação) quando o período de tempo termina.
Regras muito simples baseadas em evento	Quando se detecta movimento (condição de evento) na câmera 1, a câmera 1 inicia a gravação (ação) imediatamente e, depois, interrompe a gravação (ação Parar) após 10 segundos. Mesmo que uma regra baseada em eventos seja ativado por um evento em um dispositivo, você pode especificar que ações devem ocorrer em um ou mais dispositivos.

Exemplo	Explicação
Regra envolvendo vários dispositivos	Quando o movimento é detectado (condição de evento) na Câmera 1, a Câmera 2 deve começar a gravar (ação) imediatamente, e a sirene conectada à saída 3 deve soar (ação) imediatamente. Então, depois de 60 segundos, a câmera 2 deve parar a gravação (ação de parar), e a sirene conectada à saída 3 deve parar de soar (ação de parar).
Regra combinando tempo, eventos e dispositivos	Quando o movimento é detectado (condição de evento) na Câmera 1, e o dia da semana é sábado ou domingo (condição de tempo), a Câmera 1 e a Câmera 2 devem começar a gravar (ação) imediatamente, e uma notificação deve ser enviada para o gerente de segurança (ação). Então, 5 segundos depois que o movimento não for detectado na Câmera 1 ou Câmera 2, as duas câmeras devem parar a gravação (ação de parar).

Dependendo das necessidades da sua organização, muitas vezes é uma boa ideia criar muitas regras simples, em vez de algumas regras complexas. Mesmo que isso signifique que você tenha mais regras em seu sistema, ele fornece uma maneira fácil para manter uma síntese do que suas regras fazem. Manter suas regras simples também significa que você tem muito mais flexibilidade quando se trata de desativar/ativar elementos de regras individuais. Com regras simples, você pode desativar / ativar regras inteiras quando necessário.

Regras e eventos (explicados)

Regras são um elemento central no seu sistema. As regras determinam as configurações altamente importantes, como quando as câmeras devem gravar, quando as câmeras PTZ devem patrulhar, quando as notificações devem ser enviadas, etc.

Exemplo – uma regra especificando que uma câmera especial deve começar a gravar quando detectar movimento:

Eventos são elementos centrais ao utilizar o assistente **Gerenciar regra**. No assistente, os eventos são utilizados principalmente para desencadear ações. Por exemplo, você pode criar uma regra que especifica que, em **caso** de detecção de movimento, o sistema de monitoramento deve tomar as **medidas** de iniciar a gravação de vídeo de uma câmera específica.

Os seguintes tipos de condições podem disparar regras:

Nome	Descrição
Eventos	Quando eventos ocorrem no sistema de monitoramento, por exemplo, quando o movimento é detectado ou o sistema recebe a entrada de sensores externos.
Intervalo de tempo	Quando você insere períodos específicos de tempo, por exemplo: `Thursday 16th August 2007 from 07.00 to 07.59` ou `every Saturday and Sunday`
Intervalo de tempo de emergência	Períodos de tempo onde o serviço de emergência está ativo ou inativo.
Tempo recorrente	Quando você define uma ação a ser executada em uma programação detalhada e recorrente. Por exemplo: • A cada semana, todas as terças-feiras, a cada 1 hora entre 15:00 e 15:30 • No dia 15, a cada 3 meses às 11:45 • Todos os dias, a cada 1 hora entre 15:00 e 19:00 A hora é baseada nas configurações de hora locais do servidor no qual o Management Client está instalado.

Você pode trabalhar com o seguinte em **Regras e eventos**:

- **Regras**: As regras são um elemento central no sistema. O comportamento do seu sistema de monitoramento é, em grande parte, determinado por regras. Ao criar uma regra, você pode trabalhar com todos os tipos de eventos
- **Perfis de tempo**: Os perfis do tempo de períodos de tempo definidos no Management Client. Você os usa quando cria regras no Management Client, por exemplo, para criar uma regra que especifica que uma determinada ação deve ocorrer dentro de um determinado perfil de tempo
- **Perfis de notificação**: Você pode usar perfis de notificação para configurar notificações por e-mail já prontas, que podem ser automaticamente acionadas por uma regra, por exemplo, quando ocorre um evento específico

- **Eventos definidos pelo usuário**: Os eventos definidos pelo usuário são eventos feitos sob medida que tornam possível que os usuários acionem manualmente os eventos no sistema ou reajam às entradas do sistema
- **Eventos analíticos**: Os eventos analíticos são dados recebidos de fornecedores externos de uma análise de conteúdo de vídeo (VCA). Você pode usar os eventos de análise como base para alarmes
- **Eventos genéricos**: Os eventos genéricos permitem desencadear ações no servidor de eventos do XProtect, enviando sequências simples através da rede IP para o seu sistema

Perfis de tempo (explicados)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

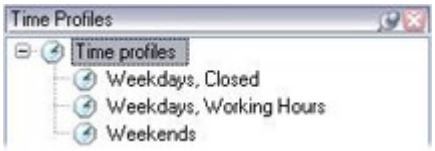
Perfis de tempo são períodos de tempo definidos pelo administrador. Você pode usar perfis de tempo ao criar regras, por exemplo, uma regra especificando que uma determinada ação deve ocorrer dentro de um determinado período de tempo.

Os perfis de tempo também são atribuídos a funções, junto com perfis do Smart Client. Como padrão, todas as funções são atribuídas ao perfil de tempo padrão **Sempre**. Isso significa que os membros de funções com esse perfil de tempo padrão anexado não têm limites baseados em tempo para suas permissões de usuário no sistema. Você também pode atribuir um perfil de tempo alternativo para uma função.

Os perfis de tempo são altamente flexíveis: você pode baseá-los em um ou mais períodos de tempo individuais, em um ou mais períodos recorrentes de tempo, ou em uma combinação de tempos individuais e recorrentes. Muitos usuários podem ter familiaridade com conceitos de períodos únicos e recorrentes em aplicativos de calendário, como aquele no Microsoft® Outlook.

Os perfis de tempo sempre se aplicam ao horário local. Isto significa que se o sistema tem servidores de gravação colocados em diferentes fusos horários, todas as ações, por exemplo, a gravação em câmeras, associadas com perfis de tempo são realizadas no horário local de cada servidor de gravação. Exemplo: Se você tem um perfil de tempo para o período de 08.30h às 09.30h, todas as ações associadas em um servidor de gravação colocado em Nova York são realizadas quando a hora local for das 08.30h às 09.30h em Nova York, enquanto que as mesmas ações em um servidor de gravação colocado em Los Angeles serão realizadas algumas horas depois, quando a hora local for das 08.30h às 09.30h, em Los Angeles.

Você pode criar e gerenciar perfis de tempo, expandindo **Regras e eventos** > **Perfis de tempo**. A lista de **Perfis de tempo** abre. Somente exemplo:



Para uma alternativa a perfis de tempo, consulte Perfis de tempo diurnos (explicado).

Perfis de tempo diurno (explicado)

Ao colocar câmeras do lado de fora, você deve muitas vezes reduzir a resolução da câmera, permitir preto/branco ou mudar outras configurações quando escurece ou quando fica claro. Quanto mais ao norte ou sul do equador as câmeras são colocadas, mais o tempo de nascer do sol e pôr-do-sol varia durante o dia. Isso torna impossível usar perfis normais de tempo fixo para ajustar as configurações da câmera de acordo com as condições de luz.

Em tais situações, você pode criar perfis de tempo de duração diurna, em vez de definir o nascer e o pôr do sol em uma área geográfica específica. Através das coordenadas geográficas, o sistema calcula a hora do nascer e do pôr do sol, incorporando, até mesmo, o horário de verão, numa base diária. Como resultado, o perfil de tempo segue automaticamente as alterações anuais do nascer e do pôr do sol na área selecionada, garantindo que o perfil fique ativo apenas quando necessário. Todos os horários e datas são baseados nas configurações de data e tempo dos servidores de gerenciamento. Você também pode definir um deslocamento positivo ou negativo (em minutos) para o início (nascer do sol) e fim (pôr do sol). A compensação para o horário de início e de término podem ser idênticas ou diferentes.

Você pode usar perfis de duração do dia ao criar regras e funções.

Perfis de notificação (explicados)

Perfis de notificação permitem que você configure notificações de e-mail pré-prontas. Notificações podem ser automaticamente acionadas por uma regra, por exemplo, quando ocorre um evento específico.

Quando você cria o perfil de notificação, você especifica o texto da mensagem e decide se deseja incluir imagens estáticas e clipes de vídeo AVI nas notificações de e-mail.

> Além disso, você pode precisar desativar todos os scanners de e-mail que possam impedir que o aplicativo envie as notificações por e-mail.

Requisitos para a criação de perfis de notificação

Antes de criar perfis de notificação, você deve especificar as configurações do servidor de e-mail de saída para as notificações por e-mail.

Você pode proteger a comunicação ao servidor de e-mail, se instalar os certificados de segurança necessários no servidor de e-mail.

Se quiser que as notificações por e-mail possam incluir clipes de filmes AVI, você também deve especificar as configurações de compactação:

1. Vá para **Ferramentas** > **Opções**. Isso abre a janela **Opções**.
2. Configure o servidor de correio o na guia **Servidor de correio** (Guia Servidor de correio (opções) na página 398) e as configurações de compressão na guia **Geração de AVI** Guia Geração AVI (opções) na página 399.

Eventos definidos pelo usuário (explicado)

Se o evento que você precisa não está na lista **Visão geral de eventos**, você pode criar seus próprios eventos definidos pelo usuário. Use esses eventos definidos pelo usuário para integrar outros sistemas com o sistema de monitoramento.

Com eventos definidos pelo usuário, você pode utilizar os dados recebidos de um sistema de controle de acesso de terceiros como eventos no sistema. Os eventos podem acionar ações posteriormente. Desta forma, você pode, por exemplo começar a gravar um vídeo a partir de câmeras relevantes quando alguém entrar no prédio.

Você também pode usar os eventos definidos pelo usuário para disparar manualmente eventos durante a visualização de vídeo ao vivo no XProtect Smart Client ou automaticamente, se você usá-los em regras. Por exemplo, quando o evento 37 definido pelo usuário ocorre, a câmera PTZ 224 deve parar de patrulhar e ir para a posição predefinida 18.

Através de funções, você define quais de seus usuários podem acionar os eventos definidos pelo usuário. Você pode usar eventos definidos pelo usuário de duas maneiras e, ao mesmo tempo, caso necessário:

Eventos	Descrição
Para fornecer a capacidade de disparar manualmente os eventos em XProtect Smart Client	Neste caso, os eventos definidos pelo usuário permitem que os usuários finais acionem eventos manualmente durante a visualização de vídeo ao vivo em XProtect Smart Client. Quando um evento definido pelo usuário ocorre porque um usuário do XProtect Smart Client o aciona manualmente, uma regra pode disparar uma ou mais ações que deve ocorrer no sistema.
Para fornecer a capacidade de acionar eventos através da API	Neste caso, você pode acionar eventos definidos pelo usuário fora do sistema de monitoramento. O uso de eventos definidos pelo usuário dessa maneira exige uma API separada (Application Program Interface. Um conjunto de blocos de construção para criar ou personalizar aplicativos de software). Isso é usado ao acionar o evento definido pelo usuário. Autenticação através de Active Directory é exigido para usar eventos definidos pelo usuário desta maneira. Isso garante que, mesmo que os eventos definidos pelo usuário possam ser acionados de fora do sistema de monitoramento, somente os usuários autorizados terão acesso a eles.

Eventos	Descrição
	Ainda, eventos definidos por usuários podem ser associados via API com metadados, definindo certos dispositivos ou grupos de dispositivos. Isto é altamente útil ao usar eventos definidos por usuário para ativar regras: evita-se ter uma regra por dispositivo, fazendo basicamente a mesma coisa. Exemplo: Uma companhia usa controle de acesso, tendo 35 entradas, cada uma com um dispositivo de controle de acesso. Quando um dispositivo de controle de acesso é ativado, um evento definido pelo usuário é acionado no sistema. Este evento definido pelo usuário é usado em uma regra para iniciar a gravação em uma câmera associada com o dispositivo de controle de acesso ativado. É definido no metadados qual câmera é associada coma qual regra. Desta forma, a empresa não precisa ter 35 eventos definidos pelo usuário e 35 regras acionadas pelos eventos definidos pelo usuário. Um único evento definido pelo usuário e uma única regra são suficientes. Ao usar eventos definidos pelo usuário desta forma, você pode nem sempre querer que eles estejam disponíveis para serem disparados manualmente no XProtect Smart Client. Você pode usar funções para definir quais eventos definidos pelo usuário devem estar visíveis no XProtect Smart Client.

Eventos de analítico (explicados)

Eventos de análise são, tipicamente, dados recebidos de um fornecedor de VCA (Video Content Analysis, Análise de Conteúdo de Vídeo) externo.

Usar eventos analíticos como base de alarmes é basicamente um processo de três passos:

- Parte um, permitir o recurso de eventos de análise e configurar a sua segurança. Use uma lista de endereços permitidos para controlar quem pode enviar dados de eventos para o sistema e qual porta o servidor escuta
- Parte dois, criar o evento de analítico, possivelmente com uma descrição do evento, e testá-lo
- Parte três, usar o evento analítico como a fonte de uma definição de alarme

Você configura os eventos analíticos na lista **Regras e eventos** no painel **Navegação do site**.

Para utilizar eventos baseados em VCA, uma ferramenta VCA de terceiros é necessária para o fornecimento de dados para o sistema. A ferramenta VCA a ser usada depende inteiramente de você, contanto que os dados fornecidos pela ferramenta sigam o formato. Este formato é explicado na MIP SDK Documentação em eventos analíticos.

Entre em contato com o seu fornecedor de sistema para mais detalhes. As ferramentas VCA de terceiros são desenvolvidas por parceiros independentes produzindo soluções com base em uma plataforma aberta Milestone. Estas soluções podem afetar a performance do sistema.

Eventos genéricos (explicados)

Os eventos genéricos permitem desencadear ações no servidor de eventos do XProtect, enviando sequências simples através da rede IP para o seu sistema.

Você pode usar qualquer software ou hardware que possa enviar sequências via TCP ou UDP para acionar eventos genéricos. Seu sistema pode analisar pacotes de dados TCP ou UDP recebidos e automaticamente acionar eventos genéricos quando os critérios específicos forem satisfeitos. Dessa forma, você pode integrar o seu sistema com fontes externas, por exemplo, sistemas de controle de acesso e sistemas de alarme. O objetivo é permitir que o maior número de fontes possíveis interajam com o sistema.

Com o conceito de fontes de dados, você evita ter que adaptar ferramentas de terceiros para atender aos padrões de seu sistema. Com fontes de dados, você pode se comunicar com um determinado software ou hardware em uma porta IP específica e definir como os bytes que chegam nessa porta serão interpretados. Cada tipo de evento genérico combina com uma fonte de dados e cria uma linguagem usada para comunicação com uma peça de hardware ou software específica.

Trabalhar com fontes de dados exige conhecimento geral de rede IP e conhecimento geral daqueles hardware ou softwares que deseja fazer a interface. Há muitos parâmetros que você pode usar e nenhuma solução pronta de como fazê-los. Basicamente, o seu sistema fornece as ferramentas, mas não a solução. Ao contrário de eventos definidos pelo usuário, os eventos genéricos não têm autenticação. Isto os torna mais fáceis de ativar mas, para evitar comprometimento de segurança, somente eventos do host local são aceitos. Você pode permitir outros endereços IP do cliente na guia **Eventos genéricos** do menu **Opções**.

Webhooks (explicação)

Webhooks são solicitações HTTP que permitem que aplicativos da web se comuniquem entre si e facilitam o envio de dados em tempo real de um aplicativo para outro quando ocorre um evento predefinido. Por exemplo, o envio de dados de um evento a um endpoint de webhook quando um usuário faz logon no sistema ou quando uma câmera relata um erro.

Um endpoint de webhook (URL de webhook) é o endereço predefinido ao qual os dados de evento serão enviados, como um número de telefone unidirecional.

Você pode usar webhooks para construir integrações que são submetidas a eventos selecionados em XProtect. Quando um evento é disparado, um POST HTTP é enviado ao endpoint de webhook que você definiu para tal evento. O corpo do POST HTTP contém dados de evento em JSON.

Webhooks não buscam dados ou eventos disparados no sistema; em vez disso, o sistema leva dados de evento ao endpoint de webhook quando ocorre um evento, o que reduz a demanda de webhooks por recursos e acelera sua configuração em comparação com soluções de polling.

Também é possível configurar a integração de webhooks com ou sem o uso de scripts de código.

> ⚠ Você precisa verificar se os dados de evento enviados de XProtect estão em conformidade com os dados existentes e a legislação de proteção à privacidade do seu país.

Por padrão, a funcionalidade de webhooks vem instalada e pronta para utilização no XProtect 2023R1 ou versões posteriores, além de exibir a ação **Webhooks** na guia **Regras** no Management Client.

Alarmes

Alarmes (explicados)

Este recurso funciona apenas se você tiver o XProtect Event Server instalado.

Este artigo descreve como configurar alarmes para aparecer no sistema, disparados por eventos.

Com base na funcionalidade tratada no servidor de eventos, o recurso de alarmes oferece a visão geral central, o controle e a escalabilidade de alarmes em qualquer número de instalações (incluindo outros sistemas do XProtect) em toda a sua organização. Você pode configurá-lo para gerar alarmes com base em:

- **Eventos relacionados ao sistema interno**

  Por exemplo, movimento, servidor que responde/não responde, problemas de arquivamento, falta de espaço em disco e muito mais.

- **Eventos integrados externos**

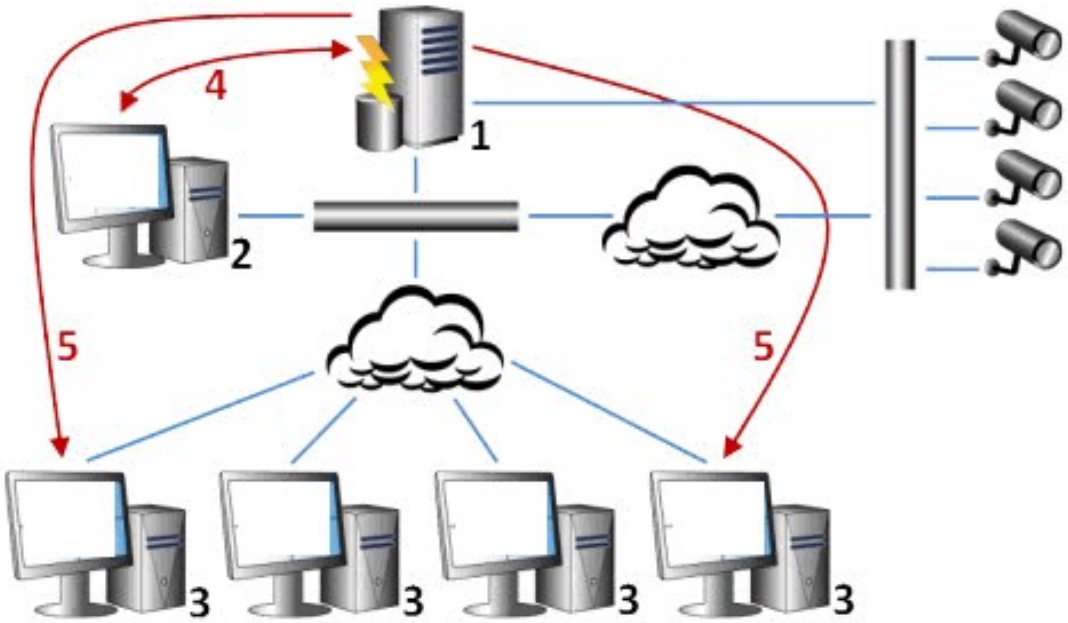
  Este grupo consiste em diversos tipos de eventos externos:

  - **Eventos analíticos**

    Eventos de análise são, tipicamente, dados recebidos de um fornecedor de VCA (Video Content Analysis, Análise de Conteúdo de Vídeo) externo.

  - **Eventos de plug-in MIP**

    Através do MIP SDK, um fornecedor terceirizado pode desenvolver plug-ins personalizados (por exemplo, integração a sistemas de controle de acesso externo ou semelhante) para o seu sistema.



Legenda:

1. Sistema de monitoramento
2. Management Client
3. XProtect Smart Client
4. Configuração de alarme
5. Fluxo de dados de alarme

Você processa e atribui alarmes na lista de alarmes no XProtect Smart Client. Você também pode integrar alarmes com o mapa inteligente do XProtect Smart Client e a funcionalidade de mapa.

Configuração de alarme

A configuração de alarme inclui:

- Manutenção de configuração de alarme baseado em função dinâmica
- Visão geral técnica centralizada de todos os componentes: servidores, câmeras e unidades externas
- Configuração de registro central de todos os alarmes recebidos e informações do sistema
- Tratamento de plug-ins, permitindo a integração personalizada de outros sistemas, por exemplo, o controle de acesso externo ou sistemas baseados em VCA

Em geral, alarmes são controlados pela visibilidade do objeto causando o alarme. Isso significa que quatro aspectos possíveis podem desempenhar uma função no que diz respeito aos alarmes e quem pode controlar/gerenciá-los e até que ponto:

Nome	Descrição
Visibilidade de dispositivo/fonte	Se o dispositivo que está causando o alarme não está definido para estar visível para a função do usuário, o usuário não pode ver o alarme na lista de alarmes no XProtect Smart Client.
O direito para acionar eventos definidos pelo usuário	Essa permissão determina se a função do usuário pode acionar eventos definidos pelo usuário selecionados em XProtect Smart Client.
Plug-ins externos	Se algum plug-in externo estiver configurado no seu sistema, ele pode controlar as permissões dos usuários para lidar com alarmes.
Direitos gerais de função	Determine se o usuário está autorizado a apenas ver ou também a gerenciar alarmes. O que um usuário de **alarmes** pode fazer com alarmes depende da função do usuário e das configurações definidas para essa função específica.

Na guia **Alarmes e Eventos**, em **Opções**, é possível especificar as definições para alarmes, eventos e registros.

Mapa inteligente

Sobre o Mapa Inteligente

No XProtect® Smart Client e no XProtect Mobile, o recurso de mapa inteligente permite que você visualize e acesse dispositivos em diversos locais ao redor do mundo de modo geograficamente correto. Ao contrário de mapas, onde você tinha um mapa diferente para cada local, o Mapa Inteligente lhe oferece o panorama geral em uma única visualização.

A seguinte configuração do recurso de mapa inteligente é feita no Management Client:

- Configure os fundos geográficos que você pode escolher para o seu mapa inteligente. Isto inclui a integração do seu mapa inteligente com um dos seguintes serviços:
  - Bing Maps
  - Google Maps
  - Milestone Map Service
  - OpenStreetMap
- Ativar Bing Maps ou Google Maps no XProtect Management Client ou no XProtect Smart Client
- Ativar a edição de mapas inteligentes, incluindo dispositivos no XProtect Smart Client
- Posicionar seus dispositivos geograficamente no XProtect Management Client
- Configurar o seu mapa inteligente com Milestone Federated Architecture

Integração do mapa inteligente com o Google Maps (explicado)

Para integrar o Google Maps no seu mapa inteligente, você precisa de uma chave API estática para mapas do Google. Para obter uma chave API, primeiro você precisa criar uma conta de faturamento do Google Cloud. Você receberá uma fatura de acordo com o volume de carregamentos de mapas por mês.

Quando tiver a chave API você deve inseri-la no XProtect Management Client. Consulte também Ativar Bing Maps ou Google Maps no Management Client na página 332.

Se você tiver um firewall restritivo ativado, é importante permitir acesso aos domínios usados. Você pode ter que permitir o tráfego de saída para Google Maps usando maps.googleapis.com em cada máquina em que o Smart Client esteja em funcionamento.

Para obter mais informações, consulte:

- Google Maps Platform - introdução: https://cloud.google.com/maps-platform/
- Guia para o faturamento da Google Maps Platform: https://developers.google.com/maps/billing/gmp-billing
- Guia do desenvolvedor para Maps Static API:https://developers.google.com/maps/documentation/maps-static/dev-guide

Adicionar assinatura digital à chave API de Mapas estáticos

Se você espera que os operadores do XProtect Smart Client façam mais de 25.000 solicitações de mapa por dia, você precisará de uma assinatura digital para a sua chave Maps Static API. A assinatura digital permite que os servidores do Google verifiquem se qualquer site gerando solicitações usando a sua chave API está autorizado a fazê-lo. No entanto, independentemente dos requisitos de uso, o Google recomenda usar uma assinatura

digital como camada de segurança adicional. Para obter a assinatura digital. você deve recuperar um segredo de assinatura de URL. Para obter mais informações, consulte https://developers.google.com/maps/documentation/maps-static/get-api-key#dig-sig-manual.

Integração do mapa inteligente com o Bing Maps (explicado)

Para integrar o Bing Maps no seu mapa inteligente, você precisa de uma Chave básica ou uma Chave corporativa. A diferença é que as chaves básicas são gratuitas, mas permitem um número limitado de transações, antes que elas se tornem passíveis de cobrança ou o acesso ao serviço de mapas seja negado. A chave corporativa não é gratuita mas permite um número de transações ilimitadas.

Para mais informações sobre Bing Maps, consulte https://www.microsoft.com/en-us/maps/licensing/.

Quando tiver a chave API você deve inseri-la no XProtect Management Client. Consulte Ativar Bing Maps ou Google Maps no Management Client na página 332.

> Se você tiver um firewall restritivo ativado, é importante permitir acesso aos domínios usados. Você pode ter que permitir o tráfego de saída para o Bing Maps usando *.virtualearth.net em cada máquina em que o Smart Client esteja em funcionamento.

Arquivos do mapa inteligente do cache (explicados)

> Se você estiver usando o Google Maps como plano de fundo geográfico, os arquivos não serão armazenados em cache.

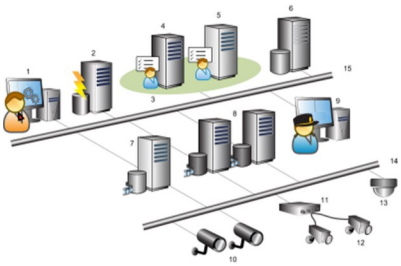
Os arquivos que você usa para seu fundo geográfico são recuperados a partir de um servidor de imagens. A hora em que os arquivos são armazenados na pasta de cache, depende do valor selecionado na lista **Arquivos de mapa inteligentes em cache removidos** na caixa de diálogo **Configurações** em XProtect Smart Client. Os arquivos são armazenados:

- Indefinidamente (**Nunca**)
- Por 30 dias se o arquivo não for usado (**Quando não for usado por 30 dias**)
- Quando o operador sai do XProtect Smart Client (**Na saída**).

Quando você altera o endereço do servidor de imagens, automaticamente uma nova pasta de cache é criada. Os arquivos do mapa anterior são mantidos na pasta do cache associada no seu computador local.

Arquitetura

Configuração de sistema



Exemplo de uma configuração de sistema distribuído. O número de câmeras e de servidores de gravação, assim como o número de clientes conectados, pode ser tão grande quanto se requeira.

> Todos os computadores em uma configuração distribuída devem estar em um domínio ou em um grupo de trabalho.

Legenda:

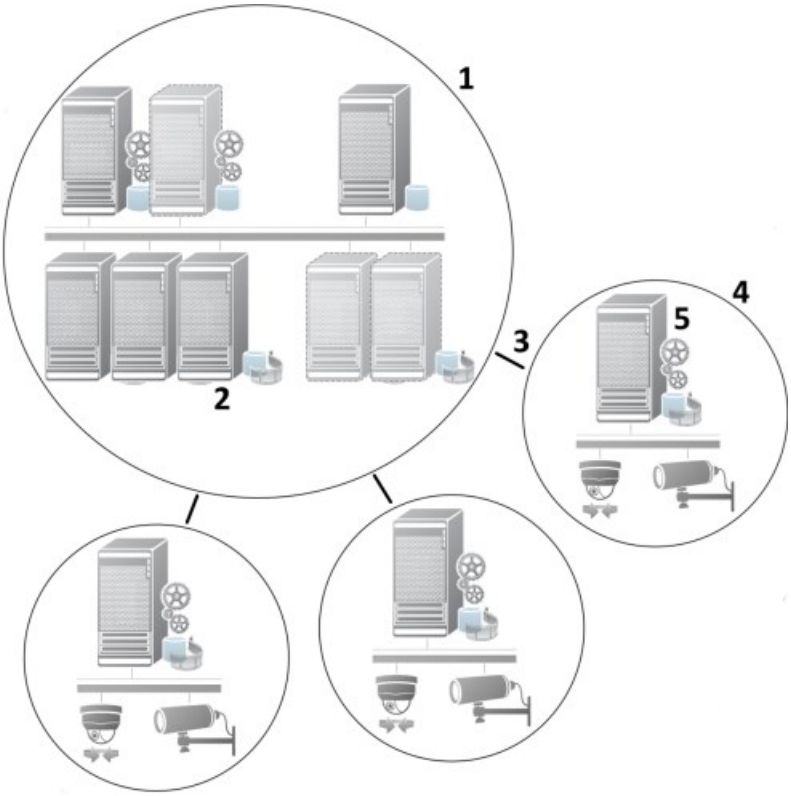
1. Management Client(s)
2. Servidor de eventos
3. Grupo Microsoft
4. Servidor de gerenciamento
5. Servidor de gerenciamento da recuperação de falhas (failover)
6. Servidor com SQL Server
7. Servidor do sistema de gravação ininterrupta (failover)
8. Servidor(es) de gravação
9. XProtect Smart Client(s)
10. Câmeras de vídeo IP
11. Codificador de vídeo
12. Câmeras analógicas
13. Câmera IP PTZ
14. Rede de câmera
15. Rede de servidor

Milestone Interconnect (explicado)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Milestone Interconnect™ permite que você integre várias instalações menores, fragmentadas fisicamente e remotas do XProtect com uma central de controle XProtect Corporate. Você pode instalar esses sites menores, chamados de bases remotas, em unidades móveis, por exemplo, barcos, ônibus ou trens. Isto significa que esses sites não precisam estar permanentemente conectados a uma rede.

A ilustração a seguir mostra como você pode configurar Milestone Interconnect no seu sistema:



1. Milestone Interconnect central XProtect Corporate de controle
2. Drivers Milestone Interconnect (lidam com a conexão entre os servidores de gravação das centrais de controle e a base remota, devem ser selecionados na lista de drivers ao se adicionar sistemas remotos através do assistente **Adicionar hardware**)
3. Conexão Milestone Interconnect
4. Base remota do Milestone Interconnect (base remota completa com a instalação do sistema, os usuários, as câmeras e assim por diante)
5. Sistema remoto do Milestone Interconnect (a instalação técnica na base remota)

Você adiciona bases remotas à sua central de controle com o assistente **Adicionar Hardware** da central de controle (consulte Adicione uma base remota para o seu site central Milestone Interconnect na página 325).

Cada base remota funciona de forma independente e pode executar quaisquer tarefas normais de vigilância. Dependendo das conexões de rede e das permissões de usuário apropriadas (consulte Atribua permissões de usuário na página 326), o Milestone Interconnect oferece visualização direta ao vivo de câmeras de locais remotos e reprodução de gravações de locais remotos no local central.

A central de controle só pode ver e acessar dispositivos aos quais a conta do usuário especificada tenha acesso. Isso permite que os administradores de sistema local controlem quais dispositivos devem ser disponibilizados para a central de controle e seus usuários.

Sobre a central de controle, você pode visualizar o status do próprio sistema de câmeras interconectadas, mas não diretamente o estado da base remota. Em vez disso, para monitorar a base remota, você pode usar os eventos de bases remotas para disparar alarmes ou outras notificações na central de controle (consulte Configure a sua central de controle para responder aos eventos de bases remotas na página 327).

Ele também lhe oferece a possibilidade de transferir gravações da base remota para a central de controle com base tanto em eventos, regras/programações quanto em solicitações manuais de usuários do XProtect Smart Client.

Apenas os sistemas XProtect Corporate podem funcionar como centrais de controle. Todos os outros produtos podem agir como base remota, incluindo XProtect Corporate. Isso varia conforme a configuração, as versões, quantas câmeras, e como os dispositivos e eventos originários da base remota são tratados - se esse for o caso - pela central de controle. Para mais detalhes sobre como produtos específicos XProtect interagem em uma configuração Milestone Interconnect, acesse o website Milestone Interconnect (https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/).

Selecionar Milestone Interconnect ou Milestone Federated Architecture (explicado)

Em um sistema distribuído fisicamente no qual usuários na central de controle precisam acessar o vídeo na base remota, é possível escolher entre Milestone Interconnect™ ou Milestone Federated Architecture™.

A Milestone recomenda Milestone Federated Architecture quando:

- A conexão de rede entre a central de controle e os sites federados é estável
- A rede usa o mesmo domínio
- Há poucos sites de grande porte
- A largura de banda é suficiente para o uso exigido

A Milestone recomenda Milestone Interconnect quando:

- A conexão de rede entre a central de controle e as bases remotas é instável
- Você ou sua organização querem usar outro produto XProtect nas bases remotas
- A rede utiliza diferentes domínios ou grupos de trabalho
- Há muitos sites de pequeno porte

Milestone Interconnect e licenciamento

Para executar Milestone Interconnect, você precisa de licenças de câmera Milestone Interconnect na sua central de controle para visualizar vídeos a partir de dispositivos de hardware em base remota. O número de licenças de câmeras Milestone Interconnect necessárias depende do número de dispositivos de hardware nos sites remotos, dos quais você quer receber dados. Apenas XProtect Corporate pode atuar como uma central de controle.

O estado das suas licenças de câmera Milestone Interconnect está listado na página **Informações de licença** da central de controle.

Configurações Milestone Interconnect (explicado)

Existem três formas possíveis de executar Milestone Interconnect. A forma de executar a sua configuração depende da sua conexão de rede, da maneira de reproduzir as gravações e se você recupera gravações remotas e até que ponto o faz.

A seguir, os três cenários mais prováveis estão descritos:

Reprodução direta de bases remotas (boas conexões de rede)

A configuração mais simples. A central de controle está permanentemente on-line com suas bases remotas e os usuários da central de controle reproduzindo gravações remotas diretamente de bases remotas. Isso exige o uso da opção **Reproduzir gravações do sistema remoto** (consulte Permitir a reprodução diretamente da câmera da base remota na página 326).

A recuperação baseada em regra ou no XProtect Smart Client de sequências selecionadas de gravação remota de bases remotas (conexões de rede limitadas periodicamente)

Usada quando as sequências selecionadas (provenientes de bases remotas) devem ser armazenadas centralmente para garantir a independência de bases remotas. A independência é crucial em caso de falha de rede ou restrições de rede. Você pode configurar as definições de recuperação de gravações remotas na guia **Recuperação remota** (consulte Guia Recuperação remota na página 444).

A recuperação de gravações remotas pode ser iniciada a partir do XProtect Smart Client quando necessário ou uma regra pode ser configurada. Em alguns cenários, as bases remotas estão on-line e, em outros, off-line a maior parte do tempo. Isso é muitas vezes determinado pela indústria. Para algumas indústrias, é comum que a central de controle esteja permanentemente on-line com suas bases remotas (por exemplo, uma sede principal de varejo (central de controle) e um número de lojas (locais remotos)). Para outras indústrias, como o transporte, as bases remotas são móveis (por exemplo, ônibus, trens, navios, e assim por diante) e só podem estabelecer conexão de rede de forma aleatória. Caso a conexão de rede falhe durante uma recuperação de gravação remota já iniciada, o trabalho continua na próxima oportunidade dada.

Se o sistema detectar uma recuperação automática ou solicitação de recuperação a partir do XProtect Smart Client fora do intervalo de tempo que você especificou na guia **Recuperação remota**, ele é aceito, mas não

iniciado até que o intervalo de tempo selecionado seja atingido. Novos trabalhos de recuperação de gravação remota farão fila e começarão quando o intervalo de tempo permitido for atingido. Você pode ver os trabalhos pendentes de recuperação de gravação remota do **Painel do sistema** -> **Tarefas atuais**.

Após falha de conexão, as gravações remotas faltantes são, por padrão, recuperadas de bases remotas

Usa bases remotas como um servidor de gravação utiliza o armazenamento de borda em uma câmera. Normalmente, as bases remotas estão on-line com o central de controle, alimentando um fluxo ao vivo que a própria central registra. Caso a rede falhe por algum motivo, a central de controle omite sequências de gravação. No entanto, uma vez que a rede é restabelecida, a central de controle recupera automaticamente as gravações remotas cobrindo o período de inatividade. Isso requer o uso da opção **Recuperar automaticamente as gravações remotas quando a conexão for restaurada** (consulte Recuperar gravações remotas da câmera da base remota na página 327) na guia **Gravar** para a câmera.

Você pode misturar qualquer uma das soluções acima para atender às necessidades especiais da sua organização.

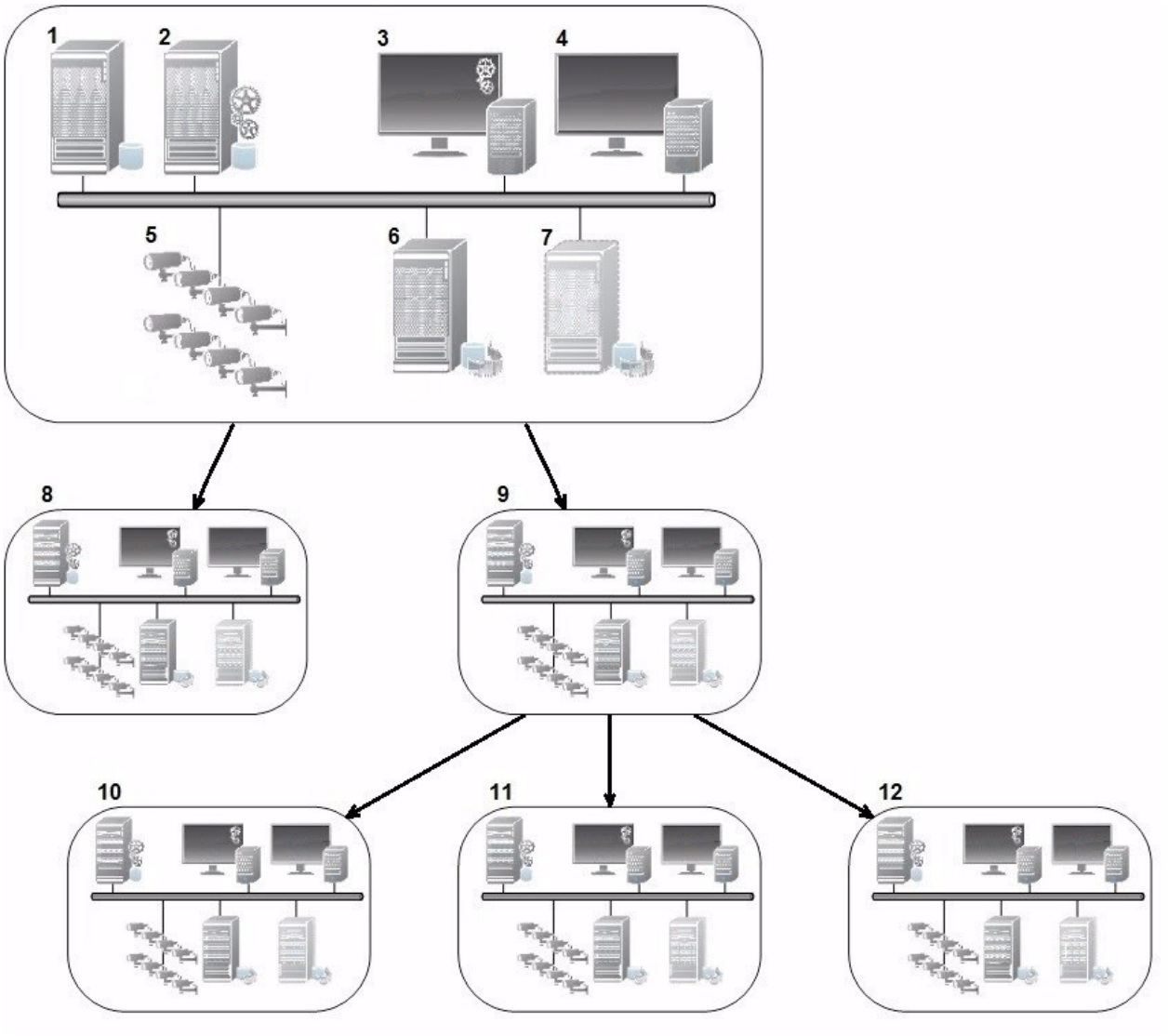
Configurando Milestone Federated Architecture

XProtect Expert só podem ser federados como sites filho.

A Milestone Federated Architecture interconecta vários sistemas individuais padrão em uma hierarquia federada de sites primário/secundário. Usuários clientes com permissão suficiente têm acesso direto a vídeo, áudio e outros recursos em sites individuais. Os administradores podem centralizar o gerenciamento de todos os sites da versão 2018 R1 e mais recente dentro da hierarquia federada, baseada em permissões de administrador para sites individuais.

Usuários básicos não são compatíveis com sistemas Milestone Federated Architecture, portanto é preciso adicionar usuários como usuários do Windows por meio do serviço Active Directory.

Milestone Federated Architecture é configurada com uma central de controle (site principal) e um número ilimitado de sites federados (consulte Configure seu sistema para executar sites federados na página 319). Quando logado a um site, você tem informações sobre todos os sites secundários e os sites secundários dos sites secundários. A ligação entre dois sites é estabelecida quando você solicita o link do site pai (consulte Adicionar site à hierarquia na página 321). Um site secundário só pode ser ligado a um site primário. Se você não for o administrador do site secundário, ao adicioná-lo à hierarquia de sites federados o pedido deve ser aceito pelo administrador do site secundário.



Os componentes de uma configuração da Milestone Federated Architecture:

1. Servidor com SQL Server
2. Servidor de gerenciamento
3. Management Client
4. XProtect Smart Client
5. Câmeras
6. Servidor de gravação
7. Servidor do sistema de gravação ininterrupta (failover)
8. para 12. Sites federados

Sincronização de hierarquia

Um site primário contém uma lista atualizada de todos os seus sites secundários anexados atualmente, sites secundários dos sites secundários, e assim por diante. A hierarquia de sites federados tem sincronização regular entre sites, bem como sincronização toda vez que um site é adicionado ou removido pelo sistema. A sincronização da hierarquia ocorre nível a nível, cada nível de comunicação avançando e retornando, até alcançar o servidor que requisitou a informação. O sistema envia menos de 1 MB de cada vez. Dependendo do número de níveis a ser atualizado, as alterações em uma hierarquia podem levar algum tempo para se tornarem visíveis no Management Client. Não é possível agendar suas próprias sincronizações.

Tráfego de dados

O sistema envia configurações ou dados de configuração quando um usuário ou administrador visualiza vídeo ao vivo ou gravado ou configurar um site. A quantidade de dados vai depender do que e quanto se visualiza ou configura.

Milestone Federated Architecture com outros produtos e requisitos do sistema

- A abertura do Management Client em um Milestone Federated Architecture é suportada para três versões principais, incluindo a que está sendo lançada no momento. Em uma configuração do Milestone Federated Architecture além deste escopo, você precisará de um Management Client separado que corresponda à versão do servidor.
- Se a central de controle usar XProtect Smart Wall, você também pode usar os recursos do XProtect Smart Wall na hierarquia de sites federados.
- Se a central de controle usar XProtect Access e um usuário do XProtect Smart Client se conectar a um site de uma hierarquia de sites federados, as notificações de solicitação de acesso a sites federados também aparecem em XProtect Smart Client
- Você pode adicionar sistemas XProtect Expert 2013 ou mais recentes à hierarquia de sites federados como sites filho, não como sites pai
- A Milestone Federated Architecture não requer licenças adicionais
- Para mais informações sobre casos de uso e benefícios, consulte o informativo sobre o Milestone Federated Architecture.

Estabelecendo uma Hierarquia de sites federados

Antes de começar a construir a hierarquia no Management Client, a Milestone recomenda que você mapeie como deseja que seus sites sejam vinculados.

Cada site em uma hierarquia federada é instalado e configurado como sistema autônomo normal com componentes de sistema, configurações, regras, agendas, administradores, usuários e permissões de usuários. Se você já tem os sites instalados e configurados e só precisa combiná-los em uma hierarquia de sites federados, seus sistemas estão prontos para ser configurados.

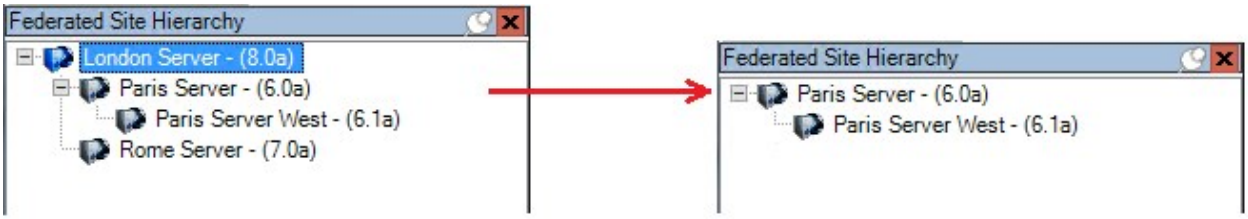
Uma vez que os sites individuais estejam instalados, você deve configurá-los para serem executados como sites federados (consulte Configure seu sistema para executar sites federados na página 319).

Para iniciar a hierarquia, você pode fazer login no site que você deseja trabalhar como a central de controle e adicionar (consulte Adicionar site à hierarquia na página 321) o primeiro site federado. Quando o link é estabelecido, os dois sites automaticamente criam uma hierarquia de sites federados no painel **Hierarquia de sites federados** no Management Client, no qual mais sites podem ser adicionados para aumentar a hierarquia federada.

Criada a hierarquia de sites federados, usuários e administradores podem fazer login em um site para acessá-lo e a qualquer site federado que desejar. O acesso a sites federados depende das permissões do usuário.

Não há limite para o número de sites que você pode adicionar à hierarquia de sites federados. Além disso, é possível ter um site com uma versão mais antiga do produto ligado a uma versão mais nova e vice-versa. Os números de versão aparecem automaticamente e não podem ser excluídos. O servidor primário em que você está logado está sempre no topo do painel da **hierarquia de sites federados** e é chamado home site.

Abaixo está um exemplo de site federado no Management Client. À esquerda, o usuário fez o login no site superior. À direita, o usuário fez o login em um dos sites filhos, o servidor de Paris, que é o home site.



Status dos ícones na Milestone Federated Architecture

Os ícones representam os estados possíveis de um site:

Descrição	Ícone
O site superior de toda a hierarquia está operacional.	
O site superior de toda a hierarquia ainda está operacional, mas um ou mais problemas requerem atenção. Mostrado em cima do ícone do site superior.	
O site está operacional.	
O site aguarda ser aceito na hierarquia.	
O site está atribuído, mas ainda não está operacional.	

Portas usadas pelo sistema

Todos os componentes XProtect e portas necessitadas por eles estão listados abaixo. Para garantir, por exemplo, que o firewall bloqueie apenas o tráfego indesejado, você precisa especificar as portas que o sistema usa. Você deve habilitar apenas estas portas. As listas também incluem as portas usadas para processos locais.

Elas são organizadas em dois grupos:

- **Componentes do servidor** (serviços) oferecem os seus serviços em portas específicas e é por isso que eles precisam para escutar as solicitações de clientes em uma dessas portas. Portanto, estas portas precisam ser abertas no Firewall do Windows para conexões de entrada e saída
- **Componentes de cliente** (clientes) iniciam as conexões para portas particulares sobre os componentes de servidor. Por conseguinte, essas portas precisam ser abertas para as conexões de saída. As conexões de saída normalmente são abertas por padrão no Firewall do Windows

Se nada mais for mencionado, as portas para os componentes do servidor devem ser abertas para as conexões de entrada, e as portas para os componentes do cliente devem ser abertas para as conexões de saída.

Tenha em mente que os componentes do servidor podem agir como clientes para outros componentes do servidor. Elas não estão explicitamente listadas neste documento.

Os números de porta são os números padrão, mas isto pode ser alterado. Contate o Suporte da Milestone se precisar mudar portas que não são configuráveis através do Management Client.

Componentes do servidor (conexões de entrada)

Cada uma das seções a seguir lista as portas que devem ser abertas para um serviço específico. Para descobrir quais portas precisam ser abertas em um determinado computador, você precisa considerar todos os serviços em execução no computador.

Serviço Management Server e processos relacionados

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
80	HTTP	IIS	Todos os servidores e o XProtect Smart Client e o Management Client	A finalidade da porta 80 e da porta 443 é a mesma. No entanto, qual porta o sistema de gerenciamento de vídeo usa depende se você usou certificados para proteger a comunicação. • Se você não protegeu a comunicação com certificados, o VMS usa a porta 80. • Quando você protege a comunicação com certificados, o VMS usa a porta 443, exceto para comunicação do servidor de eventos com o servidor de gerenciamento. A comunicação do servidor de eventos com o servidor de gerenciamento usa o Windows Secured Framework (WCF) e autenticação do Windows na porta 80.
443	HTTPS	IIS		
6473	TCP	Serviço Management Server	Management Server Manager ícone de bandeja, conexão local apenas.	Exibindo o status e gerenciando o serviço.
8080	TCP	Servidor de gerenciamento	Apenas conexão local.	Comunicação entre processos internos do servidor.
9000	HTTP	Servidor de gerenciamento	Serviços Recording	Serviço da web para comunicação interna entre servidores.

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
			Server	
12345	TCP	Serviço Management Server	XProtect Smart Client	Comunicação entre o sistema e os destinatários Matrix. Você pode alterar o número da porta no Management Client.
12974	TCP	Serviço Management Server	Serviço Windows SNMP	A comunicação com o agente de extensão SNMP. Não use a porta para outros fins, mesmo que o seu sistema não use SNMP. Nos sistemas XProtect 2014 ou mais antigos, o número da porta era 6475. Nos sistemas XProtect 2019 R2 e anteriores, o número da porta era 7475.

SQL ServerServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
1433	TCP	SQL Server	Serviço Management Server	Como armazenar e recuperar configurações através do Identity Provider.
1433	TCP	SQL Server	Serviço Event Server	Como armazenar e recuperar eventos através do Identity Provider.
1433	TCP	SQL Server	Serviço Log Server	Como armazenar e recuperar entradas de registro através do Identity Provider.

Data CollectorServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
7609	HTTP	IIS	No computador do servidor de gerenciamento: Serviços Data Collector em todos os outros servidores. Em outros computadores: Serviço Data Collector no servidor de gerenciamento.	Monitor do Sistema.

Event ServerServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
1234	TCP/UDP	Serviço Event Server	Qualquer servidor enviando eventos genéricos para o seu sistema XProtect.	Ouvir eventos genéricos de sistemas ou dispositivos externos. Apenas se a fonte de dados relevante estiver ativada.
1235	TCP	Serviço Event Server	Qualquer servidor enviando eventos genéricos para o seu sistema XProtect.	Ouvir eventos genéricos de sistemas ou dispositivos externos. Apenas se a fonte de dados relevante estiver ativada.
9090	TCP	Serviço Event Server	Qualquer sistema ou dispositivo que envia eventos analíticos para o seu sistema XProtect.	Ouvir eventos de análise de sistemas ou dispositivos externos. Só é relevante se o recurso Eventos de Análise estiver ativado.

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
22331	TCP	Serviço Event Server	XProtect Smart Client e o Management Client	Configuração, eventos, alarmes e dados do mapa.
22332	WS/WSS HTTP/HTTPS*	Serviço Event Server	API Gateway e o Management Client	Assinatura de evento/estado, API REST de eventos, API Websockets Messaging e API REST de alarmes.
22333	TCP	Serviço Event Server	Plug-ins e aplicativos MIP.	Mensagens MIP.

*Um erro 403 será apresentado durante a tentativa de acessar HTTP para visualizar um endpoint exclusivo de HTTPS.

Recording ServerServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
25	SMTP	Serviço Recording Server	Câmeras, codificadores e dispositivos de E/S.	Ouvir as mensagens de eventos de dispositivos. A porta está desativada por padrão. (Obsoleto) Habilitar isto abrirá uma porta para conexões não criptografadas e não é recomendado.
5210	TCP	Serviço Recording Server	Servidores de gravação de failover.	Mesclagem dos bancos de dados após um servidor do sistema de gravação ininterrupta (failover) ter sido executado.

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
5432	TCP	Serviço Recording Server	Câmeras, codificadores e dispositivos de E/S.	Ouvir as mensagens de eventos de dispositivos. A porta está desativada por padrão.
7563	TCP	Serviço Recording Server	XProtect Smart Client, Management Client	Recuperando fluxos de vídeo e áudio, comandos PTZ.
8966	TCP	Serviço Recording Server	Recording Server Manager ícone de bandeja, conexão local apenas.	Exibindo o status e gerenciando o serviço.
9001	HTTP	Serviço Recording Server	Servidor de gerenciamento	Serviço da web para comunicação interna entre servidores. Se diversas instâncias do Servidor de gravação estiverem em uso, cada instância precisa de sua própria porta. Portas adicionais serão 9002, 9003, etc.
11000	TCP	Serviço Recording Server	Servidores de gravação de failover	Sondagem (verificação regular) do estado dos servidores de gravação.
12975	TCP	Serviço Recording Server	Serviço Windows SNMP	A comunicação com o agente de extensão SNMP. Não use a porta para outros fins, mesmo que o seu sistema não use SNMP. Nos sistemas XProtect 2014 ou mais antigos, o número da porta era 6474. Nos sistemas XProtect 2019 R2 e

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
				anteriores, o número da porta era 7474.
65101	UDP	Serviço Recording Server	Apenas conexão local	Ouvir notificações de eventos dos drivers.

Além das conexões de entrada para o serviço Recording Server listado acima, o serviço Recording Server estabelece conexões de saída para:

- Câmeras
- NVRs
- Sites interconectados remotos (Interconectar ICP Milestone)

Serviço Failover Server e serviço Failover Recording Server

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
25	SMTP	Serviço Failover Recording Server	Câmeras, codificadores e dispositivos de E/S.	Ouvir as mensagens de eventos de dispositivos. A porta está desativada por padrão. (Obsoleto) Habilitar isto abrirá uma porta para conexões não criptografadas e não é recomendado.
5210	TCP	Serviço Failover Recording Server	Servidores de gravação de failover	Mesclagem dos bancos de dados após um servidor do sistema de gravação ininterrupta (failover) ter sido executado.

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
5432	TCP	Serviço Failover Recording Server	Câmeras, codificadores e dispositivos de E/S.	Ouvir as mensagens de eventos de dispositivos. A porta está desativada por padrão.
7474	TCP	Serviço Failover Recording Server	Serviço Windows SNMP	A comunicação com o agente de extensão SNMP. Não use a porta para outros fins, mesmo que o seu sistema não use SNMP.
7563	TCP	Serviço Failover Recording Server	XProtect Smart Client	Recuperando fluxos de vídeo e áudio, comandos PTZ.
8844	UDP	Serviço Failover Recording Server	Comunicação entre serviços do Failover Recording Server.	Comunicação entre os servidores.
8966	TCP	Serviço Failover Recording Server	Failover Recording Server Manager ícone de bandeja, conexão local apenas.	Exibindo o status e gerenciando o serviço.
8967	TCP	Serviço Failover Server	Failover Server Manager ícone de bandeja, conexão local apenas.	Exibindo o status e gerenciando o serviço.
8990	HTTP	Serviço Failover Server	Serviço Management Server	Monitorar o status do serviço Failover Server.
9001	HTTP	Serviço Failover Server	Servidor de gerenciamento	Serviço da web para comunicação interna entre servidores.

Além das conexões de entrada para o serviço de servidor de emergência/Failover Recording Server listado acima, o serviço servidor de emergência/Failover Recording Server estabelece conexões de saída para os gravadores e câmeras regulares e para Vídeo Push.

Log ServerServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
22337	HTTP	Serviço Log Server	Todos os componentes Management Client exceto para XProtect e o servidor de gravação.	Escreva para, leia do e configure o servidor de registros.

Mobile ServerServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
8000	TCP	Serviço Mobile Server	Mobile Server Manager ícone de bandeja, conexão local apenas.	Aplicativo SysTray.
8081	HTTP	Serviço Mobile Server	Clientes móveis, clientes da Web e Management Client.	Enviando fluxos de dados; vídeo e áudio.
8082	HTTPS	Serviço Mobile Server	Clientes móveis e clientes da Web.	Enviando fluxos de dados; vídeo e áudio.
40001 - 40099	HTTP	Serviço Mobile Server	Serviço do servidor de gravação	Mobile Server Vídeo Push. Esta porta está desativada por padrão.

LPR ServerServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
22334	TCP	Serviço LPR Server	Servidor de eventos	Recuperando as placas de licença reconhecidas e o status do servidor. Para conectar o Servidor de eventos é preciso ter o plug-in LPR instalado.
22334	TCP	Serviço LPR Server	LPR Server Manager ícone de bandeja, conexão local apenas.	Aplicativo SysTray.

Milestone Open Network BridgeServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
580	TCP	Serviço Milestone Open Network Bridge	Clientes ONVIF	Autenticação e solicitações para configuração de fluxo de vídeo.
554	RTSP	Serviço RTSP	Clientes ONVIF	Fluxo de vídeo solicitado para clientes do ONVIF.

XProtect DLNA ServerServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
9100	HTTP	Serviço DLNA	Dispositivo DLNA	Descoberta de dispositivos e fornecimento de configuração de canais DLNA.

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
		Server		Solicitações de fluxos de vídeo.
9200	HTTP	Serviço DLNA Server	Dispositivo DLNA	Fluxo de vídeo solicitado para dispositivos DLNA.

XProtect Screen RecorderServiço

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
52111	TCP	XProtect Screen Recorder	Serviço Recording Server	Fornece vídeo de um monitor. Aparece e funciona da mesma forma que uma câmera no servidor de gravação. Você pode alterar o número da porta no Management Client.

Serviço XProtect Incident Manager

Número da porta	Protocolo	Processo	Conexões de...	Objetivo
80	HTTP	IIS	XProtect Smart Client e o Management Client	A finalidade da porta 80 e da porta 443 é a mesma. No entanto, qual porta o sistema de gerenciamento de vídeo usa depende se você usou certificados para proteger a comunicação. • Se você não protegeu a comunicação com certificados, o VMS usa a porta 80. • Se você protegeu a comunicação com certificados, o VMS usa a porta 443.
443	HTTPS	IIS		

Componentes do servidor (conexões de saída)

Management ServerServiço

Número da porta	Protocolo	Conexões de...	Objetivo
443	HTTPS	O servidor de licença que hospeda o serviço de gerenciamento de licenças. A comunicação acontece via https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx	Ativação de licenças.

Serviço Recording Server

Número da porta	Protocolo	Conexões de...	Objetivo
80	HTTP	Câmeras, NVRs, codificadores Locais interconectados	Autenticação, configuração, fluxos de dados, vídeo e áudio. Login
443	HTTPS	Câmeras, NVRs, codificadores	Autenticação, configuração, fluxos de dados, vídeo e áudio.
554	RTSP	Câmeras, NVRs, codificadores	Fluxos de dados, vídeo e áudio.
7563	TCP	Locais interconectados	Fluxos de dados e eventos.
11000	TCP	Servidores de gravação de failover	Sondagem (verificação regular) do estado dos servidores de gravação.
40001 - 40099	HTTP	Serviço de servidor móvel	Vídeo push de servidor móvel. Esta porta está desativada por padrão.

Serviço Failover Server e serviço Failover Recording Server

Número da porta	Protocolo	Conexões de...	Objetivo
11000	TCP	Servidores de gravação de failover	Sondagem (verificação regular) do estado dos servidores de gravação.

Serviço Event Server

Número da porta	Protocolo	Conexões de...	Objetivo
80	HTTP	API Gateway e o Management Server	Acessar a API de configuração do API Gateway
443	HTTPS	API Gateway e o Management Server	Acessar a API de configuração do API Gateway
443	HTTPS	Via Milestone Customer Dashboard https://service.milestonesys.com/	Enviar status, eventos e mensagens de erro do sistema XProtect para Milestone Customer Dashboard.

Serviço Log Server

Número da porta	Protocolo	Conexões de...	Objetivo
443	HTTP	Servidor de registros	Encaminhar mensagens para o servidor de registros.

API Gateway

Número da porta	Protocolo	Conexões de...	Objetivo
443	HTTPS	Management Server	RESTful API
22332	WS/WSS HTTP/HTTPS*	Management Client	Assinatura de evento/estado, API REST de eventos, API Websockets Messaging e API REST de alarmes.

Câmeras, codificadores e dispositivos I/O (conexões de entrada)

Número da porta	Protocolo	Conexões de...	Objetivo
80	TCP	Servidores de gravação e servidores de gravação de failover	Autenticação, configuração e fluxos de dados; vídeo e áudio.
443	HTTPS	Servidores de gravação e servidores de gravação de failover	Autenticação, configuração e fluxos de dados; vídeo e áudio.
554	RTSP	Servidores de gravação e servidores de gravação de failover	Fluxos de dados; vídeo e áudio.

Câmeras, codificadores e dispositivos I/O (conexões de saída)

Número da porta	Protocolo	Conexões de...	Objetivo
25	SMTP	Servidores de gravação e servidores de gravação de failover	Enviando notificações de eventos (obsoleto).
5432	TCP	Servidores de gravação e servidores de gravação de failover	Enviando notificações de eventos. A porta está desativada por

Número da porta	Protocolo	Conexões de...	Objetivo
			padrão.
22337	HTTP	Servidor de registros	Encaminhar mensagens para o servidor de registros.

Apenas alguns modelos de câmera são capazes de estabelecer conexões de saída.

Componentes do cliente (conexões de saída)

XProtect Smart Client, XProtect Management Client, servidor XProtect Mobile

Número da porta	Protocolo	Conexões de...	Objetivo
80	HTTP	Serviço API Gateway e Management Server	APIs de autenticação e de outros tipos no API Gateway.
443	HTTPS	Serviço API Gateway e Management Server	Autenticação de usuários básicos quando a criptografia está ativada e outras APIs no API Gateway.
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com at 52.178.114.226)	Management Client e Smart Client ocasionalmente verificam se a ajuda on-line está disponível acessando o URL de ajuda.
7563	TCP	Serviço Recording Server	Recuperando fluxos de vídeo e áudio, comandos PTZ.
22331	TCP	Serviço Event Server	Alarmes.

XProtect Web Client, cliente XProtect Mobile

Número da porta	Protocolo	Conexões de...	Objetivo
8081	HTTP	Servidor XProtect Mobile	Recuperando fluxos de vídeo e áudio.
8082	HTTPS	Servidor XProtect Mobile	Recuperando fluxos de vídeo e áudio.

API Gateway

Número da porta	Protocolo	Conexões de...	Objetivo
80	HTTP	Management Server	RESTful API
443	HTTPS	Management Server	RESTful API

Grupos de aplicativos

O VMS contém grupos de aplicativos padrão, como.NET v4.5, .NET v4.5 Classic e o DefaultAppPool. Os grupos de aplicativos disponíveis em seu sistema aparecem no Internet Information Services (IIS) Manager. Além dos pools de aplicativos padrão mencionados acima, um conjunto de pools de aplicativos VideoOS é fornecido com o Milestone XProtect VMS.

Grupos de aplicativos em Milestone XProtect

Na tabela abaixo, você pode obter uma visão geral dos grupos aplicativos VideoOS fornecidos com o Milestone XProtect.

Nome	Identidade	Objetivo
.NET v4.5	ApplicationPoolId	Recurso padrão IIS
.NET v4.5 Clássico	ApplicationPoolId	Recurso padrão IIS
DefaultAppPool	ApplicationPoolId	Recurso padrão IIS

Nome	Identidade	Objetivo
VideoOS ApiGateway	NetworkService	Hospeda o API Gateway XProtect, que é a futura API pública e gateway para o VMS.
VideoOS Clássico	NetworkService	Hospeda componentes legados, como a ajuda local, principalmente para cumprir a compatibilidade com versões anteriores.
VideoOS IDP	NetworkService	Hospeda a API Identity Provider. O Identity Provider cria, mantém e gerencia informações de identidade para usuários básicos e fornece serviços de autenticação e registro para aplicativos ou serviços confiáveis.
VideoOS IM	NetworkService	Hospeda a API XProtect Incident Manager. Os XProtect Incident Manager documentos incidentes e combinam com evidências de sequência (vídeo e, potencialmente, áudio) de seu VMS XProtect.
VideoOS Management Server	NetworkService	Hospeda a API de configuração, APIs de componentes de servidor e outros serviços do Management Server, além de gerenciar a autorização do usuário.
VideoOS ReportServer	NetworkService	Hospeda o aplicativo Web responsável por coletar e criar relatórios de alarmes e eventos.
VideoOS ShareService	NetworkService	Hospeda o serviço que facilita compartilhamento de marcadores e de vídeos ao vivo entre os usuários do cliente do XProtect Mobile.

Trabalhando com grupos de aplicativos

Na página **Grupos de aplicativos** na janela **Serviços de Informações da Internet (IIS),** você pode adicionar grupos de aplicativos ou definir padrões de grupo de aplicativos e pode visualizar os aplicativos hospedados por cada grupo de aplicativos.

Abra a página Grupos de aplicativos

1. No menu **Iniciar** do Windows, abra **Gerenciador do Serviço de Informações da Internet (IIS)**.
2. No painel **Conexões**, clique no nome do seu ambiente e, em seguida, clique em **Grupos de aplicativos**.
3. Em **Ações**, clique em **Adicionar Grupo de aplicativos** ou **Definir Padrões de grupo de aplicativos** para executar qualquer uma dessas tarefas.
4. Selecione um grupo de aplicativos na página **Grupo de aplicativos** para exibir outras opções em **Ações** para cada grupo de aplicativos.

Comparação de produto

O XProtect VMS inclui os seguintes produtos:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Licenciamento

Licenças (explicadas)

XProtect Essential+ gratuito

Se você tiver instalado o XProtect Essential+, poderá executar o sistema e oito licenças de dispositivo gratuitamente. A ativação automática da licença está ativada e o hardware será ativado assim que adicioná-lo ao sistema.

Apenas quando você atualizar para um produto XProtect mais avançado e precisar mudar o seu SLC (Código de licença de software) (consulte Alterar o código da licença de software na página 129), o resto deste tópico e outros tópicos relacionados neste documentação poderão ser relevantes a você.

Licenças para produtos VMS XProtect (exceto XProtect Essential+)

Arquivo de licença de software e SLCs

Quando tiver adquirido o seu software e licenças, irá receber:

- Uma confirmação de pedido e um arquivo de licença de software (SLC) com o mesmo nome de seu SLC (código da licença de software) e com a extensão .lic recebido por e-mail
- Uma cobertura Milestone Care

O seu SLC é também impresso na confirmação do seu pedido e consiste de vários números e letras agrupados por hifens, como:

- Versão 2014 ou anterior do produto: xxx-xxxx-xxxx
- Versão 2016 ou posterior do produto: xxx-xxx-xxx-xx-xxxxxx

O arquivo de licença de software contém todas as informações sobre seus produtos, extensões XProtect e licenças de VMS adquiridos. Milestone recomenda que você armazene as informações sobre o seu SLC e uma cópia do seu arquivo de licença de software em um lugar seguro para uso posterior. Você também pode ver seu SLC na janela **Informações da Licença** no Management Client. Você pode abrir a janela **Informações da licença** no painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**. Você pode precisar do arquivo de licença de software ou do seu SLC quando, por exemplo, criar uma conta de usuário My Milestone. Nesse caso, entre em contato com o seu revendedor para obter suporte ou se precisar fazer alterações ao sistema.

Processo geral de instalação e licenciamento

Para começar, faça o download do software a partir do nosso site (https://www.milestonesys.com/downloads/). Quando estiver instalando o software (consulte Instalar um novo sistema XProtect na página 152), será solicitado que forneça um arquivo de licença válido. Você não pode

concluir a instalação sem um arquivo de licença de software.

Assim que a instalação for concluída e você tiver adicionado algumas câmeras, é preciso ativar suas licenças (consulte Ativação de licença (explicado) na página 121). Você ativa suas licenças na janela **Informações da Licença** em Management Client. Aqui você também pode ter uma visão geral de suas licenças para todas as instalações no mesmo SLC. Você pode abrir a janela **Informações da licença** no painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**.

Tipos de licença

Existem vários tipos de licença no sistema de licenciamento do XProtect.

Licenças básicas

No mínimo, você tem uma licença básica para um dos produtos VMS XProtect. Você também pode ter uma ou mais licenças básicas para extensões XProtect.

Licenças do dispositivo

No mínimo, você tem várias licenças de dispositivo. Geralmente, você precisa de uma licença de dispositivo por dispositivo de hardware com uma câmera que deseja adicionar ao seu site. Mas isso pode variar de um dispositivo de hardware para outro e dependendo do dispositivo de hardware ser um dispositivo de hardware compatível com Milestone ou não. Para obter mais informações, consulte Dispositivos de hardware compatíveis na página 120 e Dispositivos de hardware não suportados na página 121.

Se deseja usar o recurso vídeo push em XProtect Mobile, você também precisa de uma licença de dispositivo de hardware por dispositivo móvel ou tablet que deve ser capaz de enviar vídeo push ao seu site.

Não são necessárias licenças de dispositivo para alto-falantes, microfones ou dispositivos de entrada e de saída conectados às suas câmeras.

Dispositivos de hardware compatíveis

Geralmente, você precisa de uma licença de dispositivo por dispositivo de hardware com uma câmera que deseja adicionar ao seu site. Mas alguns dispositivos de hardware com suporte exigem mais de uma licença de dispositivo. Você pode ver quantas licenças de dispositivo seus dispositivos de hardware exigem, na lista de hardware compatível no Milestone site (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Para codificadores de vídeo com até 16 canais, você precisa apenas de uma licença de dispositivo por endereço IP do codificador de vídeo. Um codificador de vídeo pode ter um ou mais endereços IP.

No entanto, se o codificador de vídeo tiver mais de 16 canais, é necessária uma licença de dispositivo por câmera ativada no codificador de vídeo – também para as primeiras 16 câmeras ativadas.

Dispositivos de hardware não suportados

Um dispositivo de hardware não compatível requer uma licença de dispositivo por câmera ativada usando um canal de vídeo.

Dispositivos de hardware sem suporte não aparecem na lista de hardware com suporte no site da Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Licenças da câmera para Milestone Interconnect™

Para executar Milestone Interconnect, você precisa de licenças de câmera Milestone Interconnect na sua central de controle para visualizar vídeos a partir de dispositivos de hardware em base remota. O número de licenças de câmeras Milestone Interconnect necessárias depende do número de dispositivos de hardware nos sites remotos, dos quais você quer receber dados. Apenas XProtect Corporate pode atuar como uma central de controle.

Licenças para extensões XProtect

A maioria das extensões XProtect exigem tipos adicionais de licença. O arquivo de licença de software também inclui informações sobre suas licenças de extensão. Algumas extensões têm seus próprios arquivos distintos de licença de software.

Ativação de licença (explicado)

Seu SLC deve ser registrado antes da instalação (consulte Registrar o código da licença de software na página 149). É necessário ativar suas diferentes licenças conectadas aos seus códigos da licença de software (SLCs) para que o VMS XProtect e as extensões XProtect instalados funcionem e os dispositivos de hardware individuais possam enviar dados para o sistema. Para uma visão geral de todos os tipos de licença XProtect, consulte Tipos de licença na página 120.

Existem várias maneiras de ativar licenças. Todas elas estão disponíveis na janela de **Informações da licença**. A melhor forma de ativação depende das políticas da sua organização e se o seu servidor de gerenciamento tem acesso à internet ou não. Para saber como ativar licenças, consulte Ative suas licenças na página 126.

Após a ativação da licença inicial de seu VMS XProtect, você não precisa ativar licenças de dispositivo toda vez que adicionar um dispositivo de hardware com uma câmera devido às flexibilidades integradas ao sistema de licenciamento XProtect. Para obter mais informações sobre essas flexibilidades, consulte Período de gratuidade para ativação da licença (explicado) na página 122 e Alterações do dispositivo sem ativação (explicado) na página 122.

Ativação automática de licença (explicado)

Para fácil manutenção e flexibilidade – e quando as políticas da sua organização permitirem – a Milestone recomenda que você habilite a ativação automática da licença. A ativação automática de licença exige que o seu servidor de gerenciamento esteja on-line. Para sber como habilitar a ativação automática de licença, consulte Habilitar ativação automática de licença na página 126.

Benefícios de habilitar ativação automática de licença

- O sistema ativa os dispositivos de hardware poucos minutos depois de você ter adicionado, removido ou substituído dispositivos de hardware ou feito outras mudanças que afetem o uso de suas licenças. Portanto, raramente você deve iniciar manualmente uma ativação de licença. Consulte as poucas exceções em Quando a ativação manual da licença ainda é necessária na página 122.
- O número de alterações no dispositivo sem ativação é sempre zero.
- Nenhum dispositivo de hardware está dentro de um período de carência e em risco de expirar.
- Se uma das suas licenças básicas expirar dentro de um período de 14 dias, o seu sistema XProtect também - como uma precaução extra - tentará automaticamente ativar suas licenças todas as noites.

Quando a ativação manual da licença ainda é necessária

Se você fizer as seguintes alterações em seu site, será necessário fazer a ativação manual da licença.

- Adquirir licenças adicionais (consulte Obter licenças adicionais na página 128)
- Atualizar para uma versão mais recente ou um sistema VMS mais avançado (consulte Requisitos para atualização na página 383)
- Comprar ou renovar uma assinatura Milestone Care
- Receba permissão para mais mudanças de dispositivo sem ativação (ver Alterações do dispositivo sem ativação (explicado) na página 122)

Período de gratuidade para ativação da licença (explicado)

Depois de instalar o VMS e adicionar dispositivos (dispositivos de hardware, câmeras Milestone Interconnect ou licenças de porta), os dispositivos funcionam em um período de gratuidade de 30 dias se você decidiu não habilitar a ativação automática da licença. Antes do final do período gratuito de 30 dias e se você não tiver mais alterações de dispositivo sem ativação restante, você deve ativar suas licenças, ou seus dispositivos deixarão de enviar vídeos para seu site de vigilância.

Alterações do dispositivo sem ativação (explicado)

A funcionalidade do dispositivo muda sem ativação oferece flexibilidade integrada ao sistema de licenciamento XProtect. Portanto, mesmo que tenha decidido ativar as licenças manualmente, você não precisa necessariamente ativar as licenças sempre que adicionar ou remover dispositivos de hardware.

O número de alterações no dispositivo sem ativação difere de instalação para instalação e é calculado com base em diversas variáveis. Para uma descrição detalhada, consulte Cálculo do número disponível de alterações de dispositivo sem ativação (explicado) na página 123.

Um ano após a sua última ativação da licença, o seu número de alterações no dispositivo sem ativação utilizadas é automaticamente redefinido para zero. Uma vez a redefinição feita, você pode continuar a adicionar e substituir os dispositivos de hardware sem ativar as licenças.

Se o seu sistema de monitoramento estiver off-line por períodos de tempo mais longos, por exemplo, nos casos com um sistema de monitoramento em um navio, em um longo cruzeiro ou um sistema de monitoramento em um local remoto sem qualquer acesso à Internet, você pode entrar em contato com o seu revendedor Milestone e solicitar um número maior de alterações no dispositivo sem ativação.

Você deve explicar a razão pela qual você acha que se qualifica para um maior número de alterações no dispositivo sem ativação. A Milestone decide cada pedido individualmente. Para receber um número maior de alterações no dispositivo sem ativação, você deve ativar suas licenças para registrar o número maior no seu sistema XProtect.

Cálculo do número disponível de alterações de dispositivo sem ativação (explicado)

O número de alterações no dispositivo disponível sem ativação é calculado com base em três variáveis. Se você tiver várias instalações do software Milestone, as variáveis se aplicam a cada uma delas separadamente. As variáveis são as seguintes:

- **C%** que é uma porcentagem fixa do valor total de licenças ativadas.
- **Cmin** que é um valor mínimo fixado do número de alterações no dispositivo sem ativação
- **Cmax** que é um valor máximo fixado do número de alterações no dispositivo sem ativação

O número de alterações no dispositivo sem ativação nunca pode ser menor que o valor **Cmin** ou maior do que o valor **Cmax**. O valor calculado com base no **C%** da variável muda de acordo com o número de dispositivos ativados que você tem em cada instalação, em seu sistema. Dispositivos adicionados com alterações no dispositivo sem ativação não são contados como ativados pelo **C%** da variável.

Milestone define os valores de todas as três variáveis e os valores estão sujeitos a alterações sem notificação. Os valores das variáveis diferem dependendo do produto.

Exemplos baseados em C% = 15 %, Cmin = 10º e Cmax =100

Você compra 100 licenças de dispositivo. Em seguida, você adiciona 100 câmeras ao site. A menos que tenha habilitado a ativação automática de licença, suas alterações no dispositivo sem ativação ainda serão zero. Você ativa suas licenças e agora tem 15 alterações no dispositivo sem ativação.

Você compra 100 licenças de dispositivo. Então você acrescenta 100 câmeras ao sistema e ativa as licenças. Suas alterações no dispositivo sem ativação são agora 15. Você decide então excluir um dispositivo de hardware do sistema. Agora você tem 99 dispositivos ativados e o número de alterações no dispositivo sem ativação caiu para 14.

Você compra 1000 licenças de dispositivo. Você adiciona 1000 câmeras e ativa as licenças. Suas alterações no dispositivo sem ativação são agora 100. Segundo o **C%** da variável, ele já deveria ter tido 150 alterações no dispositivo sem ativação, mas a variável **Cmax** só lhe permite ter 100 modificações de dispositivos sem ativação.

Você compra 10 licenças de dispositivo. Então você adiciona 10 câmeras ao sistema e ativa as licenças. O número de alterações no dispositivo sem ativação é agora 10 por causa da variável **Cmin**. Se o número foi calculado apenas com base no **C%** da variável, você teria apenas 1 (15% de 10 = 1,5 arredondado para 1).

Você compra 115 licenças de dispositivo. Então você acrescenta 100 câmeras ao sistema e ativa as licenças. Suas alterações no dispositivo sem ativação são agora 15. Você adiciona mais 15 câmeras sem ativá-las, usando 15 das 15 das suas alterações no dispositivo sem ativação. Agora você remove 50 das câmeras do sistema e o número de alterações de dispositivo sem ativação cai para 7. Isso significa que 8 das câmeras adicionadas anteriormente nas 15 alterações de dispositivo sem ativação entram em um período de gratuidade. Agora você adiciona 50 novas câmeras. Como você ativou 100 câmeras no sistema na última vez que ativou suas licenças, o número de alterações no dispositivo sem ativação voltará para 15, e as 8 câmeras, que foram transferidas para um período gratuito, voltam para as alterações no dispositivo sem ativação. As 50 novas câmeras entram em um período gratuito.

Milestone Care™ (explicado)

Milestone Care é o nome do programa completo de serviço e suporte para produtos XProtect ao longo de sua vida útil.

Milestone Care dá acesso a diferentes tipos de material de autoajuda como artigos da Knowledge Base, guias e tutoriais em nosso site de suporte (https://www.milestonesys.com/support/).

Para benefícios adicionais, você pode comprar mais Milestone Care assinaturas antecipadas.

Milestone Care Plus

Se você tem uma Milestone Care Plus assinatura, também tem acesso a atualizações gratuitas para seu produto XProtect VMS atual e pode atualizar para produtos XProtect VMS mais avançados a um preço vantajoso. Milestone Care Plus também oferece funcionalidade adicional:

- O serviço Painel de controle do cliente
- O recurso Smart Connect
- A funcionalidade completa de notificação push

Milestone Care Premium

Se você tiver uma assinatura do Milestone Care Premium, também pode entrar em contato com a equipe de suporte Milestone diretamente. Lembre-se de incluir informações sobre a sua ID Milestone Care quando entrar em contato com o suporte Milestone.

Expiração, renovação e compra de Milestone Care assinaturas avançadas

A data de expiração dos tipos de assinatura de Milestone Care Plus e Milestone Care Premium mais avançados pode ser vista na janela **Informações da licença** na tabela **Produtos instalados**. Consulte Produtos instalados na página 130.

Se você decidir comprar ou renovar uma assinatura do Milestone Care após ter instalado o seu site, você deve ativar suas licenças manualmente antes de a informação correta do Milestone Care aparecer. Consulte Ativar licenças on-line na página 127 ou Ativar licenças offline na página 127.

Licenças e substituição de dispositivos de hardware (explicado)

Se uma câmera do site apresentar defeito ou se você, por outros motivos, quiser substituir a câmera por uma nova, existem algumas práticas recomendadas de como isso deve ser feito.

Se remover uma câmera de um servidor de gravação, você libera uma licença de dispositivo, mas também perde acesso total a todos os bancos de dados (câmeras, microfones, entradas, saídas) e às configurações da câmera antiga. Para manter o acesso aos bancos de dados da câmera antiga e reutilizar suas configurações ao substituí-la por uma nova, use a opção relevante abaixo.

Substituir câmera por uma câmera similar

Se você substituir uma câmera por uma câmera similar (fabricante, marca e modelo) e der à nova câmera o mesmo endereço IP da anterior, você mantém acesso completo a todos os bancos de dados da câmera antiga. A nova câmera continua usando os mesmos bancos de dados e configurações da câmera antiga. Neste caso, você move o cabo de rede da câmera antiga para a nova sem mudar nenhuma configuração no Management Client.

Substituir câmera por uma câmera diferente

Se substituir uma câmera por uma câmera diferente (outro fabricante, marca e modelo), você deve usar o assistente **Substituir hardware** (consulte Substituir hardware na página 355) para mapear todos os bancos de dados relevantes da câmera antiga para a nova e reutilizar as configurações da câmera antiga.

Ativação de licença após substituição de hardware

Se você habilitou a ativação automática da licença (consulte Habilitar ativação automática de licença na página 126), a nova câmera será ativada automaticamente.

Se a ativação automática da licença estiver desabilitada e se todas as alterações de dispositivo disponíveis sem ativação tiverem sido usadas (consulte Alterações do dispositivo sem ativação (explicado) na página 122), você deve ativar suas licenças manualmente. Para obter mais informações sobre a ativação manual de licenças, consulte Ativar licenças on-line na página 127 ou Ativar licenças offline na página 127.

Obter uma visão geral de suas licenças

Há muitos motivos para desejar obter uma visão geral de suas SLCs, do número de licenças adquiridas e seus status. Eis alguns:

- Você deseja adicionar um ou mais novos dispositivos de hardware, mas tem licenças de dispositivo não utilizadas ou precisa comprar novas?
- O período de gratuidade para alguns de seus dispositivos de hardware terminará em breve? Então você deve ativá-los antes que parem de enviar dados ao VMS.

- Você sabe por contatos anteriores ao suporte que eles precisam de informações do seu SLC e de sua ID Milestone Care para poder ajudar. Mas quais são eles?
- Você tem muitas instalações do XProtect e usa o mesmo SLC para todas as instalações, mas onde as licenças são usadas e quais são seus status?

Você pode encontrar todas as informações acima e ainda mais na janela **Informações da licença**.

Você pode abrir a janela **Informações da licença** no painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**.

Para saber mais sobre os vários recursos e informações disponíveis na janela **Informações da licença**, consulte Janela Informações da licença na página 130.

Ative suas licenças

Existem várias maneiras de ativar licenças. Todas elas estão disponíveis na janela de **Informações da licença**. A melhor forma de ativação depende das políticas da sua organização e se o seu servidor de gerenciamento tem acesso à internet ou não.

Você pode abrir a janela **Informações da licença** no painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**.

Para saber mais sobre os vários recursos e informações disponíveis na janela **Informações da licença**, consulte Janela Informações da licença na página 130.

Habilitar ativação automática de licença

Para fácil manutenção e flexibilidade – e quando as políticas da sua organização permitirem – a Milestone recomenda que você habilite a ativação automática da licença. A ativação automática de licença exige que o seu servidor de gerenciamento esteja on-line.

Se você quiser saber todos os benefícios de habilitar a ativação automática da licença, consulte Ativação automática de licença (explicado) na página 121.

1. No painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**, selecione **Habilitar ativação automática de licença**.
2. Introduza o nome de usuário e a senha que deseja utilizar na ativação automática de licença:
   - Se você é um usuário existente, insira seu nome de usuário e senha para fazer log in no sistema de registro de software
   - Se você é um novo usuário, clique no link **Criar novo usuário** para configurar uma nova conta de usuário e siga o procedimento de registro. Se ainda não tiver registrado o código da licença de software (SLC), você precisa fazê-lo

   As credenciais são salvas em um arquivo no servidor de gerenciamento.
3. Clique em **OK**.

Se, mais tarde, você desejar alterar o seu nome e/ou senha de usuário de ativação automática, clique no link **Editar credenciais de ativação**.

Desabilitar ativação automática de licença

Se não é permitido usar a ativação automática de licença em sua organização ou você simplesmente mudou de ideia, você pode desabilitar a ativação automática de licença.

A forma como você a desativa depende se planeja usar a ativação automática da licença novamente ou não.

Desativa, mas mantém a senha para uso posterior:

1. No painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**, desmarque **Habilitar ativação automática de licença**. O nome de usuário e senha ainda estão salvos no servidor de gerenciamento.

Desative e exclua a senha:

1. No painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**, clique em **Editar credenciais de ativação**.
2. Clique em **Excluir senha**.
3. Confirme que você deseja excluir o nome de usuário e senha do servidor de gerenciamento.

Ativar licenças on-line

Se o servidor de gerenciamento tiver acesso à internet, mas você preferir iniciar manualmente o processo de ativação, esta é a opção de ativação de licença mais fácil para você.

1. No painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**, selecione **Ativar licença manualmente** e, em seguida, **On-line**.
2. A caixa de diálogo **Ativar on-line** abre:
   - Se você é um usuário existente, insira seu nome de usuário e senha
   - Se você é um novo usuário, clique no link **Criar novo usuário** para configurar uma nova conta de usuário. Se ainda não tiver registrado o código da licença de software (SLC), você precisa fazê-lo
3. Clique em **OK**.

Se você receber uma mensagem de erro durante a ativação online, siga as instruções na tela para resolver o problema ou entre em contato com o suporte Milestone.

Ativar licenças offline

Se a sua organização não permitir que o servidor de gerenciamento tenha acesso à internet, você deve ativar as licenças manualmente e off-line.

1. No painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**, selecione **Ativar licença manualmente** > **Off-line** > **Exportar licença para ativação** para exportar um arquivo de solicitação de licença (.lrq) com informações sobre os dispositivos de hardware adicionados e outros elementos que requerem uma licença.
2. O arquivo de solicitação de licença (.lrq) recebe automaticamente o mesmo nome que o seu SLC. Se você tiver vários sites, lembre-se de renomear os arquivos para poder identificar facilmente qual arquivo pertence a qual site.
3. Copie o arquivo de solicitação de licença para um computador com acesso à internet e efetue o login no nosso site (https://online.milestonesys.com/) para obter o arquivo de licença de software ativado (.lic).
4. Copie o arquivo .lic que você receber para o seu computador com Management Client. O arquivo recebeu o mesmo nome de seu arquivo de solicitação de licença.
5. No painel **Navegação no site** -> nó **Fundamentos** -> **Informações da licença**, selecione **Ativar licença off-line** > **Importar llicença ativada** e selecione o arquivo de licença de software ativado para importá-lo e, assim, ativar suas licenças.
6. Selecione **Finalizar** para terminar o processo de ativação.

Ativar licenças após o período gratuito

Se você decidiu usar a ativação de licença manual e se esqueceu de ativar uma licença dentro do período de gratuidade (dispositivo de hardware, câmera Milestone Interconnect, licenças de porta ou outros), o dispositivo que usa essa licença fica indisponível e não pode enviar dados para o site de vigilância

Mesmo que o período de gratuidade de uma licença tenha expirado, a configuração do dispositivo e as configurações feitas por você são salvas e usadas quando a licença é ativada.

Para habilitar os dispositivos indisponíveis novamente, você ativa as licenças manualmente da sua maneira preferida. Para obter mais informações, consulte Ativar licenças offline na página 127 ou Ativar licenças on-line na página 127.

Obter licenças adicionais

Se desejar adicionar ou se já adicionou mais dispositivos de hardware, sistemas Milestone Interconnect, portas ou outros elementos para os quais tenha licenças no momento, você deve comprar licenças adicionais para permitir que os dispositivos enviem dados para o seu site:

- Para obter licenças adicionais para o seu sistema, entre com contato com o revendedor do produto XProtect

Se você comprou novas licenças para a versão já existente de seu sistema de monitoramento:

- Basta ativar suas licenças manualmente para obter acesso a novas licenças. Para obter mais informações, consulte Ativar licenças on-line na página 127 ou Ativar licenças offline na página 127.

Se você comprou novas licenças e uma versão atualizada do sistema de monitoramento:

- Você recebe um arquivo de licença de software atualizado (.lic) com novas licenças e uma nova versão. Você deve usar o novo arquivo de licença de software durante a instalação da nova versão. Para obter mais informações, consulte Requisitos para atualização na página 383

Alterar o código da licença de software

Se você executar uma instalação em um código de licença de software (Software License Code, SLC) temporário ou se tiver atualizado para um produto XProtect mais avançado, poderá alterar seu SLC para um SLC permanente ou um mais avançado. Você pode alterar seu SLC sem nenhuma ação de desinstalação ou reinstalação quando tiver recebido seu novo arquivo de licença de software.

Você pode fazer isso localmente no servidor de gerenciamento ou remotamente do Management Client.

A partir do ícone da bandeja do servidor de gerenciamento

1. No servidor de gerenciamento, vá para a área de notificação na barra de tarefas.

2. Clique com o botão direito do mouse no ícone **Gerenciador do servidor** e selecione **Alterar Licença**.
3. Clique em **Importar licença**.
4. Em seguida, selecione o arquivo de licença de software salvo para este propósito. Depois de concluído, o local do arquivo de licença de software selecionado é adicionado logo abaixo do botão **Importar licença**.
5. Clique em **OK**, e você estará pronto para registrar o SLC. Consulte Registrar o código da licença de software na página 149.

Do Management Client

1. Copie o arquivo .lic que você receber para o seu computador com o Management Client.
2. No painel **Navegação no site** -> nó **Fundamentos** -> **Informações da licença**, selecione **Ativar licença off-line** > **Importar llicença ativada** e selecione o arquivo de licença de software para importá-lo.
3. Quando aberto, aceite que o arquivo de licença do software é diferente daquele atualmente em uso.
4. Agora você está pronto para registrar o SLC. Consulte Registrar o código da licença de software na página 149.

O arquivo de licença de software só é importado e alterado, mas não ativado. Lembre-se de ativar sua licença. Para obter mais informações, consulte Ative suas licenças na página 126.

Ao executar o XProtect Essential+, você só pode alterar a licença no ícone da bandeja do servidor de gerenciamento. Não é possível alterar a licença do Management Client.

Janela Informações da licença

Na janela **Informações da licença**, você pode acompanhar todas as licenças que compartilham o mesmo arquivo de licença de software tanto neste site como em todos os outros sites, suas assinaturas Milestone Care e decidir como deseja ativar as suas licenças.

Você pode abrir a janela **Informações da licença** no painel **Navegação do site** -> nó **Fundamentos** -> **Informações da licença**.

Se você deseja ter uma compreensão geral de como funciona o sistema de licenciamento do XProtect, consulte Licenças (explicadas) na página 119.

Licenciado para

Esta área da janela **Informações da licença**, lista os detalhes de contato do proprietário da licença que foram inseridos durante o registro do software.

Se você não puder ver a área **Licenciado para**, clique no botão **Atualizar** no canto inferior direito da janela.

Clique em **Editar detalhes** para editar as informações do proprietário da licença. Clique no **Contrato de Licença de Usuário Final** para ver o contrato de licença do usuário final que você aceitou antes da instalação.

Milestone Care

Aqui você pode consultar as informações sobre a sua assinatura Milestone Care™ atual. As datas de expiração de suas assinaturas são exibidas na tabela de **Produtos instalados** abaixo.

Para obter mais informações sobre Milestone Care, use os links ou consulte Milestone Care™ (explicado) na página 124.

Produtos instalados

Lista as seguintes informações sobre todas as suas licenças básicas instaladas para o XProtect VMS e extensões XProtect que compartilhem o mesmo arquivo de licença de software:

- Produtos e versões
- O código de licença de software dos produtos (SLC)
- A data de expiração do seu SLC. Normalmente ilimitada
- A data de expiração da sua assinatura do Milestone Care Plus
- A data de expiração da sua assinatura do Milestone Care Premium

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 20 R	M01-C01-211-01-	Unlimited	16-11-20	16-11-20
Milestone XProtect Smart Wall	M01-P03-100-01-	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact	M01-P08-100-01-	Unlimited	Unlimited	

Visão geral da licença - Todos os sites

Lista o número de licenças de dispositivos ativadas e outras licenças no seu arquivo de licença de software e a quantidade total de licenças disponíveis no seu sistema. Aqui você pode facilmente ver se ainda pode aumentar o seu sistema sem ter de adquirir licenças adicionais.

Para uma visão detalhada do estado das suas licenças ativadas em outros sites, clique no link **Detalhes da Licença - Todos os sites**. Veja a seção **Detalhes da licença - Site atual** abaixo para obter as informações disponíveis.

License Overview - All sites License Details - All Sites...

License Type	Activated
Device Licenses	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

Se você tiver licenças para as extensões XProtect, poderá ver mais detalhes sobre elas nos nós específicos da extensão XProtect no painel **Navegação do site**.

Detalhes da licença – Site Atual

A coluna **Ativada** lista o número de dispositivos ativados ou outras licenças neste site.

Você também pode ver o número de alterações dos dispositivos sem ativação utilizados (consulte Alterações do dispositivo sem ativação (explicado) na página 122) e quantas você tem disponível por ano na coluna de **Alterações sem ativação**.

Se você tiver as licenças que ainda não ativou e que, por conseguinte, são executadas em um período gratuito, esses itens são listados na coluna **Período gratuito**. A data de vencimento da primeira licença a expirar, aparece em vermelho abaixo da tabela.

Se você esquecer de ativar as licenças antes da expiração do período de carência, elas vão parar de enviar vídeos para o sistema. Essas licenças são exibidas na coluna **Período Gratuito Expirado**. Para obter mais informações, consulte Ativar licenças após o período gratuito na página 128.

Se você tiver usado mais licenças do que as que tem disponível, elas são listadas na coluna **Sem Licença** e não podem ser usadas no seu sistema. Para obter mais informações, consulte Obter licenças adicionais na página 128.

Se você tiver licenças em um período gratuito, com um prazo gratuito vencido ou sem licença, uma mensagem pop-up será exibida para lembrá-lo toda vez que fizer o login no seu Management Client.

License Details - Current Site: [redacted]

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Device Licenses	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

Se você tiver dispositivos de hardware que usam mais de uma licença, um link **Clique aqui para abrir o relatório de licença de dispositivo completo** aparecerá abaixo da tabela **Detalhes da Licença - Site Atual**. Ao clicar no link, você pode ver quantas licenças de dispositivo cada um desses dispositivos de hardware exige.

Os dispositivos de hardware sem licença são identificados com um ponto de exclamação no Management Client. O ponto de exclamação também é utilizado para outros fins. Coloque o mouse sobre o ponto de exclamação para ver o objetivo.

Recursos para ativação de licenças

Abaixo dos três quadros estão:

- Uma caixa de seleção para possibilitar ativação automática de licença e um link para editar as credenciais do usuário para a ativação automática. Para obter mais informações, consulte Ativação automática de licença (explicado) na página 121 e Habilitar ativação automática de licença na página 126.
  Se a ativação automática tiver falhado, uma mensagem de erro aparecerá em vermelho. Para mais informações, clique no link **Detalhes**.
  Algumas licenças , como XProtect Essential+ e , são instaladas com a ativação automática de licença habilitada e não é possível desabilitá-las.
- Uma caixa de lista suspensa para ativação de licenças on-line ou off-line. Para obter mais informações, consulte Ativar licenças on-line na página 127 e Ativar licenças offline na página 127.
- No canto inferior direito da janela, você pode ver quando as suas licenças foram ativadas pela última vez (automática ou manualmente) e quando as informações da janela foram atualizadas. Os carimbos de data/hora são do servidor e não do computador local

Requisitos e considerações

Horário de verão (explicado)

O horário de verão significa, na prática, adiantar relógios para que a luz solar seja melhor aproveitada ao longo do dia e a noite inicie mais tarde. O uso do horário de verão varia entre países e regiões.

Quando você trabalha com um sistema de monitoramento, que é inerentemente sensível a horários, é importante que você saiba como o sistema lida com o horário de verão.

> ⚠ Não altere a configuração de horário de verão quando estiver no período de horário de verão ou se tiver gravações de um período de horário de verão.

Primavera: Muda do horário padrão para o horário de verão

A mudança do horário padrão para o horário de verão não é um problema, já que só avança uma hora.

Exemplo:

O relógio pula das 02:00h do horário padrão para as 03:00h do horário de verão (DST) e o dia tem 23 horas. Nesse caso, não há informação entre as 2:00h e as 3:00h da manhã, já que, naquele dia, esse período de tempo não existiu.

Outono: Muda do horário de verão para o horário padrão

Quando você volta do horário de verão para o horário normal, no verão, você volta uma hora.

Exemplo:

O relógio volta das 02:00h do horário de verão (DST) para a 01:00h do horário padrão, repetindo aquela hora, e o dia tem 25 horas. Você chega a 01:59:59, então imediatamente reverte para 01:00:00. Se o sistema não reagir, ele basicamente regravará essa hora, então a primeira gravação de 1:30h será sobrescrita pela segunda gravação de 1:30h.

Para impedir que esse problema ocorra, seu sistema arquiva o vídeo atual quando o horário do sistema varia em mais de cinco minutos. Você não pode visualizar a primeira gravação de 01:00h diretamente em nenhum cliente, mas os dados estão gravados e armazenados em segurança. Você pode navegar nesse vídeo no XProtect Smart Client, abrindo diretamente o banco de dados arquivado.

Servidores de tempo (explicado)

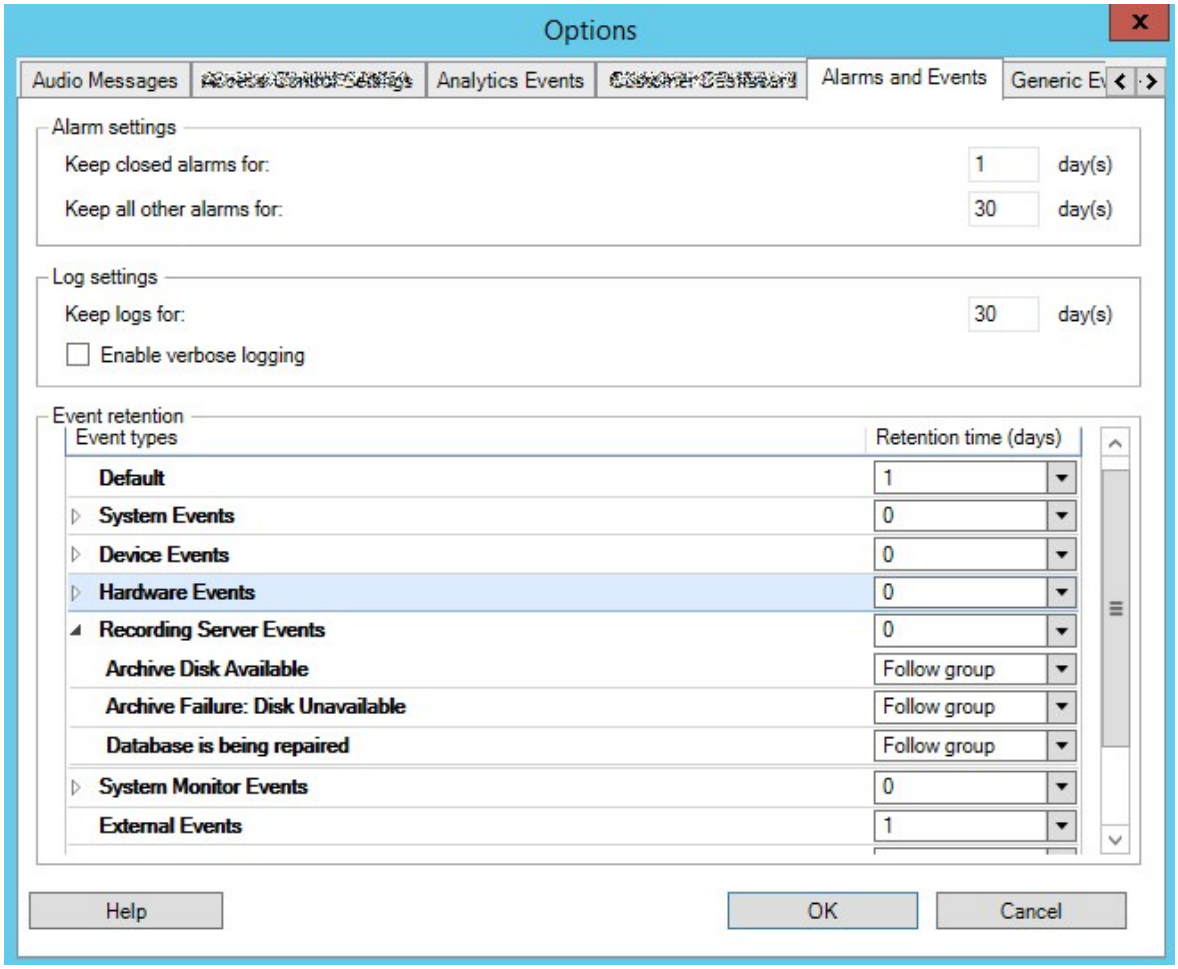
Após o sistema receber imagens, elas são instantaneamente carimbadas com a data/hora. No entanto, já que as câmeras são unidades independentes que podem ter dispositivos de tempo independentes, o tempo da câmera e o tempo do sistema podem não corresponder completamente. Isto pode ocasionalmente causar confusão. Se carimbos de data/hora forem suportados por suas câmeras, a Milestone recomenda que você sincronize automaticamente o tempo da câmera ao do sistema através de um servidor de tempo para sincronização coerente.

Para informações sobre como configurar um servidor de tempo, pesquise no site da Microsoft (https://www.microsoft.com/) por **"servidor de tempo"**, **"serviço de tempo"** ou termos semelhantes.

Tamanho limite do banco de dados

Para evitar que o banco de dados SQL Server (consulte SQL Server instalações e bancos de dados (explicado) na página 35) cresça para um tamanho que afete o desempenho do sistema, você pode especificar por quantos dias os diferentes tipos de eventos e alarmes são armazenados no banco de dados.

1. Abra a menu **Ferramentas**.
2. Cliquenaguia**Opções**>**Alarmeseeventos**.



3. Faça as configurações necessárias. Para obter mais informações, consulte Guia Alarmes e Eventos (opções) na página 408.

IPv6 e IPv4 (explicado)

Seu sistema é compatível com IPv6 e com IPv4. E o XProtect Smart Client também.

IPv6 é a versão mais recente do protocolo de internet (IP). O protocolo de internet determina o formato e o uso de endereços IP. IPv6 coexiste com a ainda muito mais amplamente utilizada versão IPv4. IPv6 foi desenvolvido para resolver a exaustão dos endereços IP do IPv4. Endereços IPv6 têm 128 bits de comprimento, enquanto endereços IPv4 têm somente 32.

Isso significa que o catálogo de endereços da Internet cresceu de 4,3 bilhões de endereços únicos para 340 undecilhões (340 trilhões de trilhões de trilhões) de endereços. Um fator de crescimento de 79 octilhões (bilhões de bilhões de bilhões).

Mais e mais organizações estão implementando suas redes para IPv6. Por exemplo, todas as infraestruturas de agências federais dos Estados Unidos devem ser compatíveis com o IPv6. Exemplos e ilustrações neste manual refletem o uso de IPv4 porque esta ainda é a versão de IP mais usada. O IPv6 funcionará igualmente bem com o sistema.

Usando o sistema com IPv6 (explicado)

As seguintes condições se aplicam ao usar o sistema com IPv6:

Servidores

Os servidores geralmente são capazes de usar IPv4 bem como IPv6. No entanto, se apenas um servidor em seu sistema (por exemplo, um servidor de gerenciamento ou servidor de gravação) precisar de uma versão específica de IP, todos os outros servidores no seu sistema devem se comunicar usando a mesma versão IP.

Exemplo: Todos os servidores no seu sistema, com exceção de um, podem usar IPv4 e IPv6. A exceção é um servidor que é somente capaz de usar IPv6. Isto significa que todos os servidores comunicam-se uns com os outros usando IPv6.

Dispositivos

Você pode usar dispositivos (câmeras, entradas, saídas, microfones, alto-falantes) com um versão de IP diferente da que está sendo usada para comunicação com o servidor desde que seu equipamento de rede e os servidores de gravação também suportem as versões do IP dos dispositivos. Veja também a ilustração abaixo.

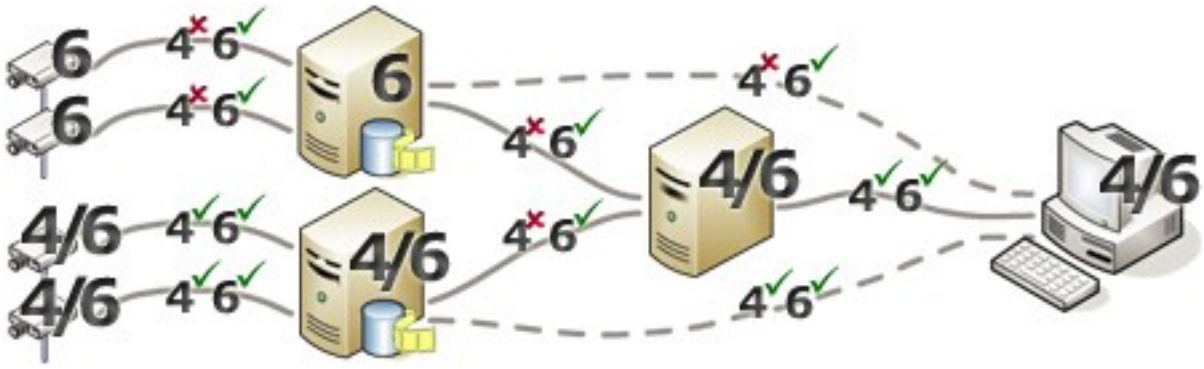
Clientes

Se o seu sistema usa IPv6, os usuários devem se conectar com o XProtect Smart Client. O XProtect Smart Client é compatível com IPv6, bem como IPv4.

Se um ou mais servidores no seu sistema **só** pode usar IPv6, os usuários do XProtect Smart Client **devem** usar o IPv6 para a sua comunicação com aqueles servidores. Neste contexto, é importante lembrar que instalações XProtect Smart Client tecnicamente conectam-se a um servidor de gerenciamento para a autenticação inicial, e depois aos servidores de gravação desejados para acesso às gravações.

No entanto, os usuários XProtect Smart Client não tem que estar em redes IPv6, desde que seu equipamento de rede suporte comunicação entre versões de IP diferentes, e que eles tem sido instalados o protocolo IPv6 em seus computadores. Veja também a ilustração. Para instalar IPv6 em um computador cliente, abra o prompt de comando, digite ***Ipv6 install***, e pressione **ENTER**.

Ilustração de exemplo



Exemplo: Uma vez que um servidor no sistema só pode usar o IPv6, toda a comunicação com esse servidor deve usar IPv6. Contudo, esse servidor também determina a versão do IP para a comunicação entre todos os outros servidores no sistema.

Escrevendo endereços IPv6 (explicado)

Um endereço IPv6 é normalmente escrito como oito blocos de quatro dígitos hexadecimais, com os blocos separados por uma vírgula.

Exemplo: *2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

Você pode encurtar endereços, eliminando zeros à esquerda em um bloco. Perceba também que alguns dos blocos de quatro dígitos podem consistir em zeros apenas. Se quaisquer números em tais blocos de 0000 são consecutivos, você pode encurtar endereços através da substituição dos blocos de 0000 com dois pontos duplos, contanto que haja apenas um desses pontos duplos no endereço.

Exemplo:
2001:0B80:0000:0000:0000:0F80:3FA8:18AB pode ser encurtado para

2001:B80:0000:0000:0000:F80:3FA8:18AB se removendo os zeros à esquerda, ou para

2001:0B80::0F80:3FA8:18AB se removendo os blocos com 0000, ou ainda

2001:B80::F80:3FA8:18AB se removendo os zeros a esquerda bem como os blocos com 0000.

Usando endereços IPv6 em URLs

Endereços IPv6 contém dois pontos. Dois pontos, no entanto, também são usados em outros tipos de sintaxes de endereçamento de rede. Por exemplo, IPv4 usa dois pontos para separar o endereço IP e o número da porta quando ambos são usados na URL. O IPv6 herdou este princípio. Portanto, para evitar confusão colchetes são colocados em volta de endereços IPv6 quando são usados em URLs.

Exemplo de uma URL com endereço IPv6:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB], que pode é claro ser encurtado para, por exemplo, *http://[2001:B80::F80:3FA8:18AB]*

Exemplo de uma URL com endereço IPv6 e um número de porta:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234, que pode, é claro, ser encurtado para, por exemplo, *http://[2001:B80::F80:3FA8:18AB]:1234*

Para mais informações sobre IPv6, consulte, por exemplo, o site da IANA (https://www.iana.org/numbers/). IANA, Autoridade de Números Atribuídos na Internet, é a organização responsável pela coordenação global de endereçamento IP.

Servidores virtuais

Você pode executar todos os componentes de sistema em servidores Windows® virtualizados, como VMware® e Microsoft® Hyper-V®.

Visualizações são frequentemente preferidas para melhor utilizar os recursos do hardware. Normalmente, servidores virtuais em execução no servidor de host de hardware não carregam o servidor virtual até certo ponto, e normalmente não ao mesmo tempo. No entanto, os servidores de gravação gravam todas as câmeras e fluxos de vídeo. Este procedimento coloca alta carga na CPU, memória, rede e sistema de armazenamento. Assim, executar em um servidor virtual, faz desaparecer boa parte do ganho normal da virtualização, posto que - em muitos casos - usará todos os recursos disponíveis.

Ao executar em um ambiente virtual, é importante que o host de hardware tenha a mesma quantidade de memória física alocada para o os servidores virtuais e que o servidor virtual que executa o servidor de gravação tenha CPU e memória suficiente alocadas, o que não é padrão. Geralmente, o servidor de gravação precisa de 2-4 GB dependendo da configuração. Um outro gargalo é a alocação do adaptador de rede e a performance do disco rígido. Considere alocar o adaptador de rede físico no servidor de host do servidor virtual executando o servidor de gravação. Esse procedimento assegura mais facilmente que o adaptador de rede não esteja sobrecarregado com o tráfico de outros servidores virtuais. Se o adaptador de rede for usado por diversos servidores virtuais, o tráfico de rede pode resultar no servidor de gravação não recuperar e gravar o número de imagens para o qual ele está configurado.

Servidores de gerenciamento múltiplos (clustering) (explicado)

O servidor de gerenciamento pode ser instalado em vários servidores em um grupo de servidores. Isso garante que o sistema tenha muito pouco tempo de inatividade. Se um servidor do cluster falhar, outro servidor do cluster assume automaticamente o trabalho do servidor que falhou executando o servidor de gerenciamento.

Somente é possível ter um servidor de gerenciamento possível por configuração de vigilância, mas outros servidores de gerenciamento podem configurar para assumir em caso de falha.

Por padrão, o serviço Management Server limita o número de vezes que uma emergência ocorre para duas vezes dentro de um período de seis horas. Se isso for excedido, os serviços Management Server não são inicializados automaticamente pelo serviço de clustering. Este limite pode ser alterado para se adequar melhor às suas necessidades.

Requisitos de clustering

- Duas máquinas com Microsoft Windows Server 2016 ou superior. Assegure-se de que:
  - Todos os servidores que você deseja adicionar como nós de cluster estejam executando a mesma versão do Windows Server
  - Todos os servidores que você deseja adicionar como nós de cluster são reunidos no mesmo domínio.
  - Você tem acesso de login à conta do Windows, como administrador local

  Informações sobre clusters nos servidores Microsoft Windows, consulte clusters de Failover https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster.
- Uma instalação do Microsoft SQL Server

  Ou um SQL Server externo e um banco de dados instalado **fora** do cluster do servidor **ou** um serviço SQL Server **interno** (em grupo) dentro do cluster do servidor (a criação de um serviço SQL Server interno exige o uso da versão Microsoft® SQL Server® Standard ou Microsoft® SQL Server® Enterprise, que podem funcionar como um SQL Server em grupo).

  Ao conectar o servidor de gerenciamento ao banco de dados, dependendo das configurações de senha dos ajustes do sistema, você pode ser solicitado a fornecer a senha de configuração do sistema atual. Consulte Configurações de senha do sistema (explicado) na página 342.

Se trabalhar em um ambiente com cluster de emergência, recomenda-se que você pause o cluster, antes de iniciar tarefas no Server Configurator. Isto é porque o Server Configurator pode precisar interromper serviços enquanto aplica as alterações e o ambiente de cluster de emergência pode interferir com esta operação.

Proteger o banco de dados de gravação de corrosão

Bancos de dados de câmeras podem corromper-se. Existem várias opções de reparo de banco de dados para resolver tal problema, mas Milestone recomenda que você adote medidas para assegurar que os bancos de dados da sua câmera não se corrompam.

Falha no disco rígido: proteger suas unidades

As unidades de disco rígido são dispositivos mecânicos e são vulneráveis a fatores externos. Os seguintes fatores são exemplos de fatores externos que podem danificar as unidades de disco rígido e levar a bancos de dados de câmera danificados:

- Vibração (certifique-se de que o servidor de sistema de monitoramento e suas proximidades sejam estáveis)
- Calor forte (certifique-se de que o servidor tenha ventilação adequada)
- Campos magnéticos fortes (evite)
- A falta de energia (certifique-se de usar um UPS - fornecimento de energia ininterrupta)
- Eletricidade estática (certifique-se de aterrar-se se for tocar em uma unidade de disco rígido)
- Fogo, água, etc. (evitar)

Gerenciador de Tarefas do Windows: tenha cuidado ao finalizar processos

Quando trabalhar com o Gerenciador de Tarefas do Windows, tenha cuidado de não finalizar nenhum processo que possa afetar o sistema de monitoramento. Se você finalizar um aplicativo ou sistema de serviço clicando em **Finalizar Processo** no Gerenciador de Tarefas do Windows, o processo não pode salvar seu estado ou dados antes de ser finalizado. Isso pode gerar bancos de dados corrompidos.

O Gerenciador de Tarefas do Windows normalmente exibe um aviso se você tentar finalizar um processo. A menos que você tenha certeza absoluta de que finalizar o processo não afetará o sistema de segurança, clique **Não** quando a mensagem de aviso lhe perguntar se você realmente deseja finalizar o processo.

Interrupção de energia: use uma UPS

O motivo mais comum para bancos de dados danificados é o servidor de gravação ser desligado abruptamente, sem arquivos terem sido salvos e sem o sistema operacional ter sido desligado corretamente. Isso pode ocorrer devido a quedas de energia, devido a alguém retirar o cabo de alimentação do servidor acidentalmente ou algo parecido.

A melhor forma de proteger o servidor de gravação de vigilância contra desligamento repentino é equipar o seu servidor do sistema de monitoramento com uma UPS (Uninterruptible Power Supply, também conhecido como no-break).

A UPS funciona como uma fonte de alimentação secundária com bateria, fornecendo a energia necessária para salvar arquivos abertos e desligar com segurança o seu sistema no caso de irregularidades de energia. UPSs variam em sofisticação, mas muitos incluem software para salvar arquivos automaticamente, para alertar administradores de sistemas, etc.

A seleção do tipo correto de UPS para o ambiente de sua organização é um processo individual. Ao avaliar suas necessidades, no entanto, tenha em mente a quantidade de tempo de execução que você precisa caso ocorra uma falha de energia. Salvar os arquivos abertos e desligar o sistema operacional corretamente podem levar vários minutos.

Registro de transações do banco de dados SQL Server (explicado)

Cada vez que uma alteração é gravada em um banco de dados do SQL Server, o banco de dados do SQL Server registra essa alteração em seu registro de transações.

Quando o registro de transações, você pode rolar de volta e desfazer alterações ao banco de dados SQL Server através do Microsoft® SQL Server Management Studio. Por padrão, o banco de dados SQL Server armazena seu registro de transações indefinidamente, o que ao longo do tempo, significa que o registro de transações terá cada vez mais entradas. O registro de transações do SQL server está, por padrão, localizado na unidade do sistema e, se o registro de transações continua a crescer, ele pode impedir o Windows de ser executado corretamente.

Para evitar tal cenário, é bom descarregar o registro de transações regularmente. O descarregamento não diminuirá o tamanho do arquivo de registro de transações, mas impedirá que ele cresça fora de controle. O seu sistema VMS não elimina registros de transação. No SQL Server, há três formas de eliminar o registro de transações. Acesse a página de suporte da Microsoft https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017 e pesquise por se por *Truncamento de registros de transação*.

Requisitos mínimos do sistema

Para obter informações sobre os requisitos mínimos do sistema para os vários aplicativos VMS e componentes do seu sistema, acesse o site do Milestone (https://www.milestonesys.com/systemrequirements/).

Antes de você iniciar a instalação

A Milestone recomenda que você cumpra os requisitos descritos nas próximas seções antes de iniciar efetivamente a instalação.

Preparar seus servidores e a rede

Sistema operacional

Certifique-se de que todos os servidores tenham uma instalação limpa de um sistema operacional Microsoft Windows com todas as atualizações mais recentes do Windows.

Para obter informações sobre os requisitos mínimos do sistema para os vários aplicativos VMS e componentes do seu sistema, acesse o site do Milestone (https://www.milestonesys.com/systemrequirements/).

Microsoft® .NET Framework

Verifique se todos os servidores possuem Microsoft .NET Framework 4.8 ou uma versão mais recente instalada.

Rede

Atribua endereços IP estáticos ou crie reservas DHCP para todos os componentes e câmeras do sistema. Para garantir que a largura de banda necessária esteja disponível na sua rede, é preciso compreender como e quando o sistema consome a largura de banda. A carga principal em sua rede é composta por três elementos:

- Fluxos de câmera de vídeo
- Clientes exibindo o vídeo
- Arquivamento de vídeo gravado

O servidor de gravação recupera fluxos de vídeo das câmeras, o que resulta em uma carga constante na rede. Clientes exibindo o vídeo consomem a largura de banda da rede. Se não houver alterações no conteúdo das visualizações do cliente, a carga é constante. Alterações na exibição de conteúdo, pesquisa de vídeo, ou na reprodução tornam a carga dinâmica.

O arquivamento de vídeos gravados é um recurso opcional que permite que o sistema transfira gravações para um armazenamento em rede se não houver espaço suficiente no sistema de armazenamento interno do computador. Este é um processo programado que você precisa definir. Normalmente, você arquiva em uma unidade de rede, o que causa uma carga dinâmica na rede.

Sua rede deve ter espaço livre na banda larga para lidar com esses picos no tráfego. Isso aumenta a agilidade do sistema e a experiência geral do usuário.

Preparar o Active Directory

Para adicionar usuários no seu sistema por meio do serviço Active Directory, você deverá ter um servidor com o Active Directory instalado e agindo como controlador de domínio, disponível na sua rede.

Para facilitar o gerenciamento de usuário e de grupo, a Milestone recomenda que você tenha o Microsoft Active Directory ® instalado e configurado antes de você instalar o seu sistema XProtect. Se você adicionar o servidor de gerenciamento do Active Directory depois de instalar o seu sistema, você deve reinstalar o servidor de gerenciamento e substituir os usuários com os novos usuários Windows definidos no Active Directory.

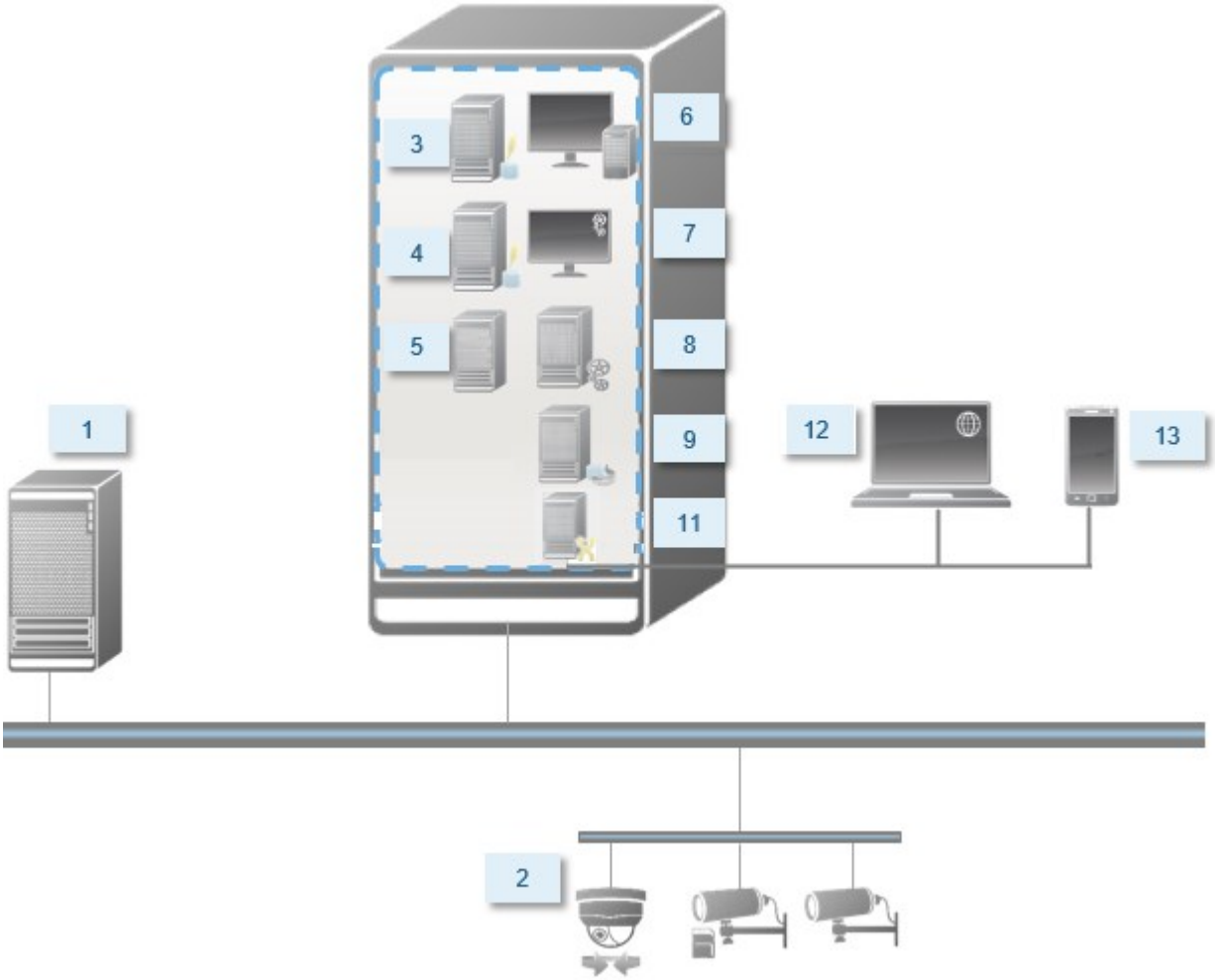
Usuários básicos não são compatíveis em sistemas Milestone Federated Architecture, portanto, se planejar utilizar Milestone Federated Architecture, adicione os usuários como usuários do Windows através do serviço Active Directory. Se você não instalar o Active Directory, siga as etapas em Instalação para grupos de trabalho na página 186 quando fizer a instalação.

Método de instalação

Como parte do assistente de instalação, você deve decidir qual o método de instalação que será usado. Você deve basear sua seleção nas necessidades da sua organização, mas é muito provável que já tenha decidido o método quando adquiriu o sistema.

Opções	Descrição
Único Computador	Instala todos os componentes de servidor e cliente, assim como o SQL Server no computador atual. Quando a instalação for concluída, você terá a possibilidade de configurar o seu sistema através de um assistente. Se você concordar em continuar, o servidor de gravação verifica a sua rede quanto ao hardware e você pode selecionar os dispositivos de hardware para adicionar ao seu sistema. O número máximo de dispositivos de hardware que podem ser adicionados no assistente de configuração depende da sua licença básica. Além disso, as câmeras são pré-configuradas nas visualizações e uma função de Operador padrão é criada. Após a instalação, XProtect Smart Client abre e você está pronto para usar o sistema.
Personalizado	O servidor de gerenciamento é sempre selecionado na lista de componentes e é sempre instalado, mas você pode selecionar livremente o que instalar no computador atual, entre os outros componentes de servidor e cliente. Por padrão, o servidor de gravação não está selecionado na lista de componentes, mas você pode mudar isso. Você pode instalar os componentes não selecionados em outros computadores posteriormente.

Instalação de um Único Computador

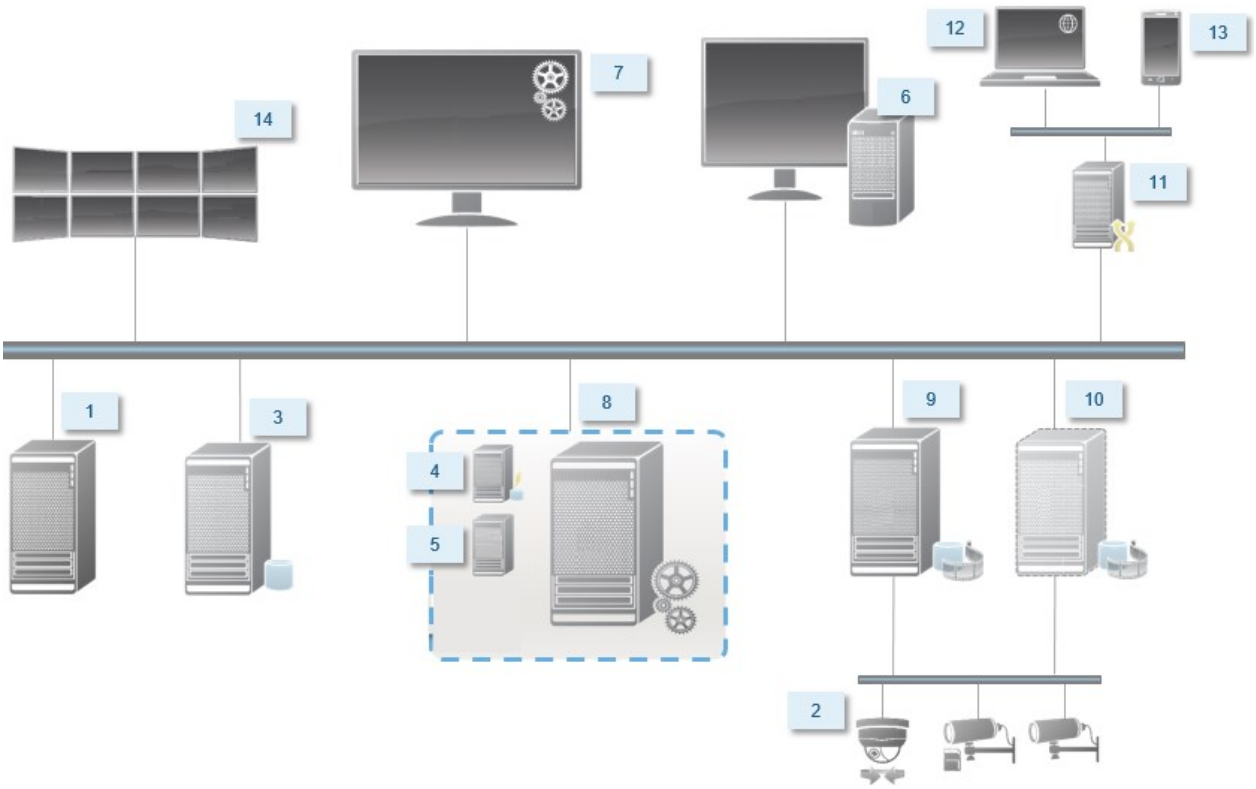


Componentes de sistema típicos em um sistema:

1. **Active Directory**
2. **Dispositivos**
3. **Servidor com SQL Server**
4. **Servidor de eventos**
5. **Servidor de registros**
6. **XProtect Smart Client**
7. **Management Client**
8. **Servidor de gerenciamento**
9. **Servidor de gravação**

10. **Servidor do sistema de gravação ininterrupta (failover)**
11. **Servidor XProtect Mobile**
12. **XProtect Web Client**
13. **Cliente XProtect Mobile**
14. **XProtect Smart Client com XProtect Smart Wall**

Instalação personalizada - exemplo de componentes do sistema distribuídos



Optar por uma edição do SQL Server

Microsoft® SQL Server® Express é uma versão gratuita SQL Server e é fácil de instalar e preparar para o uso, em comparação a outras versões do SQL Server. Durante uma instalação de um **Único computador**, o Microsoft SQL Server Express é instalado a menos que o SQL Server já esteja instalado no computador.

A instalação do XProtect VMS inclui Microsoft SQL Server Express na versão 2019. Nem todos os sistemas operacionais do Windows oferecem suporte para essa edição do SQL Server. Antes de você instalar o XProtect VMS, verifique se o seu sistema operacional suporta o SQL Server 2019. Se o seu sistema operacional não suportar essa edição do SQL Server, instale uma edição compatível do SQL Server antes de começar a instalação do XProtect VMS installation. Para obter informações sobre as edições SQL Server suportadas, consulte https://www.milestonesys.com/systemrequirements/.

Para sistemas muito grandes ou com muitas transações para e do banco de dados SQL Server, a Milestone recomenda que você use a edição Microsoft® SQL Server® Standard ou Microsoft® SQL Server® Enterprise do SQL Server em um computador dedicado na rede e em uma unidade de disco rígido não utilizada para outros fins. Instalar o SQL Server em sua própria unidade melhorará o desempenho de todo o sistema.

Selecione a conta de serviços

Como parte da instalação, você será solicitado a especificar uma conta para executar os serviços da Milestone nesse computador. Os serviços são sempre executados nessa conta não importando qual usuário está conectado. Certifique-se de que a conta tem todas as permissões de usuário necessárias como, por exemplo, as permissões adequadas para executar tarefas, uma boa rede e acesso a arquivos, além de acesso a pastas compartilhadas na rede.

Você pode selecionar tanto uma conta predefinida como uma conta de usuário. A sua decisão deve ser baseada no ambiente no qual você deseja instalar o seu sistema:

Ambiente de Domínio

Em um ambiente de domínio:

- Milestone recomenda que você utilize a conta integrada de Serviço de Rede

  Ela é mais fácil de usar, mesmo se você precisar de expandir o sistema para vários computadores.
- Você também pode usar contas de usuário de domínio, mas, potencialmente, são um pouco mais difíceis de configurar.

Ambiente de grupo de trabalho

Em um ambiente de grupo de trabalho, o Milestone recomenda que você use uma conta de usuário local que tenha todas as permissões necessárias. Isso é muitas vezes a conta de administrador.

> ⚠ Se você instalou os componentes do sistema em vários computadores, a conta do usuário selecionada deve existir em todos os computadores em suas instalações com idêntico nome de usuário, senha e permissões de acesso.

Autenticação Kerberos (explicado)

Kerberos é um protocolo de autenticação de rede baseado em tíquetes. Foi projetado para oferecer autenticação forte para aplicativos cliente/servidor ou servidor/servidor.

Utilize a autenticação Kerberos como uma alternativa ao protocolo de autenticação mais antigo Microsoft NT LAN (NTLM).

A autenticação Kerberos requer autenticação mútua, em que o cliente autentica o serviço e o serviço autentica o cliente. Assim, é possível autenticar de maneira mais segura de clientes XProtect para servidores XProtect sem expor sua senha.

Para possibilitar a autenticação mútua em seu XProtect VMS, você precisa registrar Nomes da Entidade de Serviço (SPN, Service Principal Names) no Active Directory. Um SPN é um alias que identifica inequivocamente uma entidade, como um serviço do servidor XProtect. Todo serviço que utiliza autenticação mútua deve ter um SPN registrado de modo que os clientes possam identificar o serviço na rede. Sem SPNs corretamente registrados, a autenticação mútua não é possível.

A tabela abaixo lista os diferentes serviços da Milestone com os números de porta correspondentes que você precisa registrar:

Serviço	Número da porta
Management Server - IIS	80 - Configurável
Management Server - Interno	8080
Recording Server - Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334

O número de serviços que você precisa registrar no Active Directory depende de sua instalação atual. O Data Collector é instalado automaticamente durante a instalação do serviço de Management Server, Recording Server, Event Server ou Failover Server.

Você deve registrar dois SPNs para o usuário executando o serviço: um com o nome do host, e outro com o nome de domínio totalmente qualificado.

Se você estiver executando o serviço usando uma conta de serviço de usuário de rede, deve registrar os dois SPNs para cada computador que estiver executando esse serviço.

Este é o esquema de nomeação SPN Milestone:

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

O exemplo a seguir mostra SPNs para o serviço Recording Server em um computador com os seguintes detalhes:

```
Hostname: Record-Server1
Domain: Surveillance.com
```

SPNs para registrar:

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

Exclusões da verificação de vírus (explicado)

Como ocorre com qualquer outro software de banco de dados, se um programa antivírus está instalado em um computador executando o software XProtect, é importante excluir determinados tipos e pastas de arquivo, bem como determinado tráfego de rede. Sem a implementação destas exceções, a verificação de vírus usa uma quantidade considerável de recursos do sistema. Além disso, o processo de verificação pode bloquear arquivos temporariamente, resultando em interrupção do processo de gravação e mesmo na corrupção de dados.

Quando fizer a verificação de vírus, não verifique os diretórios de Servidor de gravação contendo bancos de dados de gravação (por padrão, `C:\mediadatabase\` e todas as subpastas). Evite também a verificação de vírus em diretórios de armazenamento de arquivo.

Defina as seguintes exclusões adicionais:

- Tipos de arquivo: .blk, .idx, .pic
- Pastas e subpastas:
  - `C:\Program Files\Milestone` ou `C:\Program Files (x86)\Milestone`
  - `C:\ProgramData\Milestone\IDP\Logs`
  - `C:\ProgramData\Milestone\KeyManagement\Logs`
  - `C:\ProgramData\ \ MilestoneMIPSDK`
  - `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Event Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Log Server`
  - `C:\ProgramData\Milestone\XProtect Management Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Secure\TablesDb`
- Excluir a verificação de rede nas seguintes portas TCP:

Produto	Portas TCP
XProtect VMS	80, 8080, 7563, 25, 21, 9000
XProtect Mobile	8081

ou

- Excluir a verificação dos seguintes processos da rede:

Produto	Processos
XProtect VMS	VideoOS.Recorder.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

A sua organização pode ter diretrizes rigorosas relativas à verificação de vírus, entretanto é importante que você exclua da verificação de vírus as pastas e arquivos mencionados acima.

Como o XProtect VMS pode ser configurado para funcionar no modo compatível com FIPS 140-2?

Para executar o XProtect VMS em um modo de operação FIPS 140-2, é preciso:

- Execute o sistema operacional Windows no modo de operação aprovado pelo FIPS 140-2. Consulte o site da Microsoft para obter informações sobre como ativar o FIPS.
- Certificar-se de que integrações independentes de terceiros possam ser executadas em um sistema operacional Windows habilitado para FIPS
- Conectar-se a dispositivos de uma forma que garanta um modo de operação compatível com FIPS 140-2
- Certificar-se de que os dados no banco de dados de mídia sejam criptografados com cifras compatíveis com FIPS 140-2

  Isso é feito executando a ferramenta de atualização do banco de dados de mídia. Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

Antes de instalar o XProtect VMS em um sistema habilitado para FIPS

Embora novas instalações XProtect VMS possam ser feitas em computadores habilitados para FIPS, não é possível atualizar o XProtect VMS quando o FIPS está habilitado no sistema operacional Windows.

Se você estiver fazendo uma atualização, antes da instalação, desative a política de segurança FIPS do Windows em todos os computadores que fazem parte do VMS, incluindo o computador que hospeda o SQL Server.

O instalador XProtect VMS verifica a política de segurança FIPS e impedirá que a instalação seja iniciada se o FIPS estiver ativado.

Mas, se você estiver atualizando da versão 2020 R3 do XProtect VMS e posteriores, não precisa desabilitar o FIPS.

Depois de instalar os componentes XProtect VMS em todos os computadores e preparar o sistema para FIPS, você pode habilitar a política de segurança FIPS no Windows em todos os computadores em seu VMS.

Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

Registrar o código da licença de software

Antes de instalar, você deve ter o nome e a localização do arquivo de licença de software que recebeu da Milestone.

Você pode instalar uma versão gratuita de XProtect Essential+. Esta versão fornece recursos limitados de XProtect VMS para um número limitado de câmeras. Você deve ter conexão de Internet para instalar XProtect Essential+.

O Código de Licença do Software (Software License Code, SLC) está impresso na confirmação do seu pedido, e o arquivo de licença de software é nomeado de acordo com o seu SCL.

Milestone recomenda que você registre o seu SLC no nosso website (https://online.milestonesys.com/) antes da instalação. Seu revendedor pode ter feito isso para você.

Drivers de dispositivos (explicado)

O sistema usa os drivers de dispositivo de vídeo para controlar e se comunicar com os dispositivos de câmera conectados a um servidor de gravação. Você deve instalar os drivers de dispositivos em cada servidor de gravação em seu sistema.

A partir da versão 2018 R1, os drivers de dispositivos estão divididos em dois pacotes: o pacote de dispositivos regular, com drivers mais recentes, e um pacote de dispositivos herdados com drivers mais antigos.

O pacote de dispositivos regular é instalado automaticamente quando você instala o servidor de gravação. Posteriormente, você pode atualizar os drivers baixando e instalando uma versão mais recente do pacote de dispositivos. A Milestone lança regularmente novas versões de drivers de dispositivo e as disponibiliza na página de download (https://www.milestonesys.com/downloads/) em nosso site como pacotes de dispositivos. Ao atualizar um pacote de dispositivos, você pode instalar a versão mais recente sobre qualquer versão que você tenha instalado.

O pacote de dispositivos herdados só pode ser instalado se o sistema tiver um pacote de dispositivos regular instalado. Os drivers do pacote de dispositivos herdados são instalados automaticamente se uma versão anterior já estiver instalada em seu sistema. Está disponível para download manual e instalação na página de download de software (https://www.milestonesys.com/downloads/).

Interrompa o serviço Recording Server antes da instalação; caso contrário, será necessário reiniciar o computador.

Para garantir o melhor desempenho, use sempre a versão mais recente dos drivers de dispositivos.

Requisitos para instalação off-line

Se instalar o sistema em um servidor que esteja off-line, é necessário o seguinte:

- Oarquivo `Milestone XProtect VMS Products 2023 R3 System Installer.exe`
- O arquivo de licença de software (SLC) para seu sistema XProtect
- Mídia de instalação do OS incluindo a versão .NET necessária (https://www.milestonesys.com/systemrequirements/)

Comunicação segura (explicado)

Hypertext Transfer Protocol Secure (HTTPS) é uma extensão do Hypertext Transfer Protocol (HTTP) para a comunicação segura através de uma rede de computadores. No HTTPS, o protocolo de comunicação é criptografado usando o Transport Layer Security (TLS), ou seu predecessor, Secure Sockets Layer (SSL).

No XProtect VMS, a comunicação segura é obtida usando TLS/SSL com criptografia assimétrica (RSA).

O TLS/SSL usa um par de chaves — uma privada, uma pública — para autenticar, proteger e gerenciar conexões seguras.

Uma autoridade de certificação (CA) é qualquer pessoa que possa emitir certificados raiz. Pode ser um serviço de Internet que emite certificados raiz ou qualquer pessoa que gere e distribua manualmente um certificado. Uma autoridade de certificação pode emitir certificados para serviços da web, ou seja, para qualquer software que use comunicação https. Esse certificado contém duas chaves, uma privada e uma pública. A chave privada é instalada nos clientes de um serviço da web (clientes de serviço) pela instalação de um certificado público. A chave privada é usada para assinar certificados de servidor que devem ser instalados no servidor. Sempre que um cliente de serviço chama o serviço da web, ele envia o certificado do servidor, incluindo a chave pública, ao cliente. O cliente do serviço pode validar o certificado do servidor usando o certificado de CA público já instalado. O cliente e o servidor agora podem usar os certificados de servidor público e privado para trocar uma chave secreta e, assim, estabelecer uma conexão TLS/SSL segura.

Para certificados distribuídos manualmente, os certificados devem ser instalados antes que o cliente possa fazer tal verificação.

Veja Transport Layer Security para obter mais informações sobre TLS.

> Os certificados têm uma data de vencimento. XProtect VMS não o avisará quando um certificado estiver prestes a vencer. Se um certificado expirar:
> Os clientes não mais confiarão no servidor de gravação com o certificado expirado e, assim, não poderão ser comunicar com ele
> • Os servidores de gravação não mais confiarão no servidor de gerenciamento com o certificado expirado e, assim, não poderão ser comunicar com ele
> • Os dispositivos móveis não mais confiarão no servidor móvel com o certificado expirado e, assim, não poderão ser comunicar com ele
>
> Para renovar os certificados, siga as etapas neste guia, como você fez ao criar certificados.

Para obter mais informações, consulte o guia de certificados sobre como proteger suas XProtect VMS instalações.

Instalação

Instalar um novo sistema XProtect

Instalar XProtect Essential+

Você pode instalar uma versão gratuita de XProtect Essential+. Esta versão fornece recursos limitados de XProtect VMS para um número limitado de câmeras. Você deve ter conexão de Internet para instalar XProtect Essential+.

Esta versão está instalada em um único computador, usando a opção de instalação **Único computador**. A opção **Único computador** instala todos os componentes do servidor e do cliente no computador atual.

A Milestone recomenda a leitura cuidadosa da seção a seguir, antes da instalação: Antes de você iniciar a instalação na página 140.

Para instalações FIPS, você não pode atualizar o XProtect VMS quando o FIPS estiver ativado no sistema operacional Windows. Antes de instalar, desative a política de segurança FIPS do Windows em todos os computadores que fazem parte do VMS, incluindo o computador que hospeda o SQL Server. Mas, se você estiver atualizando da versão 2020 R3 do XProtect VMS e posteriores, não precisa desabilitar o FIPS. Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

Após a instalação inicial, você pode continuar com o assistente de configuração. Dependendo do seu hardware e configuração, o servidor de gravação verifica a sua rede para hardware. Você pode então selecionar os dispositivos de hardware para adicionar ao seu sistema. As câmeras são pré-configuradas nas visualizações e você tem a opção de ativar outros dispositivos, como microfones e alto-falantes. Você também tem a opção de adicionar usuários com função de Operadores ou função de Administradores no sistema. Após a instalação, XProtect Smart Client abre e você está pronto para usar o sistema.

Caso contrário, se você fechar o assistente de instalação, o XProtect Management Client abre e você pode fazer configurações manuais, como adicionar hardware e usuários ao sistema.

Se você fizer atualização de uma versão anterior do produto, o sistema não procurará por hardware nem criará novas visualizações e perfis de usuário.

1. Baixe o software da internet https://www.milestonesys.com/downloads/) e execute o arquivo `Milestone XProtect VMS Products 2023 R3 System Installer.exe`.
2. Os arquivos de instalação descompactam. Dependendo das configurações de segurança, um ou mais avisos de segurança do Windows® aparecerão. Aceite-as e a descompactação continuará.
3. Após a conclusão, o assistente de instalação do **Milestone XProtect VMS** aparecerá.
    1. Selecione o **Idioma** a ser usado durante a instalação (esse não é o idioma que o seu sistema usará após a instalação; esse será selecionado mais tarde). Clique em **Continuar**.
    2. Leia o *Contrato de Licença de Usuário Final da Milestone*. Selecione a caixa de seleção **Aceito os termos do contrato de licença** e clique em **Continuar**.
    3. Na página **Configurações de privacidade**, selecione se deseja compartilhar dados de uso e clique em **Continuar**.

        > Você não deve ativar a coleta de dados se quiser que o sistema tenha uma instalação compatível com a EU GDPR. Para obter mais informações sobre proteção de dados e coleta de dados de uso, consulte o guia de privacidade do GDPR.

        > Você sempre pode alterar sua configuração de privacidade mais tarde. Consulte também Configurações do sistema (caixa de diálogo Opções).

    4. Clique no link **XProtect Essential+** para fazer o download de um arquivo de licença gratuito.

        O arquivo de licença gratuita é baixado e aparece no campo **Insira ou navegue para o local do arquivo de licença**. Clique em **Continuar**.
4. Selecione **Único computador**.

    Uma lista de componentes a serem instalados aparece (você não pode editar esta lista). Clique em **Continuar**.

5. Na página **Atribuir uma senha de configuração do sistema**, digite uma senha que proteja a configuração do seu sistema. Você precisará desta senha em caso de recuperação do sistema ou ao expandir seu sistema, por exemplo, ao adicionar clusters.

   > É importante que você salve esta senha e a mantenha em segurança. Se perder essa senha, você poderá comprometer sua capacidade de recuperar a configuração do sistema.

   Se não quiser que a configuração do sistema seja protegida por senha, selecione **Eu escolho não usar uma senha de configuração do sistema e entendo que a configuração do sistema não será criptografada**.

   Clique em **Continuar**.

6. Na página **Atribuir uma senha de proteção de dados do servidor móvel** e insira uma senha para criptografar suas investigações. Como administrador do sistema, você precisará inserir esta senha para acessar os dados do servidor móvel em caso de recuperação do sistema ou ao expandir seu sistema com servidores móveis adicionais.

   > Você deve salvar esta senha e mantê-la segura. Não fazer isso pode comprometer a sua capacidade de recuperar dados do servidor móvel.

   Se não desejar que suas investigações sejam protegidas por senha, selecione **Eu opto por não usar uma senha de proteção de dados do servidor móvel e compreendo que as investigações não serão criptografadas**.

   Clique em **Continuar**.

7. Na página **Especificar configurações do servidor de gravação**, especifique as diferentes configurações do servidor de gravação:

   1. No campo **Nome do servidor de gravação**, digite o nome do servidor de gravação. O padrão é o nome do computador.
   2. O campo **Endereço do servidor de gerenciamento** mostra o endereço e o número da porta do servidor de gerenciamento: localhost:80.
   3. No campo **Selecione o local da mídia e banco de dados**, selecione o local onde deseja salvar sua gravação de vídeo. Milestone recomenda que você salve as suas gravações de vídeo em um local diferente de onde você instalar o software, e não na unidade do sistema. A localização padrão é a unidade com o maior espaço disponível.
   4. No campo **Tempo de retenção para gravações de vídeo**, defina por quanto tempo você deseja salvar as gravações. Você pode inserir entre 1 e 365,000 dias, onde 7 dias é o tempo de retenção padrão.
   5. Clique em **Continuar**.

8. Na página **Selecionar criptografia**, você pode proteger os fluxos de comunicação:

   - Entre os servidores de gravação, coletores de dados e o servidor de gerenciamento

     Para ativar a criptografia para fluxos de comunicação internos, selecione um certificado na seção **Certificado do servidor**.

     > ⚠ Se você criptografar a conexão do servidor de gravação para o servidor de gerenciamento, o sistema requer que você também criptografe a conexão do servidor de gerenciamento para o servidor de gravação.

   - Entre os servidores de gravação e clientes

     Para ativar a criptografia entre servidores de gravação e componentes clientes que recuperam fluxos de dados do servidor de gravação, selecione um certificado na seção **Certificado de mídia de streaming**.

   - Entre o servidor móvel e os clientes

     Para habilitar a criptografia entre os componentes do cliente que recuperam fluxos de dados do servidor móvel, na seção **Certificado de mídia de fluxo móvel**, selecione um certificado.

   - Entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos

     Para ativar a criptografia entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos, incluindo o LPR Server, selecione um certificado na seção **Servidor de eventos e extensões**.

   Você pode usar o mesmo arquivo de certificado para todos os componentes do sistema ou usar arquivos de certificado diferentes, dependendo dos componentes do sistema.

   Para obter mais informações sobre preparar seu sistema para comunicação segura, consulte:

   - Comunicação segura (explicado) na página 151
   - O guia Milestone sobre certificados

   Você também pode ativar a criptografia após a instalação, a partir do Server Configurator no ícone de bandeja Management Server Manager na área de notificação.

9. Na página **Selecionar localização do arquivo e idioma do produto**, faça o seguinte:

    1. No campo **Localização do arquivo**, selecione o local onde você deseja instalar o software.

    > Se algum produto Milestone XProtect VMS já estiver instalado no computador, este campo é desativado. O campo exibe o local onde o componente será instalado.

    2. Em **Idioma do produto**, selecione o idioma no qual o seu produto XProtect deve ser instalado.
    3. Clique em **Instalar**.

    O software agora instala. Se ainda não instalados no computador, Microsoft® SQL Server® Express e o Microsoft IIS são automaticamente instalados durante a instalação.

10. Você pode ser solicitado a reiniciar o computador. Após a reinicialização do computador, dependendo das configurações de segurança, um ou mais avisos de segurança do Windows podem aparecer. Aceite-as e a instalação conclui.
11. Quando a instalação for concluída, uma lista mostra os componentes instalados no computador.

    Clique em **Continuar** para adicionar hardware e usuários ao sistema.

    > Se você clicar em **Fechar** agora, você dispensa o assistente de configuração e o XProtect Management Client abre. Você pode configurar o sistema, por exemplo, adicionar hardware e usuários ao sistema, no Management Client.

12. Na página **Insira nomes de usuário e senhas para hardware**, insira os nomes e senhas de hardware que você alterou dos padrões do fabricante.

    O instalador procurará esse hardware, assim como hardware com credenciais padrão do fabricante.

    Clique em **Continuar** e aguarde enquanto o sistema procura por hardware.

13. Na página **Selecione o hardware para adicionar ao sistema**, selecione o hardware que deseja adicionar ao sistema. Clique em **Continuar** e aguarde até que o sistema adicione o hardware.

14. Na página **Configurar os dispositivos**, você pode dar nomes descritivos ao hardware clicando no ícone de edição ao lado do nome do hardware. Este nome é, então, prefixado para os dispositivos de hardware.

    Expanda o nó de hardware para ativar ou desativar os dispositivos de hardware como câmeras, alto-falantes e microfones.

    > As câmeras estão ativadas por padrão, e os alto-falantes e os microfones estão desativados por padrão.

    Clique em **Continuar** e aguarde até que o sistema configure o hardware.

15. Na página **Adicionar usuários**, você pode adicionar usuários ao sistema como usuários do Windows ou básicos. Os usuários podem ter a função de Administradores ou a função de Operadores.

    Defina o usuário e clique em **Adicionar**.

    Quando terminar de adicionar usuários, clique em **Continuar**.

16. Quando a instalação e configuração iniciais estiverem concluídas, a página **A configuração está completa** aprece, onde você vê:
    - Uma lista de dispositivos de hardware que estão adicionados ao sistema
    - Uma lista de usuários que estão adicionados ao sistema
    - Endereços para o XProtect Web Client e o cliente XProtect Mobile, que você pode compartilhar com seus usuários

    Quando você clica em **Fechar**, o XProtect Smart Client abre e fica pronto para usar.

Instale o seu sistema – opção Único computador

A opção **Único computador** instala todos os componentes do servidor e do cliente no computador atual.

> A Milestone recomenda a leitura cuidadosa da seção a seguir, antes da instalação: Antes de você iniciar a instalação na página 140.

Para instalações FIPS, você não pode atualizar o XProtect VMS quando o FIPS estiver ativado no sistema operacional Windows. Antes de instalar, desative a política de segurança FIPS do Windows em todos os computadores que fazem parte do VMS, incluindo o computador que hospeda o SQL Server. Mas, se você estiver atualizando da versão 2020 R3 do XProtect VMS e posteriores, não precisa desabilitar o FIPS. Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

Após a instalação inicial, você pode continuar com o assistente de configuração. Dependendo do seu hardware e configuração, o servidor de gravação verifica a sua rede para hardware. Você pode então selecionar os dispositivos de hardware para adicionar ao seu sistema. As câmeras são pré-configuradas nas visualizações e você tem a opção de ativar outros dispositivos, como microfones e alto-falantes. Você também tem a opção de adicionar usuários com função de Operadores ou função de Administradores no sistema. Após a instalação, XProtect Smart Client abre e você está pronto para usar o sistema.

Caso contrário, se você fechar o assistente de instalação, o XProtect Management Client abre e você pode fazer configurações manuais, como adicionar hardware e usuários ao sistema.

Se você fizer atualização de uma versão anterior do produto, o sistema não procurará por hardware nem criará novas visualizações e perfis de usuário.

1. Baixe o software da internet https://www.milestonesys.com/downloads/) e execute o arquivo `Milestone XProtect VMS Products 2023 R3 System Installer.exe`.
2. Os arquivos de instalação descompactam. Dependendo das configurações de segurança, um ou mais avisos de segurança do Windows® aparecerão. Aceite-as e a descompactação continuará.
3. Após a conclusão, o assistente de instalação do **Milestone XProtect VMS** aparecerá.
    1. Selecione o **Idioma** a ser usado durante a instalação (esse não é o idioma que o seu sistema usará após a instalação; esse será selecionado mais tarde). Clique em **Continuar**.
    2. Leia o *Contrato de Licença de Usuário Final da Milestone*. Selecione a caixa de seleção **Aceito os termos do contrato de licença** e clique em **Continuar**.
    3. Na página **Configurações de privacidade**, selecione se deseja compartilhar dados de uso e clique em **Continuar**.

> Você não deve ativar a coleta de dados se quiser que o sistema tenha uma instalação compatível com a EU GDPR. Para obter mais informações sobre proteção de dados e coleta de dados de uso, consulte o guia de privacidade do GDPR.

> Você sempre pode alterar sua configuração de privacidade mais tarde. Consulte também Configurações do sistema (caixa de diálogo Opções).

4. Em **Insira ou vá ao local do arquivo de licença**, insira o arquivo de licença do seu provedor XProtect. Alternativamente, navegue para o local do arquivo ou clique no link **XProtect Essential+** para baixar um arquivo de licença gratuita. Para limitações do produto XProtect Essential+ gratuito, consulte Comparação de produto na página 118. O sistema verifica seu arquivo de licença antes de continuar. Clique em **Continuar**.

4. Selecione **Único computador**.

   Uma lista de componentes a serem instalados aparece (você não pode editar esta lista). Clique em **Continuar**.

5. Na página **Atribuir uma senha de configuração do sistema**, digite uma senha que proteja a configuração do seu sistema. Você precisará desta senha em caso de recuperação do sistema ou ao expandir seu sistema, por exemplo, ao adicionar clusters.

   > É importante que você salve esta senha e a mantenha em segurança. Se perder essa senha, você poderá comprometer sua capacidade de recuperar a configuração do sistema.

   Se não quiser que a configuração do sistema seja protegida por senha, selecione **Eu escolho não usar uma senha de configuração do sistema e entendo que a configuração do sistema não será criptografada**.

   Clique em **Continuar**.

6. Na página **Atribuir uma senha de proteção de dados do servidor móvel** e insira uma senha para criptografar suas investigações. Como administrador do sistema, você precisará inserir esta senha para acessar os dados do servidor móvel em caso de recuperação do sistema ou ao expandir seu sistema com servidores móveis adicionais.

   > ⚠ Você deve salvar esta senha e mantê-la segura. Não fazer isso pode comprometer a sua capacidade de recuperar dados do servidor móvel.

   Se não desejar que suas investigações sejam protegidas por senha, selecione **Eu opto por não usar uma senha de proteção de dados do servidor móvel e compreendo que as investigações não serão criptografadas**.

   Clique em **Continuar**.

7. Na página **Especificar configurações do servidor de gravação**, especifique as diferentes configurações do servidor de gravação:

   1. No campo **Nome do servidor de gravação**, digite o nome do servidor de gravação. O padrão é o nome do computador.
   2. O campo **Endereço do servidor de gerenciamento** mostra o endereço e o número da porta do servidor de gerenciamento: localhost:80.
   3. No campo **Selecione o local da mídia e banco de dados**, selecione o local onde deseja salvar sua gravação de vídeo. Milestone recomenda que você salve as suas gravações de vídeo em um local diferente de onde você instalar o software, e não na unidade do sistema. A localização padrão é a unidade com o maior espaço disponível.
   4. No campo **Tempo de retenção para gravações de vídeo**, defina por quanto tempo você deseja salvar as gravações. Você pode inserir entre 1 e 365,000 dias, onde 7 dias é o tempo de retenção padrão.
   5. Clique em **Continuar**.

8. Na página **Selecionar criptografia**, você pode proteger os fluxos de comunicação:

   - Entre os servidores de gravação, coletores de dados e o servidor de gerenciamento

     Para ativar a criptografia para fluxos de comunicação internos, selecione um certificado na seção **Certificado do servidor**.

     > Se você criptografar a conexão do servidor de gravação para o servidor de gerenciamento, o sistema requer que você também criptografe a conexão do servidor de gerenciamento para o servidor de gravação.

   - Entre os servidores de gravação e clientes

     Para ativar a criptografia entre servidores de gravação e componentes clientes que recuperam fluxos de dados do servidor de gravação, selecione um certificado na seção **Certificado de mídia de streaming**.

   - Entre o servidor móvel e os clientes

     Para habilitar a criptografia entre os componentes do cliente que recuperam fluxos de dados do servidor móvel, na seção **Certificado de mídia de fluxo móvel**, selecione um certificado.

   - Entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos

     Para ativar a criptografia entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos, incluindo o LPR Server, selecione um certificado na seção **Servidor de eventos e extensões**.

   Você pode usar o mesmo arquivo de certificado para todos os componentes do sistema ou usar arquivos de certificado diferentes, dependendo dos componentes do sistema.

   Para obter mais informações sobre preparar seu sistema para comunicação segura, consulte:

   - Comunicação segura (explicado) na página 151
   - O guia Milestone sobre certificados

   Você também pode ativar a criptografia após a instalação, a partir do Server Configurator no ícone de bandeja Management Server Manager na área de notificação.

9. Na página **Selecionar localização do arquivo e idioma do produto**, faça o seguinte:

    1. No campo **Localização do arquivo**, selecione o local onde você deseja instalar o software.

    > Se algum produto Milestone XProtect VMS já estiver instalado no computador, este campo é desativado. O campo exibe o local onde o componente será instalado.

    2. Em **Idioma do produto**, selecione o idioma no qual o seu produto XProtect deve ser instalado.
    3. Clique em **Instalar**.

    O software agora instala. Se ainda não instalados no computador, Microsoft® SQL Server® Express e o Microsoft IIS são automaticamente instalados durante a instalação.

10. Você pode ser solicitado a reiniciar o computador. Após a reinicialização do computador, dependendo das configurações de segurança, um ou mais avisos de segurança do Windows podem aparecer. Aceite-as e a instalação conclui.
11. Quando a instalação for concluída, uma lista mostra os componentes instalados no computador.

    Clique em **Continuar** para adicionar hardware e usuários ao sistema.

    > Se você clicar em **Fechar** agora, você dispensa o assistente de configuração e o XProtect Management Client abre. Você pode configurar o sistema, por exemplo, adicionar hardware e usuários ao sistema, no Management Client.

12. Na página **Insira nomes de usuário e senhas para hardware**, insira os nomes e senhas de hardware que você alterou dos padrões do fabricante.

    O instalador procurará esse hardware, assim como hardware com credenciais padrão do fabricante.

    Clique em **Continuar** e aguarde enquanto o sistema procura por hardware.

13. Na página **Selecione o hardware para adicionar ao sistema**, selecione o hardware que deseja adicionar ao sistema. Clique em **Continuar** e aguarde até que o sistema adicione o hardware.

14. Na página **Configurar os dispositivos**, você pode dar nomes descritivos ao hardware clicando no ícone de edição ao lado do nome do hardware. Este nome é, então, prefixado para os dispositivos de hardware.

    Expanda o nó de hardware para ativar ou desativar os dispositivos de hardware como câmeras, alto-falantes e microfones.

    > As câmeras estão ativadas por padrão, e os alto-falantes e os microfones estão desativados por padrão.

    Clique em **Continuar** e aguarde até que o sistema configure o hardware.

15. Na página **Adicionar usuários**, você pode adicionar usuários ao sistema como usuários do Windows ou básicos. Os usuários podem ter a função de Administradores ou a função de Operadores.

    Defina o usuário e clique em **Adicionar**.

    Quando terminar de adicionar usuários, clique em **Continuar**.

16. Quando a instalação e configuração iniciais estiverem concluídas, a página **A configuração está completa** aprece, onde você vê:
    - Uma lista de dispositivos de hardware que estão adicionados ao sistema
    - Uma lista de usuários que estão adicionados ao sistema
    - Endereços para o XProtect Web Client e o cliente XProtect Mobile, que você pode compartilhar com seus usuários

    Quando você clica em **Fechar**, o XProtect Smart Client abre e fica pronto para usar.

Instale o seu sistema - opção Personalizado

A opção **Personalizada** instala o servidor de gerenciamento, mas permite selecionar que outros componentes do servidor e cliente você deseja instalar no computador atual. Por padrão, o servidor de gravação não está selecionado na lista de componentes. Dependendo de suas seleções, você pode instalar os componentes do sistema não selecionados, em outros computadores posteriormente. Para obter mais informações sobre cada componente do site e sua função, consulte Visão geral do produto na página 33. A instalação em outros computadores é feita através da página de download do servidor de gerenciamento chamada Download Manager. Para obter mais informações sobre a instalação através de Download Manager, consulte Download Manager/página da Web de download na página 191.

> A Milestone recomenda a leitura cuidadosa da seção a seguir, antes da instalação: Antes de você iniciar a instalação na página 140.

Para instalações FIPS, você não pode atualizar o XProtect VMS quando o FIPS estiver ativado no sistema operacional Windows. Antes de instalar, desative a política de segurança FIPS do Windows em todos os computadores que fazem parte do VMS, incluindo o computador que hospeda o SQL Server. Mas, se você estiver atualizando da versão 2020 R3 do XProtect VMS e posteriores, não precisa desabilitar o FIPS. Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

1. Baixe o software da internet https://www.milestonesys.com/downloads/) e execute o arquivo `Milestone XProtect VMS Products 2023 R3 System Installer.exe`.
2. Os arquivos de instalação descompactam. Dependendo das configurações de segurança, um ou mais avisos de segurança do Windows® aparecerão. Aceite-as e a descompactação continuará.
3. Após a conclusão, o assistente de instalação do **Milestone XProtect VMS** aparecerá.
    1. Selecione o **Idioma** a ser usado durante a instalação (esse não é o idioma que o seu sistema usará após a instalação; esse será selecionado mais tarde). Clique em **Continuar**.
    2. Leia o *Contrato de Licença de Usuário Final da Milestone*. Selecione a caixa de seleção **Aceito os termos do contrato de licença** e clique em **Continuar**.
    3. Na página **Configurações de privacidade**, selecione se deseja compartilhar dados de uso e clique em **Continuar**.

        Você não deve ativar a coleta de dados se quiser que o sistema tenha uma instalação compatível com a EU GDPR. Para obter mais informações sobre proteção de dados e coleta de dados de uso, consulte o guia de privacidade do GDPR.

        Você sempre pode alterar sua configuração de privacidade mais tarde. Consulte também Configurações do sistema (caixa de diálogo Opções).

    4. Em **Insira ou vá ao local do arquivo de licença**, insira o arquivo de licença do seu provedor XProtect. Alternativamente, navegue para o local do arquivo ou clique no link **XProtect Essential+** para baixar um arquivo de licença gratuita. Para limitações do produto XProtect Essential+ gratuito, consulte Comparação de produto na página 118. O sistema verifica seu arquivo de licença antes de continuar. Clique em **Continuar**.

4. Selecione **Personalizado**. Uma lista de componentes a serem instalados é mostrada. Além do servidor de gerenciamento, todos os componentes da lista são opcionais. O servidor de gravação e o servidor móvel não são selecionados por padrão. Selecione os componentes do sistema que deseja instalar e clique em **Continuar**.

   Para que seu sistema funcione corretamente, é necessário instalar pelo menos uma instância do XProtect API Gateway.

   Nas etapas abaixo, todos os componentes do sistema estão instalados. Para um sistema mais distribuído, instale menos componentes do sistema neste computador e os componentes restantes do sistema em outros computadores. Se não puder reconhecer uma etapa de instalação, provavelmente é porque você não optou por instalar o componente no sistema ao qual essa página pertence. Neste caso, continue para a próxima etapa. Consulte também Instalando através do Download Manager (explicado) na página 170, Instalar um servidor de gravação através de Download Manager na página 171 e Instalando silenciosamente através de uma shell da linha de comando (explicado) na página 177.

5. A página **Selecionar um site no IIS para usar com o seu sistema XProtect** só é mostrada se você tiver mais do que um site IIS disponível no computador. Você deve selecionar que site usará com o seu sistema XProtect. Selecione um site com ligação HTTPS. Clique em **Continuar**.

   Se o Microsoft ® IIS não estiver instalado no computador, ele é instalado.

6. Na página **Selecionar Microsoft SQL Server**, selecione o SQL Server que deseja usar. Consulte também SQL Server opções durante a instalação personalizada na página 169. Clique em **Continuar**.

   Caso não tenha o SQL Server em seu computador local, é possível instalar o Microsoft SQL Server Express. Porém, em um sistema maior distribuído, normalmente você usaria um SQL Server dedicado na sua rede.

7. Em **Selecionar banco de dados** (a opção só será exibida se você tiver selecionado um SQL Server existente), selecione ou crie um banco de dados do SQL Server para armazenar a configuração do sistema. Se você escolher um banco de dados SQL Server existente, opte por **Manter** ou **Substituir** os dados existentes. Se estiver fazendo um upgrade, opte por manter os dados existentes, para não perder as configurações do sistema. Consulte também SQL Server opções durante a instalação personalizada na página 169. Clique em **Continuar**.

8. Na página **Configurações de banco de dados**, selecione **Deixar o instalador criar ou recriar um banco de dados** ou **Usar um banco de dados pré-criado**.

9. Para fazer com que seus bancos de dados sejam criados ou recriados automaticamente, selecione **Deixar o instalador criar ou recriar um banco de dados** e clique em **Continuar**.
10. Para usar bancos de dados que você configurou com essa finalidade ou bancos de dados que já foram criados, selecione **Usar um banco de dados pré-criado**. Em seguida, você verá a página **Configuração de banco de dados avançada**.
11. Na página **Configuração avançada do banco de dados**, insira o nome do servidor e do banco de dados para os componentes do XProtect.
12. Selecione **Autenticação do Windows, não confiar no certificado do servidor (recomendado)** ou **Autenticação do Windows, confiar no certificado do servidor** ou selecione **Azure Active Directory Integrated, não confiar no certificado do servidor (recomendado)**.

    Dependendo do tipo de autenticação que você deseja usar, será necessário criar a conta a ser usada para a instalação no Azure AD ou no Windows AD. Não há compatibilidade com autenticação multifator nas contas.

    A opção **(não confiar no certificado do servidor)** é recomendada para a autenticação do Windows e obrigatória para o Azure Active Directory Integrated. Ela serve para garantir que os certificados do servidor sejam validados e verificados antes da instalação. Você encontrará mais informações sobre certificados inválidos de servidor no arquivo de registro de instalação. Com a opção **autenticação do Windows, confiar no certificado do servidor**, você ignora a validação dos certificados do servidor.

13. Clique no ícone para verificar a conexão. Ao clicar no ícone, você também valida os certificados do servidor.
14. Clique em **Continuar**
15. Na página **Atribuir uma senha de configuração do sistema**, digite uma senha que proteja a configuração do seu sistema. Você precisará desta senha em caso de recuperação do sistema ou ao expandir seu sistema, por exemplo, ao adicionar clusters.

    É importante que você salve esta senha e a mantenha em segurança. Se perder essa senha, você poderá comprometer sua capacidade de recuperar a configuração do sistema.

    Se não quiser que a configuração do sistema seja protegida por senha, selecione **Eu escolho não usar uma senha de configuração do sistema e entendo que a configuração do sistema não será criptografada**.

    Clique em **Continuar**.

16. Na página **Atribuir uma senha de proteção de dados do servidor móvel** e insira uma senha para criptografar suas investigações. Como administrador do sistema, você precisará inserir esta senha para acessar os dados do servidor móvel em caso de recuperação do sistema ou ao expandir seu sistema com servidores móveis adicionais.

    > Você deve salvar esta senha e mantê-la segura. Não fazer isso pode comprometer a sua capacidade de recuperar dados do servidor móvel.

    Se não desejar que suas investigações sejam protegidas por senha, selecione **Eu opto por não usar uma senha de proteção de dados do servidor móvel e compreendo que as investigações não serão criptografadas**.

    Clique em **Continuar**.

17. Em **Selecionar conta de serviço para servidor de gravação**, selecione **Esta conta predefinida** ou **Esta conta** para selecionar a conta de serviço para o servidor de gravação.

    Se necessário, digite uma senha.

    > O nome de usuário da conta deve ser uma única palavra. Não deve ter um espaço.

    Clique em **Continuar.**

18. Na página **Especificar configurações do servidor de gravação**, especifique as diferentes configurações do servidor de gravação:

    1. No campo **Nome do servidor de gravação**, digite o nome do servidor de gravação. O padrão é o nome do computador.
    2. O campo **Endereço do servidor de gerenciamento** mostra o endereço e o número da porta do servidor de gerenciamento: localhost:80.
    3. No campo **Selecione o local da mídia e banco de dados**, selecione o local onde deseja salvar sua gravação de vídeo. Milestone recomenda que você salve as suas gravações de vídeo em um local diferente de onde você instalar o software, e não na unidade do sistema. A localização padrão é a unidade com o maior espaço disponível.
    4. No campo **Tempo de retenção para gravações de vídeo**, defina por quanto tempo você deseja salvar as gravações. Você pode inserir entre 1 e 365,000 dias, onde 7 dias é o tempo de retenção padrão.
    5. Clique em **Continuar**.

19. Na página **Selecionar criptografia**, você pode proteger os fluxos de comunicação:

    - Entre os servidores de gravação, coletores de dados e o servidor de gerenciamento

      Para ativar a criptografia para fluxos de comunicação internos, selecione um certificado na seção **Certificado do servidor**.

      > Se você criptografar a conexão do servidor de gravação para o servidor de gerenciamento, o sistema requer que você também criptografe a conexão do servidor de gerenciamento para o servidor de gravação.

    - Entre os servidores de gravação e clientes

      Para ativar a criptografia entre servidores de gravação e componentes clientes que recuperam fluxos de dados do servidor de gravação, selecione um certificado na seção **Certificado de mídia de streaming**.

    - Entre o servidor móvel e os clientes

      Para habilitar a criptografia entre os componentes do cliente que recuperam fluxos de dados do servidor móvel, na seção **Certificado de mídia de fluxo móvel**, selecione um certificado.

    - Entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos

      Para ativar a criptografia entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos, incluindo o LPR Server, selecione um certificado na seção **Servidor de eventos e extensões**.

    Você pode usar o mesmo arquivo de certificado para todos os componentes do sistema ou usar arquivos de certificado diferentes, dependendo dos componentes do sistema.

    Para obter mais informações sobre preparar seu sistema para comunicação segura, consulte:

    - Comunicação segura (explicado) na página 151
    - O guia Milestone sobre certificados

    Você também pode ativar a criptografia após a instalação, a partir do Server Configurator no ícone de bandeja Management Server Manager na área de notificação.

20. Na página **Selecionar local do arquivo e idioma do produto**, selecione o **Local do arquivo** para os arquivos de programa.

    > Se algum produto Milestone XProtect VMS já estiver instalado no computador, este campo é desativado. O campo exibe o local onde o componente será instalado.

21. No campo **Idioma do produto**, selecione o idioma no qual o seu produto XProtect deve ser instalado. Clique em **Instalar**.

    O software agora instala. Quando a instalação estiver concluída, você verá uma lista de componentes do sistema instalados com sucesso. Clique em **Fechar**.

22. Você pode ser solicitado a reiniciar o computador. Após a reinicialização do computador, dependendo das configurações de segurança, um ou mais avisos de segurança do Windows podem aparecer. Aceite-as e a instalação conclui.

23. Configure o seu sistema no Management Client. Consulte Lista inicial de tarefas de configuração na página 199.

24. Dependendo de suas seleções, instale os componentes de sistema restantes em outros computadores através do Download Manager. Consulte Instalando através do Download Manager (explicado) na página 170.

SQL Server opções durante a instalação personalizada

Decidir qual SQL Server e banco de dados usar com as opções abaixo.

SQL Server opções:

- **Instale Microsoft® SQL Server® Express neste computador**: Essa opção só será exibida se o SQL Server não estiver instalado no computador
- **Use o SQL Server neste computador**: Essa opção só será exibida se o SQL Server já estiver instalado no computador
- **selecione um SQL Server na sua rede, através da pesquisa**: Permite que você pesquise todas as instalações do SQL Server detectáveis em sua subrede
- **selecione um SQL Server na sua rede**: Permite que você insira o endereço (nome do host ou endereço IP) de um SQL Server que talvez não seja detectável por meio da pesquisa

Opções do banco de dados SQL Server:

- **Criar um novo banco de dados**: Principalmente para novas instalações
- **Usar o banco de dados existente**: Principalmente para atualizações de instalações existentes. A Milestone recomenda que você reutilize o banco de dados SQL Server existente e mantenha os dados existentes nele, para não perder a configuração do seu sistema. Você também pode optar por substituir os dados no banco de dados SQL Server

Instalar novos componentes do XProtect

Instalando através do Download Manager (explicado)

Se desejar instalar componentes do sistema em computadores diferentes de onde o servidor de gerenciamento está instalado, você deve instalar esses componentes do sistema através da página da web de download do Management Server Download Manager.

1. A partir do computador onde Management Server está instalado, vá para a página da web de download do Management Server. No menu **Iniciar** do Windows, selecione **Milestone** > **Página de instalação administrativa** e anote ou copie o endereço da Internet para uso posterior ao instalar os componentes do sistema em outros computadores. Normalmente, o endereço é *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Faça o login em cada um dos outros computadores para instalar um ou mais dos outros componentes do sistema:
   - Recording Server(Para obter mais informações, consulte Instalar um servidor de gravação através de Download Manager na página 171 ou Instalar silenciosamente um servidor de gravação na página 179)
   - Management Client (Para obter mais informações, consulte Instale um Management Client através do Download Manager na página 171)
   - Smart Client
   - Event Server Lembre-se de reiniciar o API gateway após a instalação. Se você renomear o computador em uma data posterior, também será necessário reiniciar o API gateway.

     > ⚠ Se estiver instalando o Event Server em um ambiente compatível com FIPS, você deve desativar o modo FIPS 140-2 do Windows antes da instalação.

   - Log Server (Para obter mais informações, consulte Instalar um servidor de gravação silenciosamente na página 181)
   - Mobile Server (Para obter mais informações, consulte o manual do XProtect Mobileservidor)
3. Abra um navegador de Internet, insira o endereço da página da web de download do Management Server no campo de endereço e faça o download do instalador do servidor de gravação.
4. Execute o instalador.

Consulte Instale o seu sistema – opção Personalizado na página 163 se estiver em dúvida sobre as seleções e configurações em diferentes etapas da instalação.

Instale um Management Client através do Download Manager

Se houver vários administradores do sistema XProtect ou você simplesmente quiser gerenciar o sistema XProtect a partir de vários computadores, você pode instalar o Management Client seguindo as instruções abaixo.

O Management Client é sempre instalado no servidor de gerenciamento.

1. A partir do computador onde Management Server está instalado, vá para a página da web de download do Management Server. No menu **Iniciar** do Windows, selecione **Milestone** > **Página de instalação administrativa** e anote ou copie o endereço da Internet para uso posterior ao instalar os componentes do sistema em outros computadores. Normalmente, o endereço é *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Faça login no computador em que você deseja instalar o componente do sistema.
1. Abra um navegador da internet e insira o endereço da página de download do Management Server no campo de endereço e pressione Enter.
3. Clique em **Todos os idiomas** para o instalador do Management Client. Execute o arquivo baixado.
4. Clique em **Sim** para todos os avisos. A descompactação começa.
5. Selecione o idioma para o instalador. Clique em **Continuar**.
6. Leia e aceite o contrato de licença. Clique em **Continuar**.
7. Selecione a localização do arquivo e idioma do produto. Clique em **Instalar**.
8. A instalação está concluída. A lista de componentes instalados com sucesso é exibida. Clique em **Fechar**.
9. Clique no ícone na área de trabalho para abrir o Management Client.
10. A caixa de diálogo de login do Management Client aparece.
11. Especifique o nome do host ou o endereço IP do seu servidor de gerenciamento no campo **Computador**.
12. Selecione autenticação, digite seu nome de usuário e senha. Clique em **Conectar**. O Management Clienté inicializado.

    Para ler detalhadamente sobre as funções no Management Client e o que você pode realizar com o seu sistema, clique em **Ajuda** no menu de ferramentas.

Instalar um servidor de gravação através de Download Manager

Se os componentes do seu sistema estão distribuídos em computadores separados, você pode instalar os servidores de gravação seguindo as instruções abaixo.

O servidor de gravação já está instalado se você fez uma instalação em um **único computador**, mas você pode usar as mesmas instruções para adicionar mais servidores de gravação se precisar de mais capacidade.

Se precisar instalar um servidor de gravação de failover, consulte Instale um servidor do sistema de gravação ininterrupta através do Download Manager na página 175.

1. A partir do computador onde Management Server está instalado, vá para a página da web de download do Management Server. No menu **Iniciar** do Windows, selecione **Milestone** > **Página de instalação administrativa** e anote ou copie o endereço da Internet para uso posterior ao instalar os componentes do sistema em outros computadores. Normalmente, o endereço é *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Faça login no computador em que você deseja instalar o componente do sistema.
3. Abra um navegador da internet e insira o endereço da página de download do Management Server no campo de endereço e pressione Enter.
4. Baixe o instalador do servidor de gravação selecionando **Todos os idiomas** embaixo do **Instalador do servidor de gravação**. Salve o instalador ou execute-o diretamente a partir da página da web.
5. Selecione o **Idioma** que desejar usar durante a instalação. Clique em **Continuar**.
6. No a página **Selecione um tipo de instalação**, selecione:

   Típica para instalar um servidor de gravação com valores padrão, ou

   Personalizada para instalar um servidor de gravação com valores personalizados.

7. Na página **Especificar configurações do servidor de gravação**, especifique as diferentes configurações do servidor de gravação:
    1. No campo **Nome do servidor de gravação**, digite o nome do servidor de gravação. O padrão é o nome do computador.
    2. O campo **Endereço do servidor de gerenciamento** mostra o endereço e o número da porta do servidor de gerenciamento: localhost:80.
    3. No campo **Selecione o local da mídia e banco de dados**, selecione o local onde deseja salvar sua gravação de vídeo. Milestone recomenda que você salve as suas gravações de vídeo em um local diferente de onde você instalar o software, e não na unidade do sistema. A localização padrão é a unidade com o maior espaço disponível.
    4. No campo **Tempo de retenção para gravações de vídeo**, defina por quanto tempo você deseja salvar as gravações. Você pode inserir entre 1 e 365,000 dias, onde 7 dias é o tempo de retenção padrão.
    5. Clique em **Continuar**.
8. A página **Endereços IP dos servidores de gravação** só é mostrada se você selecionar **Personalizada**. Especifique o número de servidores de gravação que você desejar instalar no computador. Clique em **Continuar**.
9. Em **Selecionar conta de serviço para servidor de gravação**, selecione **Esta conta predefinida** ou **Esta conta** para selecionar a conta de serviço para o servidor de gravação.

    Se necessário, digite uma senha.

    > O nome de usuário da conta deve ser uma única palavra. Não deve ter um espaço.

    Clique em **Continuar.**

10. Na página **Selecionar criptografia**, você pode proteger os fluxos de comunicação:

    - Entre os servidores de gravação, coletores de dados e o servidor de gerenciamento

      Para ativar a criptografia para fluxos de comunicação internos, selecione um certificado na seção **Certificado do servidor**.

      > Se você criptografar a conexão do servidor de gravação para o servidor de gerenciamento, o sistema requer que você também criptografe a conexão do servidor de gerenciamento para o servidor de gravação.

    - Entre os servidores de gravação e clientes

      Para ativar a criptografia entre servidores de gravação e componentes clientes que recuperam fluxos de dados do servidor de gravação, selecione um certificado na seção **Certificado de mídia de streaming**.

    - Entre o servidor móvel e os clientes

      Para habilitar a criptografia entre os componentes do cliente que recuperam fluxos de dados do servidor móvel, na seção **Certificado de mídia de fluxo móvel**, selecione um certificado.

    - Entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos

      Para ativar a criptografia entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos, incluindo o LPR Server, selecione um certificado na seção **Servidor de eventos e extensões**.

    Você pode usar o mesmo arquivo de certificado para todos os componentes do sistema ou usar arquivos de certificado diferentes, dependendo dos componentes do sistema.

    Para obter mais informações sobre preparar seu sistema para comunicação segura, consulte:

    - Comunicação segura (explicado) na página 151
    - O guia Milestone sobre certificados

    Você também pode ativar a criptografia após a instalação, a partir do Server Configurator no ícone de bandeja Management Server Manager na área de notificação.

11. Na página **Selecionar local do arquivo e idioma do produto**, selecione o **Local do arquivo** para os arquivos de programa.

    > Se algum produto Milestone XProtect VMS já estiver instalado no computador, este campo é desativado. O campo exibe o local onde o componente será instalado.

12. No campo **Idioma do produto**, selecione o idioma no qual o seu produto XProtect deve ser instalado. Clique em **Instalar**.

    O software agora instala. Quando a instalação estiver concluída, você verá uma lista de componentes do sistema instalados com sucesso. Clique em **Fechar**.

13. Após ter instalado o servidor de gravação, você pode verificar seu estado a partir do ícone de bandeja do Recording Server Manager e configurá-lo no Management Client. Para obter mais informações, consulte Lista inicial de tarefas de configuração na página 199.

Instale um servidor do sistema de gravação ininterrupta através do Download Manager

> ⚠ Se você executa grupos de trabalho, deve usar o método de instalação alternativo para servidores de gravação de failover (consulte Instalação para grupos de trabalho na página 186).

1. A partir do computador onde Management Server está instalado, vá para a página da web de download do Management Server. No menu **Iniciar** do Windows, selecione **Milestone** > **Página de instalação administrativa** e anote ou copie o endereço da Internet para uso posterior ao instalar os componentes do sistema em outros computadores. Normalmente, o endereço é *http://[management server address]/installation/Admin/default-en-US.htm*.

   Faça login no computador em que você deseja instalar o componente do sistema.

2. Abra um navegador da internet e insira o endereço da página de download do Management Server no campo de endereço e pressione Enter.

3. Baixe o instalador do servidor de gravação selecionando **Todos os idiomas** embaixo do **Instalador do servidor de gravação**. Salve o instalador ou execute-o diretamente a partir da página da web.

4. Selecione o **Idioma** que desejar usar durante a instalação. Clique em **Continuar**.

5. Abra a página **Selecionar um tipo de instalação**, selecione **Failover** para instalar um servidor de gravação como servidor do sistema de gravação ininterrupta.

6. Na página **Especificar configurações do servidor de gravação**, especifique as diferentes configurações do servidor de gravação. O nome do servidor do sistema de gravação ininterrupta, o endereço do servidor de gerenciamento e o caminho para o banco de dados de mídias. Clique em **Continuar**.

7. Na página **Selecionar conta de serviço para servidor de gravação** e ao instalar um servidor do sistema de gravação ininterrupta, você deve usar a conta de usuário particular chamada **Esta conta**. Isso criar a conta de usuário do serviço de emergência. Se necessário, digite uma senha e confirme isso. Clique em **Continuar**.

8. Na página **Selecionar criptografia**, você pode proteger os fluxos de comunicação:

   - Entre os servidores de gravação, coletores de dados e o servidor de gerenciamento

     Para ativar a criptografia para fluxos de comunicação internos, selecione um certificado na seção **Certificado do servidor**.

     > Se você criptografar a conexão do servidor de gravação para o servidor de gerenciamento, o sistema requer que você também criptografe a conexão do servidor de gerenciamento para o servidor de gravação.

   - Entre os servidores de gravação e clientes

     Para ativar a criptografia entre servidores de gravação e componentes clientes que recuperam fluxos de dados do servidor de gravação, selecione um certificado na seção **Certificado de mídia de streaming**.

   - Entre o servidor móvel e os clientes

     Para habilitar a criptografia entre os componentes do cliente que recuperam fluxos de dados do servidor móvel, na seção **Certificado de mídia de fluxo móvel**, selecione um certificado.

   - Entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos

     Para ativar a criptografia entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos, incluindo o LPR Server, selecione um certificado na seção **Servidor de eventos e extensões**.

   Você pode usar o mesmo arquivo de certificado para todos os componentes do sistema ou usar arquivos de certificado diferentes, dependendo dos componentes do sistema.

   Para obter mais informações sobre preparar seu sistema para comunicação segura, consulte:

   - Comunicação segura (explicado) na página 151
   - O guia Milestone sobre certificados

   Você também pode ativar a criptografia após a instalação, a partir do Server Configurator no ícone de bandeja Management Server Manager na área de notificação.

9. Na página **Selecionar local do arquivo e idioma do produto**, selecione o **Local do arquivo** para os arquivos de programa.

   > Se algum produto Milestone XProtect VMS já estiver instalado no computador, este campo é desativado. O campo exibe o local onde o componente será instalado.

10. No campo **Idioma do produto**, selecione o idioma no qual o seu produto XProtect deve ser instalado. Clique em **Instalar**.

    O software agora instala. Quando a instalação estiver concluída, você verá uma lista de componentes do sistema instalados com sucesso. Clique em **Fechar**.

11. Após instalar o servidor do sistema de gravação ininterrupta, você pode verificar seu estado a partir do ícone da bandeja de serviço do Failover Server e configurá-lo no Management Client. Para obter mais informações, consulte Lista inicial de tarefas de configuração na página 199.

Instalar XProtect VMS usando portas não padrão

Uma instalação de XProtect VMS requer portas específicas. Em particular, o Management Server e o API Gateway são executados no IIS, e algumas portas precisam estar disponíveis. Esse tópico descreve como instalar o XProtect VMS e usar portas não padrão no IIS. Isso também se aplica ao instalar apenas o API Gateway.

Para obter uma visão geral de todas as portas que o VMS usa, consulte o XProtect VMS manual do administrador (https://doc.milestonesys.com/2023r3/pt-BR/portal/htm/chapter-page-mc-administrator-manual.htm).

Se o IIS ainda não estiver instalado no sistema, o instalador do XProtect VMS instala IIS e usa o site padrão com portas padrão.

Para evitar o uso do XProtect VMS padrão, instale o IIS primeiro. Opcionalmente, adicione um novo site ou prossiga usando o site padrão.

Adicione uma ligação para HTTPS, caso ela ainda não exista, e selecione um certificado válido no computador (será necessário selecioná-lo durante a instalação do XProtect VMS). Edite os números das portas em ambas as ligações HTTP e HTTPS para portas disponíveis de sua escolha.

Execute o instalador do XProtect VMS e selecione uma instalação **personalizada**.

Durante a instalação, a página **Selecione um site no IIS para usar com seu XProtect sistema** aparece se houver mais de um site disponível. Você deve selecionar que site usará com o seu sistema XProtect. O instalador usa os números das portas alterados.

Instalando silenciosamente através de uma shell da linha de comando (explicado)

Com a instalação silenciosa, os administradores de sistemas podem instalar e atualizar o software XProtect VMS e Smart Client por toda uma rede grande sem interações por parte do usuário, e com o mínimo de interferência possível para os usuários.

Os instaladores XProtect VMS e Smart Client (arquivos .exe) têm diferentes argumentos da linha de comando. Cada um deles têm seu próprio conjunto de parâmetros da linha de comando que podem ser invocados diretamente em uma shell da linha de comando ou através de um arquivo de argumentos. Na shell da linha de comando, você também pode usar opções da linha de comando com os instaladores.

Você pode combinar os instaladores do XProtect, seus parâmetros da linha de comando e opções da linha de comando com ferramentas para a distribuição silenciosa e instalação de software como o Gerenciador de configuração da Microsoft System Center (SCCM, também conhecido como ConfigMgr). Para obter mais informações sobre tais ferramentas, visite o site do fabricante. Você também pode usar o Milestone Software Manager para a instalação remota e atualização do XProtect VMS, pacotes de dispositivos e Smart Client. Para obter mais informações, consulte o manual do administrador do Milestone Software Manager.

Parâmetros da linha de comando e arquivos de argumento

Durante a instalação silenciosa, você pode especificar configurações vinculadas de perto a diferentes componentes do sistema VMS e sua comunicação interna, com parâmetros da linha de comando e arquivos de argumento. Parâmetros da linha de comando e arquivos de argumentos devem ser usados somente para novas instalações pois você não pode alterar as configurações que os parâmetros da linha de comando representam durante uma atualização.

Para ver os parâmetros da linha de comando disponíveis e para gerar um arquivo de argumentos para um instalador, na shell da linha de comando, navegue para o diretório onde o instalador está localizado e digite o seguinte comando:

```
[NameOfExeFile].exe --generateargsfile=[path]
```

Exemplo:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

No arquivo de argumentos salvo (Arguments.xml), cada parâmetro da linha de comando tem uma descrição que explica sua finalidade. Você pode modificar e salvar o arquivo de argumentos, de forma que os valores do parâmetro da linha de comando atendam as suas necessidades de instalação.

Quando você quiser usar um arquivo de argumentos com seu instalador, use a opção da linha de comando `--arguments` digitando o seguinte comando:

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

Exemplo:

```
Milestone XProtect VMS Products 2023 R3 System Installer.exe --quiet
--arguments=C:\temp\arguments.xml
```

Opções da linha de comando

Na shell da linha de comando, você também pode combinar instaladores com as opções da linha de comando. As opções da linha de comando geralmente modificam o comportamento de um comando.

Para ver a lista completa de opções da linha de comando, na shell da linha de comando, navegue para o diretório onde o instalador está localizado e digite `[NameOfExeFile].exe --help`. Para que a instalação seja bem-sucedida, você precisa especificar um valor para as opções da linha de comando que exigem um valor.

Você também pode usar ambos os parâmetros da linha de comando e as opções da linha de comando no mesmo comando. Use a opção da linha de comando `--parameters` e divida cada parâmetro da linha de comando com dois pontos (:). No exemplo abaixo `--quiet`, `--showconsole`, e `--parameters` são opções da linha de comando e `ISFAILOVER` e `RECORDERNAME` são parâmetros da linha de comando:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

Instalar silenciosamente um servidor de gravação

Ao instalar de modo silencioso, você não é notificado quando a instalação for concluída. Para ser notificado, inclua a opção da linha de comando `--showconsole` no comando. O ícone de bandeja do Milestone XProtect Recording Server aparece quando a instalação é concluída.

Nos exemplos de comando abaixo, o texto dentro de colchetes ([ ]) e os próprios colchetes devem ser substituídos por valores reais. Exemplo: em vez de "[caminho]", você pode inserir `d:\program files\`, `d:\record\` ou `\\network-storage-02\surveillance`. Use a opção da linha de comando `--help` para ler sobre os formatos legais de cada valor da opção da linha de comando.

1. Efetue login no computador onde deseja instalar o componente Recording Server.
2. Abra um navegador da internet e insira o endereço da página de download do Management Server direcionada para os administradores, no campo de endereço e pressione Enter.

   Normalmente, o endereço é `http://[management server address]:[porta]/installation/Admin/default-en-US.htm`.
3. Baixe o instalador do servidor de gravação selecionando **Todos os idiomas** embaixo do **Instalador do Recording Server**.
4. Abra a shell da linha de comando preferencial. Para abrir o prompt de comando do Windows, abra o menu Iniciar do Windows Start e digite **cmd**.
5. Navegue para o diretório com o instalador baixado.
6. Continue a instalação dependendo de um dos dois cenários abaixo:

   Cenário 1: Atualizar uma instalação existente ou instalar no servidor com o componente do Management Server com valores padrão

   - Insira o seguinte comando e a instalação começa.

     ```
     MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
     ```

Cenário 2: Instalar em um sistema distribuído

1. Insira o seguinte comando para gerar um arquivo de argumentos com parâmetros da linha de comando.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=
[path]
```

2. Abra o arquivo de argumentos (Arguments.xml) a partir do caminho especificado e modifique os valores do parâmetro da linha de comando.

Não deixe de dar os valores válidos aos parâmetros da linha de comando SERVERHOSTNAME e SERVERPORT. Se não, a instalação não poderá ser concluída.

4. Salve o arquivo de argumentos.
5. Retorne para a shell da linha de comando e insira o comando abaixo para instalar com os valores do parâmetro da linha de comando especificados no arquivo de argumentos.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=[path]\[filename]
```

Instale XProtect Smart Client de modo silencioso

Ao instalar de modo silencioso, você não é notificado quando a instalação for concluída. Para ser notificado, inclua a opção da linha de comando `--showconsole` no comando. Um atalho para o XProtect Smart Client aparece na área de trabalho quando a instalação é concluída.

Nos exemplos de comando abaixo, o texto dentro de colchetes ([ ]) e os próprios colchetes devem ser substituídos por valores reais. Exemplo: em vez de "[caminho]", você pode inserir `d:\program files\`, `d:\record\` ou `\\network-storage-02\surveillance`. Use a opção da linha de comando `--help` para ler sobre os formatos legais de cada valor da opção da linha de comando.

1. Abra um navegador da internet e insira o endereço da página de download do Management Server direcionada para os usuários finais, no campo de endereço e pressione Enter.

   Normalmente, o endereço é `http://[management server address]:[porta]/installation/default-en-US.htm`.

2. Baixe o instalador XProtect Smart Client selecionando **Todos os idiomas** embaixo do **Instalador do XProtect Smart Client**.
3. Abra a shell da linha de comando preferencial. Para abrir o prompt de comando do Windows, abra o

menu Iniciar do Windows Start e digite **cmd**.

4. Navegue para o diretório com o instalador baixado.
5. Continue a instalação dependendo de um dos dois cenários abaixo:

Cenário 1: Atualizar uma instalação existente ou instalar com valores do parâmetro da linha de comando padrão

- Insira o seguinte comando e a instalação começa.

```
"XProtect Smart Client 2023 R3 Installer.exe" --quiet
```

Cenário 2: Instalar com valores de parâmetro da linha de comando usando um arquivo de argumentos xml como entrada

1. Insira o seguinte comando para gerar um arquivo xml de argumentos com parâmetros da linha de comando.

```
"XProtect Smart Client 2023 R3 Installer.exe" --generateargsfile=
[path]
```

2. Abra o arquivo de argumentos (Arguments.xml) a partir do caminho especificado e modifique os valores do parâmetro da linha de comando.
3. Salve o arquivo de argumentos.
4. Retorne para a shell da linha de comando e insira o comando abaixo para instalar com os valores do parâmetro da linha de comando especificados no arquivo de argumentos.

```
"XProtect Smart Client 2023 R3 Installer.exe" --quiet --arguments=
[path]\[filename]
```

Instalar um servidor de gravação silenciosamente

Ao instalar de modo silencioso, você não é notificado quando a instalação for concluída. Para ser notificado, inclua a opção da linha de comando `--showconsole` no comando.

Nos exemplos de comando abaixo, o texto dentro de colchetes ([ ]) e os próprios colchetes devem ser substituídos por valores reais. Exemplo: em vez de “[caminho]”, você pode inserir `d:\program files\`, `d:\record\` ou `\\network-storage-02\surveillance`. Use a opção da linha de comando `--help` para ler sobre os formatos legais de cada valor da opção da linha de comando.

1. Efetue login no computador onde deseja instalar o componente Log Server.
2. Abra um navegador da internet e insira o endereço da página de download do Management Server direcionada para os administradores, no campo de endereço e pressione Enter.

   Normalmente, o endereço é `http://[management server address]:[porta]/installation/Admin/default-en-US.htm`.
3. Baixe o instalador do servidor de registros selecionando **Todos os idiomas** embaixo do **Instalador do Servidor de registros**.
4. Abra a shell da linha de comando preferencial. Para abrir o prompt de comando do Windows, abra o menu Iniciar do Windows Start e digite **cmd**.
5. Navegue para o diretório com o instalador baixado.
6. Continue a instalação dependendo de um dos dois cenários abaixo:

Cenário 1: Atualizar uma instalação existente ou instalar com valores do parâmetro da linha de comando padrão

- Insira o seguinte comando e a instalação começa.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --showconsole
```

Cenário 2: Instalar com valores personalizados de parâmetro da linha de comando usando um arquivo de argumentos XML como entrada

1. Insira o seguinte comando para gerar um arquivo xml de argumentos com parâmetros da linha de comando.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --generateargsfile=[path]
```

2. Abra o arquivo de argumentos (Arguments.xml) a partir do caminho especificado e modifique os valores do parâmetro da linha de comando.
3. Salve o arquivo de argumentos.
4. Retorne para a shell da linha de comando e insira o comando abaixo para instalar com os valores do parâmetro da linha de comando especificados no arquivo de argumentos.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --arguments=[path]\[filename] --showconsole
```

Instalar no modo silencioso usando uma conta de serviço dedicada

Se quiser instalar o XProtect VMS sem supervisão, será necessário iniciar o instalador com os argumentos da tabela abaixo. É necessário criar e salvar os argumentos em um arquivo XML de argumentos gerado por você antes da instalação.

Argumento	Descrição
`--quiet`	Força a instalação silenciosa.
`--arguments`	O caminho para o arquivo XML de argumentos com a configuração completa. O caminho pode ser: `C:\Arguments.xml`.
`--license`	O caminho para o arquivo de licença.

Usar uma conta de serviço dedicada

Esta descrição se baseia no uso de uma conta de serviço dedicada para segurança integrada. Os serviços sempre são executados na conta dedicada, independentemente do usuário que estiver conectado, e você deverá garantir que a conta tenha todas as permissões necessárias para, por exemplo, executar tarefas e acessar a rede, os arquivos e as pastas compartilhadas.

É necessário especificar a conta de serviço em um arquivo XML de argumento para as seguintes chaves:

`SERVICEACCOUNT`
`SERVICEACCOUNT_NONLOC`

É necessário especificar a senha da conta de serviço em texto sem formatação no valor da chave a seguir:

`ENCRYPTEDPASSWORD`

Exemplo: linha de comando para iniciar a instalação no modo silencioso:

```
"Milestone XProtect VMS Products 2023 R2 System Installer.exe" --quiet --
arguments=C:\Arguments.xml --license=C:\M01-C01-231-01-ABCDEF.lic
```

Exemplo: Arquivo de argumentos baseado no uso de uma conta de serviço dedicada

```
<?xml version="1.0" encoding="utf-8"?>
<CommandLineArguments xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:milestone-systems">
  <InstallEnvironment>
    <Parameters>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>USERACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT_NONLOC</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>sampleaccountpasswordplaintext</Value>
        <Key>ENCRYPTEDPASSWORD</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>%PROGRAMFILES%\Milestone</Value>
        <Key>TARGETDIR</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsXPCO</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsDPInstaller</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>false</Value>
        <Key>LEGACY</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>yes</Value>
        <Key>SQL-KEEP-DATA</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>no</Value>
        <Key>SQL-CREATE-DATABASE</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>True</Value>
        <Key>IS_EXTERNALLY_MANAGED</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_MS</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IDP;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IDP</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IM;Persist
```

```
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IM</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_ES</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_
LogServerV2;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated;Application
Name=Surveillance_LogServerV2</Value>
        <Key>SQL_CONNECTION_STRING_LOG</Key>
      </KeyValueParametersOfStringString>
    </Parameters>
  </InstallEnvironment>
</CommandLineArguments>
```

Pré-requisitos a serem concluídos antes de realizar a instalação:

- É necessário que a conta de serviço e a conta usada para realizar a instalação estejam criadas.
- A conta de serviço precisa ter permissão para fazer logon como um serviço no computador no qual a instalação será realizada. Consulte Log-on-as-a-service.
- É necessário que os bancos de dados a serem usados pelo XProtect estejam criados, e os bancos de dados precisam ser indicados no arquivo XML de argumentos, por exemplo:

Nome do banco de dados
Monitoramento
Surveillance_IDP
Surveillance_IM
Surveillance_LogServerV2

- É necessário configurar os bancos de dados de acordo com a lista a seguir:

Configuração de banco de dados

O agrupamento deve ser definido como “SQL_Latin1_General_CP1_CI_AS”
ALLOW_SNAPSHOT_ISOLATION deve ser definido como ON
READ_COMMITTED_SNAPSHOT deve ser definido como ON

- É necessário criar um logon no Microsoft® SQL Server® para a conta de serviço e para a conta que será usada na instalação em cada um dos bancos de dados. É necessário criar um usuário de banco de dados em cada um dos bancos de dados, e o usuário precisa ser membro da função db_owner em cada banco de dados.

Instalação para grupos de trabalho

Se você não usa uma configuração de domínio com um servidor do Active Directory, mas uma configuração de grupo de trabalho, faça o seguinte quando instalar.

Todos os computadores em uma configuração distribuída devem estar em um domínio ou em um grupo de trabalho.

1. Acesse o Windows usando a conta de administrador comum.

   Certifique-se de usar a mesma conta em todos os computadores do sistema.

2. Dependendo de suas necessidades, inicie a instalação do servidor de gravação ou de gerenciamento e clique em **Personalizar**.
3. Dependendo do que você selecionou na etapa 2, selecione para instalar o serviço Management Server ou Recording Server usando uma conta de administrador comum.
4. Termine a instalação.
5. Repita os passos 1-4 para instalar outros sistemas que você desejar conectar. Todos eles precisam ser instalados usando uma conta de administrador comum.

Instale em um grupo

Antes de instalar em um cluster, consulte Servidores de gerenciamento múltiplos (clustering) (explicado) na página 137 e Requisitos de clustering na página 138.

Descrições e ilustrações podem diferir do que você vê na sua tela.

Instalar o servidor de gerenciamento:

1. Instalar o servidor de gerenciamento e todos os seus subcomponentes no primeiro servidor no grupo.

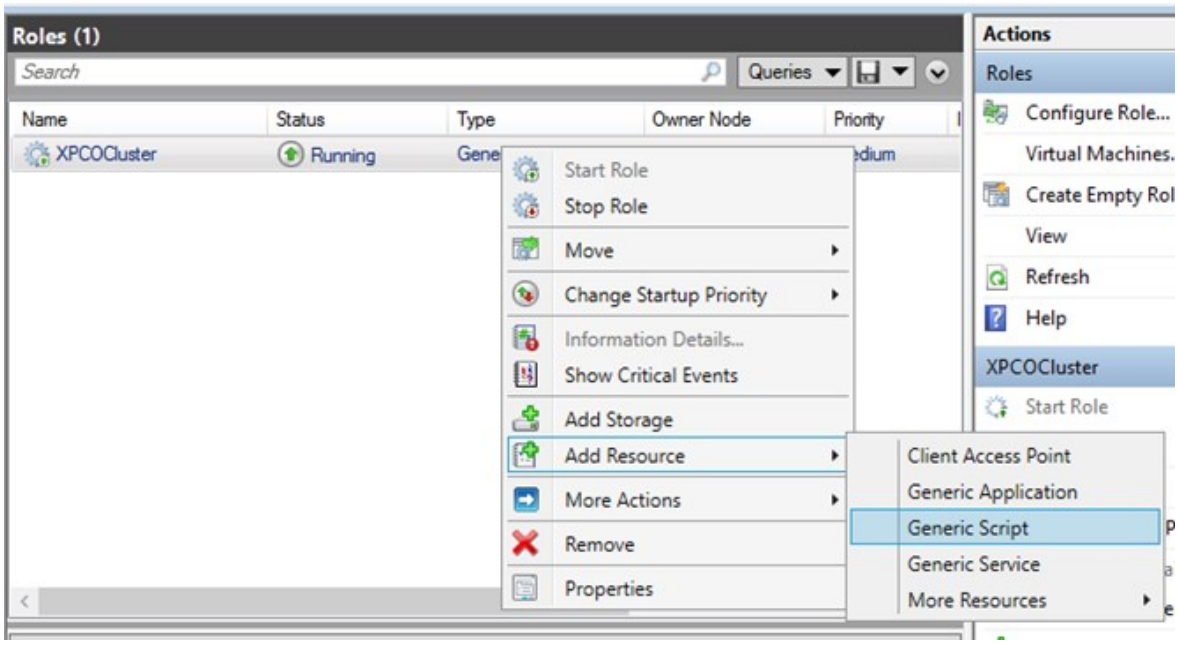
   O servidor de gerenciamento deve ser instalado com um usuário específico e não como um serviço da rede. Isso exige que você use a opção de instalação **Personalizada**. Além disso, o usuário específico deve ter acesso à unidade de rede compartilhada e, preferencialmente, uma senha sem expiração.

Configurar o serviço Management Server como serviço genérico no grupo de emergência:

1. No último servidor no qual você instalou o servidor de gerenciamento, vá para **Iniciar** > **Ferramentas Administrativas**, abra **Gerenciamento de Cluster de Failover** do Windows. Na janela **Gerenciador do Cluster de Failover**, expanda o seu grupo, clique com o botão direito em **Funções** e selecione **Configurar função**.

2. Na página **Assistente de alta disponibilidade** > **Antes de começar**, clique em **Avançar**.
3. Na página **Selecionar função**, selecione **Serviço genérico** e clique em **Avançar**.
4. Na página **Selecionar serviço**, selecione o serviço **Milestone XProtect Management Server** e clique em **Avançar**.
5. Na página **Ponto de acesso do cliente**, especifique o nome (nome do host do grupo) que os clientes usarão ao acessar o serviço. O nome do host deve ser diferente do nome do grupo. Clique em **Avançar**.
6. Na página **Selecionar armazenamento**, clique em **Avançar**, pois nenhum armazenamento é necessário para o serviço.
7. Na página **Replicar configurações do registro**, clique em **Avançar**, pois nenhuma configuração do registro deve ser replicada.

8. Na página **Confirmação**, clique em **Avançar** depois de verificar se o serviço de grupo está configurado de acordo com seus requisitos.
9. Na página **Configurar alta disponibilidade**, clique em **Avançar**.
10. Na página **Resumo**, clique em **Concluir** para completar a configuração do servidor de gerenciamento como um serviço genérico no cluster de failover.
11. Clique com o botão direito do mouse na função que você acabou de criar e clique em **Adicionar recurso** > **Script genérico**. Selecione Milestone XProtect Event Server para adicionar o serviço **Milestone XProtect Event Server** como um recurso ao serviço **Milestone XProtect Management Server Cluster**.



12. Repita a etapa 11 e adicione todos os serviços necessários no cluster, por exemplo, o Log Server. O Milestone XProtect Event Server e o Data Collector server devem ser adicionados como serviços para alcançar uma implantação ideal. Além disso, o Milestone XProtect Event Server deve ser definido como um serviço dependente do servidor de gerenciamento, para que o servidor de eventos pare quando o servidor de gerenciamento for interrompido.
13. Todos os serviços adicionados são exibidos no painel inferior da janela.

Atualizar URL do cluster:

> Ao fazer alterações na configuração do Gerenciador do Cluster de Failover da Microsoft, pause o controle e monitoramento do serviço para que o Server Configurator possa fazer as alterações e iniciar e/ou parar o serviço Management Server. Se você mudar o tipo de inicialização do serviço de cluster de emergência para manual, isso não deve resultar em conflitos com o Server Configurator.

Nos computadores Management Server:

1. Inicie o Server Configurator em cada um dos computadores que possuem um servidor de gerenciamento instalado.
2. Ir para a página de **Registro**.
3. Clique no símbolo de lápis ( ) para tornar o endereço do servidor de gerenciamento editável.
4. Altere o endereço do servidor de gerenciamento para a URL do grupo, por exemplo `http://MeuGrupo`.
5. Clique em **Registrar**.

Em computadores que possuem componentes que usam o Management Server (por exemplo, Recording Server, Mobile Server, Event Server, API Gateway):

1. Inicie o Server Configurator em cada um dos computadores.
2. Ir para a página de **Registro**.
3. Altere o endereço do servidor de gerenciamento para a URL do grupo, por exemplo `http://MeuGrupo`.
4. Clique em **Registrar**.

Use um certificado para um IDP externo em um ambiente de cluster

Ao instalar XProtect em um ambiente de servidor único, os dados de configuração do IDP externo são protegidos usando a API de proteção de dados (DPAPI). Se você configurar o servidor de gerenciamento em um cluster, os dados de configuração do IDP externo deverão ser protegidos com um certificado para garantir o failover do nó fluente.

Para obter mais informações sobre como gerar um certificado, consulte O guia Milestone sobre certificados.

Você deve importar o certificado para o armazenamento de certificados pessoal e torná-lo confiável no computador.

Para configurar a proteção de dados, você deve adicionar a impressão digital do certificado à configuração do Identity Provider.

1. Importe o certificado para o armazenamento de certificados pessoal e certifique-se de que:
   - o certificado é válido
   - a conta Identity Provider app pool (IDP) tem permissões para a chave privada do certificado.

   Para obter mais informações sobre como verificar se a conta tem permissões para a chave privada do certificado, consulte O guia Milestone sobre certificados.
2. Localize o arquivo `appsettings.json` no caminho de instalação do Identity Provider (`[Install path]\Milestone\XProtect Management Server\IIS\Identity Provider`).
3. Defina a impressão digital do certificado na seção:

```
"DataProtectionSettings": {
 "ProtectKeysWithCertificate": {
  "Thumbprint": ""
 }

},
```

4. Repita a etapa 3 em todos os nós do servidor de gerenciamento.
5. Imponha um failover de nó para garantir que a configuração do certificado esteja correta.
6. Faça login novamente usando a estação de gerenciamento e aplique a configuração do provedor externo. Se a configuração já foi aplicada, insira novamente o segredo do cliente a partir de um IDP externo na estação de gerenciamento.

Solucionar erros quando a configuração de um IDP externo for protegida com um certificado

Certificado inválido/expirado

Se o certificado de impressão digital configurado representar um certificado que não é confiável ou expirou, o Identity Provider não pode ser iniciado. O registro Identity Provider (`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`) indicará claramente se o certificado é inválido.

Solução:

Certifique-se de que o certificado seja válido e confiável no computador.

Permissões ausentes para certificados de chaves privadas

O Identity Provider não pode proteger dados sem permissões para as chaves privadas. Se o Identity Provider não tem a permissão, a seguinte mensagem de erro é registrada no arquivo de registros do Identity Provider (`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`):

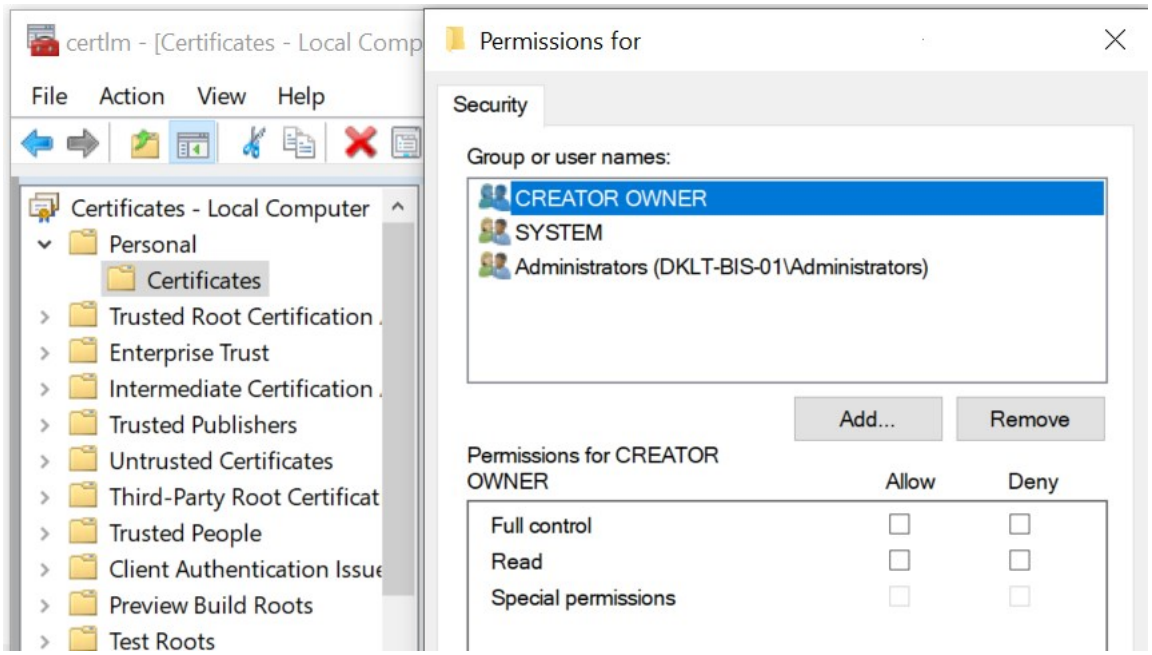
```
ERROR- An exception occurred while processing the key element '<key id="
[installation specific]" version="1" />'.
Internal.Cryptography.CryptoThrowHelper+WindowsCryptographicException:
Keyset does not exist
```

Solução:

Certifique-se de que a conta Identity Provider app pool (IDP) tem permissões para as chaves privadas do certificado.

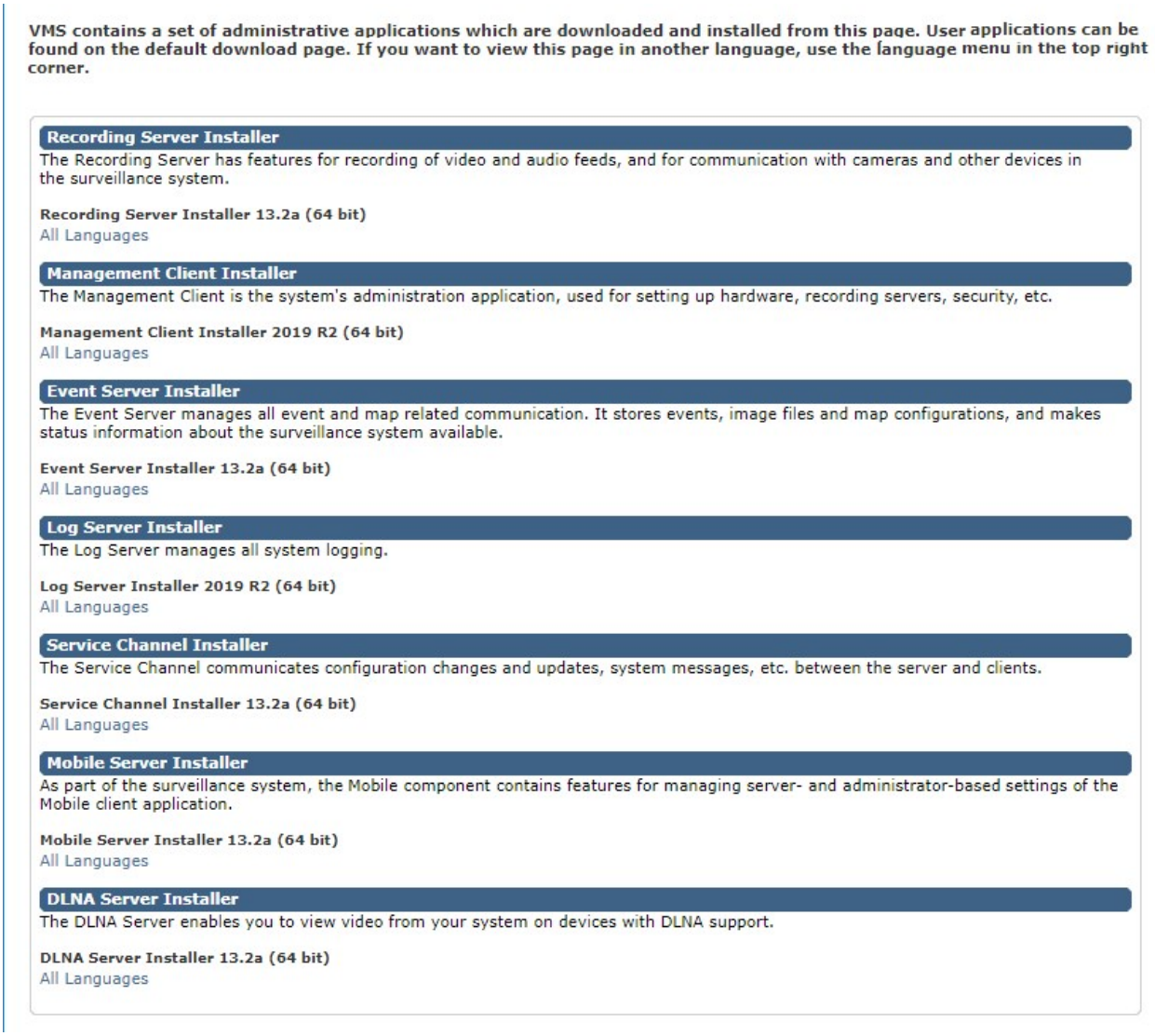
Verifique as permissões para uma chave privada de certificado:

1. Selecione **Iniciar** na barra de tarefas do Windows e abra a ferramenta Gerenciar certificados de computador (certlm.msc).
2. Navegue até o armazenamento de certificados pessoais e localize o certificado usado para a criptografia.
3. Clique com o botão direito do mouse no certificado e selecione **Todas as tarefas** > **Gerenciar chaves privadas**.
4. Em **Permissões para**, certifique-se de que a conta Identity Provider app pool (IDP) tenha permissões de leitura.



Download Manager/página da Web de download

O servidor de gerenciamento tem uma página da web integrada. Esta página da web permite que administradores e usuários finais façam o download e instalem os componentes do sistema XProtect solicitado de qualquer localização local ou remoto.



A página da web é capaz de exibir dois conjuntos de conteúdo, ambos em uma versão de idioma que por padrão corresponde ao idioma da instalação do sistema:

- Uma página da web é voltada a **administradores**, permitindo-lhes fazer o download e instalar os componentes-chave do sistema. Na maioria das vezes, a página da web é carregada automaticamente no final da instalação do servidor de gerenciamento e o conteúdo padrão é exibido. No servidor de gerenciamento, você pode acessar a página da web a partir do menu **Iniciar** do Windows, selecione **Programas** > **Milestone** > **Página de instalação administrativa**. Caso contrário, você pode digitar o URL:

  http://[endereço do servidor de gerenciamento]:[porta]/installation/admin/

  [endereço do servidor de gerenciamento] é o endereço IP ou o nome do host do servidor de gerenciamento e [porta] é o número da porta que você configurou no IIS para usar no servidor de gerenciamento.

- Uma página da web é destinada a **usuários** finais, proporcionando-lhes o acesso aos aplicativos do cliente com a configuração padrão. No servidor de gerenciamento, você pode acessar a página da web a partir do menu **Iniciar** do Windows, selecione **Programas** > **Milestone** > **Página de instalação pública**. Caso contrário, você pode digitar o URL:

  http://[endereço do servidor de gerenciamento]:[porta]/installation/

  [endereço do servidor de gerenciamento] é o endereço IP ou o nome do host do servidor de gerenciamento e [porta] é o número da porta que você configurou no IIS para usar no servidor de gerenciamento.

As duas páginas da Web têm alguns conteúdos padrão de modo que você pode usá-las imediatamente após o processo de instalação. No entanto, como administrador, ao usar Download Manager, você pode personalizar o que deve ser exibido nas páginas da web. Você também pode mover componentes entre as duas versões da página web. Para mover um componente, clique com o botão direito do mouse nele e selecione a versão da página da Web que você quer mover.

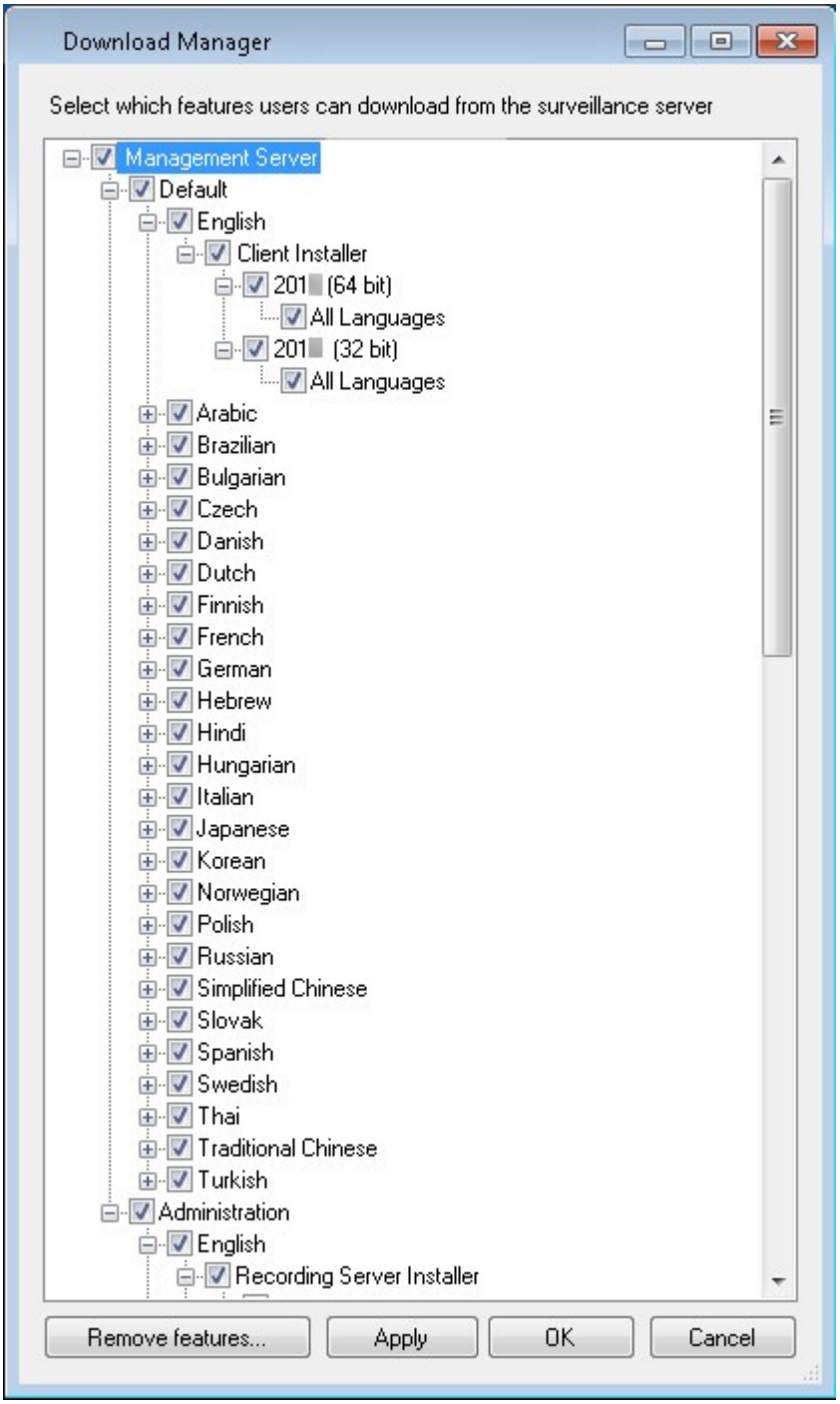
Mesmo que você possa controlar quais componentes os usuários podem baixar e instalar no Download Manager, você não pode usá-lo como uma ferramenta de gerenciamento de permissões dos usuários. Tais permissões são determinadas por papéis definidos no Management Client.

No servidor de gerenciamento, você pode acessar a XProtect Download Manager a partir do menu **Iniciar** do Windows, selecione **Programas** > **Milestone** > **XProtect Download Manager**.

Download ManagerConfiguração padrão do

O Download Manager tem uma configuração padrão. Isso garante que os usuários de sua organização possam acessar componentes padrão desde o início.

A configuração padrão fornece-lhe uma configuração padrão com acesso ao download de componentes adicionais ou opcionais. Normalmente você acessa a página da web do computador do servidor de gerenciamento, mas também pode acessar a página da web de outros computadores.



- O primeiro nível: Refere-se ao produto XProtect
- O segundo nível: Refere-se às duas versões alvo da página da web. **Padrão** refere-se à versão da página da web vista pelos usuários finais. **Administração** refere-se à versão da página da web vista pelos administradores do sistema
- O terceiro nível: Refere-se aos idiomas em que a página da web está disponível

- O quarto nível: Refere-se aos componentes que estão—ou podem ficar—disponíveis aos usuários
- O quinto nível: Refere-se a versões específicas de cada componente que estão—ou podem ficar—disponíveis aos usuários
- O sexto nível: Refere-se a versões de idiomas dos componentes que estão—ou podem ficar—disponíveis aos usuários

O fato que somente os componentes padrão estão inicialmente disponíveis—e que somente a versão do mesmo idioma como o próprio sistema—ajuda a reduzir o tempo de instalação e a salvar o espaço no servidor. Não há simplesmente necessidade de ter um componente ou idioma disponível no servidor se ninguém o usa.

Você pode disponibilizar mais componentes ou idiomas conforme necessário e você pode ocultar ou remover componentes ou idiomas indesejados.

Instaladores padrão do Download Manager (usuário)

Por padrão, os seguintes componentes estão disponíveis para instalação separada a partir da página da web de download do servidor de gerenciamento voltado para usuários (controlada pelo Download Manager):

- Servidores de gravação, incluindo servidores de gravação de failover. Servidores de gravação de failover são inicialmente baixados e instalados como servidores de gravação, durante o processo de instalação especifica que quer um servidor de gravação de failover.
- Management Client
- XProtect Smart Client
- Servidor de eventos, usado em conexão com funcionalidade do mapa
- Servidor de registros, utilizado para fornecer a funcionalidade necessária para registrar informações do sistema
- Servidor XProtect Mobile
- Mais opções podem estar disponíveis para a sua organização.

Para instalação de device packs, consulte Instalador de pacote de dispositivos - deve ser baixado na página 197.

Adicionar/publicar componentes do instalador Download Manager

Você deve realizar dois procedimentos para disponibilizar os componentes não-padrão e novas versões na página de download do servidor de gerenciamento.

Primeiro, você adiciona componentes novos e/ou não-padrão ao Download Manager. Em seguida, você o usa para sintonizar quais componentes devem ser disponibilizados nas várias versões de idiomas da página da Web.

Se o Download Manager estiver aberto, feche-o antes de instalar os novos componentes.

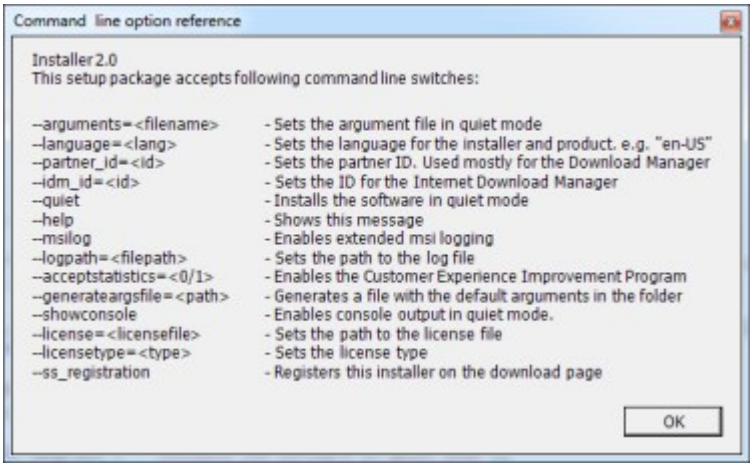
Adicionar novos arquivos/não-padrão ao Download Manager:

1. No computador em que você baixou o(s) componente(s), acesse **Iniciar** do Windows e digite um *prompt de comando*
2. No *Prompt de comando,* execute o nome do arquivo (*.exe*) com:[space] *--ss_registration*

   Exemplo: *MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   Agora o arquivo é adicionado ao Download Manager, mas não instalado no computador atual.

Para obter uma visão geral dos comandos de instalação, no *Prompt de Comando,* digite [espaço]*--help* e a seguinte janela aparece:



Após instalar novos componentes, estes são por padrão selecionados no Download Manager e estão imediatamente disponíveis para os usuários através da página da web. Você pode sempre mostrar ou ocultar recursos na página da web selecionando ou limpando as caixas de seleção na estrutura de árvore do Download Manager.

Você pode alterar a sequência na qual os componentes são exibidos na página da web. Na estrutura de árvore do Download Manager, arraste os itens componentes e solte-os na posição desejada.

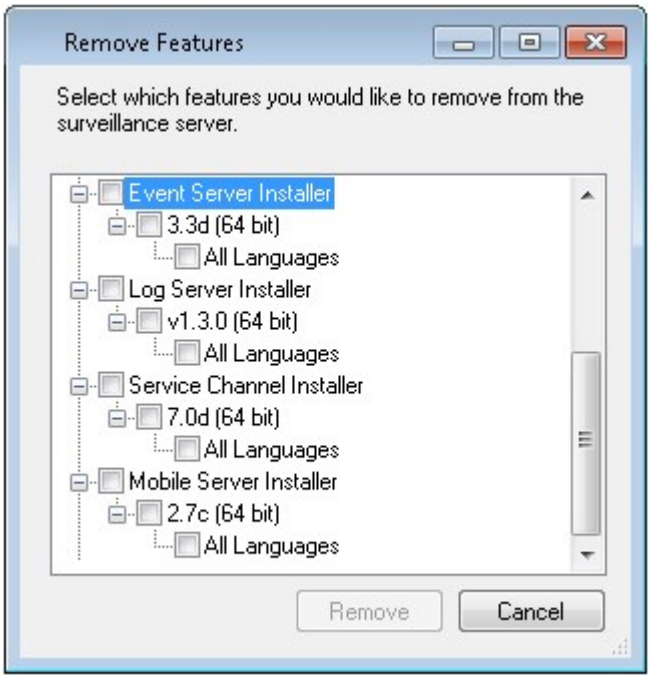
Ocultar/remover Download Manager componentes do instalador

Você tem três opções:

- **Ocultar componentes** na página da web desmarcando as caixas de seleção na estrutura em árvore do Download Manager. Os componentes ainda são instalados no servidor de gerenciamento e ao selecionar as caixas de seleção na estrutura de árvore do Download Manager, você pode disponibilizar rapidamente os componentes novamente

- **Remover a instalação de componentes** no servidor de gerenciamento. Os componentes desaparecem do Download Manager, mas os arquivos de instalação para os componentes são mantidos em `C:\Program Files (x86)\Milestone\XProtect Download Manager`, para que possa voltar a instalá-los mais tarde, caso necessário.

  1. Em Download Manager, clique em **Remover recursos**.
  2. Na janela **Remover recursos**, selecione o(s) recurso(s) que quer remover.



  3. Clique em **OK** e **Sim**.

- **Remover os arquivos de instalação para os recursos indesejados** no servidor de gerenciamento. Isso pode ajudar a poupar espaço em disco no servidor se você souber que a sua organização não usará certos recursos

Instalador de pacote de dispositivos - deve ser baixado

O pacote de dispositivos (que contém os drivers de dispositivo) incluído na instalação original não está incluído no Download Manager. Então, se você precisar reinstalar o pacote de dispositivos ou disponibilizar o instalador do pacote de dispositivos, primeiro você deve adicionar ou publicar o instalador do pacote de dispositivos mais recente para o Download Manager:

1. Obtenha o device pack regular mais recente na página de download no site Milestone (https://www.milestonesys.com/downloads/).
2. Na mesma página, você pode fazer download do pacote de dispositivos herdados com os drivers mais antigos. Para verificar se as câmeras usam drivers do legacy device pack, acesse este site (https://www.milestonesys.com/community/business-partner-tools/device-packs/).
3. Adicione/publique-o no Download Manager chamando-o com o comando *--ss_registration*.

Se você não tem uma conexão de rede, pode reinstalar todo o servidor de gravação a partir do Download Manager. Os arquivos de instalação para o servidor de gravação são colocados localmente em seu computador e, dessa forma, você recebe automaticamente uma reinstalação do pacote de dispositivos.

Arquivos de registro de instalação e resolução de problemas

Durante uma instalação, atualização ou desinstalação, as entradas no registro são gravadas em vários arquivos de registro da instalação: No principal arquivo de registro da instalação `installer.log` e nos arquivos de registro que fazem parte de diferentes componentes do sistema que você está instalando. Todas as entradas de registro têm um carimbo de ora e as entradas mais recentes do registro estão no final dos arquivos do registro.

Você pode encontrar todos os arquivos de registro da instalação na pasta `C:\ProgramData\Milestone\Installer\`. Arquivos de registro nomeados como *I.log ou *I[inteiro].log são arquivos de registro sobre novas instalações ou atualizações, enquanto que arquivos de registro nomeados como *U.log ou *U[inteiro].log são sobre desinstalações. Se você comprou um servidor com um sistema XProtect já instalado através de um parceiro Milestone, pode não haver nenhum arquivo de registro da instalação.

Os arquivos de registro contêm informações sobre os parâmetros da linha de comando e opções da linha de comando e seus valores usados durante uma instalação, atualização ou desinstalação. Para localizar os parâmetros da linha de comando nos arquivos de registro, procure por **Command Line:** ou **Parameter '** dependendo do arquivo de registro.

Para solução de problemas, o arquivo de log de instalação principal installer.log é o primeiro lugar a ser procurado. Se alguma exceção, erro ou avisos ocorreram durante a instalação eles terão sido registrados. Tente procurar por **exception**, **error**, ou **warning**. "Código de saída: 0" significa uma instalação bem-sucedida e "Código de saída: 1" o oposto. Suas descobertas nos arquivos de registro podem permitir que você encontre uma solução na Base de Conhecimento Milestone. Se não, contate o seu parceiro Milestone e compartilhe os arquivos de registro de instalação relevantes.

Configuração

Lista inicial de tarefas de configuração

A lista de verificação abaixo relaciona as tarefas iniciais para configurar seu sistema. Alguns deles talvez você já tenha concluído durante a instalação.

Uma lista de verificação completa não garante que o sistema corresponde aos requisitos exatos de sua organização. Para fazer com que o sistema corresponda às necessidades de sua organização, a Milestone recomenda que você monitore e ajuste o sistema continuamente.

Por exemplo, é uma boa ideia testar e ajustar as configurações de sensibilidade de detecção de movimento para câmeras individuais sob condições físicas diferentes, incluindo dia/noite, dia de vento/calmo, quando o sistema estiver em execução.

A configuração de regras, que determina a maioria das ações realizadas pelo sistema, incluindo quando gravar vídeo, é um outro exemplo de configuração que pode ser modificada de acordo com as necessidades da sua organização.

Etapa	Descrição
☑	Você concluiu a instalação inicial do seu sistema. Consulte Instalar um novo sistema XProtect na página 152.
☑	Mude do SLC de avaliação para um SLC permanente (caso necessário). Consulte Alterar o código da licença de software na página 129.
☑	Efetue login no Management Client. Consulte Efetuando login (explicado) na página 30.
☐	Verifique se as configurações de armazenamento de cada servidor de gravação satisfazem suas necessidades. Consulte Armazenamento e arquivamento (explicado) na página 59.
☐	Verifique se cada configuração de arquivamento do servidor de gravação atende suas necessidades. Consulte Propriedades das definições de armazenamento e gravação na página 428.

Etapa	Descrição
☐	Detecte o hardware, câmeras ou codificadores de vídeo para adicionar a cada servidor de gravação. Consulte Adicionar hardware na página 221.
☐	Configure cada câmera individual do servidor de gravação. Consulte Câmeras (nó Dispositivos) na página 448.
☐	Ative o armazenamento e o arquivamento para câmeras individuais ou um grupo de câmeras. Isto é feito a partir das câmeras individuais ou do grupo de dispositivos. Consulte Anexar um dispositivo ou um grupo de dispositivos a um armazenamento na página 206.
☐	Ative e configure dispositivos. Consulte Dispositivos (nó Dispositivos) na página 445.
☐	As regras determinam o comportamento do sistema em grande escala. Você cria regras para definir quando as câmeras devem gravar, quando as câmeras Pan/Tilt/Zoom (PTZ) devem patrulhar, e quando as notificações devem ser enviadas, por exemplo. Criar regras. Consulte Regras e eventos (explicados) na página 81.
☐	Adicione funções ao sistema. Consulte Funções e permissões de uma função (explicado) na página 71.
☐	Adicione usuários ou grupos de usuários a cada uma das funções. Consulte Atribuir/remover usuários e grupos para/de funções na página 297.
☐	Ative licenças. Consulte Ativar licenças on-line na página 127 ou Ativar licenças offline na página 127.

Para obter mais informações sobre como configurar o sistema no de **Navegação do site** consulte Painel navegação do site na página 392.

Servidores de gravação

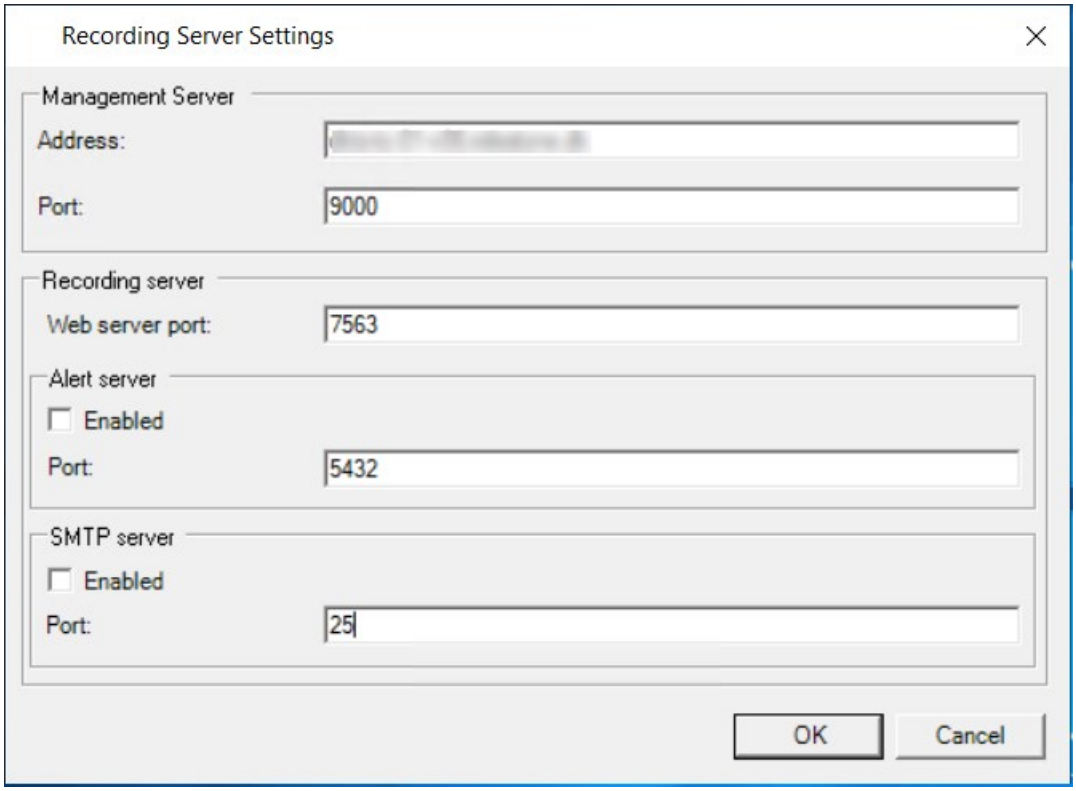
Alterar ou verificar a configuração básica de um servidor de gravação

Se o seu Management Client não lista todos os servidores de gravação que você instalou, a razão mais provável é que você tenha configurado os parâmetros de configuração (por exemplo, o endereço IP ou nome do host do servidor de gerenciamento) incorretamente durante a instalação.

Você não precisa reinstalar servidores de gravação para especificar os parâmetros dos servidores de gerenciamento, mas pode alterar/verificar sua configuração básica:

1. No computador que executa o servidor de gravação, dê um clique duplo no ícone **Servidor de gravação** na área de notificação.
2. Selecione **Parar serviço Recording Server**.
3. Clique com o botão direito do mouse no ícone **Servidor de gravação** e selecione **Alterar configurações**.

   A janela **Configurações do servidor de gravação** aparece.



4. Verifique ou altere, por exemplo, as configurações a seguir:
    - **Servidor de gerenciamento**: **Endereço**: Especifique o endereço IP ou o nome do host do servidor de gerenciamento para o qual o servidor de gravação deve ser conectado.
    - **Servidor de gerenciamento**: **Porta**: Especifique o número da porta a ser utilizada na comunicação com o servidor de gerenciamento. Você pode mudar isso, caso necessário, mas o número de porta deve sempre corresponder ao número da porta configurada no servidor de gerenciamento. Consulte Portas usadas pelo sistema na página 101.
    - **Servidor de gravação**: **Porta do servidor web**: Especifique o número da porta a ser utilizada na comunicação com o servidor web do servidor de gravação. Consulte Portas usadas pelo sistema na página 101.
    - **Servidor de gravação**: **Porta do servidor de alertas**: Habilite e especifique o número da porta a ser usado ao se comunicar com o servidor de alerta do servidor de gravação, que escuta as mensagens de eventos dos dispositivos. Consulte Portas usadas pelo sistema na página 101.
    - **Servidor SMTP**: **Porta**: Habilite e especifique o número da porta a ser usado ao se comunicar com o serviço Simple Mail Transfer Protocol (SMTP) do servidor de gravação. Consulte Portas usadas pelo sistema na página 101.
5. Clique em **OK**.
6. Para iniciar o serviço do Recording Server novamente, clique com o botão direito do mouse no ícone **Servidor de gravação** e selecione **Iniciar serviço do Recording Server**.

> A interrupção do serviço do Recording Server significa que você não pode gravar e visualizar o vídeo ao vivo ao mesmo tempo que verifica/altera a configuração básica do servidor de gravação.

Registrar um servidor de gravação

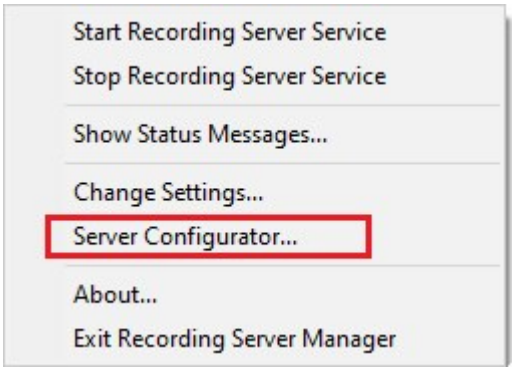
Quando você instala um servidor de gravação, ele é registrado automaticamente, na maioria dos casos. Mas você precisa fazer o registro manualmente, se:

- Você substituiu o servidor de gravação
- O servidor de gravação tiver sido instalado offline e, em seguida, adicionado depois ao servidor de gerenciamento
- O seu servidor de gerenciamento não usar as portas padrão. Os números das portas dependem da configuração da criptografia. Para obter mais informações, consulte Portas usadas pelo sistema na página 101

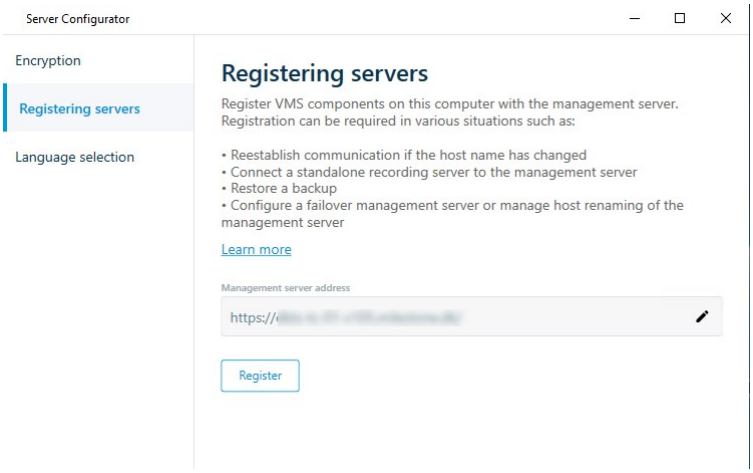
- Um registro automático falhou, por exemplo, após alterar o endereço do servidor de gerenciamento, alterar o nome do computador com o servidor de gravação, ou após ativar ou desativar as configurações de criptografia de comunicação do servidor. Para mais informações sobre alterações ao endereço do servidor de gerenciamento, consulte Alterar o nome do host do computador do servidor de gerenciamento.

Quando você registra um servidor de gravação, você o configura para se conectar ao seu servidor de gerenciamento. A parte do servidor de gerenciamento que trata o registro é o serviço do Authorization Server.

1. Abra o Server Configurator no menu iniciar do Windows ou a partir do ícone de bandeja do servidor de gravação.



2. No Server Configurator, selecione **Registrar servidores**.



3. Verifique o endereço do servidor de gerenciamento e o esquema (http ou https) ao qual você deseja que os servidores no computador se conectem e clique em **Registrar**.

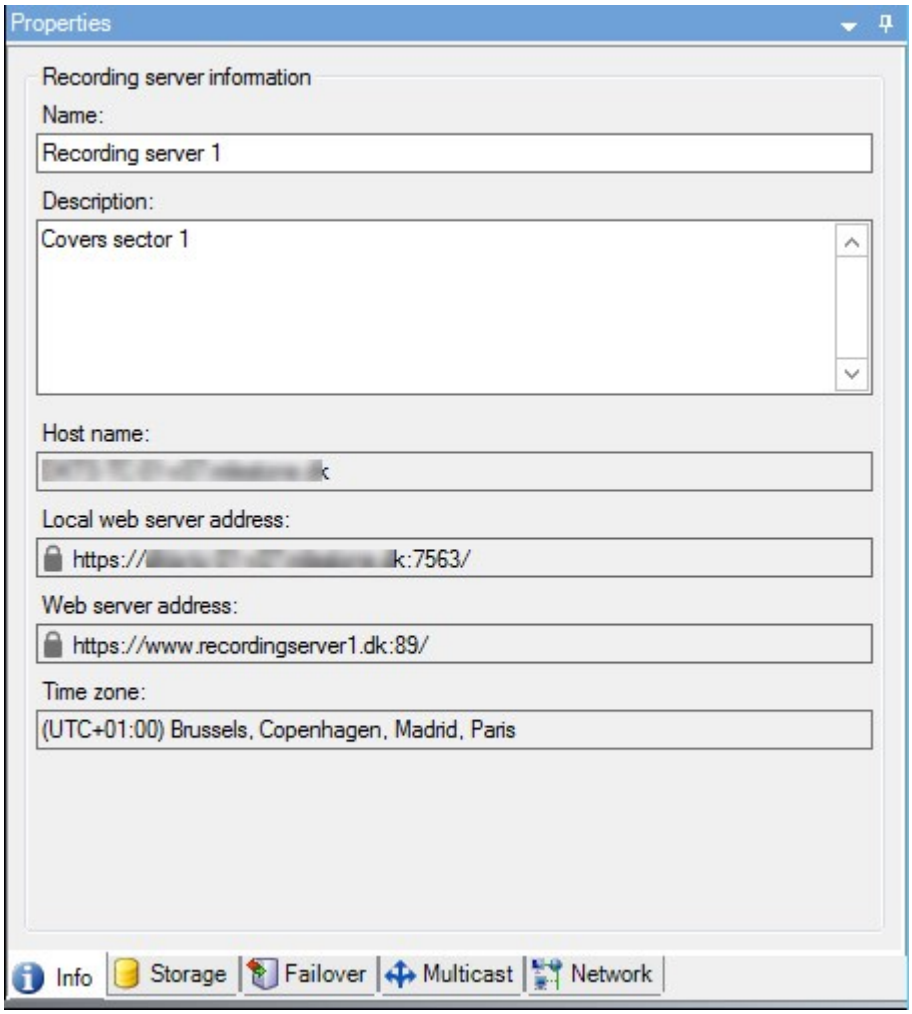
Uma confirmação é exibida, informando que o registro no servidor de gerenciamento foi bem-sucedido.

Consulte também Substituir um servidor de gravação na página 350.

Visualizar status de criptografia para clientes

Para verificar se seu servidor de gravação criptografa conexões:

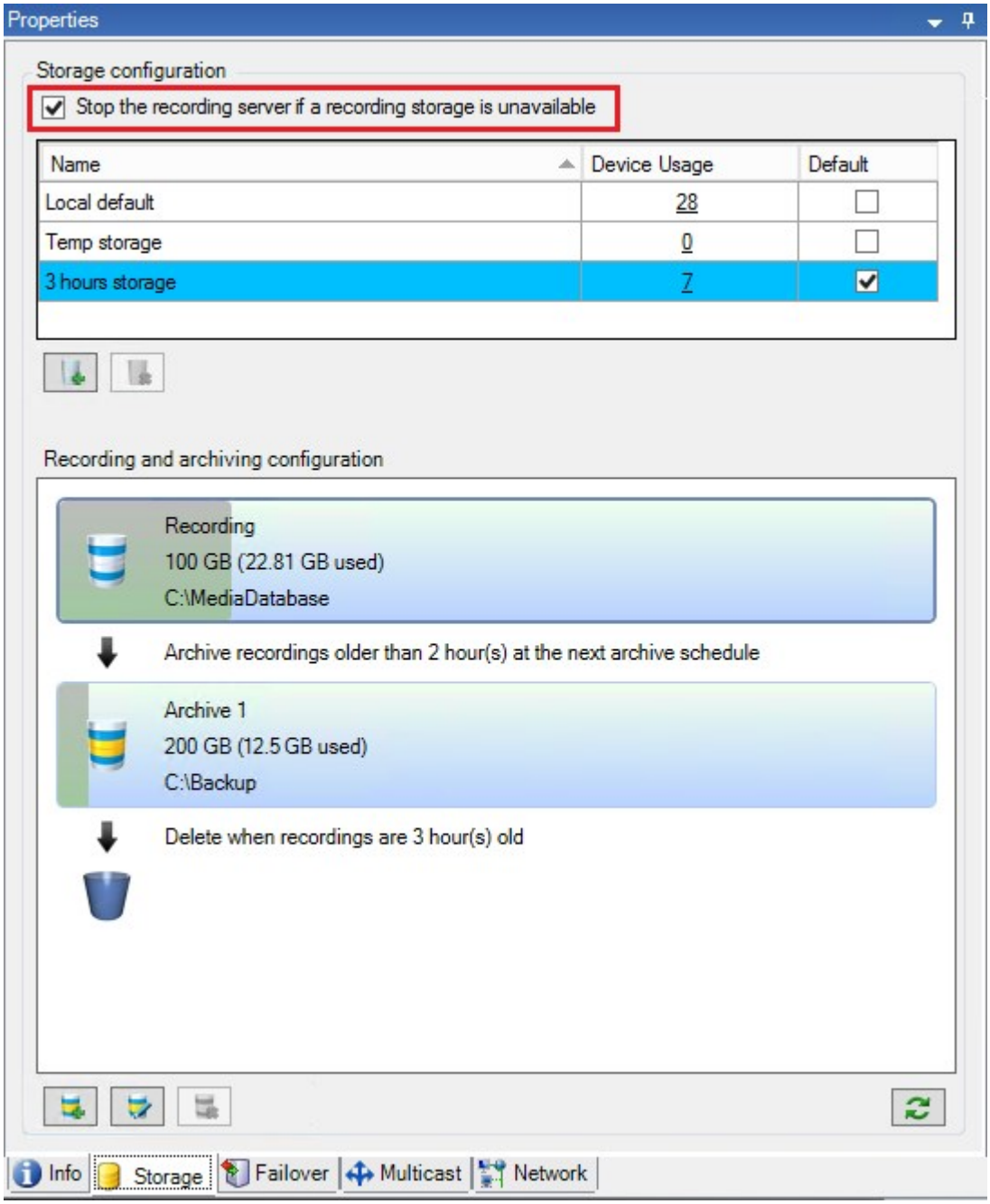
1. Abra o Management Client.
2. No painel **Navegação do Site**, selecione **Servidores** > **Servidores de gravação**. Isto abre uma lista de servidores de gravação.
3. No painel **Visão geral**, selecione o servidor de gravação relevante e acesse a guia **Informações**.
   Se a criptografia estiver ativada para clientes e servidores que recuperam fluxos de dados do servidor de gravação, um ícone de cadeado aparecerá na frente do endereço do servidor de web local e do endereço de servidor de web opcional.



Especifique o comportamento quando não houver armazenamento de gravação disponível.

Por padrão, o servidor de gravação continua em execução se um armazenamento de gravação se tornar indisponível. Se o seu sistema estiver configurado com servidores do sistema de gravação ininterrupta, você pode especificar que o servidor de gravação interrompa a execução para que os servidores failover assumam:

1. No servidor de gravação relevante, vá para a guia **Armazenamento**.
2. Selecione a opção **Parar o servidor de gravação se um armazenamento de gravação não estiver disponível**.



Adicionar um novo armazenamento

Quando você adiciona um novo armazenamento, você sempre cria um armazenamento de gravação com um banco de dados de gravação predefinido chamado **Gravação**. Você não pode renomear o banco de dados. Além do armazenamento de gravação, um armazenamento pode conter diversos arquivos.

1. Para acrescentar armazenamento extra a um servidor de gravação selecionado, clique no  botão localizado sob a lista de **Configurações de Armazenamento**. Isso abre a caixa de diálogo **Configurações de armazenamento e gravação**.
2. Especifique as configurações relevantes (consulte Propriedades das definições de armazenamento e gravação na página 428).
3. Clique em **OK**.

Caso necessário, você agora estará pronto para criar arquivo(s) dentro do seu novo armazenamento.

Criar um arquivo dentro de um armazenamento

Um armazenamento não tem arquivo padrão, mas você pode criar arquivos conforme necessário.

1. Selecione o armazenamento relevante na lista **Configuração de gravação e arquivamento**.
2. Clique no botão  localizado abaixo da lista de **Configurações de gravação e armazenamento**.
3. Na caixa de diálogo **Configurações de arquivamento**, especifique as configurações necessárias (consulte Propriedades de configurações de arquivamento na página 430).
4. Clique em **OK**.

Anexar um dispositivo ou um grupo de dispositivos a um armazenamento

Uma vez que o armazenamento foi configurado para um servidor de gravação, você poderá habilitá-lo para dispositivos individuais, como câmeras, microfones ou alto-falantes ou um grupo de dispositivos. Você também pode selecionar qual das áreas de armazenamento do servidor de gravação você desejar usar para o dispositivo individual ou para o grupo.

1. Expanda **Dispositivos** e selecione **Câmeras**, **Microfones** ou **Alto-falantes**, conforme necessário.
2. Selecione o dispositivo ou um grupo de dispositivos.
3. Selecione a guia **Gravar**.
4. Na área **Armazenamento**, selecione **Selecionar**.
5. Na caixa de diálogo que aparece, selecione o banco de dados que deve armazenar as gravações do dispositivo e, em seguida, clique em **OK**.
6. Na barra de ferramentas, clique em **Salvar**.

Quando você clica no número de uso do dispositivo para a área de armazenamento na guia Armazenamento do servidor de gravação, o dispositivo é visível no relatório de mensagem que aparece.

Dispositivos desativados

Por padrão, dispositivos desativados não são exibidos no painel **Visão geral**.

Para exibir todos os dispositivos desativados, na parte superior do painel **Visão geral**, clique em **Filtrar** para abrir a guia **Filtrar** e selecione **Mostrar dispositivos desativados**.

Para ocultar novamente os dispositivos desativados, limpe **Mostrar dispositivos desativados**.

Editar configurações para um armazenamento ou arquivo selecionado

1. Para editar um armazenamento, selecione seu banco de dados de gravação na lista **Configuração de gravação e arquivamento**. Para editar um arquivo, selecione o banco de dados do arquivo.
2. Clique no botão **Editar Armazenamento de Gravações**  localizado sob a lista de **Configurações de Gravação e Arquivamento**.
3. Ou edite um banco de dados de gravação ou edite um arquivo.

Se você alterar o tamanho máximo de um banco de dados, o sistema auto arquiva as gravações que excederem o novo limite. Ele auto arquiva as gravações para o próximo arquivo ou as exclui de acordo com as configurações de arquivamento.

Ativar a assinatura digital para exportação

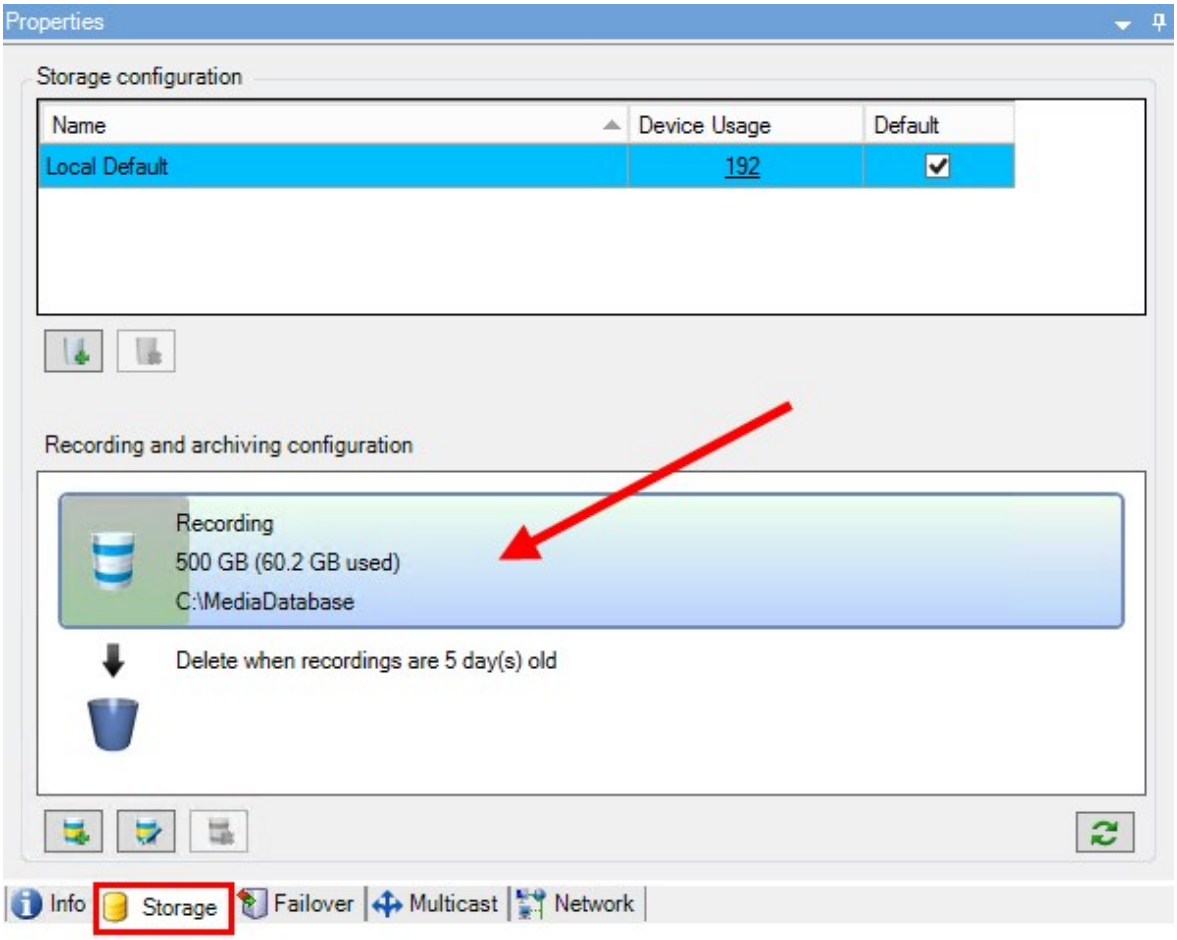
As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Você pode ativar a assinatura digital para o vídeo gravado, de modo que os usuários do cliente podem verificar que o vídeo gravado não foi adulterado desde que foi gravado. Verificar a autenticidade do vídeo é algo que o usuário faz no XProtect Smart Client – Player depois que o vídeo foi exportado.

A assinatura também deve ser ativada em XProtect Smart Client > guia **Exportações** > **Configurações de exportação** > **Formato XProtect** > **Incluir assinatura digital**. Caso contrário, o botão **Verificar Assinaturas** em XProtect Smart Client – Player não é exibido.

1. No painel **Navegação do Site**, expanda o nó **Servidores**.
2. Clique em **Servidores de Gravação**.
3. No painel Visão geral, clique no servidor de gravação em que você deseja ativar a assinatura.

4. Na parte inferior do painel **Propriedades**, clique na guia **Armazenamento**.



5. Na seção **Configuração de gravação e arquivamento**, clique duas vezes na barra horizontal que representa o banco de dados de gravação. A janela **Configurações de Armazenamento e Gravação** aparece.
6. Selecione a caixa de seleção **Assinatura**.
7. Clique em **OK**.

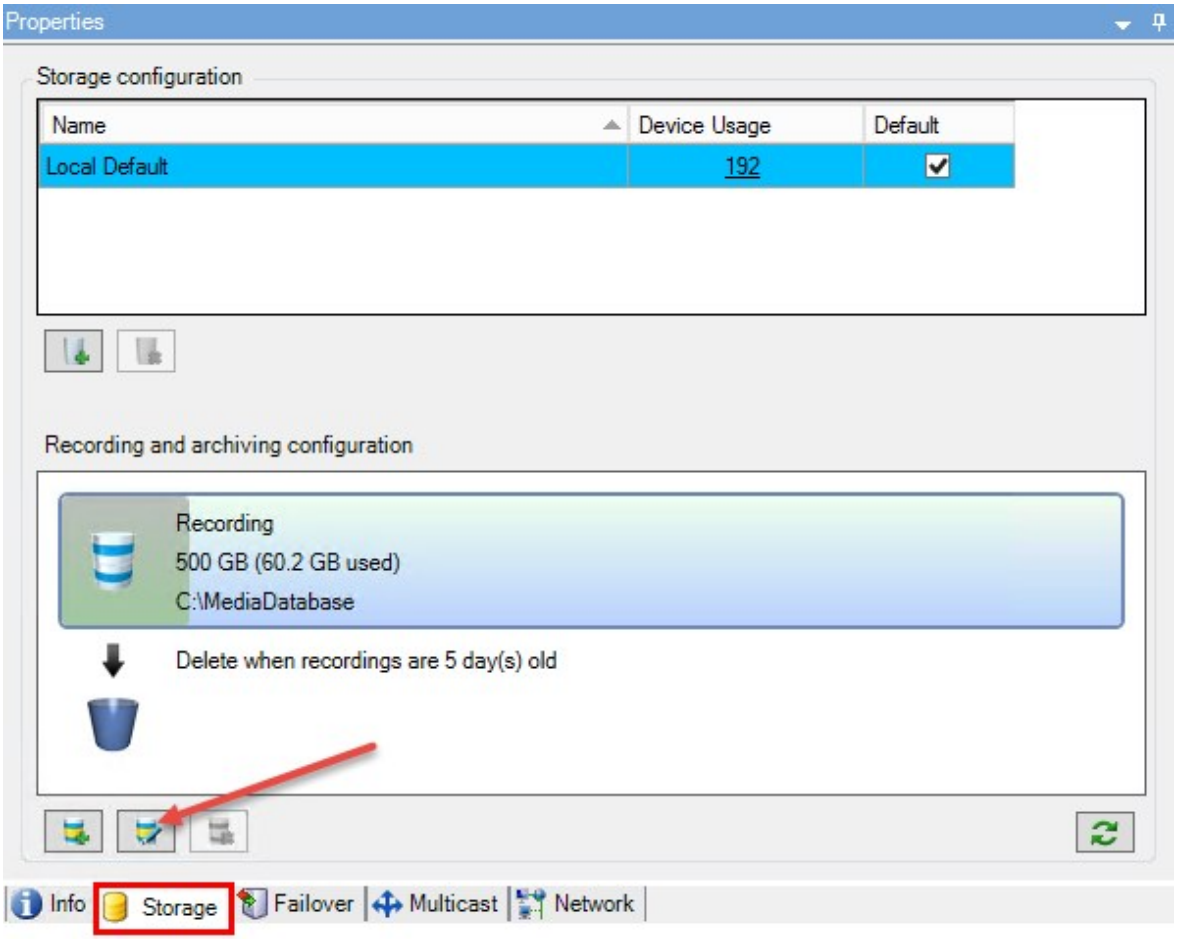
Criptografe suas gravações

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

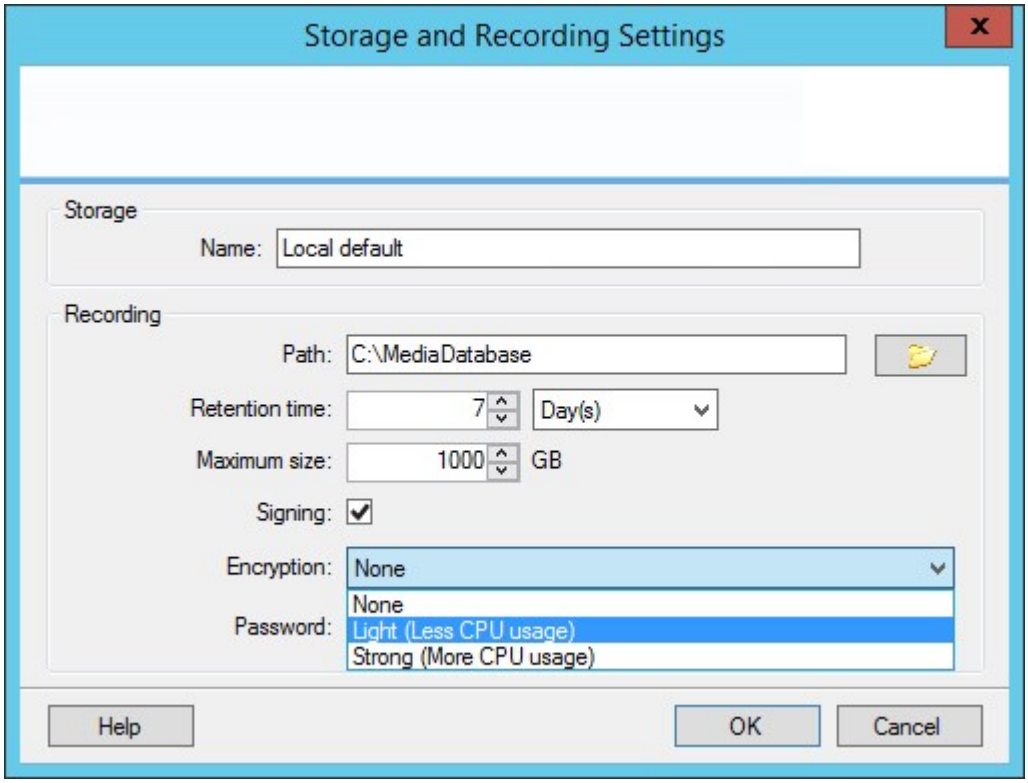
Você pode proteger suas gravações, ativando a criptografia no armazenamento e nos arquivos dos servidores de gravação. É possível selecionar entre criptografia leve e forte. Quando você ativar a criptografia, deve especificar também uma senha relacionada.

A ativação ou alteração de configurações de criptografia ou senha pode levar tempo, dependendo do tamanho do banco de dados e do desempenho da unidade. Você pode acompanhar o progresso nas **Tarefas atuais**.
Não pare o servidor de gravação enquanto esta tarefa estiver em andamento.

1. Clique no botão **Editar armazenamento de gravação** localizado sob a lista de **Configurações de gravação e arquivamento**.



2. Na caixa de diálogo que aparece, especifique o nível de criptografia.



3. Você é direcionado automaticamente para a caixa de diálogo **Configurar senha**. Insira a senha e clique em **OK**.

Fazer backup de gravações arquivadas

Muitas organizações querem fazer backup de suas gravações, usando unidades de fita ou semelhantes. Exatamente como você faz isso é altamente individual e depende da mídia de backup usada por sua organização. Entretanto, é importante ter em mente o seguinte:

Fazer backup de arquivos em vez de bancos de dados de câmera

Sempre criar backups baseados no conteúdo dos arquivos, não baseado em bancos de dados de câmera individual. Se você cria backups com base no conteúdo de bancos de dados de câmeras individuais, você pode causar violações de compartilhamento ou outros problemas de funcionamento.

Ao programar um backup, certifique-se de que o processo de backup não se sobrepõe aos tempos de arquivamento especificados. Para visualizar a programação de arquivamento de cada servidor de gravação em cada uma das áreas de armazenamento do servidor de gravação, consulte a guia **Armazenamento**.

Para garantir que o arquivamento não ocorra durante o backup, você pode desmontar o arquivo, executar o backup e montar o arquivo novamente. A montagem e desmontagem de arquivos é realizada por meio da Milestone Integration Platform VMS API.

Conhecer a estrutura de arquivo de modo que você possa visar backups

Quando você arquiva gravações, você as armazena em uma certa estrutura de sub-diretório dentro do arquivo.

Durante todo o uso regular do seu sistema, a estrutura de sub-diretórios é completamente transparente aos usuários do sistema, quando eles navegam gravações com XProtect Smart Client. Isto é verdade tanto com gravações arquivadas quanto as não arquivadas. É relevante conhecer a estrutura do subdiretório (consulte Estrutura de arquivo (explicado) na página 64) se você quiser fazer uma cópia de segurança das suas gravações arquivadas (consulte Fazendo backup e restauração da configuração do sistema na página 340).

Excluir um arquivo de uma área de armazenamento

1. Selecione o arquivo da lista **Configurações de gravação e armazenamento**.

   Somente é possível excluir o último arquivo da lista. O arquivo não precisa estar vazio.

2. Clique no botão  localizado abaixo da lista de **Configurações de gravação e armazenamento**.
3. Clique em **Sim**.

   Para arquivos indisponíveis, por exemplo arquivos offline, não é possível verificar se o arquivo contém mídia com proteção de evidências, mas o arquivo pode ser excluído após a confirmação do usuário.

   Arquivos disponíveis (arquivos online) que contêm mídia com proteção de evidências não podem ser excluídos.

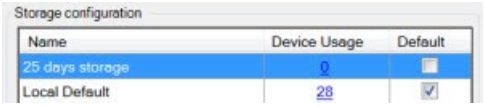
Excluir um armazenamento

Você não pode excluir o armazenamento padrão ou armazenamentos que dispositivos usam como o armazenamento de gravação para gravações ao vivo.
Isso significa que você pode precisar mover dispositivos (consulte Mover hardware na página 351) e quaisquer gravações ainda não arquivadas para uma outra área de armazenamento antes de você excluir o armazenamento.

1. Para ver a lista de dispositivos que usam esse armazenamento, clique no número de uso do dispositivo.

   > Um aviso é mostrado se o armazenamento tiver dados de dispositivos que foram movidos para outro servidor de gravação. Clique no link para ver a lista de dispositivos.

2. Sigas as etapas em Mover gravações não-arquivadas de um armazenamento para outro na página 212.
3. Continue até ter movido todos os dispositivos.
4. Selecione a área de armazenamento que desejar excluir.



5. Clique no  botão localizado sob a lista de **Configurações de armazenamento**.
6. Clique em **Sim**.

Mover gravações não-arquivadas de um armazenamento para outro

Você move as gravações de um banco de dados de gravação ao vivo para outro na aba **Gravação** do dispositivo.

1. Selecione o tipo de dispositivo. No painel **Visão geral**, selecione o dispositivo.
2. Clique na guia **Gravar**. Na parte superior da área **Armazenamento**, clique **Selecionar**.
3. Na caixa de diálogo **Selecionar armazenamento**, selecione o banco de dados.
4. Clique em **OK**.
5. Na caixa de diálogo **Ação de Gravações**, selecione se quer mover gravações existentes mas **não arquivadas** para o novo arquivamento ou se quer excluí-las.
6. Clique em **OK**.

Atribuir servidores de gravação de failover

Na aba **Failover** de um servidor de gravação, você pode escolher entre três tipos de configurações de failover:

- Nenhuma configuração de failover
- Uma configuração de failover primário/secundário
- Uma configuração em hot standby

Se você selecionar **b** e **c**, deve selecionar o servidor/grupos específicos. Com **b**, você também pode selecionar um grupo de failover secundário. Se o servidor de gravação se tornar indisponível, um servidor de gravação de failover do grupo de failover primário assume o controle. Se você também selecionou o grupo de failover

secundário, um servidor de gravação failover do grupo secundário assume o controle em caso de todos os servidores de gravação de failover do grupo primário estiverem ocupados. Desta forma, você só corre o risco de não ter uma solução de failover no caso raro quando todos os servidores de gravação de failover no primário, assim como no secundário, os grupos de failover estão ocupados.

1. No painel **Navegação do Site**, selecione **Servidores** > **Servidores de gravação**. Isto abre uma lista de servidores de gravação.
2. No painel **Visão geral**, expanda o servidor de gravação desejado e selecione a aba **Failover**.
3. Para escolher o tipo de configuração de failover, selecione entre:
   - **Nenhum**
   - **Grupo do servidor de emergência primário/Grupo do servidor de emergência secundário**
   - **Servidor em hot standby**

   Você não pode selecionar o mesmo grupo de failover como grupo de failover primário e secundário, nem selecionar servidores de failover comuns que já façam parte de um grupo de failover como servidores em espera ativa.
4. Em seguida, clique em **Configurações avançadas de failover**. Isso abre a janela **Configurações avançadas de failover**, listando todos os dispositivos conectados ao servidor de gravação selecionado. Se você selecionou **Nenhum**, as configurações avançadas de failover também estão disponíveis. O sistema mantém quaisquer seleções são para configurações de failover posteriores.
5. Para especificar o nível de suporte de failover, selecione **Suporte completo**, **Apenas ao vivo** ou **Desativado** para cada dispositivo na lista. Clique em **OK**.
6. No campo **Porta de comunicação do serviço de failover (TCP)**, edite o número da porta, se necessário.

> Se você ativar o suporte de failover e o servidor de gravação estiver configurado para continuar funcionando, caso um armazenamento de gravação não estiver disponível, o servidor do sistema de gravação ininterrupta não tomará o controle. Para fazer com que o suporte de failover funcione, você deve selecionar a opção **Parar o servidor de gravação se um armazenamento de gravação não estiver disponível** na guia **Armazenamento**.

Ativar multicasting para o servidor de gravação

Na comunicação de rede regular, cada pacote de dados é enviado de um único remetente para um único destinatário - um processo conhecido como transmissão única. Mas com o multicasting, você pode enviar um único pacote de dados (a partir de um servidor) para vários destinatários (clientes) dentro de um grupo. Multicasting pode ajudar a economizar largura de banda.

- Quando você usa **transmissão única**, a fonte deve transmitir uma transmissão de dados para cada destinatário
- Quando você usa **multicasting**, somente uma única transmissão de dados é solicitada em cada segmento de rede

Multicasting como descrito aqui **não** é transmissão de vídeo de servidores de câmera, mas de servidores a clientes.

Com o multicasting, você trabalha com um grupo de destinatários definido, com base em opções como intervalos de endereços IP, a capacidade de ativar / desativar multicasting para câmeras individuais, a capacidade de definir o maior tamanho aceitável do pacote de dados (MTU), o número máximo de roteadores que um pacote de dados deve ser transmitido (TTL), e assim por diante.

As transmissões de multicast não são criptografadas, mesmo se o servidor de gravação usar criptografia.

O multicasting não deve ser confundido com **transmissão**, o qual envia dados a todos conectados à rede, mesmo se os dados não sejam relevantes todos:

Nome	Descrição
Transmissão única	Envia dados de uma única fonte para um único destinatário.
Multicast	Envia dados de uma única fonte para múltiplos destinatários dentro de um grupo claramente definido.
Transmissão	Envia dados de uma única fonte para qualquer pessoa em uma rede. A transmissão, portanto, pode desacelerar significativamente a comunicação de rede.

Para usar multicasting, sua infraestrutura de rede deve suportar o padrão IGMP (Internet Group Management Protocol) de multicasting IP.

- Na guia **Multicast** selecione a caixa de seleção **Multicast**

Se toda a faixa de endereços IP para multicast já está em uso em um ou mais servidores de gravação, você primeiro libera alguns endereços IP de multicasting antes de habilitar o multicasting em servidores de gravação adicionais.

As transmissões de multicast não são criptografadas, mesmo se o servidor de gravação usar criptografia.

Ativar multicasting para câmeras individuais

O multicasting só funciona quando você o ativa para as câmeras relevantes:

1. Selecione o servidor de gravação e selecione a câmera desejada no painel **Visão geral**.
2. Na guia **Cliente**, selecione a caixa de seleção **Multicast ao vivo**. Repita para todas as câmeras relevantes.

As transmissões de multicast não são criptografadas, mesmo se o servidor de gravação usar criptografia.

Definir o endereço público e a porta

Se você precisar acessar o VMS com XProtect Smart Client por meio de uma rede pública ou não confiável, a Milestone recomenda que você use uma conexão segura por meio de VPN. Isso ajuda a garantir que a comunicação entre o XProtect Smart Client e o servidor VMS seja protegida.

Você define um endereço de servidor IP público do servidor de gravação na aba **rede de trabalho**.

Por que usar um endereço público?

Cliente podem conectar a partir de uma rede local bem como pela Internet e, em ambos os casos, o sistema de monitoramento deve fornecer endereços adequados para que os clientes possam acessar vídeos gravados ou em tempo real de seus servidores de gravação:

- Quando clientes conectam localmente, o sistema de monitoramento deve responder com endereços locais e número de portas
- Quando clientes se conectam pela internet, o sistema de monitoramento deve responder com o endereço público do servidor de gravação. Este é o endereço do firewall ou roteador NAT (Network Address Translation), e frequentemente também um número de porta diferente. O endereço e a porta podem então ser encaminhados para o endereço local e a porta do servidor.

1. Para ativar o acesso público, selecione a caixa de seleção **Ativar acesso público**.
2. Defina o endereço público do servidor de gravação. Digite o endereço do firewall ou o roteador NAT para que os clientes que acessam o sistema de monitoramento da Internet possam se conectar aos

servidores de gravação.

3. Especifique um número de porta pública. É sempre uma boa ideia que os números de porta usados no firewall ou roteador NAT sejam diferentes daqueles usados localmente.

> Se você usa o acesso público, configure o roteador NAT ou firewall usado de modo que as solicitações enviadas à porta e ao endereço público sejam enviadas para o endereço local e para a porta dos servidores de gravação relevantes.

Atribuir faixas de IP locais

Você define uma lista de faixas de IP locais que o sistema de monitoramento deve reconhecer como vindo de uma rede local:

- Na guia **Rede**, clique em **Configurar**

Filtre a árvore de dispositivos

A árvore de dispositivos no painel **Visão geral** pode ficar muito grande se você tiver muitos dispositivos registrados. Filtre a árvore de dispositivos para localizar mais facilmente os dispositivos com os quais você deseja trabalhar.

Ao fornecer termos de filtros que são exclusivos para alguns dispositivos específicos, é possível exibir apenas esses dispositivos específicos.

Filtre a árvore de dispositivos

- Na parte superior do painel **Visão geral**, clique em **Filtrar** para abrir a guia **Filtrar**.
- No campo **Digitar aqui para filtrar dispositivos**, insira um ou mais critérios de filtro e clique em **Aplicar filtro** para filtrar a lista de dispositivos.

Características dos critérios de filtro

Os critérios de filtro são aplicados aos valores dos campos nome do dispositivo, nome abreviado do dispositivo, endereço do hardware (IP), ID do dispositivo e ID do hardware.

Correspondências parciais do filtro não são exibidas ao filtrar os valores dos campos ID do hardware e ID do dispositivo. Consequentemente, é preciso definir o número de identificação exato e completo ao filtrar por ID do hardware ou ID do dispositivo.

Correspondências parciais de filtros são exibidas para os valores dos campos nome do dispositivo, nome abreviado do dispositivo e endereço do hardware, de forma que o termo do filtro “camer” exibirá todos os dispositivos que contenham a palavra “câmera” no nome do dispositivo.

Os critérios de filtro não diferenciam maiúsculas de minúsculas, ou seja, usar "câmera" ou "Câmera" produzirá os mesmos resultados.

Especificar vários critérios de filtro

É possível especificar vários critérios de filtro e, assim, restringir a filtragem da árvore de dispositivos. Quando o filtro é aplicado, todos os critérios de filtro definidos são considerados unidos com um E, o que significa que são cumulativos.

Por exemplo, se você inseriu dois critérios de filtro: “Câmera” e “Depósito”, a lista exibirá todos os dispositivos que contenham as palavras “Câmera” e “Depósito” no nome do dispositivo, mas não exibirá dispositivos que contenham as palavras “Câmera” e “Estacionamento” no nome do dispositivo nem dispositivos que contenham apenas a palavra "Câmera" no nome.

Remova cada critério de filtro individual do campo do filtro para ampliar o filtro se você tiver especificado um filtro muito restritivo. O filtro é automaticamente aplicado à árvore de dispositivos ao remover os critérios de filtro.

Redefinir o filtro

Se você remover todos os critérios de filtro do campo de filtro, o painel **Visão geral** será redefinido e exibirá todos os dispositivos novamente.

Além disso, pressione **F5** para redefinir o filtro e desmarcar a caixa de seleção **Mostrar dispositivos desativados**.

Dispositivos desativados

Por padrão, dispositivos desativados não são exibidos no painel **Visão geral**.

Para exibir todos os dispositivos desativados, na parte superior do painel **Visão geral**, clique em **Filtrar** para abrir a guia **Filtrar** e selecione **Mostrar dispositivos desativados**.

Para ocultar novamente os dispositivos desativados, limpe **Mostrar dispositivos desativados**.

Servidores de failover

Configurar e ativar servidores de gravação de failover

Se você tiver desativado o servidor de gravação de failover, você deve ativá-lo antes que ele assuma o controle dos servidores de gravação padrão.

Faça o seguinte para ativar um servidor de gravação de failover e edite suas propriedades básicas:

1. No painel **Navegação do site**, selecione **Servidores** > **Servidores de emergência**. Isso abre uma lista de servidores de gravação de failover e grupos de failover instalados.
2. No painel **Visão geral**, selecione o servidor de gravação de failover desejado.
3. Clique com o botão direito do mouse e selecione **Ativado**. O servidor de gravação de failover agora está ativado.
4. Para editar as propriedades do servidor de gravação de failover, vá para a guia **Informações**.
5. Ao concluir, vá para a guia **Rede**. Aqui você pode definir o endereço IP público do servidor de gravação de failover e muito mais. Isso é relevante se você usar NAT (Tradução de Endereço de Rede) e encaminhamento de portas. Consulte a guia **Rede** do servidor de gravação padrão para obter mais informações.
6. No painel **Navegação do Site**, selecione **Servidores** > **Servidores de gravação**. Selecione o servidor de gravação para o qual você quer suporte de emergência e atribua servidores do sistema de gravação ininterrupta (consulte Aba Failover (servidor de gravação) na página 432).

Para ver o status de um servidor do sistema de gravação ininterrupta, segure o mouse sobre o ícone de bandeja Failover Recording Server Manager, na área de notificação. Uma dica de ferramenta aparece, contendo o texto digitado no campo Descrição do servidor de gravação de failover. Isto pode ajudá-lo a determinar de qual o servidor de gravação o servidor de gravação de failover está configurado para assumir o lugar.

> O servidor de gravação de failover emite pings para o servidor de gerenciamento em base regular para verificar se está online e em condições de solicitar e receber a configuração dos servidores de gravação padrão quando necessário. Se bloquear o ping, o servidor de gravação de failover não assumirá o controle dos servidores de gravação padrão.

Servidores de gravação de failover do grupo para cold standby

1. Selecione **Servidores** > **Servidores de Failover**. Isso abre uma lista de servidores de gravação de failover e grupos de failover instalados.
2. No painel **Visão geral**, clique com o botão direito do mouse no nó superior **Grupos de failover** e selecione **Adicionar grupo**.
3. Especifique um nome (neste exemplo *Grupo de failover 1)* e uma descrição (opcional) de seu novo grupo. Clique em **OK**.
4. Clique com o botão direito do mouse no grupo *(Grupo de failover 1)* que você acabou de criar. Selecione **Editar membros do grupo**. Isso abre a janela **Selecionar membros do grupo**.
5. Arraste e solte ou use os botões para mover os servidores de gravação de failover selecionados do lado esquerdo para o lado direito. Clique em **OK**. Os servidores de gravação de failover selecionados

pertencem agora ao grupo (*Grupo de failover 1)* que você acabou de criar.

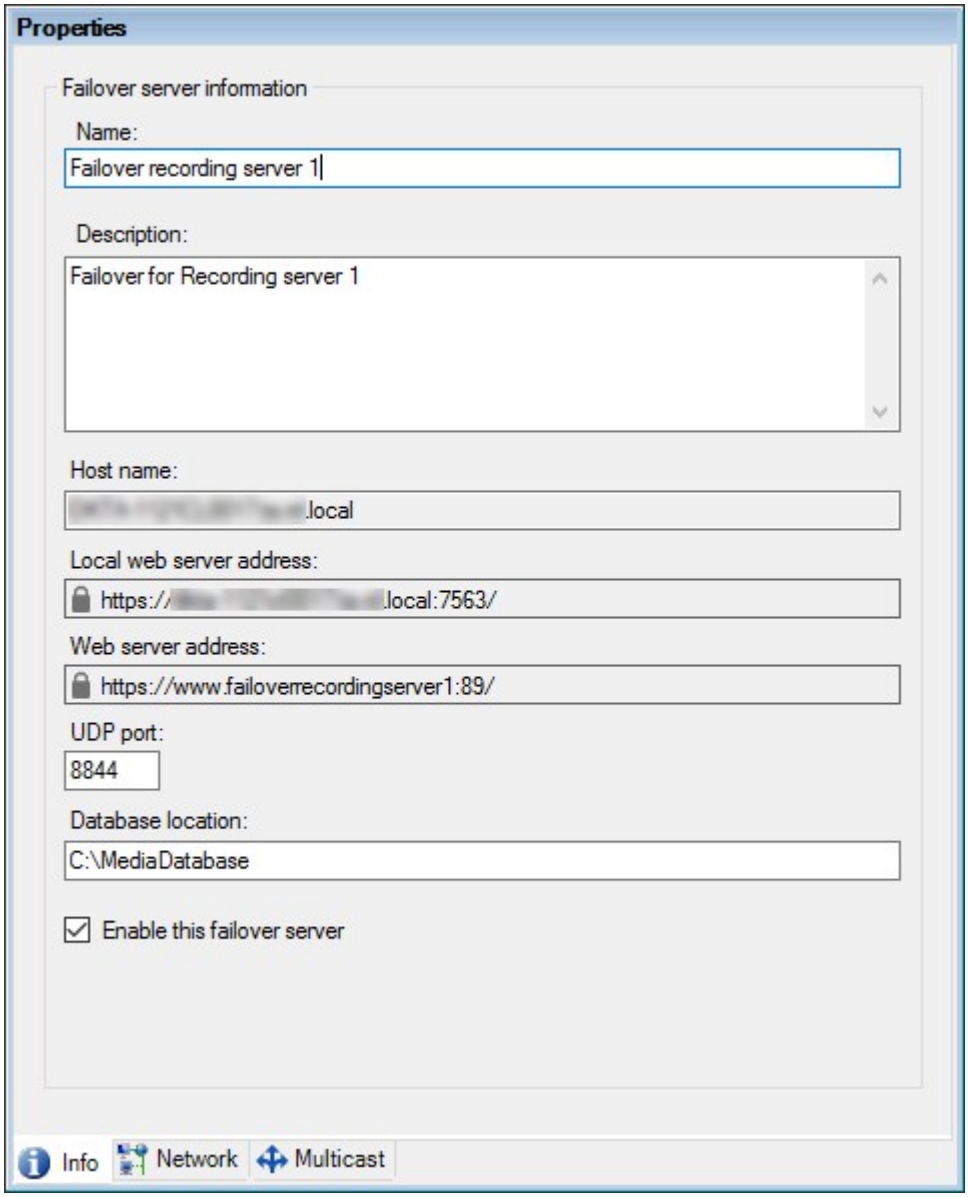
6. Vá para a aba **Sequência**. Clique em **Para cima** e **Para baixo** para definir a sequência interna dos servidores de gravação de failover regulares do grupo.

Visualize o estado da criptografia em um servidor do sistema de gravação ininterrupta

Para verificar se seu servidor do sistema de gravação ininterrupta usa criptografia, faça o seguinte:

1. No painel **Navegação do site**, selecione **Servidores** > **Servidores de emergência**. Isso abre uma lista de servidores do sistema de gravação ininterrupta.
2. No painel **Visão geral**, selecione o servidor de gravação relevante e acesse a guia **Informações**.
   Se a criptografia estiver ativada para clientes e servidores que recuperam fluxos de dados do servidor de gravação, um ícone de cadeado aparecerá na frente do endereço do servidor de web local e do

endereço de servidor de web opcional.



Visualizar mensagens de status

1. No servidor do sistema de gravação ininterrupta, clique com o botão direito no ícone do **Milestone Failover Recording Server serviço**.
2. Selecione **Exibir mensagens de status**. A janela **Mensagens de status do servidor de failover** aparece, listando as mensagens de status com carimbo da hora/data.

Visualizar informações sobre a versão

Saber a versão exata da versão de seu **Failover Recording Server serviço** é uma vantagem se você precisar entrar em contato com o suporte do produto.

1. No servidor do sistema de gravação ininterrupta, clique com o botão direito no ícone do **Milestone Failover Recording Server serviço**.
2. Selecione **Sobre**.
3. Uma pequena caixa de diálogo abre e mostra a versão exata do seu **Failover Recording Server serviço**.

Hardware

Adicionar hardware

Você tem várias opções para adicionar hardware para cada servidor de gravação em seu sistema.

> ⚠ Se seu hardware está localizado atrás de um roteador ou um firewall habilitado para NAT, você pode precisar especificar um número de porta diferente e configurar o roteador/firewall para que ele mapeie a porta e os endereços IP que o hardware utiliza.

O assistente **Adicionar hardware** ajuda você detectar hardware como câmeras e codificadores de vídeo na sua rede e adicioná-los ao servidor de gravações no seu sistema. O assistente também ajuda a adicionar servidores de gravação remotos para configurações Milestone Interconnect. Só adicione hardware para **um servidor de gravação** de cada vez.

1. Para acessar **Adicionar hardware**, clique com o botão direito do mouse no servidor de gravação desejado e selecione **Adicionar hardware**.
2. Selecione uma das opções do assistente (veja abaixo) e siga as instruções na tela.
3. Após a instalação, você pode ver o hardware e seus dispositivos no painel **Visão geral**.

> ⚠ Alguns hardwares devem ser pré-configurados serem adicionados pela primeira vez. Um assistente adicional de **Pré-configuração de dispositivos de hardware** será exibido ao se adicionar tal hardware. Consulte Pré-configuração de hardware (explicado) na página 55 para mais informações.

Adicionar Hardware (diálogo)

Hardware representa:

- A unidade física que se conecta diretamente ao servidor de gravação do sistema de monitoramento via IP, por exemplo, uma câmera, um codificador de vídeo, um módulo de I/O
- Um servidor de gravação em uma base remota em uma configuração Milestone Interconnect

Para mais informações sobre como adicionar hardware ao seu site, consulte Adicionar hardware na página 221.

Nome	Descrição
Expresso (recomendado)	O sistema verifica automaticamente se há hardware novo na rede local do servidor de gravação. Selecione a caixa **Mostrar hardware sendo executado em outro servidor de gravação** para ver se o hardware detectado está funcionando em outro servidor de gravação. Você pode selecionar esta opção cada vez que adicionar um novo hardware na sua rede e quiser usá-lo em seu sistema. Você não pode usar esta opção para adicionar sistemas remotos em configurações Milestone Interconnect.  Para adicionar hardware de HTTP e HTTPS, execute a detecção **Expressa** com o botão de opção **HTTPS (seguro)** selecionado, e depois com o botão de opção **HTTP (não seguro)** selecionado.
Digitalização do alcance de endereço	O sistema verifica sua rede para hardware e relevante e sistemas remotos Milestone Interconnect com base em suas especificações de: • nome do usuário e senhas do hardware. Não necessário se seu hardware usa os nomes de usuário e senhas padrão de fábrica. • drivers • Intervalos de IP (somente IPv4) • número da porta (padrão = 80) Você pode selecionar essa opção quando só desejar verificar uma parte de sua rede, por exemplo, ao expandir o sistema.
Manual	Especifique detalhes sobre cada hardware e sistemas remotos Milestone Interconnect separadamente. Esta pode ser uma boa opção se você quiser adicionar apenas algumas peças de hardware, e se sabe seus endereços IP, nomes de usuários e senhas relevantes ou se a câmera não suporta a função de

Nome	Descrição
	descoberta automática.
Hardware de conexão remota	O sistema procura automaticamente por hardware conectado via servidor conectado remotamente. Você pode usar esta opção se tiver instalado servidores, por exemplo, a Conexão de câmera Axis One-click. Você não pode usar esta opção para adicionar sistemas remotos em configurações Milestone Interconnect.

Desabilitar/habilitar hardware

Adicionar hardware está **desabilitado** por padrão.

Você pode ver se o hardware está ativado ou desativado desta forma:

ativado
desativado

Para desativar hardware adicionado, por exemplo, para licenciamento ou fins de desempenho

1. Expanda o servidor de gravação, clique com o botão direito do mouse no hardware que desejar desativar.
2. Selecione **Ativado** para limpar ou selecioná-lo.

Editar hardware

Clique com o botão direito no hardware adicionado e selecione **Editar hardware** para modificar a configuração da rede e as definições de autenticação de usuário de hardware no Management Client.

Editar hardware (diálogo)

Para alguns hardwares, o diálogo **Editar hardware** também permite que você aplique as configurações diretamente ao dispositivo de hardware.

Se o botão de opção **Editar Management Client configurações** estiver selecionado, o diálogo **Editar hardware** exibe as configurações que o Management Client usa para se conectar ao hardware. Para garantir que o dispositivo de hardware seja adicionado corretamente ao sistema, insira as mesmas configurações que você usa para se conectar à interface de configuração do hardware do fabricante:

Nome	Descrição
Nome	Exibe o nome do hardware em conjunto com seu endereço detectado (em parênteses).
URL de hardware	O endereço da web da interface de configuração do hardware do fabricante normalmente contendo o endereço IP do hardware. Especifique um endereço válido em sua rede.
Nome de usuário	O nome de usuário usado para conectar o hardware. O nome de usuário inserido aqui não muda o nome de usuário no dispositivo de hardware real. Selecione o botão de opção **Editar Management Client e configurações de hardware** para modificar as configurações em dispositivos de hardware suportados.
Senha	A senha usada para conectar o hardware. A senha inserida aqui não altera a senha no dispositivo de hardware real. Selecione o botão de opção **Editar Management Client e configurações de hardware** para modificar as configurações em dispositivos de hardware suportados. Para obter informações sobre como alterar senhas em diversos dispositivos de hardware, consulte Alterar senhas em dispositivos de hardware na página 229. Como um administrador do sistema, você precisar dar aos outros usuários a permissão para visualizar a senha no Management Client. Para obter mais informações, consulte Definições de funções em Hardware.

Se o botão de opção **Editar Management Client e configurações de hardware** for selecionado (para hardware suportado), o diálogo **Editar hardware** exibe as configurações que também são aplicadas diretamente ao dispositivo de hardware:

A aplicação das configurações com este botão de opção selecionado, substituirá as configurações atuais no dispositivo de hardware. O hardware perderá momentaneamente a conexão ao servidor de gravação enquanto as configurações são aplicadas.

Nome	Descrição
Nome	Exibe o nome do hardware em conjunto com seu endereço detectado (em parênteses).
Configuração de rede	As configurações de rede do hardware. Para ajustar as configurações de rede, selecione Configurar na página 225.
Configurar	Especifique o Protocolo de internet (para dispositivos de hardware suportados) usando a lista suspensa **Versão do IP**. • Para IPv4, os valores devem estar no formato: **(0-999).(0-999).(0-999).(0-999)** • Para IPv6, os valores devem estar no formato de oito grupos de dígitos hexadecimais, separados por dois pontos. A máscara de subrede deve ser um número entre **0-128**. O botão **Verificar** testa se há outro dispositivo de hardware atualmente no sistema, usando o endereço IP inserido. **Verificar** não pode detectar conflitos com dispositivos de hardware desligados, fora do sistema do XProtect VMS ou não respondendo momentaneamente de outra forma.
Nome de usuário	O nome de usuário e nível usado para conectar o hardware. Selecione outro usuário na lista suspensa e adicione uma nova senha usando o campo **Senha** descrito abaixo. Adicionar ou excluir usuários usando as ações enfatizadas na parte inferior da seção **Autenticação** (consulte Adicionar um usuário na página 226 ou Excluir usuários na página 227). A seleção de um usuário que não tenha o nível de usuário mais alto especificado pelo fabricante, pode resultar na indisponibilidade de alguns recursos.

Nome	Descrição
Senha	A senha usada para conectar o hardware. Visualizar o texto inserido no momento usando o ícone **Revelar**. Ao alterar a senha, consulte a documentação do fabricante para as regras de senha para o dispositivo de hardware específico, ou use o ícone **Gerar senha** para gerar automaticamente uma senha que corresponda às exigências. Para obter informações sobre como alterar senhas em diversos dispositivos de hardware, consulte Alterar senhas em dispositivos de hardware na página 229. Como um administrador do sistema, você precisar dar aos outros usuários a permissão para visualizar a senha no Management Client. Para obter mais informações, consulte Definições de funções em Hardware.
Adicionar um usuário	Selecione o link **Adicionar** sublinhado, para abrir a caixa de diálogo **Adicionar um usuário** e adicione um usuário ao dispositivo de hardware. A adição de um usuário o definirá automaticamente como o usuário ativo no momento e substituirá as credenciais previamente inseridas. Ao criar a senha, consulte a documentação do fabricante para as regras de senha para o dispositivo de hardware específico, ou use o ícone **Gerar senha** para gerar automaticamente uma senha que corresponda às exigências. O nível de usuário mais alto detectado no dispositivo de hardware será pré-selecionado automaticamente. Não recomendamos modificar o **nível do usuário** de seu valor padrão. A seleção de um **Nível de usuário** que não seja o nível de usuário mais alto especificado pelo fabricante, pode resultar na indisponibilidade de alguns recursos.

Nome	Descrição
Excluir usuários	Selecione o link **Excluir** sublinhado, para abrir a caixa de diálogo **Excluir usuários** e remova usuários do dispositivo de hardware. Você não pode excluir o usuário ativo no momento. Para definir um novo usuário, use a caixa de diálogo **Adicionar um usuário** descrita acima e depois, remova o usuário antigo usando esta interface.

Ativar/desativar dispositivos individuais

Câmeras estão por padrão **desabilitadas**.

Microfones, alto-falantes, metadados, entradas e **saídas** estão por padrão **desabilitados**.

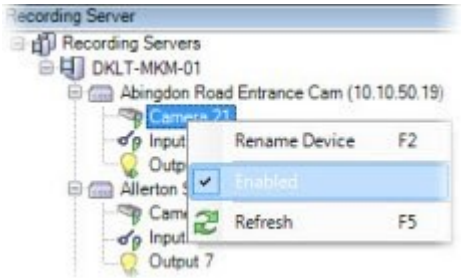
Isto significa que, microfones, alto-falantes, metadados, entradas e saídas devem ser ativados individualmente antes de você poder usá-los no sistema. O motivo para isto é que os sistemas de vigilância dependem de câmeras, ao passo que a utilização de microfones e assim por diante é altamente individual, dependendo das necessidades de cada organização.

Você pode ver se os dispositivos estão ativados ou desativados (os exemplos mostram uma saída):

desativado
ativado

O mesmo método para habilitar/desabilitar é usado por câmeras, microfones, alto-falantes, metadados, entradas e saídas.

1. Expanda o servidor de gravação e o dispositivo. Clique com o botão direito do mouse no dispositivo que você desejar ativar.
2. Selecione **Ativado** para limpar ou selecioná-lo.



Configurar uma conexão segura com o hardware

Você pode configurar uma conexão segura HTTPS usando SSL (Secure Sockets Layer) entre o hardware e o servidor de gravação.

Consulte o seu fornecedor de câmera para obter um certificado para seu hardware e carregue-o para o hardware, antes de continuar com os passos abaixo:

1. No painel **Visão geral**, clique com o botão direito do mouse no servidor de gravação e selecione Adicionar hardware.

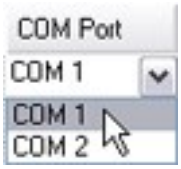
2. Na guia **Configurações**, habilite HTTPS. Isto não é habilitado por padrão.
3. Digite a porta no servidor de gravação na qual a conexão HTTPS está conectada. O número da porta deve corresponder à porta configurada na página inicial do dispositivo.
4. Faça as alterações necessárias e salve.

Habilitar a PTZ em um codificador de vídeo

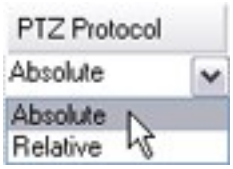
Para habilitar o uso de câmeras PTZ em um codificador de vídeo, faça o seguinte na guia **PTZ**:

1. Na lista de dispositivos conectados ao codificador de vídeo, marque a caixa **Habilitar PTZ** para as câmeras relevantes:

2. Na coluna **ID de dispositivo PTZ**, verifique a ID de cada câmera.
3. Na coluna **Porta COM**, selecione as portas COM (comunicação serial) do codificador de vídeo a serem usadas para o controle da funcionalidade PTZ:



4. Na coluna **Protocolo PTZ**, selecione qual esquema de posicionamento você deseja usar:



   - **Absoluto**: Quando o operador usa controles PTZ para a câmera, a câmera é ajustada em relação a uma posição fixa, frequentemente referida como posição inicial da câmera.
   - **Relativo**: Quando o operador usa os controles PTZ para a câmera, a câmera será ajustada em relação à sua posição atual

   O conteúdo da coluna **Protocolo PTZ** varia muito, dependendo do hardware. Alguns têm de 5 a 8 protocolos diferentes. Veja também a documentação da câmera.

5. Na barra de ferramentas, clique em **Salvar**.
6. Você está pronto para configurar posições pré-definidas e patrulhamento para cada câmera PTZ:
   - Adicionar uma posição predefinida (tipo 1)
   - Adicionar um perfil de patrulha

Alterar senhas em dispositivos de hardware

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Você pode alterar senhas em diversos dispositivos de hardware em uma operação.

Inicialmente, os dispositivos suportados são modelos da Canon, Axis, Bosch, Hanwa, Panasonic, Sony, Hikvision e dispositivos de hardware compatíveis com ONVIF, mas a interface de usuário mostra diretamente se um modelo é suportado ou não. Você também pode ir para o nosso site para saber se um modelo é compatível: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

Para dispositivos incompatíveis com o gerenciamento de senhas de dispositivos, você deve alterar a senha de um dispositivo de hardware a parir de sua página da web e inserir a nova senha manualmente em Management Client. Para obter mais informações, consulte Editar hardware na página 223.

Você pode optar por:

- Deixar o sistema gerar senhas individuais para cada dispositivo de hardware. O sistema gera senhas baseadas nos requisitos do fabricante dos dispositivos de hardware.
- Usar uma única senha definida pelo usuário para todos os dispositivos de hardware. Quando você aplica as novas senhas, os dispositivos de hardware perdem momentaneamente a conexão ao servidor de gravação. Após ter aplicado novas senhas, o resultado para cada dispositivo de hardware aparece na tela. Para alterações sem êxito, a razão da falha aparece, se o dispositivo de hardware for compatível com tais informações. De dentro do assistente, você pode criar um relatório de alterações de senha com êxito e com falha, mas os resultados também são registrados em **Registros de servidor**.

  > Para dispositivos de hardware com drivers ONVIF e várias contas de usuário, apenas um administrador do XProtect com permissões administrativas do dispositivo de hardware pode alterar as senhas do VMS.

Requisitos:

- O modelo de dispositivo de hardware suporta o gerenciamento de senha por Milestone.

Etapas:

1. No painel **Navegação do site**, selecione o nó **Servidores de gravação**.
2. Clique com o botão direito do mouse no servidor de gravação que você desejar remover no painel Visão geral.
3. Selecione **Alterar senha do hardware**. Um assistente é exibido.
4. Digitar a senha usando letras maiúsculas e minúsculas, números e os seguintes caracteres: **! ( ) * - . _**

   O número máximo de caracteres é 64.

   > O comprimento máximo da senha para a câmera externa Bosch FLEXIDOME IP NDN-50051 de 5000 MP é de 19 caracteres.

5. Siga as instruções na tela para concluir as alterações.

   > O campo **Última alteração de senha** mostra o carimbo de hora da alteração de senha mais recente, com base nas configurações de hora locais do computador a partir do qual a senha foi alterada.

6. A última página mostra o resultado. Se o sistema não conseguiu atualizar uma senha, clique em **Falha** ao lado do dispositivo de hardware para ver a razão.
7. Você também pode clicar no botão **Imprimir relatório** para ver a lista completa de atualizações com e sem êxito.

8. Se você desejar alterar a senha nos dispositivos de hardware que falharam, clique em **Tentar novamente**, e o assistente iniciará com os dispositivos de hardware que falharam.

> Se clicar em **Tentar novamente**, você não terá mais acesso ao relatório da primeira vez que concluiu o assistente.

> Por razões de segurança, alguns dispositivos de hardware podem ficar indisponíveis por um determinado período se você falhar na alteração da senha diversas vezes seguidas. Restrições de segurança variam para diferentes fabricantes.

Atualizar firmware em dispositivos de hardware

> As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Management Client permite que você atualize o firmware do hardware que foi adicionado ao seu sistema VMS. Você pode atualizar vários dispositivos de hardware simultaneamente se eles forem compatíveis com o mesmo arquivo de firmware.

A interface do usuário mostra diretamente se um modelo oferece suporte a atualizações de firmware. Você também pode ir para o site da Milestone para saber se um modelo é compatível: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Para dispositivos que não oferecem suporte a atualizações de firmware, você deve atualizar o firmware de um dispositivo de hardware em sua página da web.

Quando você atualiza o firmware, os dispositivos de hardware perdem momentaneamente a conexão ao servidor de gravação.

Após ter atualizado o firmware, o resultado para cada dispositivo de hardware aparece na tela. Para alterações sem êxito, a razão da falha aparece, se o dispositivo de hardware for compatível com tais informações. Os resultados também são registrados nos **Registros do servidor**.

> Para dispositivos de hardware com drivers ONVIF e várias contas de usuário, apenas um administrador do XProtect com permissões administrativas do dispositivo de hardware podem alterar o firmware do VMS.

Requisitos:

- O modelo do dispositivo de hardware suporta atualizações de firmware por Milestone.

Etapas:

1. No painel **Navegação do site**, selecione o nó **Servidores de gravação**.
2. Clique com o botão direito do mouse no servidor de gravação que você desejar remover no painel Visão geral.
3. Selecione **Atualizar firmware do hardware**. Um assistente é exibido.
4. Siga as instruções na tela para concluir as alterações.

> Você só pode atualizar vários dispositivos de hardware compatíveis com o mesmo arquivo de firmware. O hardware adicionado por meio do driver ONVIF pode ser encontrado em **outro**, em vez do nome do fabricante.

6. A última página mostra o resultado. Se o sistema não conseguiu atualizar o firmware, clique em **Falha** ao lado do dispositivo de hardware para ver a razão.

> Milestone não se responsabiliza pelo mau funcionamento do dispositivo de hardware se um arquivo de firmware ou dispositivo de hardware incompatível for selecionado.

Adicionar e configurar um IDP externo

1. Em Management Client, selecione **Ferramentas** > **Opções** e abra a guia **IDP externo**.
2. Na seção **IDP externo**, selecione **Adicionar**.
3. Insira as informações para o IDP externo. Para obter mais informações sobre as informações necessárias, consulte o IDP externo.

Para obter informações sobre como registrar quais alegações do IDP externo você deseja usar no VMS, consulte Registrar alegações para um IDP externo.

Dispositivos - Grupos

Adicionar um grupo de dispositivos

1. No painel **Visão geral**, clique com o botão direito no tipo de dispositivo com o qual você deseja criar um grupo de dispositivos.
2. Selecione **Adicionar grupo de dispositivos**.

3. Na caixa de diálogo **Adicionar grupo de dispositivos**, especifique um nome e a descrição do novo grupo de dispositivos:

   A descrição aparece quando você pausa o ponteiro do mouse sobre o grupo de dispositivos na lista de grupo de dispositivos.

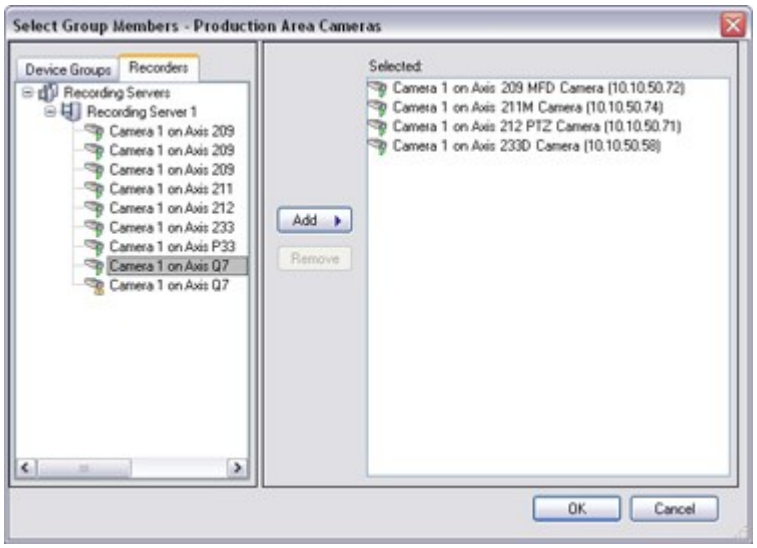
4. Clique em **OK**. A pasta que representa o novo grupo de dispositivos aparece na lista.
5. Continue para especificar quais dispositivos incluir em um grupo de dispositivos (consulte Especificar quais dispositivos incluir em um grupo de dispositivos na página 233).

Especificar quais dispositivos incluir em um grupo de dispositivos

1. No painel **Visão geral**, clique com o botão direito na pasta do grupo de dispositivos em questão.
2. Selecione **Editar membros do grupo de dispositivos**.
3. Na janela **Selecionar usuários do grupo**, selecione uma das guias para localizar o dispositivo.

   Um dispositivo pode ser um membro de mais de um grupo de dispositivo.

4. Selecione os dispositivos que desejar incluir e clique em **Adicionar** ou clique duas vezes no dispositivo:



5. Clique em **OK**.

6. Se você ultrapassar o limite de 400 dispositivos em um grupo, poderá adicionar grupos de dispositivos como subgrupos sob outros grupos de dispositivos:

Dispositivos desativados

Por padrão, dispositivos desativados não são exibidos no painel **Visão geral**.

Para exibir todos os dispositivos desativados, na parte superior do painel **Visão geral**, clique em **Filtrar** para abrir a guia **Filtrar** e selecione **Mostrar dispositivos desativados**.

Para ocultar novamente os dispositivos desativados, limpe **Mostrar dispositivos desativados**.

Especificar as propriedades comuns para todos os dispositivos em um grupo de dispositivos

Com os grupos de dispositivos, você pode especificar as propriedades comuns para todos os dispositivos dentro de um determinado grupo de dispositivos:

1. No painel **Visão geral,**, clique no grupo de dispositivos.

   No painel **Propriedades**, todas as propriedades **que estão disponíveis em todos os dispositivos do grupo de dispositivo** são listadas e agrupadas em guias.

2. Especifique as propriedades comuns relevantes.

   Na guia **Configurações**, você pode alternar entre as configurações de **todos** os dispositivos e configurações para dispositivos individuais.

3. Na barra de ferramentas, clique em **Salvar**. As configurações são salvas em dispositivos individuais, e não no grupo de dispositivos.

Dispositivos desativados

Por padrão, dispositivos desativados não são exibidos no painel **Visão geral**.

Para exibir todos os dispositivos desativados, na parte superior do painel **Visão geral**, clique em **Filtrar** para abrir a guia **Filtrar** e selecione **Mostrar dispositivos desativados**.

Para ocultar novamente os dispositivos desativados, limpe **Mostrar dispositivos desativados**.

Ativar/desativar dispositivos através de grupos de dispositivos

Você pode ativar/desativar dispositivos através do hardware configurado. A não ser quando ativados/desativados manualmente no assistente de inclusão de hardware, os dispositivos de câmera são, por padrão, ativados, e todos os outros dispositivos são, por padrão, desativados.

Por padrão, dispositivos desativados não são exibidos no painel **Visão geral**.

Para exibir todos os dispositivos desativados, na parte superior do painel **Visão geral**, clique em **Filtrar** para abrir a guia **Filtrar** e selecione **Mostrar dispositivos desativados**.

Para ocultar novamente os dispositivos desativados, limpe **Mostrar dispositivos desativados**.

Para localizar um dispositivo através dos grupos de dispositivos para ativar ou desativar:

1. No painel **Navegação do site**, selecione o dispositivo.
2. No painel **Visão geral**, expanda o grupo relevante e encontre o dispositivo.
3. Clique com o botão direito do mouse no dispositivo e selecione **Ir para hardware**.
4. Clique em "mais" para ver todos os dispositivos do hardware.
5. Clique com o botão direito do mouse no dispositivo que desejar ativar / desativar e selecione **Ativado**.

Dispositivos - Configurações da câmera

Ver ou editar as configurações da câmera

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione a câmera relevante.
3. Abra a guia **Configurações**.

Você pode ver ou editar as configurações, tais como:

- Taxa de quadros padrão
- Resolução
- Compactação
- O número máximo de quadros entre as frame-chave
- Exibição de data/hora/texto na tela para uma câmera selecionada ou para todas as câmeras dentro de um grupo de dispositivos

Os drivers para as câmeras determinam o conteúdo da guia **Configurações**. Os drivers variam dependendo do tipo de câmera.

Para câmeras que oferecem suporte a mais de um tipo de transmissão, por exemplo MJPEG e MPEG-4/H.264/H.265, você pode usar o streaming múltiplo, consulte Gerenciar multi-streaming na página 242.

Visualizar

Ao alterar uma configuração, você pode verificar rapidamente o efeito da mudança se tiver o painel **Pré-visão** ativado.

- Para ativar a **Visualização**, clique no menu **Exibir** e, em seguida, clique em **Janela de visualização**.

Você não pode usar o painel **Pré-visão** para julgar o efeito de alterações na taxa de quadros porque as imagens em miniatura do painel **Pré-visão** usam outra taxa de quadros definida na caixa de diálogo **Opções**.

Desempenho

Se você alterar as configurações de **Máx. de quadros entre as frame-chave** e **Máx. de quadros entre o modo de frame-chave**, isso poderá reduzir o desempenho de algumas funcionalidades no XProtect Smart Client. Por exemplo, XProtect Smart Client requer um frame-chave para começar a exibir o vídeo, então um longo período entre os frame-chave prolonga o início do XProtect Smart Client.

Adicionando hardware

Para mais informações sobre como adicionar hardware ao seu site, consulte Adicionar hardware na página 221.

Ativar e desativar o suporte das lentes olho de peixe

O suporte das lentes olho de peixe é desativado por padrão.

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Lentes olho de peixe** selecione ou desmarque a caixa de seleção **Ativar suporte das lentes olho de peixe**.

Especificar as configurações da lente olho de peixe

1. Na guia **Lentes olho de peixe**, selecione o tipo de lente.
2. Especifique a posição/orientação física da câmera da lista **Posição/orientação da câmera**.
3. Selecione um número de Lente Panamorph Registrada na lista **Número RPL panomorph da ImmerVision Enables®**.

   Isso garante a identificação e a configuração correta das lentes utilizadas com a câmera. Você geralmente localiza o número RPL nas próprias lentes ou na caixa em que ele veio. Para obter detalhes sobre o ImmerVision, lentes panomorph e RPLs, consulte o site da ImmerVision (https://www.immervisionenables.com/).

   Se você selecionar o perfil de lente **Remover deformação genérica**, lembre-se de configurar o **Campo de visão** desejado.

Dispositivos - Gravação

Ativar/desativar a gravação

Gravação é ativada por padrão. Para ativar/desativar a gravação:

1. No painel **Navegação do site**, selecione **Servidores de gravação**.
2. No painel **Visão geral**, selecione o dispositivo relevante.
3. Na guia **Gravação**, marque ou desmarque a caixa de seleção **Gravar**.

> Você deve ativar a gravação para o dispositivo antes de poder gravar dados da câmera. Uma regra que especifica as circunstâncias para um dispositivo gravar não funciona se você tiver desativado a gravação pelo dispositivo.

Habilitar gravação em dispositivos relacionados

Nos dispositivos de câmera, é possívelativar a gravação em dispositivos relacionados, por exemplo, microfones conectados ao mesmo servidor de gravação. Isso significa que os dispositivos relacionados são gravados quando a câmera grava.

A gravação em dispositivos relacionados são ativadas por padrão para novos dispositivos de câmera, mas você pode ativar e desativar como quiser. Nos dispositivos de câmera existentes no sistema, a caixa de seleção é desmarcada por padrão.

1. No painel **Navegação do site**, selecione **Servidores de gravação**.
2. No painel **Visão geral**, selecione o dispositivo de câmera relevante.
3. Na guia **Gravação**, marque ou desmarque a caixa de seleção **Gravar em dispositivos relacionados**.
4. Na guia **Cliente**, especifique os dispositivos que se relacionam com a câmera.

Se quiser ativar a gravação em dispositivos relacionados ligados a outro servidor de gravação, é necessário criar uma regra.

Gerenciar gravação manual

Parar a gravação manual após é ativado por padrão, com um tempo de gravação de cinco minutos. Isto é para assegurar que o sistema pare automaticamente todas as gravações iniciadas pelos usuários do XProtect Smart Client.

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante.
3. Na guia **Gravação**, marque ou desmarque a caixa de seleção **Parar a gravação manual após**.

Ao ativá-lo, especifique um tempo de gravação. O número de minutos que você especifica deve ser suficientemente grande para acomodar as necessidades das várias gravações manuais sem sobrecarregar o sistema.

Adicionar a funções:

Você deve conceder permissão para iniciar e parar a gravação manual aos usuários do cliente em cada câmera em **Funções** na guia **Dispositivo**.

Usar em regras:

Os eventos que você pode usar quando cria regras relacionadas com a gravação manual são:

- Gravação manual iniciada
- Gravação manual parada

Especificar a taxa de quadros de gravação

Você pode especificar a taxa de quadros de gravação para JPEG.

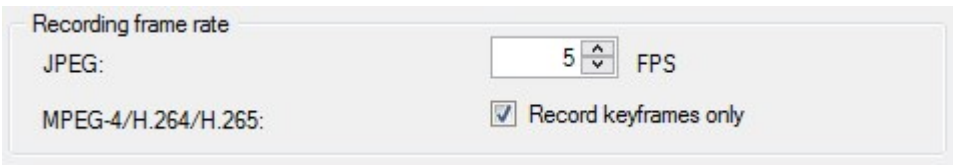
1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante.
3. Na guia **Gravação**, na **taxa de quadros de gravação: na caixa (JPEG)**, selecione ou digite a taxa de quadros de gravação (em FPS, quadros por segundo).

Ativar gravação de frame-chave

Você pode ativar a gravação de frame-chave para fluxos MPEG-4/H.264/H.265. Isso significa que o sistema alterna entre gravação apenas de frames-chave de gravação e gravação de todos os quadros, dependendo de suas configurações de regras.

Você pode, por exemplo, deixar o sistema gravar frames-chave quando não há movimento na visão e mudar para todos os quadros apenas em caso de detecção de movimento para salvar o armazenamento.

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante.
3. Na guia **Gravação**, marque a caixa de seleção **Gravar apenas frames-chaves**.



4. Configure uma regra que ativa a função, consulte Ações e ações de interrupção (explicado).

Habilitar gravação em dispositivos relacionados

Nos dispositivos de câmera, é possívelativar a gravação em dispositivos relacionados, por exemplo, microfones conectados ao mesmo servidor de gravação. Isso significa que os dispositivos relacionados são gravados quando a câmera grava.

A gravação em dispositivos relacionados são ativadas por padrão para novos dispositivos de câmera, mas você pode ativar e desativar como quiser. Nos dispositivos de câmera existentes no sistema, a caixa de seleção é desmarcada por padrão.

1. No painel **Navegação do site**, selecione **Servidores de gravação**.
2. No painel **Visão geral**, selecione o dispositivo de câmera relevante.
3. Na guia **Gravação**, marque ou desmarque a caixa de seleção **Gravar em dispositivos relacionados**.
4. Na guia **Cliente**, especifique os dispositivos que se relacionam com a câmera.

Se quiser ativar a gravação em dispositivos relacionados ligados a outro servidor de gravação, é necessário criar uma regra.

Salvar e recuperar gravações remotas

Para garantir que todas as gravações sejam salvas em caso de problemas de rede, você pode habilitar a recuperação automática de gravações remotas quando a conexão for restaurada.

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante.
3. Em **Gravações remotas**, selecione **Recuperar gravações remotas automaticamente quando a conexão for restaurada**. Isso permite a recuperação automática de gravações uma vez que a conexão for restabelecida

> A opção de gravação remota só está disponível se a câmera selecionada suporta o armazenamento de borda ou é uma câmera em uma configuração Milestone Interconnect.

O tipo de hardware selecionado determina de onde as gravações são recuperadas:

- Para uma câmera com gravação de armazenamento local, as gravações são recuperadas do armazenamento de gravação local da câmera
- Para um sistema remoto do Milestone Interconnect, as gravações são recuperadas dos servidores de gravação dos sistemas remotos

Você pode usar a seguinte funcionalidade independentemente da recuperação automática:

- Gravação manual
- A regra **Recuperar e armazenar gravações remotas de <devices>**
- A regra **Recuperar e armazenar gravações remotas entre <horário de início e término> de <dispositivos>**

Excluir registros

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante e a guia **Gravação**.
3. Clique no botão **Excluir todas as gravações** para excluir todas as gravações do dispositivo ou grupo de dispositivos.

Este método só pode ser usado se você tiver adicionado todos os dispositivos do grupo ao mesmo servidor. Dados protegidos não são excluídos.

Dispositivos - Fluxos

Streaming adaptável (explicado)

O fluxo adaptável é um método de transmissão usado quando vários fluxos de vídeo ao vivo são exibidos na mesma visualização. Ele permite que os clientes selecionem automaticamente os fluxos de vídeo ao vivo com a melhor correspondência em resolução aos fluxos solicitados pelos itens de visualização. O fluxo adaptável reduz a carga da rede e melhora a capacidade de decodificação e o desempenho do computador do cliente.

Você pode configurar a correspondência mais próxima de fluxos de vídeo disponíveis para a resolução solicitada por um item de visualização ao ativar o fluxo adaptável no XProtect Smart Client. Para obter mais informações, consulte Ativação do fluxo adaptável.

No XProtect Smart Client, o fluxo adaptável pode ser aplicado aos modos ao vivo e de reprodução. Nos clientes móveis, ele está disponível somente no modo ao vivo.

Quando aplicado no modo de reprodução, o método de transmissão é chamado de reprodução adaptável. Para obter mais informações, consulte Reprodução adaptável (explicação) na página 240

Reprodução adaptável (explicação)

A reprodução adaptável é uma configuração que permite o uso de fluxos adaptáveis no modo de reprodução.

Na reprodução adaptável, é preciso configurar dois fluxos: um fluxo primário e outro secundário. Se os dois fluxos forem ativados no Management Client, ambos os fluxos farão gravações.

- Se você reproduzir vídeos de um período anterior à configuração da gravação secundária, somente as gravações primárias serão reproduzidas.
- Se você reproduzir vídeos que foram gravados após a configuração da gravação secundária, os vídeos serão reproduzidos da gravação primária ou secundária, dependendo do que melhor corresponde ao tamanho da visualização do cliente.

Disponibilidade

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Ativar o streaming adaptável

Você pode ativar a reprodução adaptável junto ao fluxo adaptável na guia **Avançado** em **Perfis do Smart Client**. Também é necessário ativar o recurso no XProtect Smart Client em **Configurações** > **Avançado** > **Fluxo adaptável**. Para obter mais informações sobre a ativação do fluxo adaptável no XProtect Smart Client, consulte Ativação de streaming adaptável

Gravação de dispositivos

Você tem a opção de usar gravações de dispositivos na reprodução adaptável. Gravações de dispositivos permitem que você visualize sequências de um fluxo com uma resolução diferente, geralmente mais alta, do que o restante do fluxo. Por exemplo, você pode gravar um fluxo primário com baixa resolução e mesclar gravações de uma fonte de alta resolução. Você pode ativar as gravações de dispositivos mescladas ao navegar pelos dados.

Gravações de dispositivos são armazenadas no banco de dados de mídia e a resolução dessas gravações é definida em câmeras individuais.

Resolução de vídeos reproduzidos

Ao usar a reprodução adaptável, a resolução do vídeo reproduzido é determinada pelas configurações de resolução atuais das gravações primária e secundária. Isso significa que, na reprodução, a escolha do fluxo secundário ou primário é baseada na resolução configurada atualmente para os respectivos fluxos de gravação.

Adicionar uma transmissão

Os fluxos que você adicionar para gravação podem ser visualizados nos modos ao vivo e de reprodução.

Você também pode visualizar o vídeo gravado no seu item de visualização com o fluxo adaptável ativado. O fluxo adaptável no modo de reprodução é chamado de reprodução adaptável.

1. Na guia **Transmissões**, clique em **Adicionar**. Isso adiciona uma segunda transmissão na lista.
2. Na coluna **Nome**, edite o nome da transmissão. O nome aparece em XProtect Smart Client.
3. Na coluna **Modo ao vivo**, selecione quando o fluxo ao vivo é necessário:
   - **Sempre:** o fluxo é executado mesmo que nenhum usuário XProtect Smart Client solicite o fluxo
   - **Nunca:** a transmissão está desligada. Só use isso para gravar fluxos, por exemplo, se você quiser gravações em alta qualidade e precisa da largura de banda
   - **Quando necessário**: o fluxo começa quando solicitado por qualquer cliente ou se o fluxo estiver configurado para gravar
4. Na coluna **Fluxo ao vivo padrão**, selecione qual fluxo é padrão e tem que ser usado se o cliente não solicitar um fluxo específico e o fluxo adaptável estiver desativado.
5. Na coluna **Gravação**, selecione **Primária** ou **Secundária**. Para a reprodução adaptável, você tem que criar um fluxo de cada tipo. O vídeo que é reproduzido vem do fluxo de vídeo primário e o fluxo secundário é incluído quando necessário. Sempre deve haver uma gravação primária. Ademais, o fluxo que você configurar como **Primário** é usado em contextos diferentes, como para detecção de movimento e para exportação do XProtect Smart Client.
6. Em **Reprodução padrão**, selecione qual fluxo é padrão. O fluxo padrão será entregue ao cliente se a reprodução adaptável não for configurada.
7. Na coluna **Usar gravações de dispositivos**, selecione a caixa de seleção se você quiser usar gravações de dispositivos. Para obter mais informações sobre gravações de dispositivos, consulte Gravação de dispositivos na página 241.
8. Clique em **Salvar**.

> Se você não quer os fluxos ativos em nenhuma hipótese, a menos que alguém esteja assistindo vídeo ao vivo, é possível modificar a **Regra Iniciar Feed Padrão** para começar mediante solicitação com o evento predefinido **Feed Ao Vivo do Cliente Solicitado**.

Gerenciar multi-streaming

A visualização de vídeos ao vivo e reprodução de vídeos gravados não exigem necessariamente a mesma qualidade de vídeo e taxa de quadros.

Para alterar qual transmissão usar para a gravação

Na reprodução adaptável, é preciso configurar dois fluxos para a gravação: um fluxo primário e outro secundário. Para transmissões ao vivo, você pode configurar e usar quantos fluxos ao vivo a câmera suportar.

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione a câmera relevante.
3. Na guia **Fluxos**, selecione o fluxo que você quer usar para gravação.

4. Selecione a opção relevante na lista **Modo ao vivo**. As opções **Quando necessário**, **Sempre** e **Nunca** indicam quando o fluxo deve ser aplicado no cliente. Se nada for solicitado do cliente, a gravação usará o fluxo em que a caixa de seleção **Fluxo ao vivo padrão** estiver selecionada.
5. Para gravar em um fluxo, selecione **Primário** ou **Secundário** na lista **Gravação**.
6. Para usar a reprodução adaptável, configure dois fluxos e defina um dos fluxos como **Primário** e o outro como **Secundário**.
7. Para gravar em um fluxo, selecione o fluxo **Primário** ou **Secundário** na lista **Gravação**.

Limitar transmissão de dados

Você pode definir um conjunto de condições para garantir que as transmissões de vídeo sejam executadas apenas quando visualizadas por um cliente.

Para gerenciar streaming e limitar a transmissão de dados desnecessária, o streaming não inicia quando as seguintes condições são atendidas:

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione a câmera relevante.
3. Na guia **Transmissões**, na lista **Modo ao vivo**, selecione **Quando necessário**.
4. Na guia **Gravação**, desmarque a caixa de seleção **Gravar**.
5. Desmarque a caixa de seleção **Detecção de movimento** da guia **Movimento**.

Se estas condições forem atendidas, os fluxos de vídeo só serão executados quando visualizados por um cliente.

Exemplos

Exemplo 1, vídeo ao vivo e gravado:

- Para visualizar vídeo **ao vivo**, sua organização pode preferir H.264 com alta taxa de quadros
- Para reproduzir vídeo **gravado**, a sua organização pode preferir MJPEG a uma taxa de quadros mais baixa para preservar espaço em disco

Exemplo 2, vídeo ao vivo local e remoto:

- Para visualizar **vídeo ao vivo de um ponto de operação local conectado**, a sua organização pode preferir H.264 com alta taxa de quadros para ter a melhor qualidade de vídeo disponível
- Para visualizar **vídeo ao vivo de um ponto de operação remoto conectado**, a sua organização pode preferir MJPEG com baixa taxa de quadros e qualidade para preservar a largura de banda da rede

Exemplo 3, streaming adaptável:

- Para visualizar **vídeo ao vivo e reduzir a carga na CPU e GPU do XProtect Smart Client computador**, sua organização pode preferir múltiplas taxas de quadros altas H.264/H.265, mas com diferentes resoluções para corresponder à resolução solicitada pelo XProtect Smart Client ao usar o streaming adaptável. Para obter mais informações, consulte Smart Client Perfis (nó de Cliente) na página 482.

> Se você ativar o **Multicast ao vivo** na aba **Cliente** da câmera (consulte a aba Cliente (dispositivos)), ele funciona apenas na transmissão de vídeo padrão.

Mesmo quando as câmeras suportam transmissões múltiplas, as capacidades individuais de transmissões múltiplas podem variar entre diferentes câmeras. Consulte a documentação da câmera para obter mais informações.

Para ver se a câmera oferece diferentes tipos de transmissões, consulte a aba **Configurações (dispositivos)**.

Dispositivos - Armazenamento

Gerenciar pré-buffering

Câmeras, microfones e alto-falantes suportam pré-buffering. Para alto-falantes, os fluxos são enviados apenas quando o usuário XProtect Smart Client usa a função **Falar para o alto-falante**. Isso significa que, dependendo de como suas transmissões de alto-falantes são acionadas para serem gravadas, há pouco ou nenhum pré-buffering disponível.

Na maioria dos casos você configura os alto-falantes para gravar quando o usuário XProtect Smart Client usa a função **Falar para o alto-falante**. Em tais casos, não há pré-buffering disponível para o alto-falante.

> Para utilizar a função de pré-buffer, os dispositivos devem ser ativados e estarem enviando uma transmissão ao sistema.

Ativar e desativar pré-armazenamento em buffer

O pré-buffer é ativado por padrão com um tamanho do pré-buffer de três segundos e armazenamento na memória.

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante.
3. Na guia **Gravação**, marque ou desmarque a caixa de seleção **Pré-buffer**.
4. Na guia **Cliente**, especifique os dispositivos que se relacionam com a câmera.

Especificar o local de armazenamento e período de pré-buffer:

As gravações temporárias de pré-buffer são armazenadas ou na memória ou no disco:

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante e então selecione a guia **Gravação**.
3. Na lista **Local**, selecione **Memória** ou **Disco** e especifique o número de segundos.
4. Se você precisar de um período de pré-buffer de mais de 15 segundos, selecione **Disco**.

O número de segundos que você especificar deve ser suficientemente grande para acomodar suas necessidades nas várias regras de gravação que você definir.

Se você alterar o local para **Memória**, o sistema reduzirá o período para 15 segundos automaticamente.

Usar pré-buffer em regras:

Ao criar regras que acionam a gravação, você pode selecionar que as gravações devem começar algum tempo antes do evento real (pré-buffer).

Exemplo: A regra a seguir especifica que a gravação deve começar na câmera 5 segundos antes do movimento ser detectado na câmera.

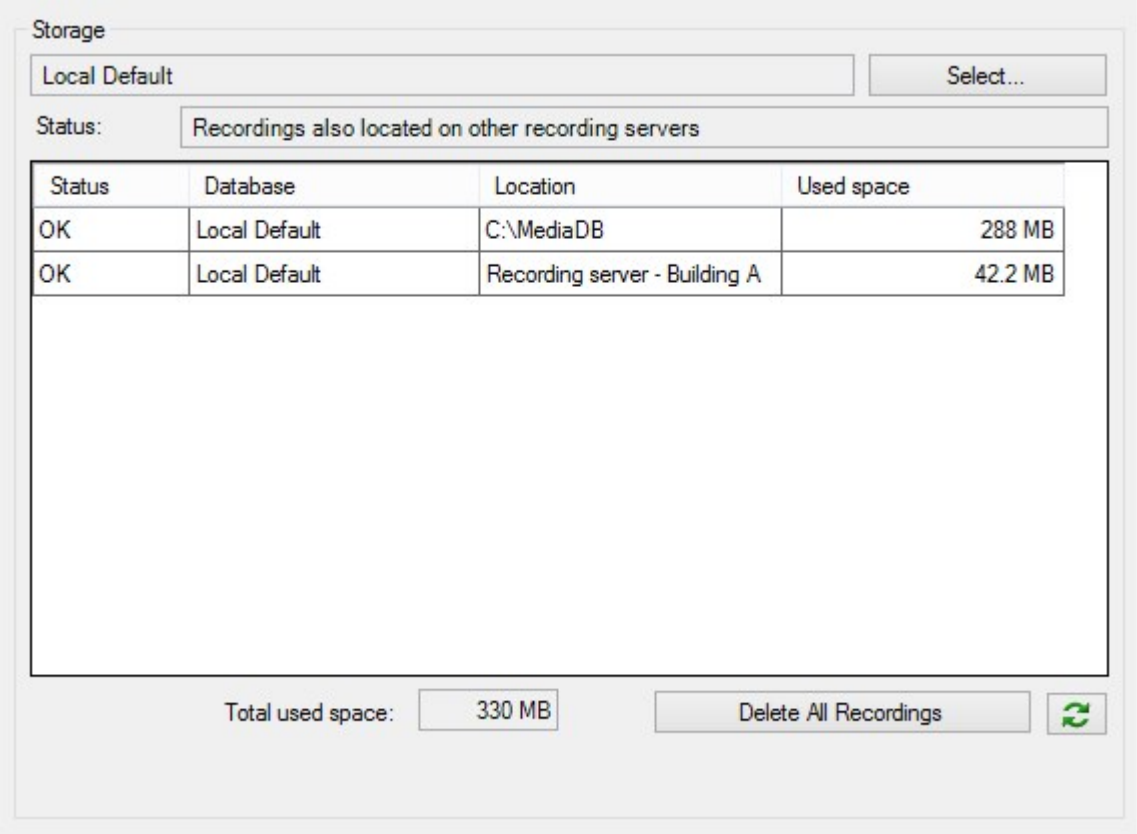
Para utilizar a função de gravação de pré-buffer na regra, você deve ativar o pré-buffering no dispositivo a ser gravado e deve definir o período de pré-buffer para, no mínimo, o mesmo tamanho, conforme especificado na regra.

Monitorar o status de bancos de dados para dispositivos

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante e a guia **Gravação**.

Em **Armazenamento** é possível monitorar e gerenciar os bancos de dados de um dispositivo ou um grupo de dispositivos adicionado ao mesmo servidor de gravação.

No topo da tabela, é possível ver o banco de dados selecionado e seu status. Neste exemplo, o banco de dados selecionado é o **Padrão Local** e o status é **Gravações também localizadas em outros servidores de gravação**. O outro servidor é o servidor de gravação no prédio A.



Status possíveis para o banco de dados selecionado

Nome	Descrição
Existem gravações localizadas em outros servidores de gravação	O banco de dados está ativo e em execução e tem arquivos localizados em áreas de armazenamento de outros servidores de gravação.
Arquivos também localizados no armazenamento anterior	O banco de dados está ativo e em execução e também tem arquivos localizados em outras áreas de armazenamento.
Ativo	O banco de dados está ativo e em execução.
Os dados de alguns dos dispositivos escolhidos estão sendo movidos para outro local	O banco de dados está ativo e em execução e o sistema movendo dados para um ou mais dispositivos selecionados em um grupo de um local para outro.
Os dados do dispositivo estão	O banco de dados está ativo e em execução e o sistema movendo

Nome	Descrição
sendo movidos para outro local	dados para o dispositivo selecionado de um local para outro.
Informações não disponíveis no modo de recuperação de falha	As informações de status sobre o banco de dados não podem ser coletadas pelo sistema quando o banco de dados está no modo de recuperação de falhas (failover).

Mais abaixo na janela, você pode ver o status individual dos bancos de dados (**OK**, **Off-line ou Armazenamento antigo**), sua localização e quanto espaço cada um deles utiliza.

Se todos os servidores estiverem on-line, no campo **Espaço usado total**, é possível ver o espaço total usado por todo o armazenamento.

Para obter informações sobre configuração de armazenamento, consulte a guia Armazenamento (servidor de gravação).

Mover dispositivos de um armazenamento a outro

Quando você seleciona uma nova localização para armazenar gravações, as gravações existentes não serão movidas. Elas permanecerão na localização atual, com as condições definidas pela configuração da armazenagem à qual pertencem.

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo relevante e a guia **Gravação**.
3. Clique em **Selecionar** em **Armazenamento** para selecionar um armazenamento de gravação no qual seus dispositivos vão gravar.

As gravações serão arquivadas de acordo com a configuração do armazenamento que você selecionar.

Dispositivos - Detecção de movimento

Detecção de movimento (explicado)

A configuração de detecção de movimento é um elemento chave no seu sistema: Sua configuração de detecção de movimento determina quando o sistema gera eventos de movimento e, normalmente, também quando o vídeo é gravado.

O tempo gasto em encontrar a melhor configuração de detecção de movimento possível para cada câmera ajuda a evitar mais tarde, por exemplo, gravações desnecessárias. Dependendo da localização física da câmera, pode ser uma boa ideia testar as configurações de detecção de movimento em diferentes condições físicas, tais como dia/noite e tempo ventoso/calmo.

Você pode especificar as definições relacionadas com a quantidade de alterações necessárias na visão de uma câmera para que a mudança seja considerada como movimento. Você pode, por exemplo, especificar intervalos entre a análise de detecção de movimento e as áreas de uma visão em que o movimento deve ser ignorado. Você também pode ajustar a precisão da detecção de movimento e, assim, a carga nos recursos do sistema.

Qualidade da imagem

Antes de configurar a detecção de movimento de uma câmera, o Milestone recomenda que você tenha definido as configurações de qualidade de imagem da câmera, por exemplo configurações de resolução, codec de vídeo e fluxo. Isso é feito na guia **Configurações** da janela **Propriedades** do dispositivo. Se você alterar as configurações de qualidade da imagem, você sempre deverá testar qualquer configuração de detecção de movimento depois.

Máscaras de privacidade

Se você definiu áreas com máscaras de privacidade permanentes, não há detecção de movimento nessas áreas.

Ativar e desativar a detecção de movimento

Especificar configuração padrão de detecção de movimento para câmeras

1. No menu **Ferramentas**, clique em **Opções**.
2. Na guia **Geral** em **Ao adicionar novos dispositivos de câmera automaticamente, ativar**, marque a caixa de seleção **Detecção de movimento**.

Ativar ou desativar detecção de movimento para uma câmera específica

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione a câmera relevante.
3. Na guia **Movimento**, marque ou desmarque a caixa de seleção **Detecção de movimento**.

Ao desativar a detecção de movimento para uma câmera, as regras relacionadas com detecção de movimento para a câmera não funcionam.

Ativar ou desativar aceleração de hardware

A decodificação automática de vídeo acelerada por hardware para detecção de movimento é a configuração padrão ao adicionar uma câmera. O servidor de gravação usa recursos de GPU, caso estejam disponíveis. Isto irá reduzir a carga da CPU durante a análise do movimento do vídeo e melhorar o desempenho geral do servidor de gravação.

Para ativar ou desativar a aceleração de hardware

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione a câmera relevante.
3. Na guia **Movimento**, em **Aceleração de hardware**, selecione **Automático** para habilitar a aceleração de hardware ou selecione **Desligado** para desabilitar a configuração.

Uso de recursos de GPU

A decodificação de vídeo acelerada por hardware para detecção de movimento usa recursos da GPU em:

- CPUs Intel que suportam Intel Quick Sync
- O NVIDIA® exibe os adaptadores conectados ao seu servidor de gravação

Balanceamento de carga e desempenho

O balanceamento de carga entre os diferentes recursos é feito automaticamente. No nó **System Monitor**, você pode verificar se a carga de análise de movimento atual nos recursos da NVIDIA GPU está dentro dos limites especificados do nó **Limites do Monitor do Sistema**. Os indicadores de carga da NVIDIA GPU são:

- Decodificação NVIDIA
- Memória NVIDIA
- Renderização NVIDIA

Se a carga for muito alta, você pode adicionar recursos de GPU em seu servidor de gravação instalando vários adaptadores de vídeo NVIDIA. Milestone não recomenda o uso da configuração Scalable Link Interface (SLI) de seus adaptadores de vídeo NVIDIA.

Os produtos NVIDIA possuem capacidades de processamento diferentes.

A decodificação de vídeo acelerada por hardware para detecção de movimento usando GPUs NVIDIA requer capacidade de computação versão 6.x (Pascal) ou mais recente.

- Para descobrir a versão de capacidade de processamento do seu produto NVIDIA, acesse o site da NVIDIA (https://developer.nvidia.com/cuda-gpus/).

- Para ver se a detecção de movimento de vídeo é acelerada por hardware para uma câmera específica, ative o login no arquivo no registro do servidor de gravação. Defina o nível para **Depuração**, e o diagnóstico será registrado no DeviceHandling.log. O log segue o padrão:
  [tempo] [274] DEBUG – [guid] [nome] decodificação configurada: Automático: Decodificação atual: Intel/NVIDIA

A versão OS do servidor de gravação e da geração da CPU podem impactar o desempenho da detecção de movimento de vídeo acelerado por hardware. A alocação de memória do GPU geralmente é o gargalo de versões mais antigas (limite típico entre 0.5 GB e 1.7 GB).

Sistemas baseados em Windows 10/Servidor 2016 e 6.a geração de CPU (Skylake) ou mais nova podem alocar 50% da memória do sistema para o GPU e, portanto, remover ou reduzir o gargalo.

As CPUs de 6.a geração da Intel não oferecem decodificação acelerada por hardware de H.265, então o desempenho é comparável ao H.264 para essas versões de CPU.

Ativar sensibilidade manual para definir movimento

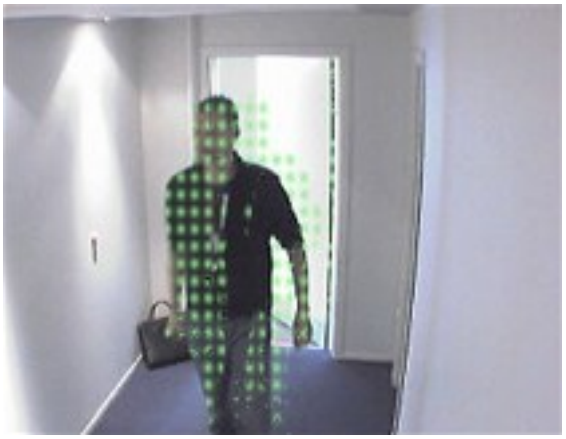
A configuração de sensibilidade determina **quanto cada pixel** na imagem precisa mudar antes de ser visto como movimento.

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione a câmera relevante.
3. Marque a caixa de seleção **Sensibilidade manual** da guia **Movimento**.
4. Arraste a barra para esquerda para um maior nível de sensibilidade e para a direita para um menor nível de sensibilidade.

   Quanto **maior** o nível de sensibilidade, menos a mudança em cada pixel é permitida antes de ser considerado como movimento.

   Quanto **menor** o nível de sensibilidade, mais a mudança em cada pixel é permitida antes de ser considerado como movimento.

   Pixels nos quais o movimento é detectado ficam destacados em verdes na imagem de visualização.
5. Selecione uma posição na barra na qual somente as detecções que você considerar movimento ficam em destaque.



Você pode comparar e definir a configuração de sensibilidade exata entre as câmeras pelo número no lado direito do controle deslizante.

Especifique o limite para definir movimento

O limite da detecção de movimento determina **quantos pixels** na imagem devem mudar antes de ser visto como movimento.

1. Arraste o controle deslizante para a esquerda para um nível mais elevado de movimento, e para a direita para um nível mais baixo de movimento.
2. Selecione uma posição do controle deslizante no qual apenas detecções que você considerar como movimento são detectadas.

A linha preta vertical na barra de indicação de movimento mostra o limiar de detecção de movimento: Quando o movimento detectado estiver acima do nível de limiar de detecção selecionado, a barra muda de cor de verde para vermelho, indicando uma detecção positiva.

Barra de indicação de movimento: muda de cor de verde para vermelho quando acima do limiar, indicando uma detecção de movimento positiva.

Especificar regiões de exclusão para detecção de movimento

Você pode configurar todas as configurações para um grupo de câmeras, mas você normalmente definiria excluir regiões por câmera.

> Áreas com máscaras de privacidade permanentes também são excluídas da detecção de movimento. Selecione a opção **Exibir máscaras de privacidade** para exibi-las.

Excluir a detecção de movimento de áreas específicas ajuda a evitar a detecção de movimento irrelevante, por exemplo, se a câmera cobre uma área onde uma árvore fica balançando ao vento, ou quando os carros passam regularmente no fundo.

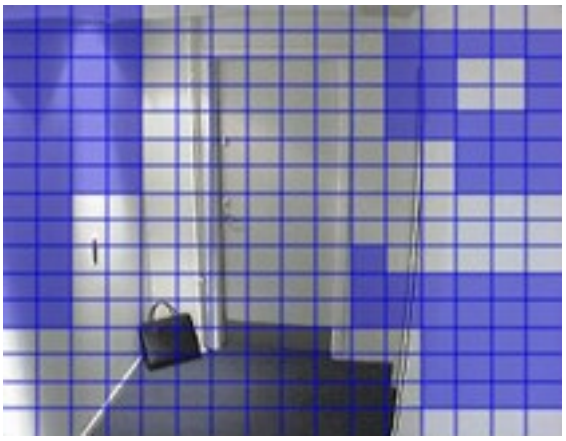
Quando você usa regiões de exclusão com câmeras PTZ e gira/inclina/aumenta (pan-tilt-zoom) a câmera, a área excluída **não** se move de acordo, pois a área está bloqueada para a imagem da câmera, e não o objeto.

1. Para usar excluir regiões, selecione a caixa **Usar excluir regiões**.

   Uma grade divide a imagem de visualização em seções selecionáveis.

2. Para definir as regiões de exclusão, arraste o ponteiro do mouse sobre as áreas necessárias na imagem de visualização enquanto pressiona o botão esquerdo do mouse. Clique com o botão direito do mouse para abrir uma seção da grade.

Você pode definir quantas regiões de exclusão desejar. Regiões excluídas aparecem em azul:



As áreas de exclusão em azul só aparecem na imagem de visualização na guia **Movimento**, e não em quaisquer outras imagens de visualização do Management Client ou de clientes de acesso.

Dispositivos - Posições de câmera predefinidas

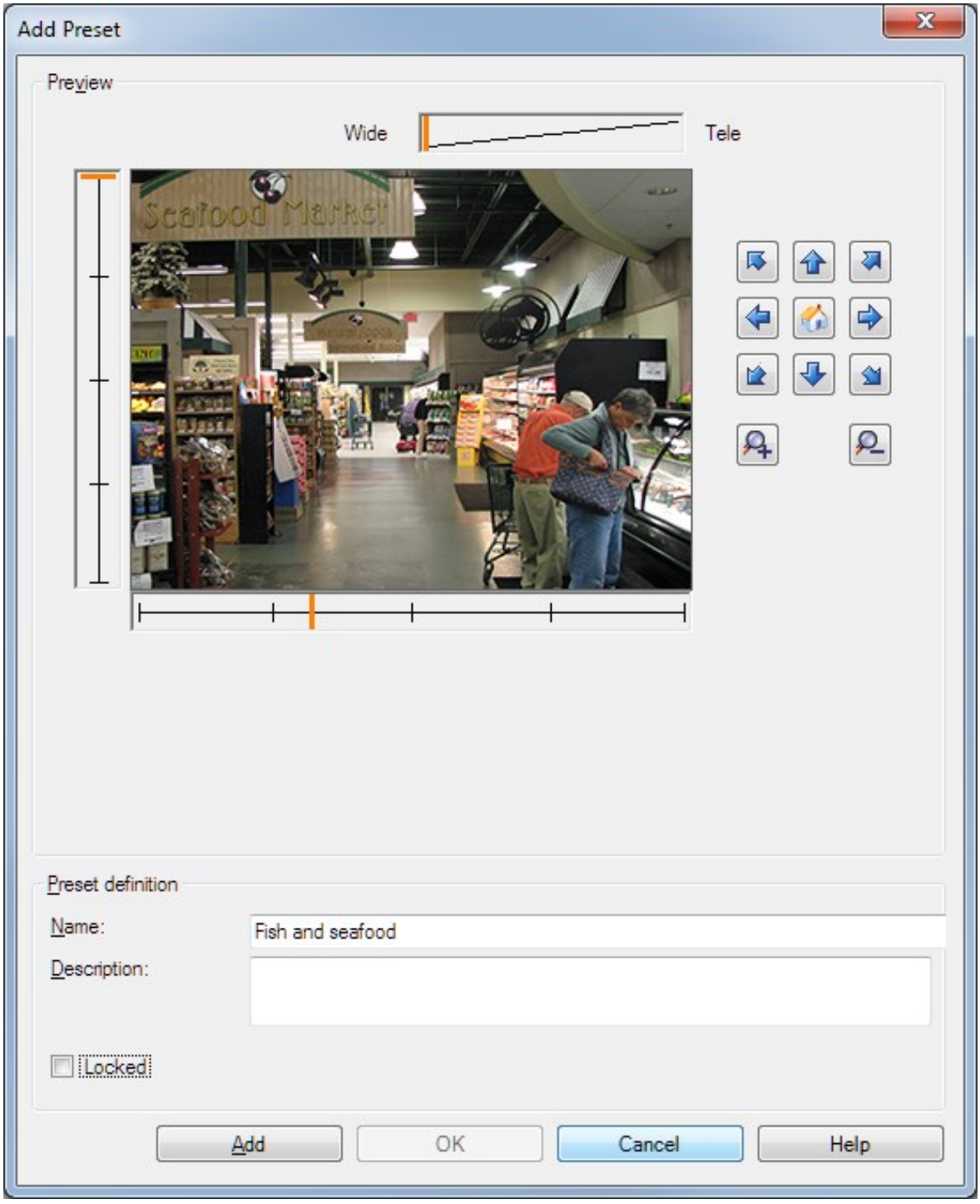
A posição predefinida inicial

Você define a posição predefinida inicial da câmera na página inicial da câmera. Os recursos PTZ disponíveis na página inicial dependem da câmera.

Adicionar uma posição predefinida (tipo 1)

Para adicionar uma posição predefinida para a câmera:

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Predefinições**, clique em **Novo**. A janela **Adicionar predefinição** aparece:



4. A janela **Adicionar predefinição** exibe uma imagem de visualização ao vivo da câmera. Use os botões de navegação e/ou os controles deslizantes para mover a câmera para a posição desejada.
5. Especifique um nome para a posição predefinida no campo **Nome**.
6. Opcionalmente, digite uma descrição de uma posição predefinida no campo **Descrição**.
7. Selecione **Locked** se você quiser bloquear a posição predefinida. Posteriormente, apenas usuários com permissões suficientes poderão desbloquear a posição.
8. Clique em **Adicionar** para especificar predefinições. Continue adicionando até que você tenha as predefinições que deseja.
9. Clique em **OK**. A janela **Adicionar predefinição** fecha e adiciona a posição na lista da guia **Predefinições** de posições predefinidas disponíveis para a câmera.

Usar posições predefinidas da câmera (tipo 2)

Como uma alternativa para especificar posições predefinidas no sistema, você pode especificar posições predefinidas para algumas câmeras PTZ na própria câmera. Você normalmente pode fazer isso acessando uma página da Web de configuração específica do produto.

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Predefinições**, selecione **Usar predefinições de dispositivo** para importar as predefinições para o sistema.

   Quaisquer predefinições que você já definiu para a câmera são excluídas e afetam todas as regras definidas e horários de patrulha, bem como removem as predefinições disponíveis para os usuários do XProtect Smart Client.
4. Clique em **Excluir** para eliminar as predefinições que seus usuários não precisam.
5. Clique em **Editar** se desejar alterar exibir nome da predefinição (consulte Renomear uma posição predefinida (tipo 2 somente)).
6. Se mais tarde você quiser editar essas predefinições definidas pelo dispositivo, edite na câmera e, em seguida, importe novamente.

Atribuir uma posição predefinida da câmera como padrão

Caso necessário, você pode atribuir uma das posições predefinidas de uma câmera PTZ como posição predefinida padrão da câmera.

Pode ser útil ter uma posição padrão predefinida, pois permite que você defina regras que especificam que a câmera PTZ deve ir para a posição predefinida padrão em circunstâncias especiais, por exemplo, depois de ter operado a câmera PTZ manualmente.

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Predefinições**, em **Posições predefinidas**, selecione a predefinição na lista de posições predefinidas definidas.
4. Selecione a caixa de seleção **Predefinição padrão** abaixo da lista.

Você só pode definir uma posição predefinida como a posição predefinida padrão.

Se você tiver selecionado **Usar predefinição padrão como posição inicial de PTZ** em **Opções** > **Geral**, o sistema usará a posição predefinida padrão em vez da posição inicial definida da câmera PTZ.

Especifique a predefinida padrão como a posição inicial PTZ

Usuários do Management Client e XProtect Smart Client com as permissões de usuário necessárias podem configurar o sistema para usar a posição predefinida padrão em vez da posição inicial de câmeras PTZ com o botão **Início** em um cliente.

Uma posição predefinida padrão precisa ser definida para a câmera. Se não houver uma posição predefinida estabelecida, nada acontecerá ao ativar o botão **Início** em um cliente.

Ativar configuração da posição inicial PTZ

1. Selecione **Ferramentas** > **Opções**.

2. Na guia **Geral**, no grupo **Servidor de gravação**, selecione **Usar predefinição padrão como posição inicial de PTZ**.

3. Atribua uma posição predefinida como a posição predefinida padrão para a câmera.

Para atribuir uma posição predefinida padrão, consulte Atribuir uma posição predefinida da câmera como padrão na página 254

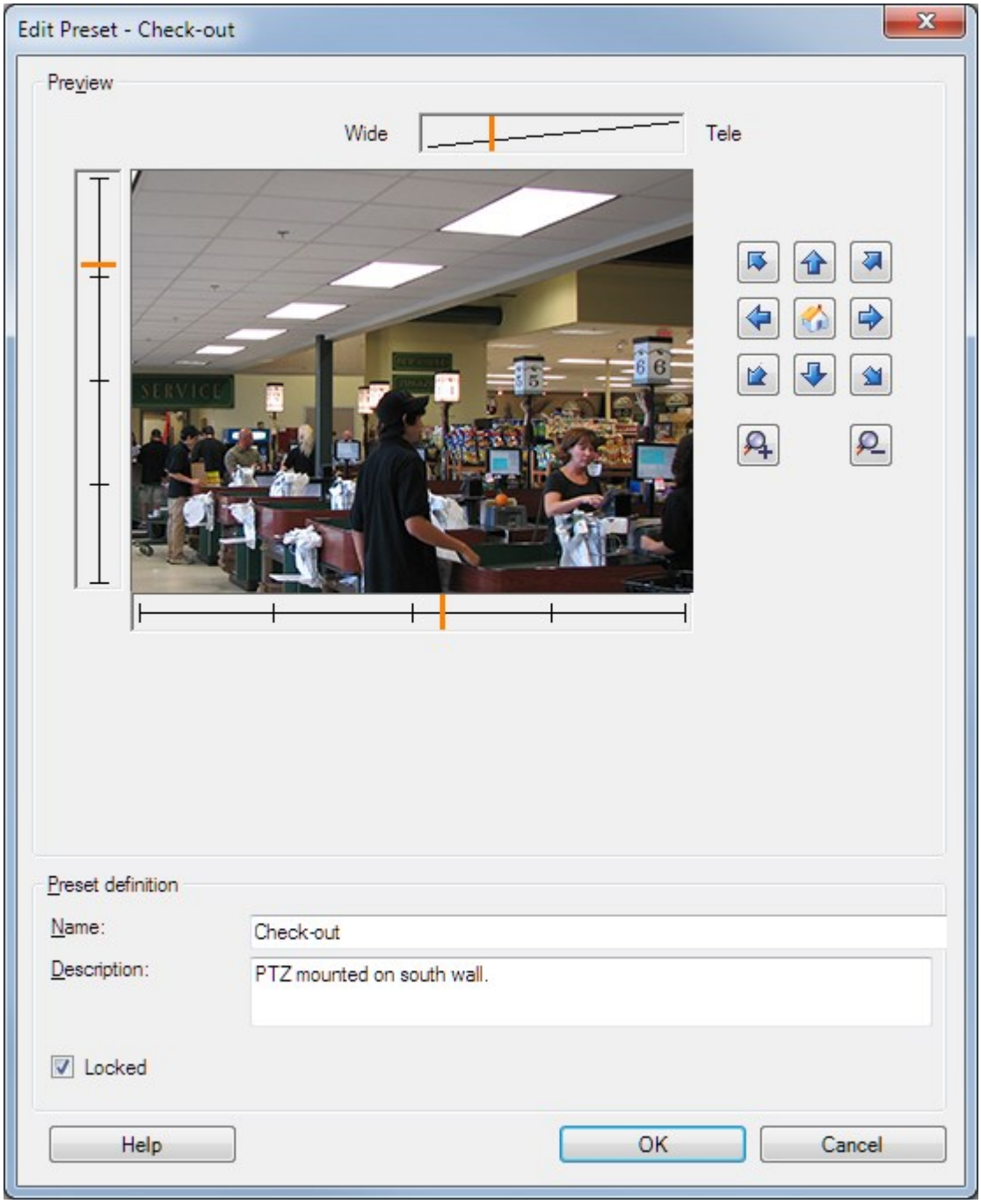
Consulte também Configurações do sistema (caixa de diálogo Opções) na página 393

Editar uma posição predefinida para uma câmera (somente tipo 1)

Para editar uma posição predefinida existente definida no sistema:

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione a câmera relevante.
3. Selecione a posição predefinida na lista da guia **Predefinições** de posições predefinidas disponíveis para a câmera.

4. Clique em **Editar**. Isso abre a janela **Editar predefinição**:



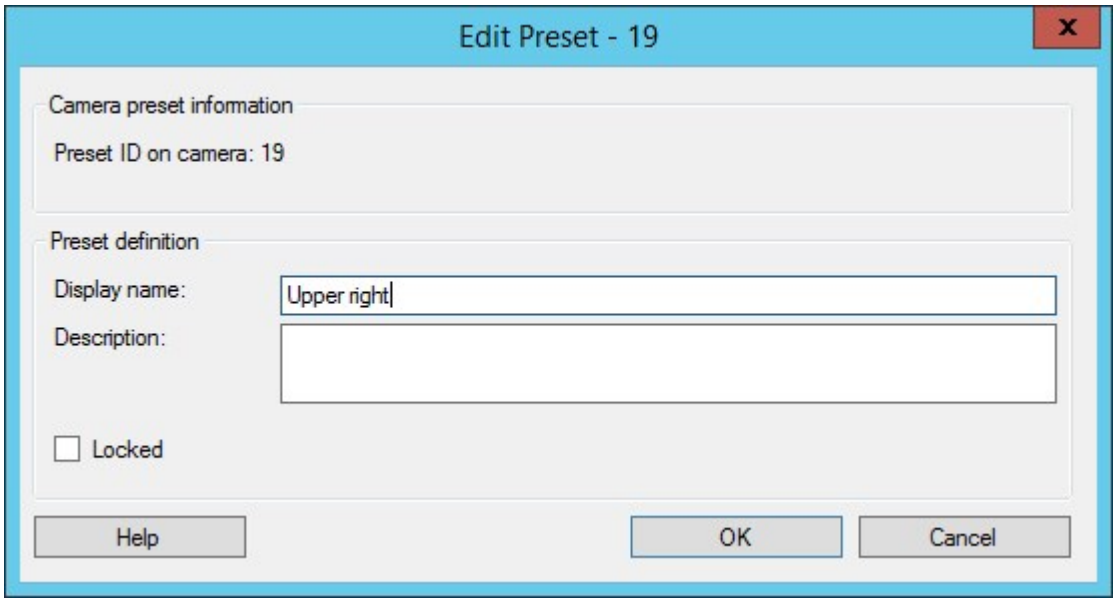
5. A janela **Editar predefinição** exibe uma imagem de visualização ao vivo da posição predefinida. Use os botões de navegação e/ou os controles deslizantes para alterar a posição predefinida conforme necessário.
6. Alterar o nome/número e a descrição da posição predefinida, se necessário.

7. Selecione **Locked** se você quiser bloquear a posição predefinida. Posteriormente, apenas usuários com permissões suficientes poderão desbloquear a posição.
8. Clique em **OK**.

Alterar o nome de uma posição predefinida (somente tipo 2)

Para editar o nome de uma posição predefinida estabelecida na câmera:

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Selecione a posição predefinida na lista da guia **Predefinições** de posições predefinidas disponíveis para a câmera.
4. Clique em **Editar**. Isso abre a janela **Editar predefinição**:



5. Alterar o nome e adicionar a descrição da posição predefinida, se necessário.
6. Selecione **Bloqueado** para bloquear o nome predefinido. Você pode bloquear um nome predefinido se quiser impedir que usuários no XProtect Smart Client ou usuários com permissões de segurança limitadas atualizem ou excluam uma predefinição. Predefinições bloqueadas são assinaladas com este ícone . Posteriormente, apenas usuários com permissões suficientes poderão desbloquear o nome predefinido.
7. Clique em **OK**.

Testar uma posição predefinida (somente tipo 1)

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Selecione a posição predefinida na lista da guia **Predefinições** de posições predefinidas disponíveis para a câmera.
4. Clique em **Ativar**.
5. A câmera se move para a posição predefinida selecionada.

Dispositivos - Patrulha

Perfis de patrulhamento e patrulhamento manual (explicado)

Perfis de patrulhamento são as definições de como o patrulhamento deve ocorrer. Isso inclui a ordem em que a câmera deve se mover entre as posições predefinidas e por quanto tempo ela deve permanecer em cada posição. Você pode criar um número irrestrito de perfis de patrulhamento e usá-los em suas regras. Por exemplo, você pode criar uma regra especificando que um perfil de patrulhamento deve ser usado durante o horário de funcionamento diurno e outro durante as noites.

Patrulha manual

Antes de aplicar um perfil de patrulha em uma regra, por exemplo, você pode testar o perfil de patrulha usando a patrulha manual. Você também pode usar a patrulha manual para assumir o controle da patrulha de outro usuário ou de uma patrulha ativada por regra, desde que você tem uma prioridade PTZ maior.

Se a câmera já está patrulhando ou controlada por outro usuário, você só pode iniciar o patrulhamento manual, se tiver prioridade mais alta.

Se você iniciar uma patrulha manual enquanto a câmera executa uma patrulha ativada por regra do sistema, esta é retomada pelo sistema quando você termina sua patrulha manual. Se outro usuário executa um patrulhamento manual, mas você tem prioridade maior e inicia sua patrulha manual, a do outro usuário não é retomada quando você termina.

Se você não parar sua patrulha manual, ela continuará até que uma patrulha baseada em regra ou um usuário com prioridade mais alta assuma. Quando a patrulha baseado em regra do sistema para, o sistema retoma o seu patrulhamento manual. Se outro usuário inicia uma patrulha manual, a sua patrulha manual para e não será retomada.

Quando você interromper seu patrulhamento manual e definir uma posição final para o seu perfil de patrulha, a câmera retornará para esta posição.

Adicionar um perfil de patrulha

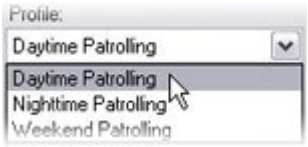
> Antes que você possa trabalhar com o patrulhamento, especifique pelo menos duas posições predefinidas para a câmera na guia **Predefinições**, consulte Adicionar uma posição predefinida (type 1).

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Patrulhamento**, clique em **Adicionar**. A caixa de diálogo **Adicionar perfil** aparece.
4. Na caixa de diálogo **Adicionar perfil**, especifique um nome para o perfil de patrulha.
5. Clique em **OK**. O botão está desabilitado se o nome não é único.

O novo perfil de patrulha é adicionado à lista **Perfis**. Agora você pode especificar as posições predefinidas e outras configurações para o perfil de patrulha.

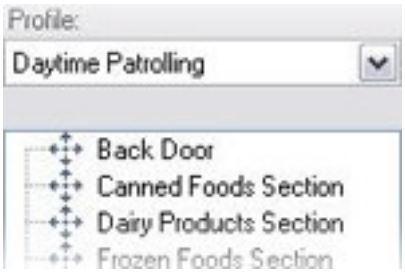
Especificar posições predefinidas em um perfil de patrulha

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Patrulhamento**, selecione o perfil de patrulhamento na lista **Perfil**:



4. Clique em **Adicionar**.
5. Na caixa de diálogo **Selecionar predefinição de PTZ**, selecione as posições predefinidas para o seu perfil de patrulhamento:

6. Clique em **OK.** As posições predefinidas selecionadas são adicionadas à lista de posições predefinidas para o perfil de patrulhamento:



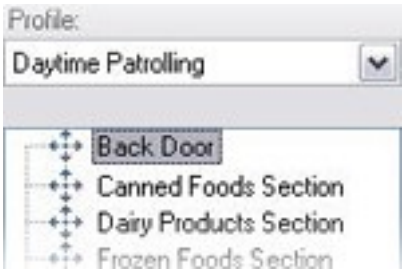
7. A câmera utiliza a posição predefinida no topo da lista como a primeira parada quando patrulha de acordo com o perfil de patrulhamento. A posição predefinida na segunda posição do topo é a segunda parada, e assim por diante.

Especificar o tempo em cada posição predefinida

Ao patrulhar, a câmera PTZ, por padrão, permanece por 5 segundos em cada posição predefinida especificada no perfil de patrulha.

Para alterar o número de segundos:

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Patrulhamento**, selecione o perfil de patrulhamento na lista **Perfil**.
4. Selecione a posição predefinida para a qual você deseja alterar o tempo:



5. Especifique o tempo no campo **Tempo na posição (seg)**.
6. Se necessário, repita para outras posições predefinidas.

Personalizar transições (PTZ)

Por padrão, o tempo necessário para mover a câmera de uma posição predefinida para outra, conhecido como **transição**, é de aproximadamente três segundos. Durante este tempo, a detecção de movimento é, por padrão, desativada na câmera, porque o movimento irrelevante é, caso contrário, possível de ser detectado enquanto a câmera se move entre as posições predefinidas.

Só é possível personalizar a velocidade para as transições se sua câmera suportar digitalização PTZ e for do tipo em que as posições predefinidas são configuradas e armazenadas no servidor do seu sistema (câmera PTZ do tipo 1). Caso contrário, a barra de **Velocidade** ficará indisponível.

Podem ser personalizados:

- O tempo de transição estimado
- A velocidade com a qual a câmera se move durante uma transição

Para personalizar as transições entre as diferentes posições predefinidas:

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Patrulhamento**, na lista **Perfil**, selecione o perfil de patrulhamento.
4. Selecione a caixa **Personalizar transições**.

   As indicações de transição são adicionadas à lista de posições predefinidas.
5. Na lista, selecione a transição.

6. Especifique o tempo de transição estimado (em número de segundos) no campo **Tempo previsto (seg)**.

7. Use o controle deslizante **Velocidade** para especificar a velocidade de transição. Quando o controle deslizante está na sua posição mais à direita, a câmera move-se com a velocidade padrão. Quanto mais você mover o controle deslizante para a esquerda, mais lenta a câmera se moverá durante a transição selecionada.
8. Repita como solicitado para outras transições.

Especificar uma posição final em patrulha

Você pode especificar que a câmera deve se mover para uma posição predefinida específica quando patrulhar de acordo com o final do perfil de patrulhamento selecionado.

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Na guia **Patrulhamento**, na lista **Perfil**, selecione o perfil de patrulhamento relevante.
4. Selecione a opção **Ir para posição específica ao concluir**. Isso abre a caixa de diálogo **Selecionar predefinição**.
5. Selecione a posição final e clique em **OK**.

   Você pode selecionar qualquer posição predefinida da câmera como posição final, você não está limitado às posições predefinidas usadas no perfil de patrulhamento.

6. A posição final selecionada é adicionada à lista de perfis.

Ao patrulhar de acordo com o final do perfil de patrulhamento selecionado, a câmera se move para a posição final especificada.

Reservar e liberar sessões PTZ

Dependendo do seu sistema de monitoramento, você pode reservar sessões PTZ.

Administradores com direitos de segurança para executar uma sessão de PTZ reservada podem usar a câmera PTZ neste modo. Isso impede outros usuários de tomarem o controle sobre a câmera. Em uma sessão de PTZ reservada, o sistema de prioridade PTZ padrão é desconsiderado para evitar que usuários com maior prioridade PTZ interrompam a sessão.

Você pode operar a câmera em uma sessão PTZ reservada do XProtect Smart Client e do Management Client.

Reservar uma sessão PTZ pode ser útil se você precisa fazer atualizações urgentes ou manutenção de uma câmera PTZ ou de suas predefinições sem ser interrompido por outros usuários.

Reservar uma sessão PTZ

1. No painel **Navegação do site**, selecione **Dispositivos** e, em seguida, selecione **Câmeras**.
2. No painel **Visão geral**, selecione o PTZ relevante.
3. Selecione a sessão PTZ na guia **Predefinições** e clique em **Reservado**.

Você não pode iniciar uma sessão de PTZ reservada se um usuário com prioridade maior do que a sua estiver controlando a câmera ou se outro usuário já reservou a câmera.

Liberar uma sessão de PTZ

O botão **Liberar** permite que você libere sua sessão PTZ atual para outro usuário poder controlar a câmera. Quando você clica em **Liberar**, a sessão PTZ termina imediatamente e estará disponível para o primeiro usuário operar a câmera.

Os administradores atribuídos com a permissão de segurança **Liberar sessão PTZ** têm permissão para liberar a sessão PTZ reservada de outros usuários a qualquer momento. Isto pode ser útil, por exemplo, em ocasiões em que você precisa manter a câmera PTZ ou suas predefinições ou quando outros usuários acidentalmente bloquearam a câmera em situações de urgência.

Especificar tempo limite das sessões PTZ

Management Client e usuários do XProtect Smart Client com as permissões de usuário necessárias pode interromper manualmente o patrulhamento de câmeras PTZ.

Você pode especificar quanto tempo deve decorrer antes do patrulhamento regular ser retomado em todas as câmeras PTZ do seu sistema:

1. Selecione **Ferramentas** > **Opções**.
2. Na guia **Geral** da janela **Opções**, selecione a quantidade de tempo na:
   - Lista dos **tempos limite de pausa das sessões de PTZ** (o padrão é 15 segundos).
   - Lista dos **tempos limite de pausa das sessões de patrulha** (o padrão é 10 minutos).
   - Lista dos **tempos limite das sessões de PTZ reservadas** (o padrão é 1 hora).

   A configuração se aplica a todas as câmeras PTZ do seu sistema.

É possível alterar os limites de tempo individualmente para cada câmera.

1. No painel **Navegação do site**, selecione **Câmera**.
2. No painel Visão geral, selecione a câmera.
3. Na guia **Predefinições**, selecione a quantidade de tempo na:
   - Lista do **tempo limite de pausa das sessões de PTZ** (o padrão é 15 segundos).
   - Lista dos **tempos limite de pausa das sessões de patrulha** (o padrão é 10 minutos).
   - Lista dos **tempos limite das sessões de PTZ reservadas** (o padrão é 1 hora).

   As configurações se aplicam apenas a esta câmera.

Dispositivos - Eventos para regras

Adicionar ou excluir um evento para um dispositivo

Adicionar um Evento de

1. No painel **Visão geral**, selecione o dispositivo.
2. Selecione a guia **Eventos** e clique em **Adicionar**. Isso abre a janela **Selecionar driver de evento**.
3. Selecione um evento. Você só pode selecionar um evento de cada vez.
4. Se desejar ver uma lista completa de todos os eventos, permitindo adicionar eventos que já foram adicionados, selecione **Mostrar eventos já adicionados**.
5. Clique em **OK**.
6. Na barra de ferramentas, clique em **Salvar**.

Excluir um evento

Apagar um evento afeta todas as regras que o usam.

1. No painel **Visão geral**, selecione o dispositivo.
2. Selecione a guia **Eventos** e clique em **Excluir**.

Especificar as propriedades de evento

Para cada evento adicionado, você pode especificar as propriedades. O número de propriedades depende do dispositivo e do evento. Para o evento funcionar como esperado, algumas ou todas as propriedades devem ser especificadas de forma idêntica no dispositivo e na guia **[Eventos]**.

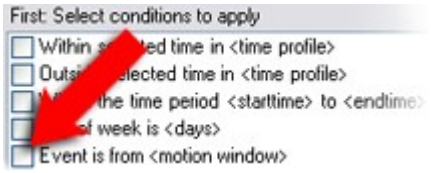
Usar várias instâncias de um evento

Para poder especificar propriedades diferentes para diferentes ocorrências de um evento, você pode adicionar um evento mais do que uma vez.

O exemplo seguinte é específico para câmeras.

Exemplo: Você configurou a câmera com duas janelas de movimento, chamado de A1 e A2. Você adicionou duas instâncias para o evento Movimento iniciado (HW). Nas propriedades de uma ocorrência, você especificou o uso da janela de movimento A1. Nas propriedades da outra ocorrência, você especificou o uso da janela de movimento A2.

Quando você usa o evento em uma regra, você pode especificar que o evento deve ser baseado em detecção de movimento em uma janela de movimento específica para que a regra seja acionada:



Dispositivos - Máscaras de privacidade

Ativar/desativar a máscara de privacidade

O recurso de máscara de privacidade está desativado por padrão.

Para ativar / desativar o recurso de máscara de privacidade para uma câmera:

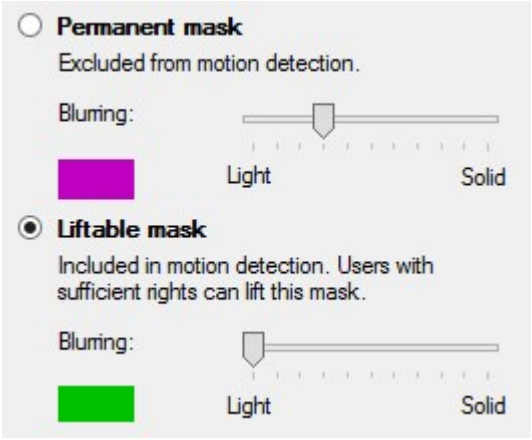
1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione o dispositivo de câmera relevante.
3. Na guia **Máscara de privacidade**, marque ou desmarque a caixa de seleção **Máscara de privacidade**.

> Em uma configuração Milestone Interconnect, a central de controle desconsidera as máscaras de privacidade definidas em uma base remota. Se você deseja aplicar as mesmas máscaras de privacidade, você deve redefini-las na central de controle.

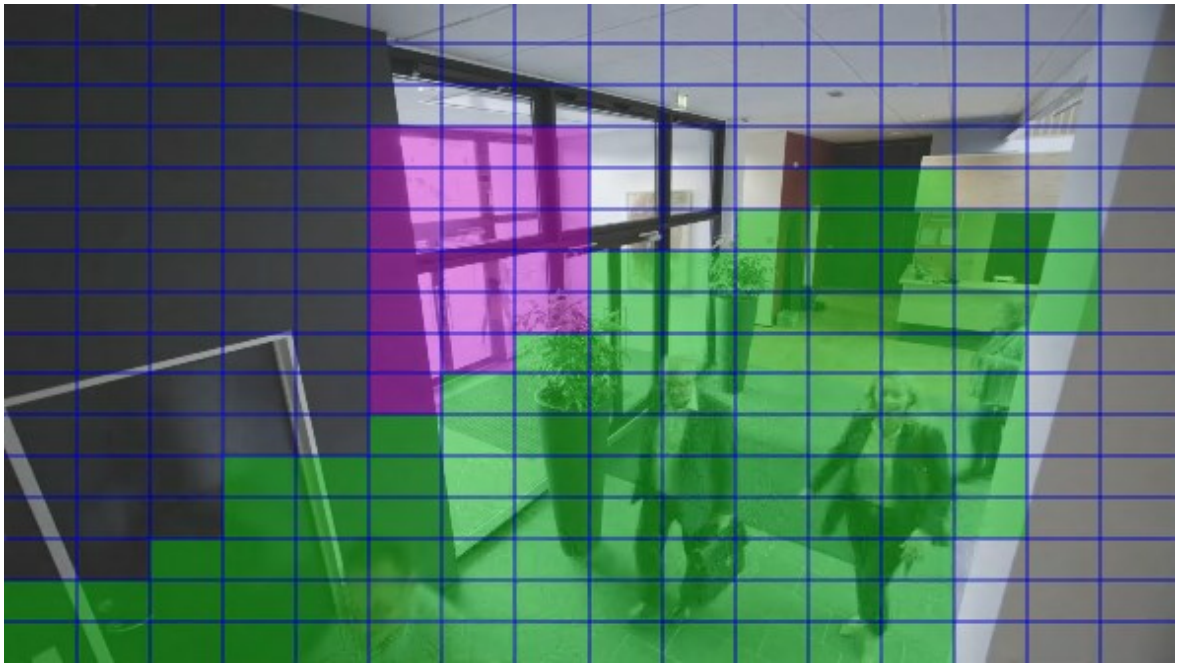
Definir máscaras de privacidade

Quando você ativa o recurso de máscara de privacidade na guia **Máscara de privacidade**, uma grade é aplicada na visualização de câmera.

1. No painel **Navegação do site**, selecione **Dispositivos**.
2. No painel **Visão geral**, selecione a câmera relevante.
3. Na guia **Máscara de privacidade**, para cobrir uma área com uma máscara de privacidade, primeiro selecione **Máscara permanente** ou **Máscara removível** para definir se deseja uma máscara de privacidade permanente ou removível.



4. Arraste o ponteiro do mouse sobre a visualização. Clique com o botão esquerdo do mouse para selecionar uma célula da grade. Clique com o botão direito do mouse para limpar uma célula da grade.
5. Você pode definir quantas áreas de máscara de privacidade forem necessárias. Áreas com máscaras de privacidade permanentes aparecem em roxo e áreas com máscaras de privacidade removíveis, em verde.



6. Defina como a cobertura das áreas deve aparecer no vídeo quando exibido nos clientes. Use os controles deslizantes para passar de um desfoque leve para uma máscara não transparente completa.

   As máscaras de privacidade permanentes também aparecem na guia **Movimento**.

7. No XProtect Smart Client, verifique se as máscaras de privacidade aparecem conforme você definiu.

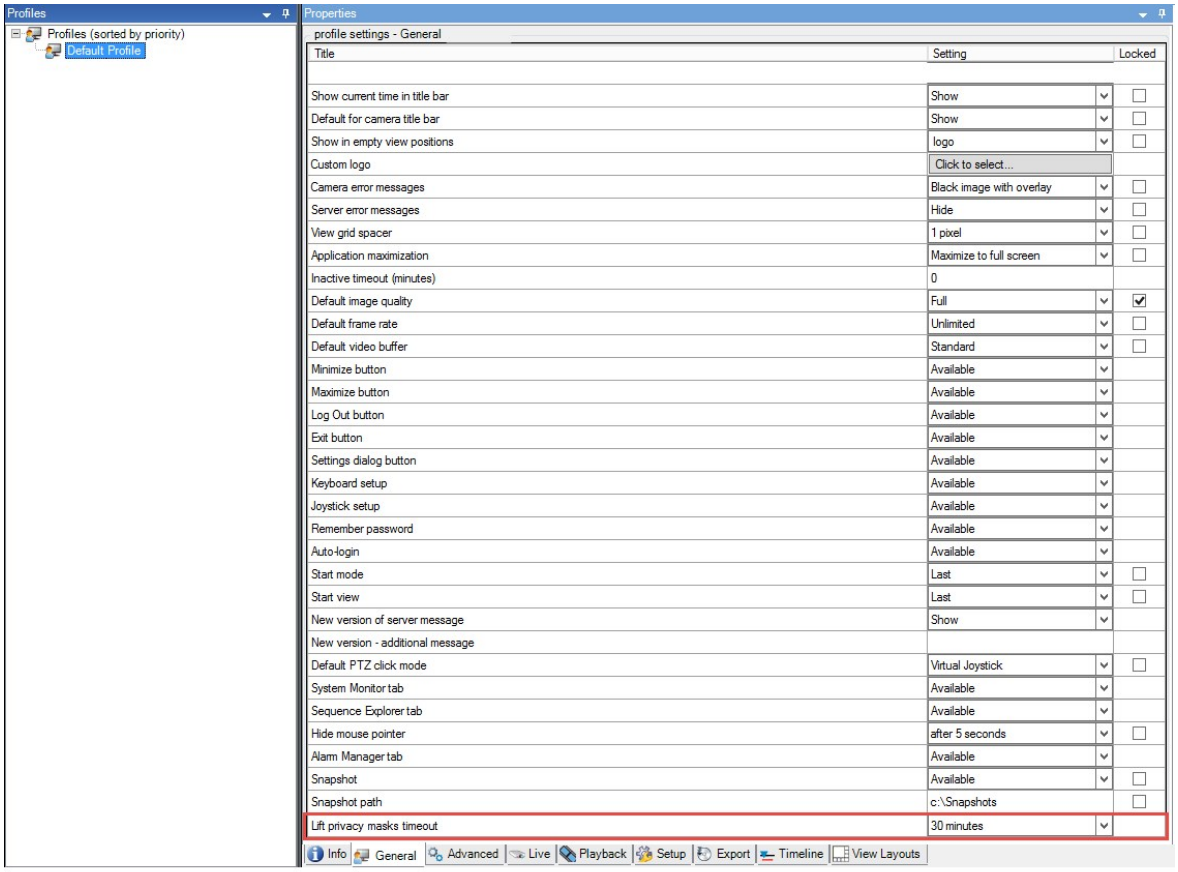
Alterar o tempo limite para máscaras de privacidade removidas

Por padrão, máscaras de privacidade são removidas por 30 minutos no XProtect Smart Client e depois aplicadas automaticamente, mas você pode alterar isso.

Quando você alterar o tempo limite, lembre-se de fazê-lo para o perfil Smart Client associado à função que tenha a permissão para remover máscaras de privacidade.

Para alterar o tempo limite:

1. Em **Smart Client Perfis**, selecione o perfil Smart Client relevante.
2. Na guia **Geral**, localize **Remover tempo limite de máscaras de privacidade**.



3. Selecione entre os valores:
   - **2 minutos**
   - **10 minutos**
   - **30 minutos**
   - **1 hora**
   - **2 horas**
   - **Até a desconexão**
4. Clique em **Salvar**.

Dar aos usuários permissão para remover máscaras de privacidade

Por padrão, nenhum usuário tem permissões para remover máscaras de privacidade no XProtect Smart Client.

Para ativar/desativar a permissão:

1. No painel **Navegação do site**, selecione **Segurança** e então selecione **Funções**.
2. Selecione a função à qual você deseja dar permissão para remover máscaras de privacidade.
3. Na guia **Segurança geral**, selecione **Câmeras**.
4. Marque a caixa de seleção **Permitir** para a permissão de **Remover máscaras de privacidade**.

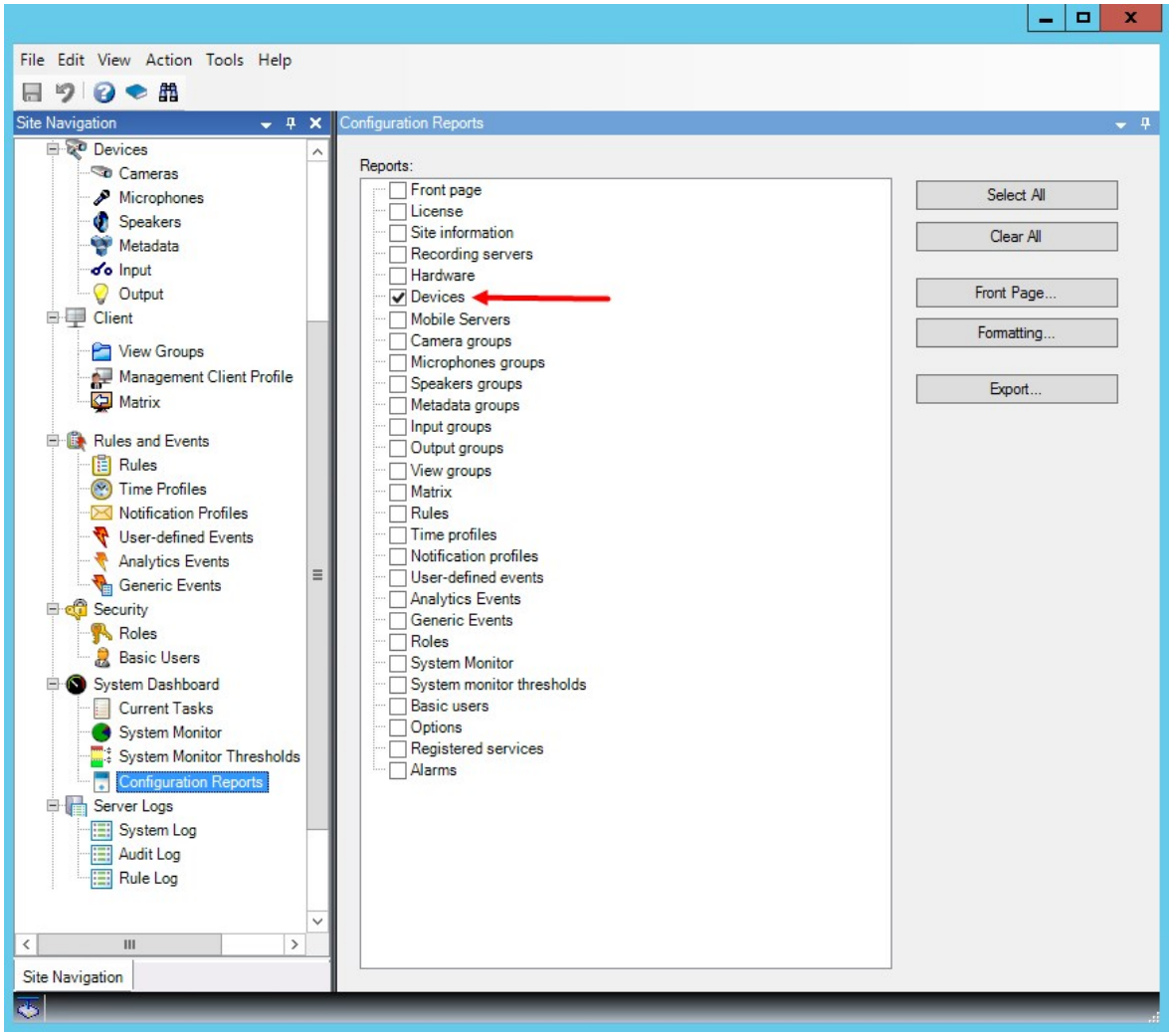
Os usuários aos quais você atribuir essa função podem remover máscaras de privacidade configuradas como máscaras removíveis para si próprios e também autorizar a remoção para outros usuários XProtect Smart Client.

Gere um relatório da configuração da máscara de privacidade

O relatório de dispositivos inclui informações sobre as configurações atuais de máscara de privacidade das câmeras.

Para configurar um relatório:

1. No painel **Navegação do site**, selecione **Painel de controle do sistema**.
2. Em **Relatórios de configuração**, selecione o relatório de **Dispositivos**.



3. Se você quiser modificar o relatório, pode alterar a página inicial e o formato.
4. Clique em **Exportar**, e o sistema gera o relatório como um arquivo PDF.

Para obter mais informações sobre relatórios, consulte Imprima um relatório com a configuração do seu sistema na página 308.

Clientes

Grupos de visualização (explicado)

A forma em que o sistema apresenta de vídeo de uma ou mais câmeras de clientes é chamado de visão. Um grupo de visão é um recipiente para um ou mais grupos lógicos de tais visões. Em clientes, um grupo de visão é apresentado como uma pasta expansível a partir da qual os usuários podem selecionar o grupo e a visão

que eles querem ver:

Exemplo de XProtect Smart Client: A seta indica um grupo de visão, que contém um grupo lógico (chamado Amenidades), que por vez contém 3 visualizações.

Por padrão, cada função que você definir no Management Client também é criada como um grupo de visão. Ao adicionar uma função no Management Client, a função, por padrão, aparece como um grupo de visão para uso em clientes.

- Você pode atribuir um grupo de visão com base em uma função para usuários / grupos atribuídos à função relevante. Você pode alterar essas permissões do grupo de visualização configurando isso na função posteriormente
- Um grupo de visão com base em uma função leva o nome da função.

  Exemplo: Se você criar uma função com o nome **Equipe de segurança do prédio A**, ela aparece no XProtect Smart Client como um grupo de visualização chamado **Equipe de segurança do prédio A**.

  Além dos grupos de visão que você adquire ao adicionar funções, você pode criar quantos grupos de visão desejar. Você pode também excluir grupos de visão, incluindo aqueles automaticamente criados quando adicionadas funções
- Mesmo que um grupo de visualização seja criado cada vez que você adicionar uma função, os grupos de visão não têm que corresponder às funções. Você pode adicionar, renomear ou remover qualquer um dos grupos de visão, caso necessário

> Se você mudar o nome de um grupo de visualização, os usuários do cliente já conectados devem sair e entrar no sistema novamente antes que a mudança de nome fique visível.

Adicionar um grupo de visão

1. Clique com o botão direito em **Grupos de visão** e selecione **Adicionar grupo de visão**. Isso abre a caixa de diálogo **Adicionar grupo de visão**.
2. Digite o nome e uma descrição opcional do novo grupo de visualização e clique em **OK**.

Nenhuma função pode usar o grupo de visão recém-adicionado até que você especifique essas permissões. Se você tiver especificado quais funções podem utilizar o grupo de visão recém-adicionado, os usuários clientes que já estejam conectados com as funções relevantes devem sair e entrar no sistema novamente antes que eles possam ver o grupo de visão.

Smart Client profiles

Adicionar e configurar um perfil do Smart Client

Você deve criar um perfil do Smart Client para que possa configurá-lo.

1. Clique com o botão direito em **Smart Client Perfis**.
2. Selecione **Adicionar perfil Smart Client**.
3. Na caixa de diálogo **Adicionar perfil Smart Client**, digite um nome e uma descrição do novo perfil e clique em **OK**.
4. No painel **Visão geral**, clique no perfil que você criou para configurá-lo.
5. Ajuste as configurações em uma, várias ou todas as guias e clique **OK**.

Copiar um perfil do Smart Client

Se você tiver um perfil Smart Client com configurações ou permissões complicadas e precisar de um perfil semelhante, pode ser mais fácil copiar um perfil já existente e fazer pequenos ajustes na cópia do que criar um novo perfil do zero.

1. Clique em **Perfis Smart Client**, clique com o botão direito no perfil no painel **Visão geral** e selecione **Copiar perfil Smart Client**.
2. Na caixa de diálogo que aparece, dê ao perfil copiado um novo nome único e descrição. Clique em **OK**.
3. No painel **Visão geral**, clique no perfil que você acabou de criar para configurá-lo. Isto é feito ajustando as configurações em uma, mais ou todas as guias disponíveis. Clique em **OK**.

Criar e configurar perfis do Smart Client, perfis de funções e de tempo

Quando você trabalha com perfis do Smart Client, é importante compreender a interação entre os perfis do Smart Client, funções e perfis de tempo:

- Perfis Smart Client lidam com as configurações de permissão do usuário no XProtect Smart Client
- As funções lidam com as configurações de segurança em clientes, MIP SDK e mais
- Perfis de tempo lidam com aspectos de tempo de dois tipos de perfis

Juntos, esses três recursos fornecem controle exclusivo e possibilidades de personalização em relação às permissões do usuário XProtect Smart Client.

Exemplo: Você precisa de um usuário na configuração do XProtect Smart Client que só deve ser autorizado a visualizar o vídeo ao vivo (sem reprodução) de câmeras selecionadas, e apenas durante o horário normal de trabalho (das 8h às 16h). Uma maneira de configurar isso seria da seguinte maneira:

1. Crie um perfil do Smart Client e dê um nome a ele, por exemplo, **Somente ao vivo**.
2. Especifique as configurações de tempo real/reprodução necessárias em **Somente tempo real**.
3. Crie um perfil de tempo e dê um nome a ele, por exemplo, **Somente durante o dia**.
4. Especifique o período de tempo necessário em **Somente durante o dia**.
5. Crie uma nova função e dê um nome a ela, por exemplo, **Guarda (câmeras selecionadas)**.
6. Especifique quais câmeras o **Guarda (câmeras selecionadas)** pode usar.
7. Atribua o perfil Smart Client **Somente ao vivo** e o perfil de tempo **Somente durante** o dia à função **Guarda (câmeras selecionadas)** para conectar os três elementos.

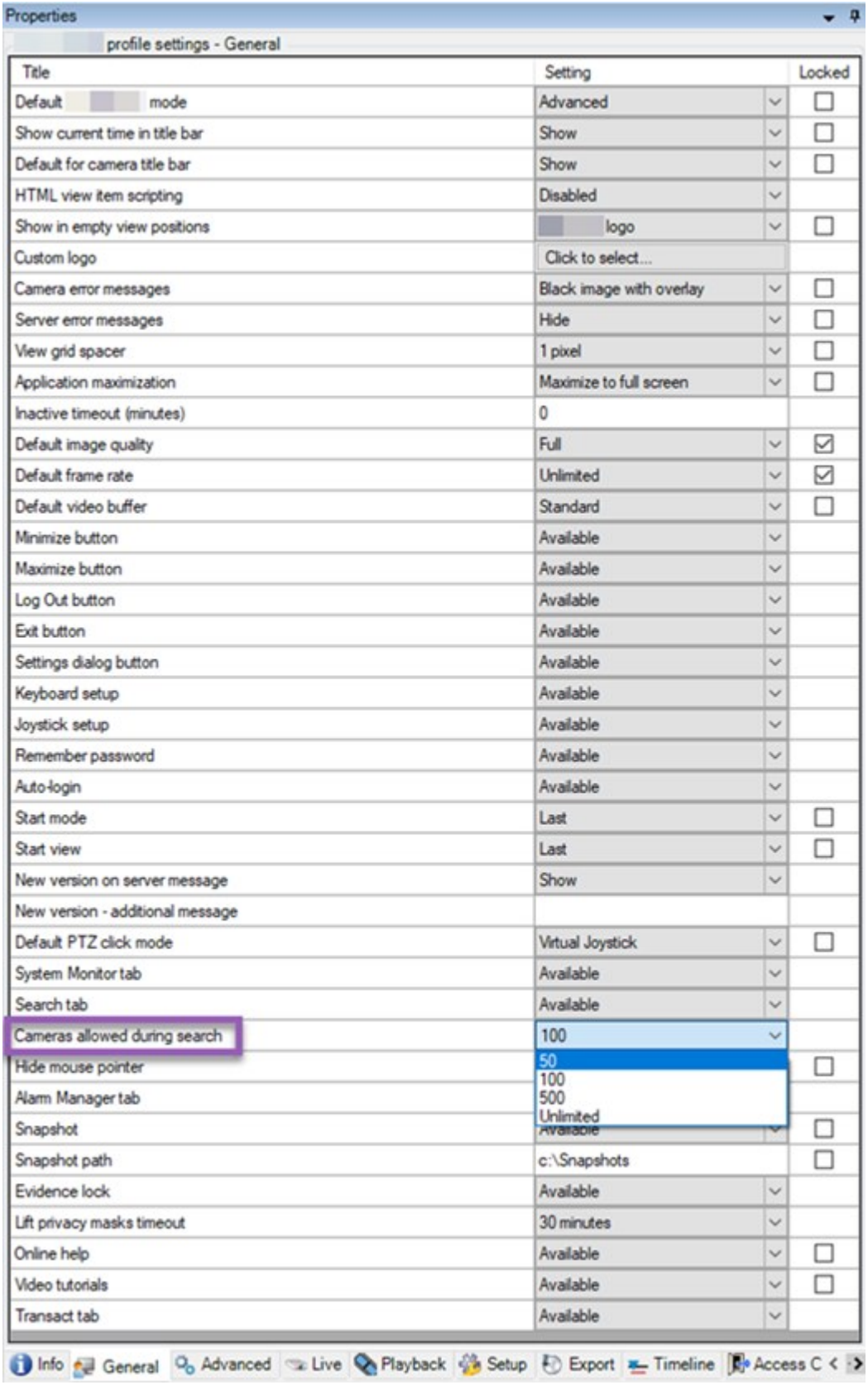
Você agora tem uma mistura de três recursos criando o resultado desejado e permitindo-lhe facilmente realizar ajustes e sintonia fina. Você pode fazer a instalação em uma ordem diferente, por exemplo, criar a função primeiro e depois o perfil do Smart Client e o perfil de tempo, ou qualquer outra ordem que preferir.

Definir o número de câmeras permitidas durante a pesquisa

Você pode configurar quantas câmeras os operadores podem adicionar a uma pesquisa no XProtect Smart Client. O valor padrão é **100**. Ao exceder o limite da câmera o operador recebe um aviso.

1. Em XProtect Management Client, expanda **Cliente** > **Smart Client Perfis**.
2. Selecione o perfil relevante.

3. Clique na guia **Geral**.


Properties
profile settings - General
Title
Setting
Locked
Default mode
Advanced
Show current time in title bar
Show
Default for camera title bar
Show
HTML view item scripting
Disabled
Show in empty view positions
logo
Custom logo
Click to select...
Camera error messages
Black image with overlay
Server error messages
Hide
View grid spacer
1 pixel
Application maximization
Maximize to full screen
Inactive timeout (minutes)
0
Default image quality
Full
Default frame rate
Unlimited
Default video buffer
Standard
Minimize button
Available
Maximize button
Available
Log Out button
Available
Exit button
Available
Settings dialog button
Available
Keyboard setup
Available
Joystick setup
Available
Remember password
Available
Auto-login
Available
Start mode
Last
Start view
Last
New version on server message
Show
New version - additional message
Default PTZ click mode
Virtual Joystick
System Monitor tab
Available
Search tab
Available
Cameras allowed during search
100
50
100
500
Unlimited
Hide mouse pointer
Alarm Manager tab
Snapshot
Snapshot path
c:\Snapshots
Evidence lock
Available
Lift privacy masks timeout
30 minutes
Online help
Available
Video tutorials
Available
Transact tab
Available
Info
General
Advanced
Live
Playback
Setup
Export
Timeline
Access C

4. Nas **Câmeras** permitidas durante a pesquisa, selecione um dos seguintes valores:
    - **50**
    - **100**
    - **500**
    - **Irrestrito**
5. Salve suas alterações.

Alterar as configurações de exportação padrão

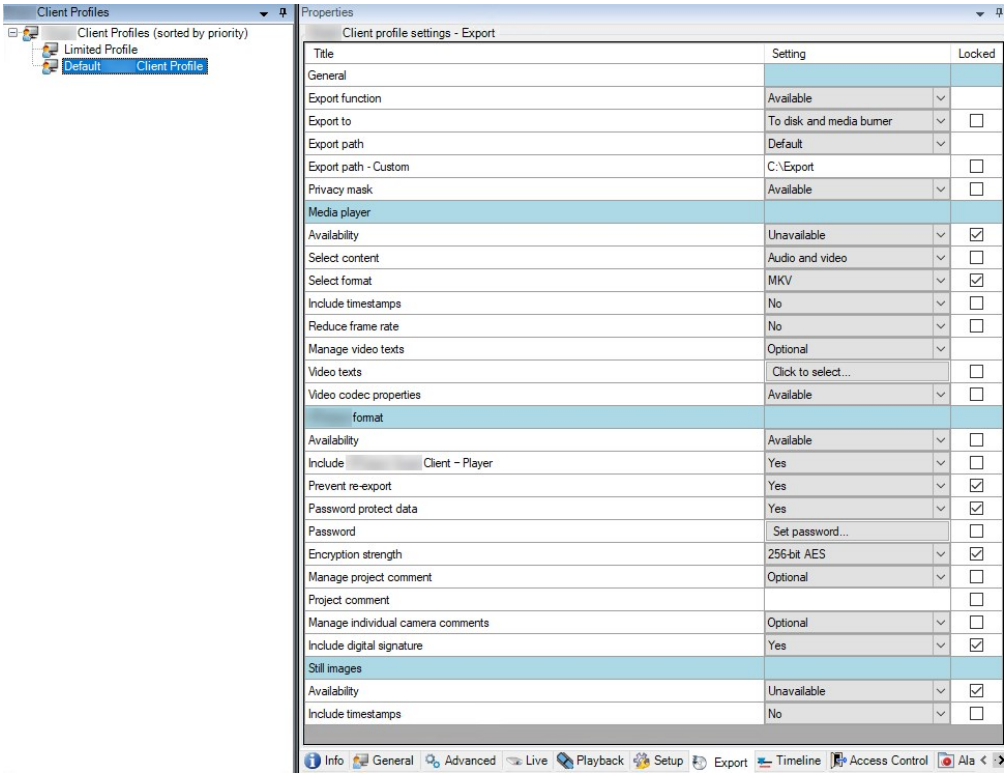
Quando você instala seu sistema VMS XProtect, as configurações de exportação padrão que definem as opções de exportação no XProtect Smart Client são restritas para garantir o mais alto nível de segurança. Você pode alterar essas configurações para dar mais opções aos operadores.

Configurações padrão

- Apenas o formato XProtect está disponível
    - A reexportação está impedida
    - As exportações são protegidas por senha
    - Criptografia AES de 256 bits
    - Assinaturas digitais são adicionadas
- Não é possível exportar para o formato MKV ou o formato AVI
- Não é possível exportar imagens estáticas

Etapas:

1. Em XProtect Management Client, expanda **Cliente** > **Smart Client Perfis**.
2. Selecione **Perfil Smart Client padrão**.
3. No painel **Propriedades**, selecione a guia **Exportar**.



4. Para disponibilizar um formato restrito no XProtect Smart Client, encontre a configuração e selecione **Disponível**.
5. Para permitir que os operadores alterem uma configuração no XProtect Smart Client, desmarque a caixa de seleção **Bloqueado** ao lado da configuração relevante.
6. Se for relevante, altere outras configurações.
7. (opcional) Faça login no XProtect Smart Client para verificar se suas configurações foram aplicadas.

Management Client profiles

Adicionar e configurar um perfil do Management Client

Se não quiser usar o perfil padrão, você pode criar um perfil de Management Client para configurá-lo.

1. Clique com o botão direito em **Management Client Perfis**.
2. Selecione **Adicionar perfil Management Client**.
3. Na caixa de diálogo **Adicionar perfil Management Client**, digite um nome e uma descrição do novo perfil e clique em **OK**.
4. No painel **Visão geral**, clique no perfil que você criou para configurá-lo.
5. Na guia **Perfil**, selecione ou limpe a funcionalidade do perfil do Management Client.

Copiar um perfil do Management Client

Se tiver um perfil do Management Client com configurações que você gostaria de reutilizar, é possível copiar um perfil já existente e fazer pequenos ajustes na cópia em vez de criar um novo perfil desde o início.

1. Clique em **Perfil Management Client**, clique com o botão direito no perfil no painel **Visão geral** e selecione **Copiar perfil Management Client**.
2. Na caixa de diálogo que aparece, dê ao perfil copiado um novo nome único e descrição. Clique em **OK**.
3. No painel **Visão geral**, clique no perfil e vá para a aba **Informações** ou aba **Perfil** para configurá-lo.

Gerenciar a visibilidade da funcionalidade para um perfil do Management Client

Faça associação de perfis do Management Client com funções para limitar a interface do usuário a apresentar apenas as funcionalidades disponíveis para cada função de administrador.

Associar um perfil do Management Client a uma função

1. Expanda o nó **Segurança** e clique em **Funções**.
2. Na guia **Informações** na janela **Configurações da função**, associe um perfil a uma função. Para obter mais informações, consulte a guia Informações (funções).

Gerenciar o acesso geral à funcionalidade do sistema para uma função

Perfis Management Client apenas tratam a representação visual da funcionalidade do sistema e não o real acesso a ele.

Para gerenciar o acesso geral à funcionalidade do sistema para uma função:

1. Expanda o nó **Segurança** e clique em **Funções**.
2. Clique na guia **Segurança geral** e selecione as caixas de verificação apropriadas. Para obter mais informações, consulte Guia Segurança Geral (funções) na página 528.

> **!** Na guia **Segurança geral** certifique-se de habilitar a permisão de segurança **Conectar** para conceder a todas as funções acesso ao Management Server.

Além do papel de administrador incorporado, somente os usuários associados a uma função a que tenham sido concedidas permissões de **Gerenciamento de segurança** para o servidor de gerenciamento na guia de **Segurança Geral** podem adicionar, editar e excluir perfis Management Client.

Limitar visibilidade de funcionalidade para um perfil.

Você pode alterar as configurações de visibilidade de todos os elementos do Management Client. Por padrão, o perfil do Management Client pode ver todas as funcionalidades no Management Client.

1. Expanda o nó Cliente e clique em Perfis do Management Client.
2. Selecione um perfil e clique na guia Perfil.
3. Limpe as caixas de verificação para a funcionalidade relevante, para remover a funcionalidade visualmente do Management Client para qualquer usuário do Management Client com uma função associada a este perfil do Management Client.

Matrix

Matrix e destinatários Matrix (explicado)

Matrix é um recurso para a distribuição de vídeo remotamente.

Um destinatário Matrix é um computador com XProtect Smart Client que esteja definido como destinatário Matrix em Management Client.

Se você usar Matrix, poderá acessar vídeo de qualquer câmera na rede do seu sistema para qualquer sistema executando o Matrix.

Para ver uma lista de destinatários do Matrix configurados no Management Client, expanda **Cliente** no painel **Navegação do site** e, em seguida, selecione **Matrix**. Uma lista de configurações Matrix é exibida no painel **Propriedades**.

No Management Client, você precisa adicionar cada destinatário do Matrix que deseja que receba o vídeo disparado pelo Matrix.

Definir regras de envio de vídeo para destinatários do Matrix

Para enviar vídeo para destinatários Matrix, você deve incluir o destinatário Matrix em uma regra que ativa a transmissão de vídeo para o destinatário Matrix relacionado. Para fazer isso:

1. No painel **Navegação do site**, expanda **Regras e Eventos** > **Regras**. Clique com o botão direito do mouse em **Regras** para abrir o assistente **Gerenciar regra**. No primeiro passo, selecione um tipo de regra e, no segundo passo, uma condição.
2. Na etapa 3 de **Gerenciar regra** (**Etapa 3: Ações**) selecione a ação **Configurar Matrix para visualizar <dispositivos>**.
3. Clique no link Matrix na descrição de regra inicial.
4. Na caixa de diálogo **Selecionar configuração Matrix**, selecione o destinatário Matrix relevante, e clique em **OK**.
5. Clique no link **dispositivos** na descrição inicial da regra e selecione de quais câmeras você gostaria de enviar vídeo para o destinatário Matrix, então clique em **OK** para confirmar sua seleção.
6. Clique em **Concluir** se a regra estiver completa ou defina, caso necessário, ações adicionais e/ou uma ação de parar.

Se você apagar um recipiente Matrix, qualquer regra que inclui o recipiente Matrix para de funcionar.

Adicionar destinatários do Matrix

Para adicionar um destinatário Matrix no Management Client:

1. Expanda **Clientes** e, em seguida, selecione **Matrix**.
2. Clique com o botão direito do mouse em **Matrix Configurações** e selecione **Adicionar Matrix**.
3. Preencha os campos na caixa de diálogo **Adicionar Matrix**.
    1. No campo **Endereços**, insira o endereço IP ou o nome do host do destinatário Matrix desejado.
    2. No campo **Porta**, digite o número da porta usada pelo destinatário de instalação Matrix.
4. Clique em **OK**.

Você agora pode usar o destinatário Matrix em regras.

Seu sistema não verifica que o número de porta ou senha especificada está correta ou que o número de porta, a senha, ou o tipo especificado corresponde com o destinatário Matrix real. Certifique-se que você digitou a informação correta.

Enviar o mesmo vídeo para várias visualizações XProtect Smart Client

Você pode enviar o mesmo vídeo para as posições do Matrix em várias visualizações do XProtect Smart Client, desde que as posições Matrix das visualizações compartilhem o mesmo número de porta e senha:

1. Em XProtect Smart Client, crie as visões relevantes, e as posições Matrix que compartilham o mesmo número de porta e senha.
2. No Management Client, adicione o XProtect Smart Client relevante como um destinatário do Matrix.
3. Você pode incluir o destinatário do Matrix em uma regra.

Regras e eventos

Adicionar regras

Ao criar regras, você é orientado pelo assistente **Gerenciar regra** que só lista as opções relevantes.

Isso garante que os elementos obrigatórios não estejam faltando em uma regra. Baseado no conteúdo da sua regra, ele sugere automaticamente ações de parada adequadas, que é o que deve acontecer quando a regra não se aplica mais, garantindo que você não acidentalmente crie uma regra que nunca termina.

Eventos

Ao adicionar uma regra baseada em eventos, você pode selecionar diferentes tipos de eventos.

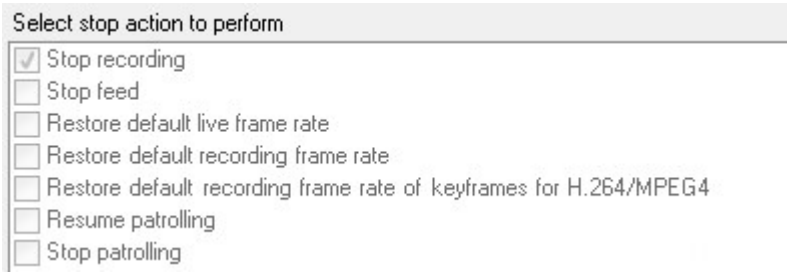
- Consulte Visão geral dos eventos para obter uma visão geral e uma descrição dos tipos de eventos que você pode selecionar.

Ações e ações de interrupção

Ao adicionar regras, você pode selecionar diferentes ações.

Algumas ações requerem uma ação de parada. Por exemplo, se você selecionar a ação **Iniciar gravação**, a gravação será iniciada e possivelmente continuará indefinidamente. Portanto, a ação **Começar gravação** tem uma interrupção compulsória chamada **Interrupção de gravação**.

O assistente **Regra de gerenciamento** garante que você especifique ações de parada quando necessário:



Selecionando ações de interrupção. No exemplo, observe a ação de parada obrigatória (selecionada, esmaecida), as ações de parada não relevantes (esmaecidas) e as ações de parada opcionais (selecionáveis).

- Consulte Ações e ações de parada para uma visão geral das ações de início e parada que você pode selecionar.

Criar uma regra

1. Clique com o botão direito no item **Regras** > **Adicionar regra**. Isso abrirá o assistente **Gerenciar regra**. O assistente o guia através do processo de especificar o conteúdo da sua regra.
2. Especifique um nome e uma descrição da nova regra nos campos **Nome** e **Descrição**, respectivamente.
3. Selecione o tipo de condição relevante para a regra: uma regra que executa uma ou mais ações quando ocorre um evento específico ou uma regra que executa uma ou mais ações quando você entra em um período de tempo específico.
4. Clique em **Avançar** para ir à etapa 2 do assistente. Na segunda etapa do assistente, defina novas condições para a regra.
5. Escolha uma ou mais condições, por exemplo **Dia da semana é <dia>**:

Dependendo de suas seleções, edite a descrição da regra na parte inferior da janela do assistente:

Clique nos itens sublinhados em **negrito itálico** para especificar seus conteúdos exatos. Por exemplo, clique no link **dias** no nosso exemplo para selecionar um ou mais dias da semana em que a deve aplicar-se a regra.

6. Após especificar as condições exatas, clique em **Avançar** para passar para a próxima etapa do assistente e selecione as ações que a regra deve cobrir. Dependendo do conteúdo e da complexidade de sua regra, você pode precisar definir mais etapas, como eventos de parada e ações de parada. Por exemplo, se uma regra especifica que um dispositivo deve executar uma ação específica durante um intervalo de tempo (por exemplo, quinta-feira entre as 8h e 10.30h), o assistente pode pedir-lhe para especificar o que deve acontecer quando o intervalo de tempo terminar.
7. Sua regra está, por padrão, ativo uma vez que você a criou se as condições da regra forem satisfeitas. Se você não quiser que a regra esteja ativa imediatamente, desmarque a caixa de seleção **Ativo**.
8. Clique em **Concluir**.

Validar regras

Você pode validar o conteúdo de uma regra individual ou de todas as regras de uma só vez. Ao criar uma regra, o assistente **Gerenciar regra** garante que todos os elementos da regra sejam válidos.

Quando uma regra já existe há algum tempo, um ou mais dos elementos da regra podem ter sido afetados por outra configuração, e a regra pode não funcionar mais. Por exemplo, se uma regra é acionada por um perfil de tempo específico, a regra não funciona se você tiver excluído ou não tiver mais permissões para esse perfil de tempo. Tais efeitos não intencionais de configuração podem ser difíceis de manter uma visão geral.

A validação de regra ajuda a manter o controle de quais regras foram afetadas. A validação ocorre conforme a regra e cada regra é validada por si mesma. Você não pode validar regras umas contra as outras, por exemplo, a fim de ver se uma regra entra em conflito com uma outra regra, nem mesmo se você usar o recurso **Validar todas as regras**.

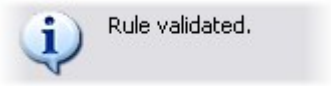
Validar uma regra

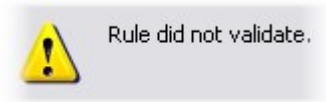
1. Clique em **Regras** e selecione a regra que você quer validar.
2. Clique com o botão direito na regra e clique em **Validar regra.**
3. Clique em **OK**.

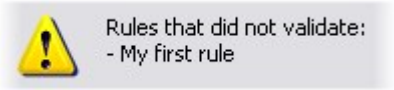
Validar todas as regras

1. Clique com o botão direito no item **Regras** e clique em **Validar todas as regras**. .
2. Clique em **OK**.

Uma caixa de diálogo informa se a(s) regra(s) foi(foram) validada(s) com sucesso ou não. Se você escolher validar mais de uma regra e uma ou mais regras não forem bem-sucedidas, a caixa de diálogo listará os nomes das regras afetadas.







Você não pode validar se a configuração de requisitos fora da própria regra puder impedir a regra de funcionar. Por exemplo, uma regra especificando que deve ocorrer quando o movimento for detectado por uma câmera especial é validada, se os elementos da regra em si estiverem corretos, mesmo que a detecção de movimento, que estiver ativada em um nível da câmera, não através de regras, não foi ativada para a câmera em questão.

Editar, copiar e renomear uma regra

1. No painel **Visão geral**, clique com o botão direito na regra relevante.
2. Selecione:

   Editar regra ou **Copiar regra** ou **Renomear regra**. O assistente **Gerenciar regra** abre.
3. Se você selecionar **Copiar regra**, o assistente abre exibindo uma cópia da regra selecionada. Clique em **Concluir** para criar uma cópia.
4. Se você selecionar **Editar regra**, o assistente é aberto e você pode inserir alterações. Clique em **Concluir** para aceitar as alterações.
5. Se você selecionar **Renomear regra**, poderá renomear o texto do nome da regra diretamente.

Desativar e ativar uma regra

O sistema aplica a regra assim que as condições da regra se aplicarem e ela estiver ativa. Se você não desejar que uma regra seja ativa, você pode desativá-la. Ao desativar a regra, o sistema não aplica a regra, mesmo que as condições da regra se aplique. Você pode facilmente ativar uma regra desativada mais tarde.

Desativar uma regra

1. No painel **Visão geral**, selecione a regra.
2. Desmarque a caixa de seleção **Ativo** no painel **Propriedades**.
3. Clique em **Salvar** na barra de ferramentas.
4. Um ícone com um X vermelho indica que a regra está desativada na lista **Regras**:

Ativar uma regra

Quando você quiser ativar a regra de novo, selecione a regra, marque a caixa de seleção **Ativar** e salve a configuração.

Especificar um perfil de tempo

1. Na lista **Perfis de tempo**, clique com o botão direito do mouse em **Perfis de tempo** > **Adicionar perfil de tempo**. Isto abre a janela **Perfil de tempo**.
2. Na janela **Perfil de tempo**, digite um nome para o novo perfil de tempo no campo **Nome**. Opcionalmente, digite uma descrição do novo perfil de tempo no campo **Descrição**.
3. No calendário da janela **Perfil de tempo**, selecione **Visualização diária**, **Visualização semanal** ou **Visualização mensal** e, em seguida, clique com o botão direito do mouse dentro do calendário e selecione **Adicionar tempo único** ou **Adicionar tempo recorrente**.
4. Quando tiver especificado os períodos de tempo para o perfil de tempo, clique em **OK** na janela **Perfil de tempo**. O sistema adiciona o novo perfil de tempo à lista **Perfis de tempo**. Se, numa fase posterior, você desejar editar ou excluir o perfil de tempo, poderá fazer isso a partir da lista **Perfis de tempo**.

Adicionar um tempo único

Quando você seleciona **Adicionar tempo único**, a janela **Selecionar tempo** aparece:

Os formatos de data e hora podem ser diferentes no seu sistema.

1. Na janela **Selecionar hora**, especifique **Hora de início** e **Hora de término**. Se o tempo deve cobrir dias inteiros, selecione a caixa **Evento de todo o dia**.
2. Clique em **OK**.

Adicionar um tempo recorrente

Quando você seleciona **Adicionar tempo recorrente**, a janela **Selecionar tempo recorrente** aparece:

1. Na janela **Selecionar hora**, especifique intervalo de tempo, o padrão de recorrência e intervalo de recorrência.
2. Clique em **OK**.

Um perfil de tempo pode conter vários períodos de tempo. Se você quiser que o seu perfil de tempo contenha mais períodos de tempo, adicione mais horas únicas ou recorrentes.

Tempo recorrente

Quando você define uma ação a ser executada em uma programação detalhada e recorrente.

Por exemplo:

- A cada semana, todas as terças-feiras, a cada 1 hora entre 15:00 e 15:30
- No dia 15, a cada 3 meses às 11:45
- Todos os dias, a cada 1 hora entre 15:00 e 19:00

A hora é baseada nas configurações de hora locais do servidor no qual o Management Client está instalado.

Editar um perfil de tempo

1. No painel **Visão geral** da lista **Perfis de tempo**, clique com o botão direito do mouse no perfil de tempo relevante e selecione **Editar perfil de tempo**. Isto abre a janela **Perfil de tempo**.
2. Edite o perfil de tempo, conforme necessário. Se você tiver feito alterações no perfil de tempo, clique em **OK** na janela **Perfil de tempo**. Você retorna à lista **Perfis de tempo**.

Na janela **Informações do Perfil de tempo**, você pode editar o perfil de tempo, conforme necessário. Ao editar perfis de tempo existentes, lembre-se de que um perfil de tempo pode conter mais do que um período de tempo e que os períodos de tempo podem ser recorrentes. A visão geral pequena do mês, no canto superior direito, pode ajudá-la a ter uma visão geral dos períodos cobertos pelo perfil de tempo, porque as datas contendo horários especificados estão destacadas em negrito.

Neste exemplo, as datas em negrito indicam que você especificou os períodos de tempo em vários dias, e que você especificou um tempo recorrente às segundas-feiras.

Criar perfis de tempo de duração diurna

1. Expanda a pasta **Regras e eventos** > **Perfis de tempo**.
2. Na lista **Perfis de tempo**, clique com o botão direito do mouse em **Perfis de tempo** e selecione **Adicionar perfil de tempo de duração diurna**.
3. Na janela **Perfil de tempo de duração diurna**, consulte a tabela de propriedades abaixo para preencher as informações necessárias. Para lidar com períodos de transição entre claro e escuro, você pode compensar a ativação e desativação do perfil. O tempo e o nome de meses são apresentados no idioma utilizado nas configurações regionais de linguagem do seu computador.
4. Para ver a localização das coordenadas geográficas inseridas em um mapa, clique em **Mostrar posição no navegador**. Isso abre um navegador onde você pode ver a localização.
5. Clique em **OK**.

Propriedades do perfil de tempo de duração diurna

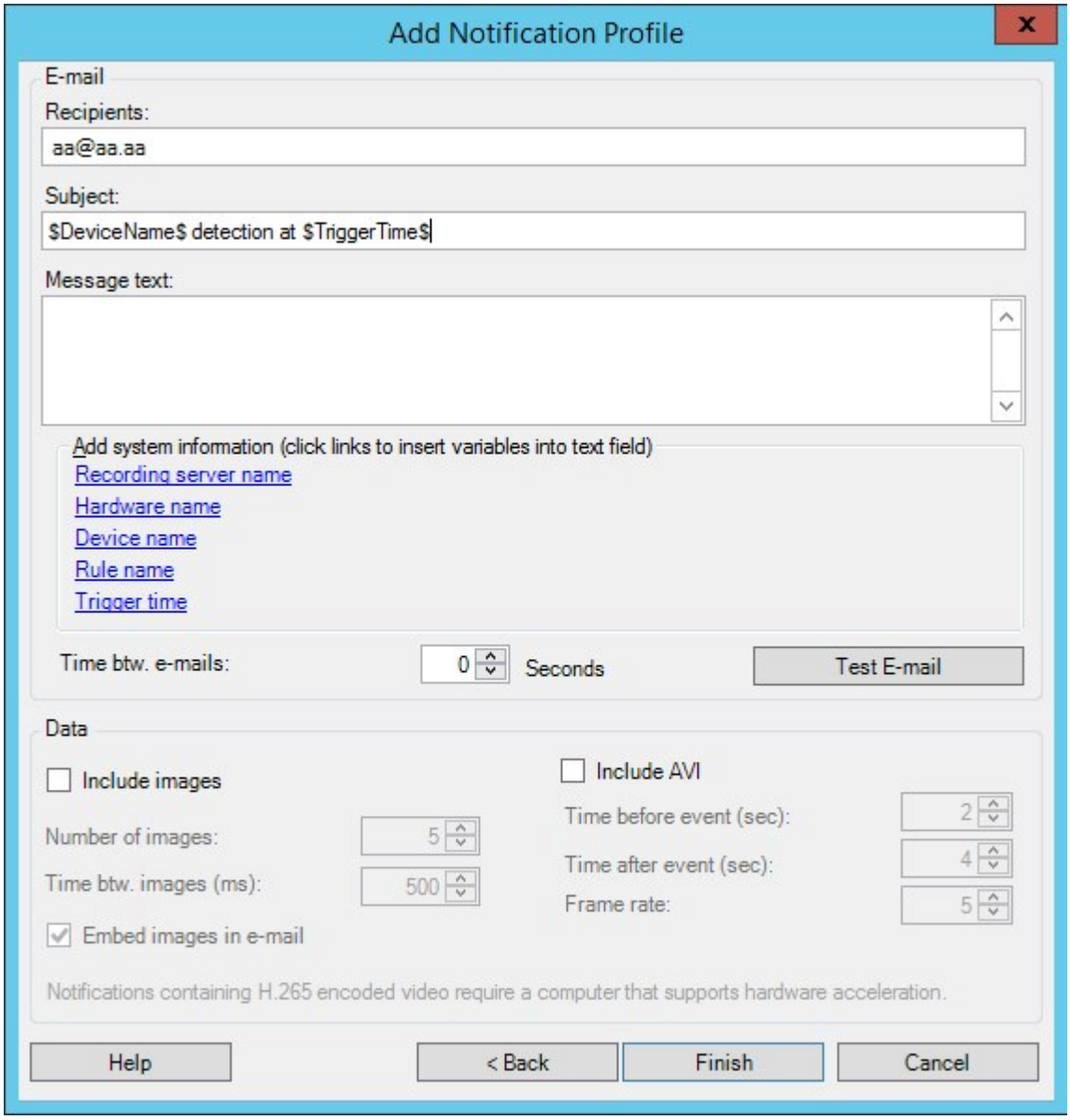
Nome	Descrição
Nome	O nome do perfil.
Descrição	Descrição do perfil (opcional).
Coordenadas geográficas	Coordenadas geográficas indicando a localização física das câmeras atribuídas ao perfil.
Compensação pelo nascer do sol	Número de minutos (+/-) através de qual ativação do perfil é compensado pelo nascer do sol.
Compensação pelo pôr do sol	Número de minutos (+/-) através de qual ativação do perfil é compensado pelo pôr do sol.
Fuso horário	Hora indicando a localização física da câmera.

Adicionar perfis de notificação

Antes de criar perfis de notificação, você deve especificar as configurações do servidor de e-mail de saída para as notificações por e-mail. Para obter mais informações, consulte Requisitos para a criação de perfis de notificação.

1. Expanda **Regras e Eventos**, clique com o botão direito do mouse em **Perfis de Notificação** > **Adicionar Perfil de Notificação**. Isso abre o assistente **Adicionar Perfil de Notificação**.
2. Especifique o nome e a descrição. Clique em **Avançar**.

3. Especifique destinatário, assunto, texto da mensagem e tempo entre e-mails:



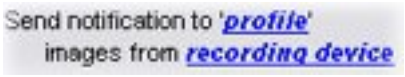
4. Para enviar um teste da notificação por e-mail para os destinatários especificados, clique em **Testar e-mail**.
5. Para incluir imagens estáticas de pré-alarme, selecione **Incluir imagens** e especifique o número de imagens, o tempo entre as imagens e se quer incorporar imagens em e-mails.
6. Para incluir clipes de vídeo AVI, selecione **Incluir AVI** e especifique o tempo antes e depois do evento e a taxa de quadros.

> As notificações que contêm o vídeo codificado H.265 requerem um computador que suporta aceleração de hardware.

7. Clique em **Concluir**.

Acionar notificações por e-mail a partir de regras

1. Clique com o botão direito no item **Regras** e então clique em > **Adicionar regra** ou **Editar regra**.
2. No assistente **Gerenciar regra**, clique em **Avançar** para ir para a lista **Selecionar ações a serem executadas** e selecione **Enviar notificação para <perfil>**.
3. Selecione o perfil de notificação relevante e selecione as câmeras de onde devem vir as gravações a serem incluídas nas notificações por e-mail do perfil de notificação.



Você não pode incluir gravações em notificações por e-mail do perfil de notificação, a menos que algo realmente esteja sendo gravado. Se você ainda quer imagens estáticas ou clipes de vídeo AVI nas notificações por e-mail, verifique se a regra especifica que a gravação deve ocorrer. O exemplo a seguir é de uma regra que inclui tanto uma ação **Iniciar a gravação** quanto uma ação **Enviar notificação para**:

Adicionar um evento definido pelo usuário

> Independentemente da maneira pela qual quer usar eventos definidos pelo usuário, você deve adicionar cada evento definido pelo usuário através do Management Client.

1. Expanda **Regras e eventos** > **Eventos definidos pelo usuário**.
2. No painel **Visão geral**, clique com o botão direito do mouse em **Eventos** > **Adicionar evento definido pelo usuário**.
3. Digite o nome do novo evento definido pelo usuário, então clique em **OK**. O evento definido pelo usuário recém-adicionado agora aparece na lista do painel **Visão geral**.

O usuário agora pode acionar o evento definido pelo usuário manualmente no XProtect Smart Client se o usuário tiver permissões para fazê-lo.

> Se você excluir um evento definido pelo usuário, isso afeta todas as regras em que o evento definido pelo usuário estiver em uso. Além disso, um evento definido pelo usuário excluído somente desaparece do XProtect Smart Client quando os usuários do XProtect Smart Client saírem do sistema.

Renomear um evento definido pelo usuário

> Se você renomear um evento definido pelo usuário, os usuários XProtect Smart Client já conectados devem sair e entrar novamente no sistema antes que a alteração de nome se torne visível.

1. Expanda **Regras e eventos** > **Eventos definidos pelo usuário**.
2. No painel **Visão geral**, selecione o evento definido pelo usuário.
3. No painel **Propriedades**, substitua o nome existente.
4. Na barra de ferramentas, clique em **Salvar**.

Adicionar e editar um evento analítico

Adicionar um evento analítico

1. Expanda **Regras e eventos**, clique com o botão direito do mouse em **Eventos de analítico** e selecione **Adicionar novo**.
2. Na janela **Propriedades**, digite um nome para o evento no campo **Nome**.
3. Digite um texto de descrição no campo **Descrição**, caso necessário.
4. Na barra de ferramentas, clique em **Salvar**. Você pode testar a validade do evento clicando em **Testar evento**. Você pode corrigir erros continuamente indicados no teste e executar o teste quantas vezes quiser e em qualquer momento durante o processo.

Edite um evento analítico

1. Clique em um evento de análise existente para visualizar a janela **Propriedades**, onde é possível editar campos relevantes.
2. Você pode testar a validade do evento clicando em **Testar evento**. Você pode corrigir erros continuamente indicados no teste e executar o teste quantas vezes quiser e em qualquer momento durante o processo.

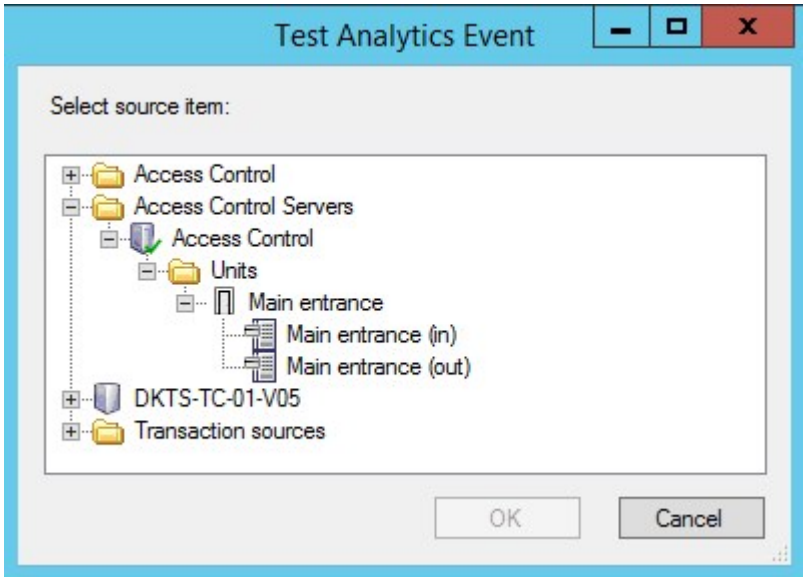
Configurações de eventos de análise

Na barra de ferramentas, clique em **Ferramentas** > **Opções** > **Eventos analíticos** para editar as configurações relevantes.

Testar a análise de um caso

Depois que você criar um evento analítico, você pode testar os requisitos (consulte Adicionar e editar um evento analítico na página 292), por exemplo, que o recurso eventos analíticos foi ativado em Management Client.

1. Selecione um evento de análise existente.
2. Empropriedades,cliquenobotão**TestarEvento**.Seráexibidaumajanelaquemostratodasasfontespossíveis deeventos.



3. Selecionar a fonte do evento de teste, por exemplo uma câmera. A janela é fechada e é exibida uma nova janela que apresenta quatro condições que têm de ser atendidas para que o evento de análise funcione.

Como um teste adicional, em XProtect Smart Client você pode verificar se o evento de analítico foi enviado para o servidor de eventos. Para fazer isso, abra XProtect Smart Client e visualize o evento na guia **Gerenciador de Alarmes**.

Adicionar um Evento Genérico

Você pode definir eventos genéricos para ajudar a VMS a reconhecer sequências específicas em TCP ou UDP de pacotes a partir de um sistema externo. Com base em um evento genérico, você pode configurar o Management Client para desencadear ações, por exemplo, para iniciar a gravação ou alarmes.

Requisitos
Você habilitou eventos genéricos e especificou destinos de fonte permitidos. Para obter mais informações, consulte Guia Eventos genéricos (opções) na página 410.

Para adicionar um evento genérico:

1. Expanda a **Regras e Eventos**.
2. Clique com o botão direito do mouse em **Eventos Genéricos** e selecione **Adicionar novo**.
3. Preencha as informações e propriedades necessárias. Para obter mais informações, consulte Eventos genéricos e fontes de dados (propriedades) na página 522.
4. (opcional) Para validar que a expressão de pesquisa é válida, digite uma sequencia de pesquisa no campo **Verificar se expressão corresponde a cadeia de evento** que corresponde aos pacotes esperados:
   - **Correspondência** - a cadeia pode ser validada contra a expressão de pesquisa
   - **Nenhuma correspondência** - a expressão de pesquisa é inválida. Mude-a e tente novamente

No XProtect Smart Client, você pode verificar se seus eventos genéricos foram recebidos pelo servidor de eventos. Você pode fazer isso na **Lista de Alarmes** na guia **Gerenciador de Alarmes** selecionando **Eventos**.

Autenticação

Registre reivindicações de um IDP externo

1. Em Management Client, selecione **Ferramentas** > **Opções** e abra a guia **IDP externo**.
2. Na seção **IDP externo**, selecione **Adicionar**.
3. A seção **Reivindicações registradas**, selecione **Adicionar**.
4. Insira as informações sobre a reivindicação. Para mais informações, consulte Registrar reivindicações.

Mapeie reivindicações de um IDPara externo para funções no XProtect

No site do IDP externo, o administrador precisa criar alegações que consistem em um nome e um valor. Posteriormente, a declaração é mapeada para uma função no VMS e os privilégios do usuário serão determinados pela função.

1. No painel **Navegação do site** no Management Client, expanda o nó **Segurança** e selecione **Funções**.
2. Selecione uma função, selecione a guia **IDP externo** e selecione **Adicionar**.
3. Selecione um IDP externo e um nome de alegação e insira um valor de alegação.

   O nome da alegação deve ser escrito exatamente como o nome da alegação proveniente do IDP externo.

4. Selecione **OK**.

Se um IDP externo for excluído, todos os usuários conectados ao VMS via IDP externo também serão excluídos. Todas as alegações registradas que estão conectadas ao IDP externo são removidas e quaisquer mapeamentos para funções também são removidos.

Faça login por meio de um IDP externo

Você pode fazer login no cliente XProtect Smart Client, XProtect Management Client, XProtect Web Client e XProtect Mobile usando um IDP externo.

1. Em **Autenticação** na caixa de diálogo de login no XProtect Smart Client ou XProtect Management Client, selecione o IDP externo e selecione **Entrar**. No primeiro login, você será redirecionado para uma página da web pertencente ao IDP externo.
2. Forneça seu nome de usuário e senha e faça login. Depois de fazer login, você retornará ao cliente XProtect e estará logado.

Em **Ferramentas** > **Opções** > **IDP externo**, é possível configurar o nome do IDP externo que é exibido na lista de **Autenticação**.

Se o IDP externo for desativado, por exemplo, uma restauração ou alteração de senha, a opção de efetuar login por meio de um IDP externo não estará disponível na lista de **Autenticação**. Além disso, se o IDP externo estiver desativado, o segredo do cliente recebido do IDP externo desaparecerá do campo **Segredo do cliente** na guia **IDP externo** em **Ferramentas** > **Opções**.

Segurança

Adicionar uma função de gerenciamento

1. Expanda **Segurança** e clique com o botão direito em **Funções**.
2. Selecione **Adicionar função**. Isso abrirá a caixa de diálogo **Adicionar função**.
3. Digite um nome e a descrição da nova função e clique em **OK**.
4. A nova função é adicionada à lista **Funções**. Por padrão, uma nova função não tem nenhum usuário/grupo associado, mas tem vários perfis padrão associados.
5. Para escolher diferentes perfis do Smart Client e Management Client, perfis de proteção de evidências ou perfis de tempo, clique nas listas suspensas.
6. Agora você pode atribuir usuários/grupos à função, e especificar quais dos recursos do sistema eles podem acessar.

Para obter mais informações, consulte Atribuir/remover usuários e grupos para/de funções na página 297 e Funões (nó Segurança) na página 525.

Copiar, renomear ou excluir uma função

Copiar uma função

Se você tem uma função com configurações complicadas e/ou permissões e precisa de uma função similar (ou quase), pode ser mais fácil copiar uma função existente e fazer ajustes menores na cópia do que criar uma função totalmente nova.

1. Expanda **Segurança**, clique em **Funções,** clique com o botão direito na função desejada e selecione **Copiar função**.
2. Na caixa de diálogo que se abre, dê à função copiada um nome e descrição novos e únicos.
3. Clique em **OK**.

Renomear uma função

Se você renomear uma função, isso não altera o nome do grupo de visualização baseado na função.

1. Expanda **Segurança** e clique com o botão direito do mouse em **Funções**.
2. Clique com o botão direito na função desejada e selecione **Renomear função**.
3. Na caixa de diálogo que se abre, mude o nome da função.
4. Clique em **OK**.

Excluir uma função

1. Expanda **Segurança** e clique em **Funções**.
2. Clique com o botão direito do mouse na função indesejada e selecione **Excluir função**.
3. Clique em **Sim**.

> Se você excluir uma função, isso não altera o nome do grupo de visualização baseado na função.

Visualizar funções efetivas

Com o recurso Funções efetivas, você pode visualizar todas as funções de um usuário ou grupo selecionado. Isto é prático se estiver usando grupos e é a única maneira de ver de quais funções um usuário específico é membro.

1. Abra a janela **Funções Efetivas** expandindo **Segurança** e em seguida clicando com o botão direito do mouse em **Funções** e selecionando **Funções Efetivas**.
2. Se desejar informações sobre um usuário básico, digite o nome no campo **Nome do usuário**. Clique em **Atualizar** para exibir as funções do usuário.
3. Se você utilizar os usuários do Windows ou grupos do Active Directory, clique no botão de navegação **"..."**. Selecione o tipo de objeto, digite o nome e clique em **OK**. Funções do usuário aparecem automaticamente.

Atribuir/remover usuários e grupos para/de funções

Para atribuir ou remover usuários ou grupos do Windows ou usuários básicos para/de uma função:

1. Expanda **Segurança** e selecione **Funções**. Escolha a função desejada no painel **Visão Geral**:
2. No painel **Propriedades**, selecione a guia **Usuários e grupos** na parte inferior.
3. Clique em **Adicionar**, escolha entre **usuário do Windows** ou **Usuário básico**.

Atribuir usuários e grupos do Windows à uma função

1. Selecione **Usuário do Windows**. Isso abre o diálogo **Selecionar Usuários**, **Computadores e Grupos**:
2. Verifique que o tipo de objeto requerido é especificado. Se, por exemplo, você precisar adicionar um computador, clique em **Tipos de objetos** e marque **Computador**. Também verifique se o domínio desejado está no campo **A partir desta localização**. Se não, clique em **Locais** para buscar o domínio desejado.
3. Na caixa **Insira os nomes de objetos a serem selecionados**, digite os nomes de usuário desejados, as iniciais ou outros tipos de identificador que o Active Directory possa reconhecer. Use o recurso **Verificar Nomes** para saber se os nomes, as iniciais etc., digitados são reconhecidos pelo Active Directory. Alternativamente, use a função **"Avançado..."** para pesquisar usuários ou grupos.

4. Clique em **OK.** Os usuários/grupos selecionados estão agora adicionados à lista de usuários da guia **Usuários e grupos** que foram atribuídos à função selecionada. Você pode adicionar mais usuários e grupos de usuários inserindo vários nomes separados por ponto e vírgula (;).

Atribuir usuários básicos a uma função

1. Selecione **Usuário básico**. Isso abre a caixa de diálogo **Selecionar usuário básico para adicionar a Função**:
2. Selecione o(s) usuário(s) básico(s) que deseja atribuir a essa função.
3. Opcional: Clique em **Novo** para criar um novo usuário básico.
4. Clique em **OK.** O(s) usuário(s) básico(s) selecionado(s) estão agora adicionados à lista de usuários da guia **Usuários e grupos** que foram atribuídos à função selecionada.

Remover usuários e grupos de uma função

1. Na guia **Usuários e grupos**, selecione o usuário ou grupo que você quer remover e clique em **Remover** na parte de baixo da guia. Você pode selecionar mais de um usuário ou grupo, ou uma combinação de grupos e usuários individuais, se necessário.
2. Confirme que você quer remover o(s) usuário(s) ou/e grupo(s). Clique em **Sim**.

> Um usuário pode também ter funções por ser membro de grupos. Quando for este o caso, você não pode remover da função o usuário individual. Os membros de grupos também podem realizar funções como indivíduos. Para descobrir quais funções usuários, grupos ou membros de grupos individuais possuem, use a função **Visualizar funções efetivas**.

Criação de usuários básicos

Há dois tipos de conta de usuário no Milestone XProtect VMS: Usuários básicos e usuários Windows.

Usuários básicos são contas de usuário criadas no Milestone XProtect VMS. Trata-se de uma conta de usuário dedicada do sistema com um nome de usuário básico e autenticação de senha para o usuário individual.

Usuários Windows são contas de usuário adicionadas através de Microsoft de Active Directory.

Há algumas diferenças entre usuários básicos e usuários Windows:

- Usuários básicos são autenticados por uma combinação de nome de usuário e senha e específicos de um sistema/site. Observe que, mesmo quando um usuário básico criado em um site federado tem o mesmo nome e a mesma senha que um usuário básico em outro site federado, o usuário básico tem acesso somente ao site em que ele foi criado.
- Os usuários do Windows são autenticados com base em seu login do Windows e são específicos de uma máquina.

Definir as configurações de login para usuários básicos

Você pode definir as configurações de login para usuários básicos em um arquivo JSON, que é encontrado aqui: `\\Arquivos de programas\Milestone\Management Server\IIS\IDP\appsettings.json`.

Nesse arquivo, você pode definir os seguintes parâmetros:

LoginSettings	
"ExpireTimeInMinutes": 5	Defina o período de tempo (em minutos) em que uma sessão de login irá expirar se o usuário não realizar nenhuma ação.
LockoutSettings	
"LockoutTimeSpanInMinutes": 5	Definir por quanto tempo (em minutos) um usuário ficará bloqueado.
"MaxFailedAccessAttempts": 5	Definir o número de tentativas que um usuário terá para fazer login antes de ser bloqueado.
PasswordSettings	
"RequireDigit": true	Definir se dígitos básicos (0 a 9) são exigidos na senha.
"RequireLowercase": true	Definir se caracteres minúsculos são exigidos na senha.
"RequireNonAlphanumeric": true	Definir se caracteres especiais (~!@#$%^&*_-+=|\(){}[]:;"'<>,.?/) são necessários na senha.
"RequireUppercase": true	Definir se caracteres maiúsculos são exigidos na senha.
"RequiredLength": 8	Definir o número de caracteres exigidos na senha. A senha mínima é de {0} caracteres e a senha máxima é de 255 caracteres.
"RequiredUniqueChars": 1	Definir o número mínimo de caracteres únicos exigidos na senha. Por exemplo, se você definir caracteres únicos necessários como 2, senhas como aaaaaa, aa, a, b, bb, bbbbbbb serão rejeitadas. Enquanto que senhas como abab, abc, aaab e assim por diante serão aceitas porque há pelo menos dois caracteres exclusivos em cada. Aumentar o número de caracteres exclusivos em uma senha aumenta a força da senha, evitando sequências repetitivas que são facilmente adivinhadas.

Para criar um novo usuário básico em seu sistema:

1. Expanda **Segurança** > **Usuários Básicos**.
2. No painel **Usuários Básicos**, clique com o botão direito e selecione **Criar Usuário Básico**.
3. Especifique um nome de usuário e uma senha. Repita a senha para confirmar que você a especificou corretamente.

   A senha deve atender à complexidade definida no arquivo **appsettings.json** (consulte Definir as configurações de login para usuários básicos na página 299).
4. Especifique se o usuário básico deve alterar a senha no próximo login. Milestone recomenda que você selecione a caixa de seleção para que usuários básicos possam especificar suas próprias senhas quando fizerem login pela primeira vez.

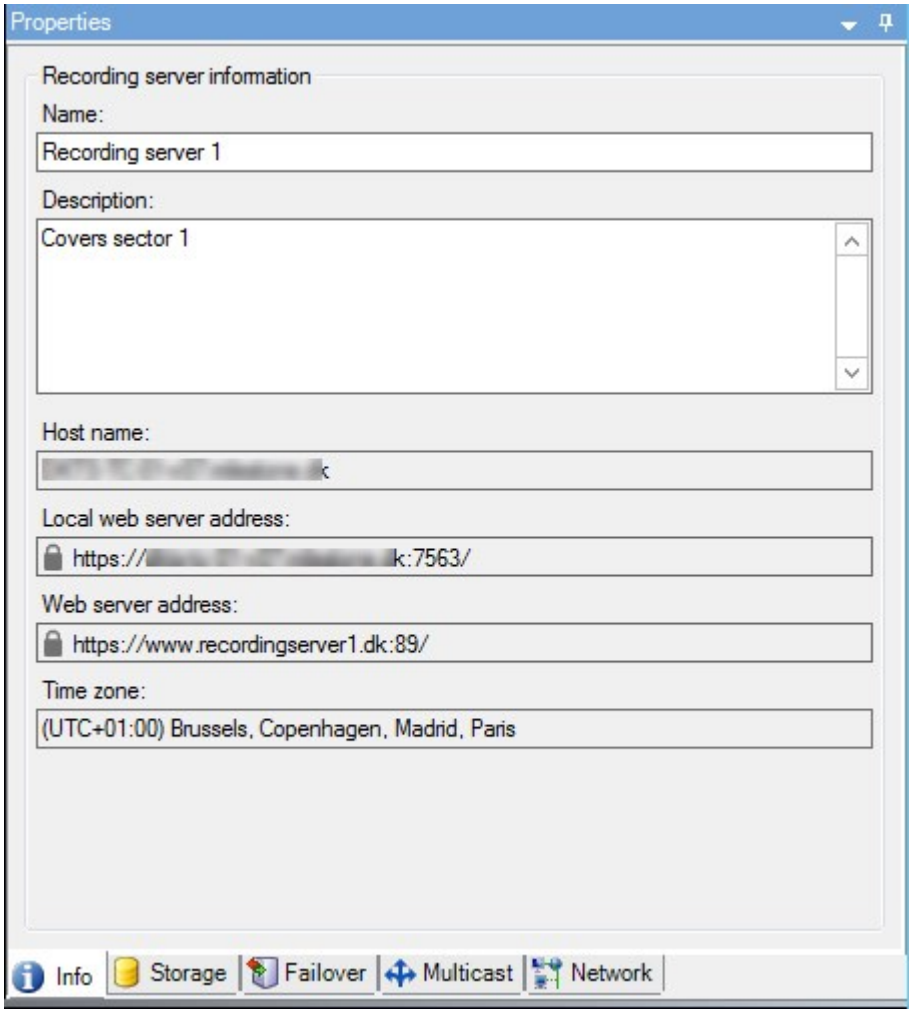
   Você pode desmarcar a caixa de seleção somente quando criar usuários básicos que não possam alterar suas senhas. Esses usuários básicos são, por exemplo, usuários do sistema usados para plug-ins e autenticação de serviços do servidor.
5. Especifique o status do usuário básico para ser **Ativado** ou **Bloqueado**.
6. Clique em **OK** para criar o usuário básico.

Visualizar status de criptografia para clientes

Para verificar se seu servidor de gravação criptografa conexões:

1. Abra o Management Client.
2. No painel **Navegação do Site**, selecione **Servidores** > **Servidores de gravação**. Isto abre uma lista de servidores de gravação.

3. No painel **Visão geral**, selecione o servidor de gravação relevante e acesse a guia **Informações**.
   Se a criptografia estiver ativada para clientes e servidores que recuperam fluxos de dados do servidor de gravação, um ícone de cadeado aparecerá na frente do endereço do servidor de web local e do endereço de servidor de web opcional.



Painel do sistema

Visualizar tarefas em andamento nos servidores de gravação

A janela **Tarefas atuais** mostra uma visão geral das tarefas em andamento em um servidor de gravação selecionado. Se você iniciou uma tarefa que leva muito tempo e é executada em segundo plano, pode abrir a janela **Tarefas atuais** para ver o andamento da tarefa. Alguns exemplos de tarefas demoradas iniciadas pelo usuário são atualizações de firmware e movimentação de hardware. Você pode ver informações sobre hora de início, hora de término estimada e progresso da tarefa.

Se a tarefa não estiver progredindo conforme o esperado, provavelmente você poderá encontrar a causa em seu hardware ou rede. Alguns exemplos são servidor não funcionando, erro do servidor, largura de banda insuficiente ou perda de conexão.

1. No painel **Navegação do site**, selecione **Painel de controle do sistema** > **Tarefas atuais**.
2. Selecione um servidor de gravação para ver suas tarefas atuais.

As informações exibidas na janela **Tarefas atuais** não são atualizadas dinamicamente, mas um instantâneo das tarefas atuais a partir do momento em que você abriu a janela. Se a janela está aberta há algum tempo, atualize as informações clicando no botão **Atualizar** no canto inferior direito da janela.

Monitor do sistema (explicado)

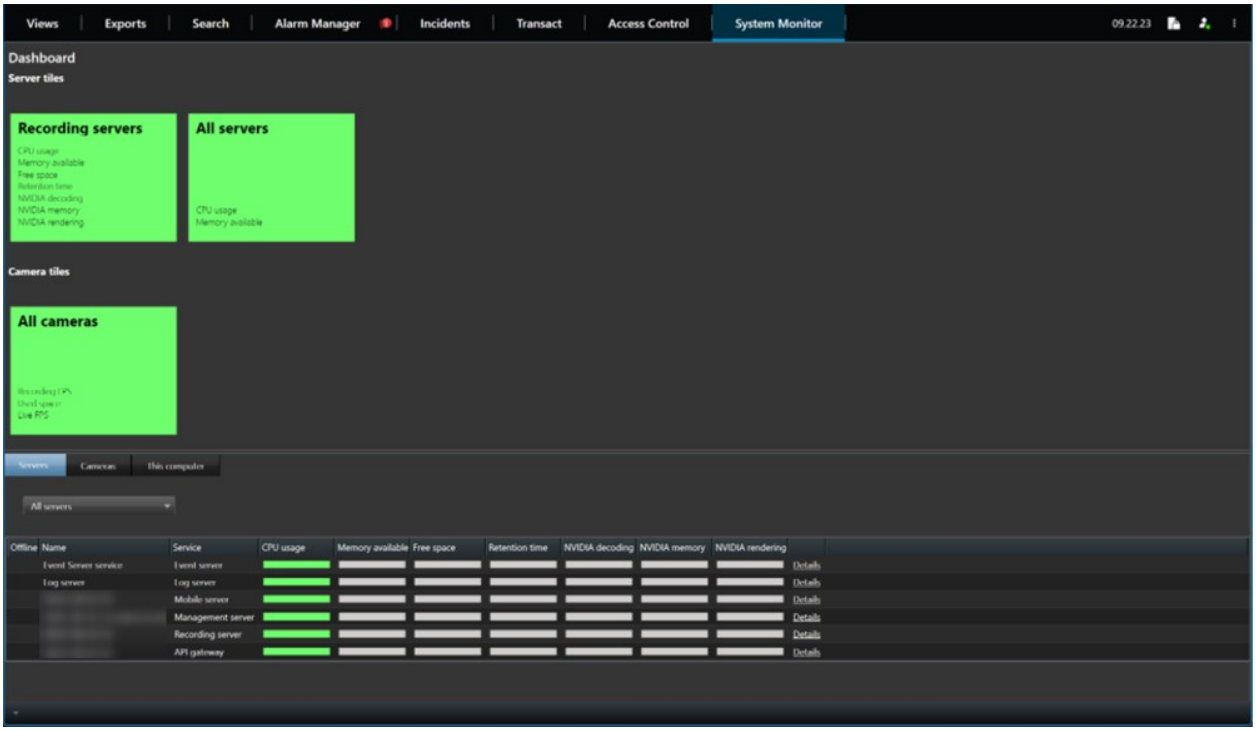
A funcionalidade do monitor do sistema requer que o serviço Data Collector esteja em execução e funciona apenas em computadores que usam um calendário gregoriano (ocidental).

Painel do monitor do sistema (explicado)

No **painel de controle do monitor do sistema**, é possível obter com facilidade uma visão geral do bem-estar do seu sistema VMS. O estado do seu hardware é visualmente representado por quadros e suas cores: verde (em execução), amarelo (alerta) e vermelho (crítico). Os quadros também podem ter ícones de erro ou alerta quando uma ou mais peças de hardware estão com defeito.

Por padrão, o site exibe quadros que representam todos os **Servidores de gravação**, **Todos os servidores** e **Todas as câmeras**. Você pode personalizar os parâmetros de monitoramento desses quadros padrão e criar novos quadros. Por exemplo, é possível configurar quadros para representar um único servidor, uma única câmera, um grupo de câmeras, ou um grupo de servidores.

Parâmetros de monitoramento são, por exemplo, o uso de CPU ou a memória disponível para um servidor. Um quadro monitora apenas os parâmetros de monitoramento que você adicionou ao quadro. Consulte Adicionar uma nova câmera ou quadro do servidor no painel do monitor do sistema na página 305, Editar uma câmera ou um bloco de servidor no painel do monitor do sistema na página 306 e Excluir uma câmera ou bloco de servidor no painel do monitor do sistema na página 306 para obter mais informações.



Limites do monitor do sistema (explicado)

Os limites do monitor do sistema permitem definir e ajustar os limites quando os quadros no **Painel de controle do monitor do sistem** a devem indicar visualmente que o hardware do sistema muda de estado. Por exemplo, quando o uso da CPU de um servidor muda de um estado normal (verde) para um estado de alerta (amarelo) ou de um estado de alerta (amarelo) para um estado crítico (vermelho).

O sistema tem valores de limite padrão para todos os hardwares do mesmo tipo para que você possa começar a monitorar o estado do hardware do sistema a partir do momento em que o sistema é instalado e você adiciona hardware. Você também pode definir valores limite para servidores, câmeras, discos e armazenagem individuais. Para alterar os valores de limite, consulte Editar limites para quando os estados do hardware devem mudar na página 306.

Para garantir que você não veja um estado **Crítico** ou **Aviso** sem casos onde o uso de ou a carga em seu hardware do sistema atinja um valor limite alto somente por um segundo ou similar, use **Intervalo de cálculo**. Com a configuração correta do intervalo de cálculo, você não receberá alertas falso-positivos sobre limites excedidos, mas apenas alertas sobre problemas constantes com, por exemplo, uso de CPU ou consumo de memória.

Você também pode definir regras – consulte Regras (explicado) – para realizar ações específicas ou ativar alarmes quando um limite mudar de um estado ao outro.

Ver estado atual do hardware e resolver problemas, se necessário

No **painel de controle do monitor do sistema**, é possível obter com facilidade uma visão geral do bem-estar do seu sistema VMS. O estado do seu hardware é visualmente representado por quadros e suas cores: verde (em execução), amarelo (alerta) e vermelho (crítico). Os quadros também podem ter ícones de erro ou alerta quando uma ou mais peças de hardware estão com defeito.

Você pode editar os limites para quando seu hardware estiver em um dos três estados. Para obter mais informações, consulte Editar limites para quando os estados do hardware devem mudar na página 306.

O **Painel de controle do monitor do sistema** responde a perguntas como: Todos os serviços de servidor e câmeras estão funcionando? O uso da CPU e a memória disponível nos diferentes servidores são suficientes para que tudo seja registrado e disponível para visualização?

1. No painel **Navegação do site**, selecione **Painel de controle do sistema** > **Monitor do sistema**.
2. Se todos os quadros estiverem verdes e sem ícones de alerta ou erro, todos os parâmetros de monitoramento e todos os servidores e câmeras representados pelos quadros estão funcionando corretamente.
   Se um ou mais quadros tiver um ícone de alerta ou erro ou estiver completamente amarelo ou vermelho, selecione um deles para solução de problemas.
3. Na lista de hardware com parâmetros de monitoramento (parte inferior da janela), encontre o hardware que não está funcionando. Passe o mouse sobre o sinal da cruz vermelha próximo ao hardware para ler qual é o problema.
4. Opcionalmente, selecione **Detalhes** no lado direito do hardware para ver há quanto tempo o problema existe. Ativar as coletas de dados históricos para ver o estado do seu hardware ao longo do tempo. Para obter mais informações, consulte Coletar dados históricos de estados de hardware na página 305.
5. Encontre uma maneira de resolver o problema. Por exemplo, reinicialização do computador, reinicialização do serviço do servidor, substituição de uma peça de hardware com defeito ou outro.

Ver estado histórico do hardware e imprimir um relatório

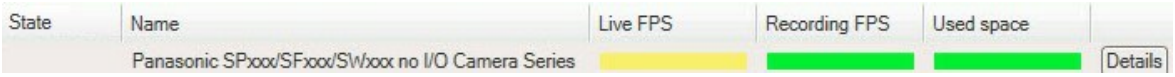
Com o recurso **Monitor do sistema**, é possível obter com facilidade uma visão geral do bem-estar do sistema VMS. Também durante um período mais longo.

O uso da CPU e a memória disponível nos diferentes servidores são suficientes para que tudo seja registrado e disponível para visualização? Encontre a resposta para isso com a funcionalidade Monitor do sistema e decida se você precisa atualizar seu hardware ou comprar um novo para evitá-lo no futuro.

Lembre-se de habilitar a coleta de dados históricos. Consulte Coletar dados históricos de estados de hardware na página 305.

1. No painel **Navegação do site**, selecione **Painel de controle do sistema** > **Monitor do sistema**.
2. Na janela **Monitor do sistema**, selecione um quadro com o hardware do qual deseja saber o histórico de bem-estar ou, na parte inferior da janela, selecione um servidor ou câmera.

3. Selecione **Detalhes** no lado direito do servidor ou câmera relevante.



4. Para servidores, selecione **Histórico** à direita do hardware que deseja investigar. Para câmeras, selecione o link.
5. Se você deseja imprimir um relatório, selecione o ícone PDF.

Somente é possível criar relatórios históricos com dados do servidor de gravação onde o dispositivo está localizado atualmente.

Se você acessar os detalhes do monitor a partir de um sistema operacional de um servidor, poderá ver uma mensagem sobre **Configuração de segurança melhorada do Internet Explorer**. Siga as instruções para adicionar a página **Monitor do sistema** à **Zona de sites confiáveis** antes de prosseguir.

Coletar dados históricos de estados de hardware

Você pode habilitar a coleta de dados históricos no hardware do sistema para ver gráficos dos estados do seu hardware ao longo do tempo e imprimir um relatório. Para obter mais informações, consulte Ver estado histórico do hardware e imprimir um relatório na página 304.

1. No painel **Navegação do site**, selecione **Painel de controle do sistema** > **Monitor do sistema**.
2. Na janela **Monitor do sistema**, selecione **Personalizar**.
3. Na janela **Personalizar painel** que se abre, selecione **Coletar dados históricos**.
4. Selecione um intervalo de amostragem. Quanto mais curto o intervalo, maior a carga no banco de dados SQL Server, na largura de banda ou em outro hardware. O intervalo de amostragem dos dados históricos também determina quão detalhados são os gráficos.

Adicionar uma nova câmera ou quadro do servidor no painel do monitor do sistema

Se deseja monitorar suas câmeras ou seus servidores em grupos menores após sua localização física, ou se deseja monitorar algum hardware com diferentes parâmetros de monitoramento, você pode adicionar blocos adicionais à janela **Monitor do Sistema**.

1. No painel **Navegação do site**, selecione **Painel de controle do sistema** > **Monitor do sistema**.
2. Na janela **Monitor do sistema**, selecione **Personalizar**.
3. Na janela **Personalizar painel de controle** que se abre, selecione **Novo** sob **Quadros de servidor** ou **Quadros de câmeras**.

4. Na janela **Novo Quadro de Servidor / Novo Quadro de Câmeras** selecione as câmeras ou servidores a monitorar.
5. Sob **Parâmetros de monitoramento**, marque ou desmarque caixas de seleção de quaisquer parâmetros para adicionar ou remover do quadro.
6. Selecione **OK.** O quadro do novo servidor ou câmera agora está adicionado aos quadros exibidos no painel de controle.

Editar uma câmera ou um bloco de servidor no painel do monitor do sistema

Se desejar monitorar suas câmeras ou servidores com outros parâmetros de monitoramento, você pode ajustá-los.

1. No painel **Navegação do site**, selecione **Painel de controle do sistema** > **Monitor do sistema**.
2. Na janela **Monitor do sistema**, selecione **Personalizar**.
3. Na janela **Personalizar painel** que se abre, selecione o quadro que deseja alterar em **Quadros de servidor** ou **Quadros de câmeras** e selecione **Editar**.
4. Na janela **Editar painel de controle de servidor/quadro de câmera**, selecione todas as câmeras ou servidores, uma câmera ou grupo de servidores ou câmeras ou servidores individuais para alterar seus parâmetros de monitoramento.
5. Em **Parâmetros de monitoramento**, selecione os parâmetros de monitoramento que deseja monitorar.
6. Selecione **OK**.

Excluir uma câmera ou bloco de servidor no painel do monitor do sistema

Se você não precisar mais monitorar o hardware representado por um quadro, poderá excluir o quadro.

1. No painel **Navegação do site**, selecione **Painel de controle do sistema** > **Monitor do sistema**.
2. Na janela **Monitor do sistema**, selecione **Personalizar**.
3. Na janela **Personalizar painel de controle** que se abre, selecione o quadro que você deseja modificar em **Quadros de servidor** ou **Quadros de Câmeras**.
4. Selecione **Excluir**.

Editar limites para quando os estados do hardware devem mudar

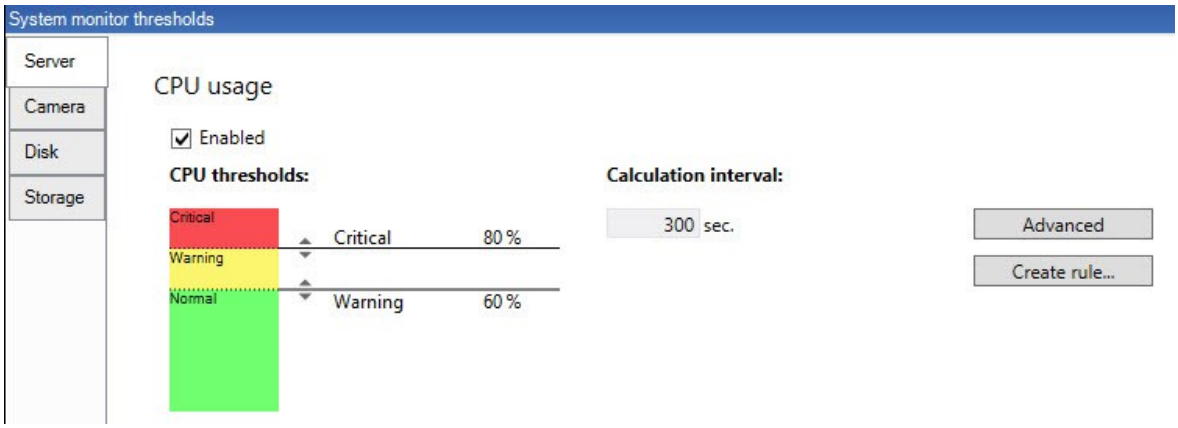
Você pode editar os limites para quando seu hardware mudar entre os três estados no **Painel de controle do monitor do sistema**. Para obter mais informações, consulte Limites do monitor do sistema (explicado) na página 303.

Você pode alterar os limites para diferentes tipos de hardware. Para obter mais informações, consulte Limites do monitor do sistema (nó Painel de controle do) na página 582.

Por padrão, o site configurado para exibir os valores limite para todas as unidades do mesmo tipo de hardware, por exemplo, todas as câmeras ou servidores. Você pode alterar esses valores de limite padrão.

Você também pode definir valores limite para servidores ou câmeras individuais ou um subconjunto destes para permitir, por exemplo, que algumas câmeras usem um **FPS ao vivo** ou **FPS de gravação** mais alto do que outras câmeras.

1. No painel **Navegação do site**, selecione **Painel de controle do sistema** > **Limites do monitor do sistema**.
2. Marque a caixa de seleção **Ativar** do hardware relevante se ainda não o tiver ativado. A figura abaixo mostra um exemplo.



3. Arraste o controle deslizante para cima ou para baixo para aumentar ou diminuir o valor limite. Existem duas barras disponíveis para cada item de hardware mostrado no controle de limites, separando os níveis **Normal**, **Alerta** e **Crítico**.
4. Insira um valor para o intervalo de cálculo ou mantenha o valor padrão.
5. Se você quiser definir valores em peças individuais de hardware, selecione **Avançado**.
6. Se você quiser especificar regras para determinados eventos ou em intervalos de tempo específicos, selecione **Criar regra**.
7. Depois de ter definido os níveis limite e os intervalos de cálculo relevantes, selecione **Arquivo** > **Salvar** no menu.

Visualizar proteção de evidências no sistema

No **Painel do Sistema**, **Proteção de evidências** exibe uma visão geral de todos os dados protegidos do sistema de monitoramento atual.

Encontre uma proteção de evidência filtrando, por exemplo, quem a criou ou quando.

1. No painel **Navegação do site**, selecione **Painel do Sistema** > **Proteção de evidências**.
2. Obtenha uma visão geral e encontre as proteções de evidências relevantes. Você pode filtrar e classificar os diferentes metadados relacionados às proteções de evidências.

Todas as informações mostradas na janela **Proteção de evidências** são instantâneos. Pressione F5 para recarregar.

Imprima um relatório com a configuração do seu sistema

Você faz muitas escolhas ao instalar e configurar seu sistema VMS e pode ser necessário documentá-las. Com o tempo, também é difícil lembrar de todas as configurações que você alterou desde a instalação e a configuração inicial – ou apenas durante os últimos meses. Por isso é possível imprimir um relatório com todas as suas opções de configuração.

Ao criar um relatório de configuração (em formato PDF), você pode incluir todos os elementos possíveis do seu sistema no relatório. Você pode, por exemplo, incluir licenças, a configuração do dispositivo, a configuração de alarmes, e muito mais. Você pode selecionar a opção **Excluir dados sensíveis** para criar um relatório compatível com o GDPR (habilitado por padrão). Você também pode personalizar a fonte, a configuração da página e a página inicial.

1. Expanda **Painel do sistema** e selecione **Relatórios de configuração**.
2. Selecione os elementos que deseja incluir ou excluir de seu relatório.
3. **Opcional**: Se você optou por incluir uma página inicial, selecione **Página inicial** para personalizar as informações em sua página inicial. Na janela que aparecer, preencha a informação necessária.
4. Selecione **Formatando** para personalizar a fonte, o tamanho e as margens da página. Na janela que aparece, selecione as configurações desejadas.
5. Quando estiver pronto para exportar, clique em **Exportar** e selecione um nome e local para salvar seu relatório.

> Somente usuários com permissões de administrador no sistema VMS podem criar relatórios de configuração.

Metadados

Mostrar ou ocultar as categorias de pesquisa de metadados e filtros de pesquisa

Os usuários XProtect Management Client com permissões de administrador podem mostrar ou ocultar as categorias de pesquisa de metadados Milestone padrão e os filtros de pesquisa no XProtect Smart Client. Por padrão, essas categorias e filtros de pesquisa estão ocultos. Mostrá-los é útil se o seu sistema de vigilância por vídeo atender os requisitos (consulte Requisitos da pesquisa de metadados na página 589).

Esta configuração afeta todos os usuários do XProtect Smart Client.

Esta configuração não afeta a visibilidade do:

- Outras categorias e filtros de pesquisa do Milestone, por exemplo, **Movimento**, **Marcadores**, **Alarmes**, e **Eventos**
- Categorias e filtros de pesquisa de terceiros

1. No XProtect Management Client, no painel **Navegação no site**, selecione **Uso de metadados** > **Pesquisa de metadados**.
2. No painel **Pesquisa de metadados**, selecione a categoria de pesquisa para a qual você deseja alterar as configurações de visibilidade.
3. Para ativar a visibilidade de uma categoria de pesquisa ou filtro de pesquisa, selecione a caixa de verificação correspondente. Para desativar a visibilidade de uma categoria de pesquisa ou filtro de pesquisa, limpe a caixa de verificação.

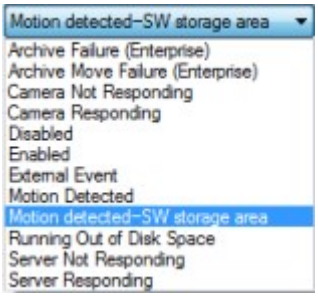
Alarmes

Adicionar um Alarme

Para definir um alarme, é necessário criar uma definição de alarme, na qual você especifica, por exemplo, o que dispara o alarme, instruções sobre o que o operador precisa fazer e o que ou quando o alarme para. Para obter informações detalhadas sobre as configurações, consulte Definições de alarme (nós de alarme).

1. No painel de **Navegação do Site**, expanda **Alarmes** e clique com o botão direito em **Definições de Alarme**.
2. Selecione **Adicionar novo**.

3. Preencha essas propriedades:
    - **Nome**: Digite um nome para a definição de alarme. O nome da definição do alarme aparece quando sempre que a definição do alarme estiver na lista.
    - **Instruções**: Você pode escrever instruções para o operador que recebe o alarme.
    - **Evento de ativação**: Use os menus suspensos para selecionar um tipo de evento e uma mensagem de evento a serem usados quando o alarme for disparado.

      Uma lista de fatos geradores selecionáveis. O destacado é criado e personalizado usando eventos de análise.
    - **Origens**: Selecione as câmeras e/ou outros dispositivos dos quais o evento deve ser originado a fim de acionar o alarme. Suas opções dependem do tipo de evento selecionado.
    - **Perfil de tempo**: Se você deseja que o alarme seja ativado durante um intervalo de tempo específico, selecione o botão e, em seguida, um perfil de tempo no menu suspenso.
    - **Baseado em evento**: Se quiser que a definição de alarme seja ativada por um evento, selecione o botão e especifique o evento que disparará a definição de alarme. Você também deve especificar um evento que desativará a definição de alarme.
4. No menu suspenso **Limite de tempo**, selecione um limite de tempo para quando a ação do operador for necessária.
5. No menu suspenso **Eventos ativados**, selecione que evento ativar quando o tempo limite for atingido.
6. Especifique configurações adicionais, por exemplo, câmeras relacionadas e proprietário inicial do alarme.

Modificar as permissões para definições individuais de alarme

Se quiser que apenas usuários específicos exibam e gerenciem um alarme, você poderá modificar as permissões para a definição de alarme no XProtect Management Client. Dessa forma, você pode garantir que:

- Os usuários recebam apenas os alarmes relevantes para eles.
- Nenhum usuário não autorizado possa reagir a alarmes.

Use funções para agrupar usuários que devam ter as mesmas permissões para todas as definições de alarme.

Para modificar as permissões de uma definição de alarme:

1. No painel **Navegação do site**, expanda **Segurança** e selecione a função para a qual deseja modificar as permissões.
2. Acesse a guia **Alarmes** e expanda **Definições de alarme** para ver a lista dos alarmes que você definiu.
3. Selecione uma definição de alarme para modificar as permissões.

Ativar criptografia

Ativar criptografia para e do servidor de gerenciamento

Você pode criptografar a conexão de duas vias entre o servidor de gerenciamento e o Data Collector afiliado, quando tiver um servidor remoto do seguinte tipo:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

Se o seu sistema contém vários servidores de gravação ou servidores remotos, você deve habilitar a criptografia em todos eles.

> Quando configurar a criptografia para um grupo de servidores, ela deve ser habilitada com um certificado pertencente ao mesmo certificado CA ou, se desabilitada, deve ser desabilitada em todos os computadores do grupo de servidores.

Pré-requisitos:

- Um certificado de autenticação do servidor é confiado no computador que abriga o servidor de gerenciamento

Primeiro, ative a criptografia no servidor de gerenciamento.

Etapas:

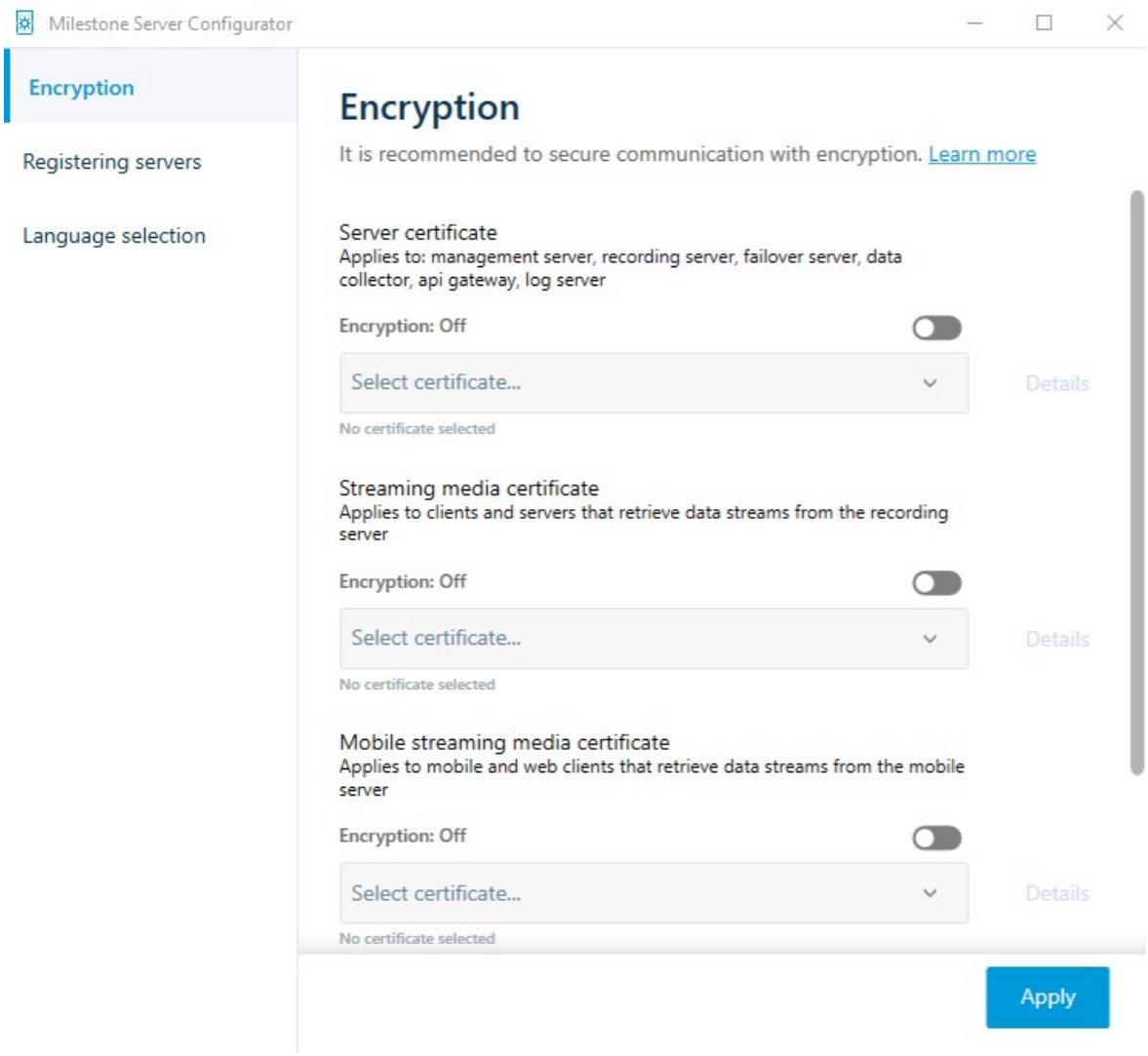
1. Em um computador com um servidor de gerenciamento instalado, abra o **Server Configurator** de:
   - Menu Iniciar do Windows Start

   ou

   - O Management Server Manager clicando com o botão direito no ícone Management Server Manager na barra de tarefas do computador
2. No **Server Configurator**, em **Certificado do servidor**, habilite o **Encryption**.

3. Clique em **Selecionar certificado** para abrir uma lista com nomes de entidade únicos que têm uma chave privada e estão instalados no Repositório de certificados do Windows no computador local.
4. Selecione um certificado para criptografar a comunicação entre o servidor de gravação, servidor de gerenciamento, servidor de emergência e Data Collector server.

   Selecione **Detalhes** para visualizar as informações do Repositório de certificados do Windows sobre o certificado selecionado.



5. Clique em **Aplicar**.

Para concluir a ativação da criptografia, o próximo passo é atualizar as configurações de criptografia em cada servidor de gravação e cada servidor com um Data Collector (Event Server, Log Server, LPR Server, e Mobile Server).

Para obter mais informações, consulte Habilitar a criptografia do servidor para servidores de gravação ou servidores remotos na página 313.

Habilitar a criptografia do servidor para servidores de gravação ou servidores remotos

É possível criptografar a conexão bidirecional entre o servidor de gerenciamento e o servidor de gravação ou outros servidores remotos que usam o Data Collector.

Se o seu sistema contém vários servidores de gravação ou servidores remotos, você deve habilitar a criptografia em todos eles.

Para obter mais informações, consulte o guia de certificados sobre como proteger suas XProtect VMS instalações.

> Quando configurar a criptografia para um grupo de servidores, ela deve ser habilitada com um certificado pertencente ao mesmo certificado CA ou, se desabilitada, deve ser desabilitada em todos os computadores do grupo de servidores.

Pré-requisitos:

- Você ativou a criptografia no servidor de gerenciamento, consulte Ativar criptografia para e do servidor de gerenciamento na página 311.

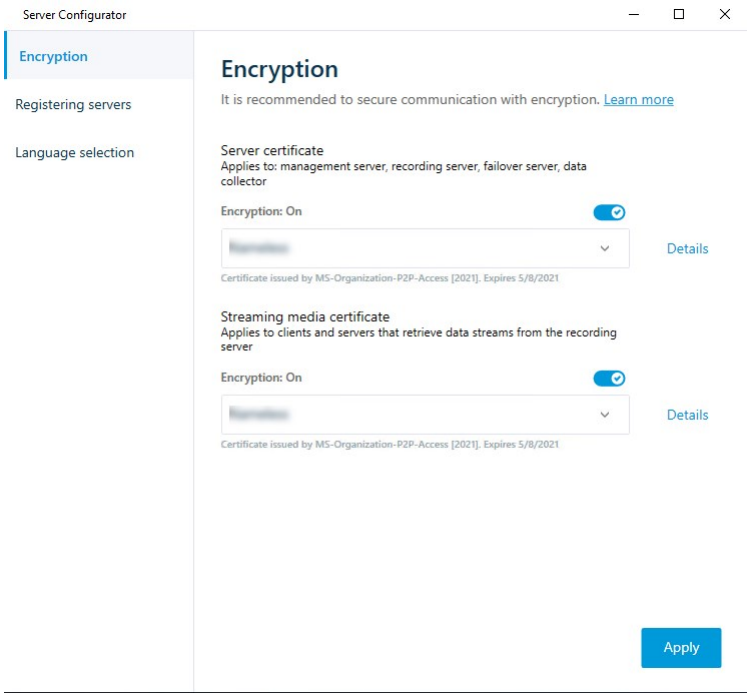
1. Em um computador com Management Server ou Recording Server instalado, abra o **Server Configurator**:
   - Menu Iniciar do Windows Start

   ou

   - Do gerenciador do servidor, clicando com o botão direito no ícone do gerenciador do servidor na barra de tarefas do computador
2. No **Server Configurator**, em **Certificado do servidor**, habilite o **Encryption**.
3. Clique em **Selecionar certificado** para abrir uma lista com nomes de entidade únicos que têm uma chave privada e estão instalados no Repositório de certificados do Windows no computador local.
4. Selecione um certificado para criptografar a comunicação entre o servidor de gravação, servidor de gerenciamento, servidor de emergência e servidor coletor de dados.

   Selecione **Detalhes** para visualizar as informações do Repositório de certificados do Windows sobre o certificado selecionado.

   O usuário do serviço Recording Server recebeu acesso à chave privada. É necessário que esse certificado seja confiável em todos os clientes.



5. Clique em **Aplicar**.

> Ao aplicar certificados, o servidor de gravação será interrompido e reiniciado. Parar o serviço do Recording Server significa que você não pode gravar e visualizar vídeo ao vivo enquanto estiver verificando ou alterando a configuração básica do servidor de gravação.

Ativar criptografia do servidor de eventos

Você pode criptografar a conexão bidirecional entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos , incluindo o LPR Server.

> Quando configurar a criptografia para um grupo de servidores, ela deve ser habilitada com um certificado pertencente ao mesmo certificado CA ou, se desabilitada, deve ser desabilitada em todos os computadores do grupo de servidores.

Pré-requisitos:

- Um certificado de autenticação do servidor é confiado no computador que abriga o servidor de eventos

Primeiro, ative a criptografia no servidor de eventos.

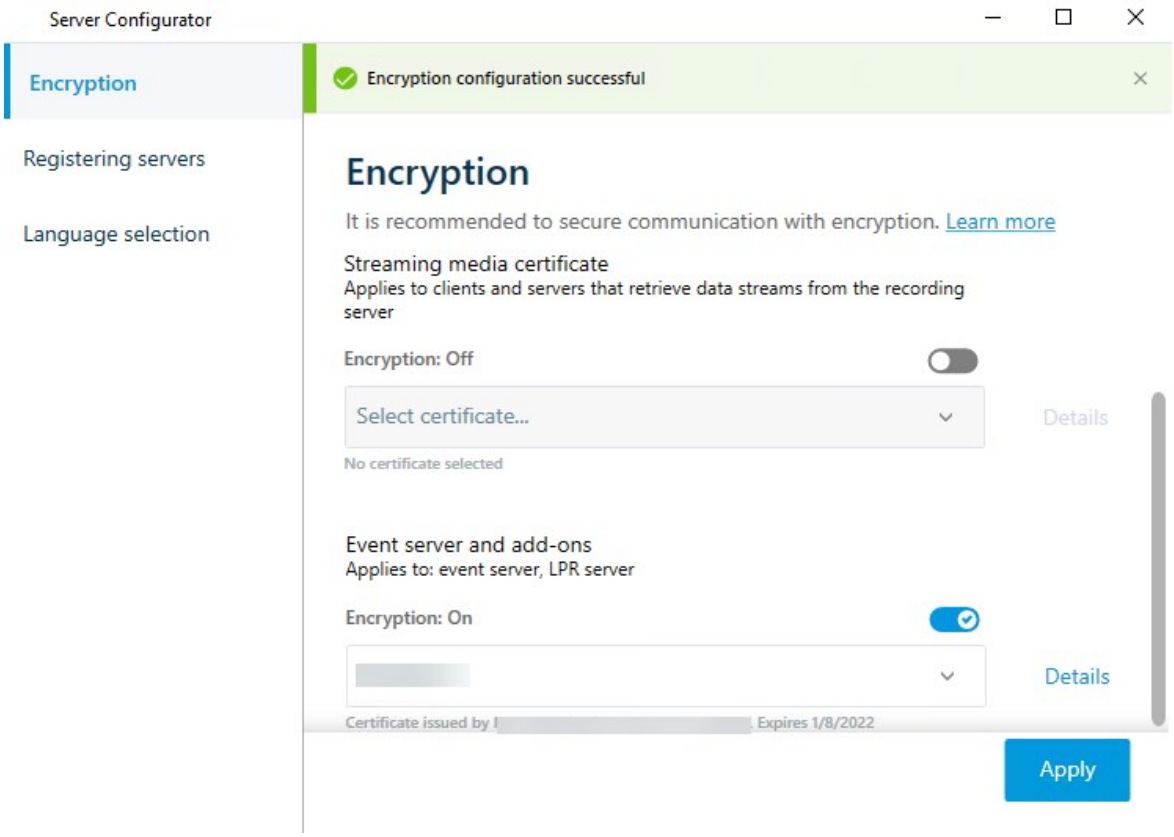
Etapas:

1. Em um computador com um servidor de eventos instalado, abra o **Server Configurator** de:
   - Menu Iniciar do Windows Start

   ou

   - O Event Server clicando com o botão direito no ícone Event Server na barra de tarefas do computador
2. No **Server Configurator**, em **Servidor de eventos e add-ons**, ative **Criptografia**.
3. Clique em **Selecionar certificado** para abrir uma lista com nomes de entidade únicos que têm uma chave privada e estão instalados no Repositório de certificados do Windows no computador local.
4. Selecione um certificado para criptografar a comunicação entre o servidor de eventos e os complementos relacionados.

   Selecione **Detalhes** para visualizar as informações do Repositório de certificados do Windows sobre o certificado selecionado.



5. Clique em **Aplicar**.

Para concluir a habilitação da criptografia, a próxima etapa é atualizar as configurações de criptografia em cada extensão relacionada do LPR Server.

Ative a criptografia para cliente e serviços

Você pode criptografar conexões do servidor de gravação para clientes e servidores que transmitem dados do servidor de gravação.

> Quando configurar a criptografia para um grupo de servidores, ela deve ser habilitada com um certificado pertencente ao mesmo certificado CA ou, se desabilitada, deve ser desabilitada em todos os computadores do grupo de servidores.

Pré-requisitos:

- O certificado de autenticação a ser usado é confiável em todos os computadores executando serviços que recuperam fluxos de dados do servidor de gravação
- XProtect Smart Client e todos os serviços que recuperam fluxos de dados do servidor de gravação devem ser da versão 2019 R1 ou superior
- Algumas soluções de terceiros criadas usando versões de MIP SDK anteriores à 2019 R1 podem precisar ser atualizadas.

Etapas:

1. Em um computador com um servidor de gravação instalado, abra o **Server Configurator** de:
   - Menu Iniciar do Windows Start

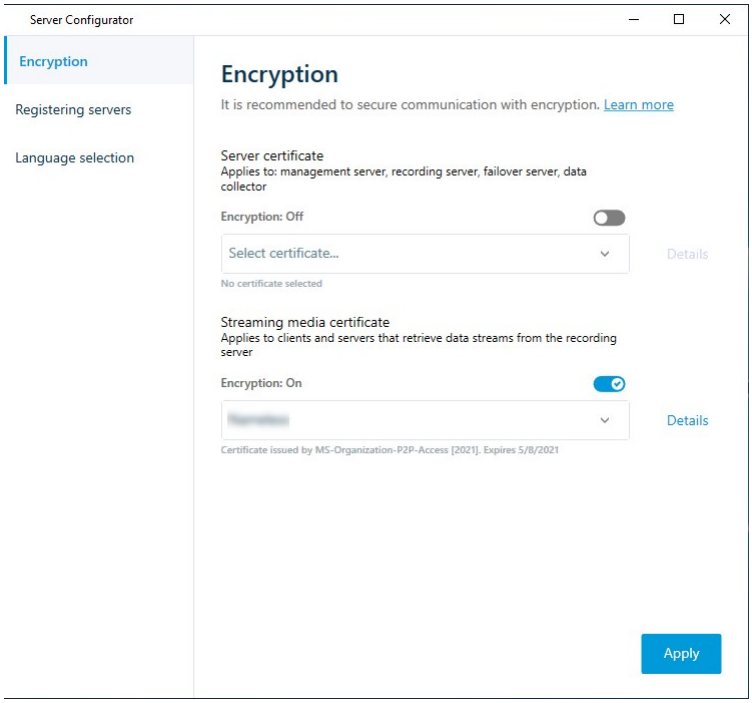
   ou

   - O Recording Server Manager clicando com o botão direito no ícone Recording Server Manager na barra de tarefas do computador
2. No **Server Configurator**, em **Certificado do servidor**, habilite a **Criptografia**.
3. Clique em **Selecionar certificado** para abrir uma lista com nomes de entidade únicos que têm uma chave privada e estão instalados no Repositório de certificados do Windows no computador local.
4. Selecione um certificado para criptografar a comunicação entre os clientes e servidores que recuperam fluxos de dados dos servidores de gravação.

   Selecione **Detalhes** para visualizar as informações do Repositório de certificados do Windows sobre o certificado selecionado.

   O usuário do serviço Recording Server recebeu acesso à chave privada. É necessário que esse

certificado seja confiável em todos os clientes.



5. Clique em **Aplicar**.

Ao aplicar certificados, o servidor de gravação será interrompido e reiniciado. Parar o serviço do Recording Server significa que você não pode gravar e visualizar vídeo ao vivo enquanto estiver verificando ou alterando a configuração básica do servidor de gravação.

Para verificar se o servidor de gravação usa criptografia, consulte Visualizar status de criptografia para clientes.

Ativar criptografia no servidor móvel

Para usar um protocolo HTTPS seguro para estabelecer conexão entre o servidor móvel e clientes e serviços, você deve aplicar um certificado válido ao servidor. O certificado confirma que o titular do certificado está autorizado a estabelecer conexões seguras.

Para obter mais informações, consulte o guia de certificados sobre como proteger suas XProtect VMS instalações.

Quando configurar a criptografia para um grupo de servidores, ela deve ser habilitada com um certificado pertencente ao mesmo certificado CA ou, se desabilitada, deve ser desabilitada em todos os computadores do grupo de servidores.

Certificados emitidos pela AC (Autoridade de Certificação) têm uma cadeia de certificados e na raiz de tal cadeia há o certificado raiz da AC. Quando um dispositivo ou navegador encontra esse certificado, ele compara seu certificado raiz com os certificados pré-instalados no SO (Android, iOS, Windows, etc.). Se o certificado raiz estiver listado na lista de certificados pré-instalados, o SO garante ao usuário que a conexão com o servidor é suficientemente segura. Esses certificados são emitidos para um nome de domínio e não são gratuitos.

Etapas:

1. Em um computador com um servidor móvel instalado, abra o **Server Configurator** de:
   - Menu Iniciar do Windows Start

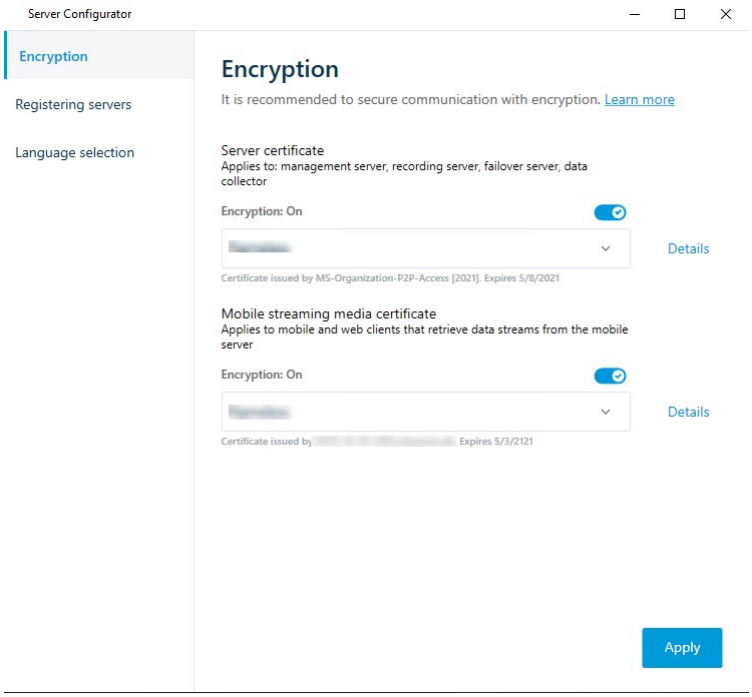
   ou

   - O Mobile Server Manager clicando com o botão direito no ícone Mobile Server Manager na barra de tarefas do computador
2. No **Server Configurator**, em **Certificado de mídia de streaming móvel**, habilite a **Criptografia**.
3. Clique em **Selecionar certificado** para abrir uma lista com nomes de entidade únicos que têm uma chave privada e estão instalados no Repositório de certificados do Windows no computador local.
4. Selecione um certificado para criptografar a comunicação do cliente XProtect Mobile e com o servidor móvel XProtect Web Client.

   Selecione **Detalhes** para visualizar as informações do Repositório de certificados do Windows sobre o certificado selecionado.

   O usuário do serviço Mobile Server recebeu acesso à chave privada. É necessário que esse certificado

seja confiável em todos os clientes.



5. Clique em **Aplicar**.

> Quando você aplica certificados, o serviço Mobile Server é reiniciado.

Milestone Federated Architecture

Configure seu sistema para executar sites federados

Para preparar seu sistema para a Milestone Federated Architecture, é necessário fazer determinadas opções ao instalar o servidor de gerenciamento. Dependendo de como sua estrutura de TI está configurada, escolha entre três alternativas diferentes.

Alternativa 1: Conectar sites no mesmo domínio (com usuário do domínio comum)

Antes da instalação do servidor de gerenciamento, deve ser criado um usuário de domínio comum e configurá-lo como administrador em todos os servidores envolvidos na hierarquia de sites federados. A forma como você conecta os sites depende da conta de usuário criada.

Com uma conta de usuário do Windows

1. Inicie a instalação do produto no servidor a ser usado como o servidor de administração e selecione **Personalizado**.
2. Selecione para instalar o serviço Management Server usando uma conta de usuário. A conta de usuário selecionada deve ser a conta de administrador usada em todos os servidores de gerenciamento. O mesmo usuário também precisa ser usado na instalação de outros servidores de gerenciamento na configuração da hierarquia de sites federados.
3. Termine a instalação. Repita os passos 1-3 para instalar outros sistemas que você queira conectar à hierarquia de sites federados.
4. Adicionar site à hierarquia (consulte Adicionar site à hierarquia na página 321).

Com uma conta de usuário interna do Windows (serviço de rede)

1. Inicie a instalação do produto no primeiro servidor para ser usado como o servidor de gerenciamento e selecione **Um único computador** ou **Personalizado**. Isto instalará o servidor de gerenciamento usando uma conta do serviço de rede. Repita essa etapa para todos os sites na hierarquia de sites federados.
2. Faça o login no site que você deseja como central de controle na hierarquia de sites federados.
3. No Management Client, expanda **Segurança** > **Funções** > **Administradores**.
4. Na guia **Usuários e Grupos**, clique em **Adicionar** e selecione **Usuário do Windows**.
5. Na caixa de diálogo, selecione **Computadores** como tipo de objeto, digite o nome do servidor do site federado e clique em **OK** para adicionar o servidor à função de **Administrador** da central de controle. Repita esta etapa até que tenha adicionado todos os sites federados desta forma e saia do aplicativo.
6. Faça login em cada site federado, e adicione os seguintes servidores à função de **Administrador**, da mesma forma como acima:
   - O servidor do site primário.
   - Os servidores dos sites secundários que deseja conectar diretamente a este site federado.
7. Adicionar site à hierarquia (consulte Adicionar site à hierarquia na página 321).

Alternativa 2: Conectar sites em domínios diferentes

Para conectar sites em domínios diferentes assegure-se de que os domínios sejam certificados uns pelos outros. A configuração de domínios para certificação de uns pelos outros é feita através da configuração de domínios do Microsoft Windows. Após estabelecida a certificação entre os diferentes domínios em cada site na hierarquia de sites federados, siga a mesma descrição que aparece na Alternativa 1. Para maiores informações sobre como configurar domínios certificados, consulte o website da Microsoft (https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/).

A Milestone recomenda o Milestone Interconnect para a criação de sistemas de múltiplos sites com vários domínios.

Alternativa 3: Conectar sites em grupo(s) de trabalho

Ao conectar sites em grupo(s) de trabalho, a mesma conta de administrador precisa estar presente em todos os computadores que você deseja conectar na hierarquia de sites federados. Você deve definir a conta de administrador antes de instalar o sistema.

1. Acesse o **Windows** usando uma conta de administrador comum.
2. Inicie a instalação do produto e clique **Personalizado**.
3. Selecione instalar o serviço Management Server usando a conta de administrador comum.
4. Termine a instalação. Repita os passos 1-4 para instalar outros sistemas que você desejar conectar. Todos os sistemas precisam ser instalados usando a conta de administrador comum.
5. Adicionar site à hierarquia (consulte Adicionar site à hierarquia na página 321).

A Milestone recomenda o Milestone Interconnect para a criação de sistemas de múltiplos sites quando os sites não são parte de um domínio.

Você não pode misturar domínio (s) e grupo de trabalho (s). Isso quer dizer que não é possível conectar sites de um domínio a sites de um grupo de trabalho e vice-versa.

Adicionar site à hierarquia

Conforme você expande seu sistema, você pode adicionar sites ao seu site principal e aos sites filho, contanto que o sistema esteja configurado corretamente.

Ao adicionar um site não seguro ao Milestone Federated Architecture, certifique-se de que a opção **Permitir conexões não seguras ao servidor** esteja ativada em **Ferramentas** > **Opções** > **Configurações gerais** no Management Client.

1. Selecione o painel **Hierarquia de sites federados**.
2. Selecione o site ao qual deseja adicionar um site filho, clique com o botão direito e clique em **Adicionar site a Hierarquia**.
3. Insira a URL do site solicitado na janela **Adicionar site à hierarquia** e clique em **OK**.
4. O site pai envia uma solicitação de conexão ao site filho e após algum tempo, um link entre os dois sites é adicionado ao painel **Hierarquia de sites federados**.

5. Se for possível estabelecer a conexão com o site filho sem solicitar aprovação ao administrador do site filho, vá para a etapa 7.

   Se **não**, o site filho apresentará o ícone aguardando a aceitação  até que o administrador do site filho autorize a solicitação.

6. Certifique-se de que o administrador do site filho autoriza a solicitação de link do site pai (consulte Aceitar inclusão na hierarquia na página 322).

7. O novo link pai/filho é estabelecido e o painel **Hierarquia de sites federados** é atualizado com o ícone  para o novo site filho.

Aceitar inclusão na hierarquia

Quando um site filho recebe uma solicitação de link de um site pai potencial onde o administrador não tem permissões de administrador para o site filho, ele tem o ícone aguardando aceitação  .

Para aceitar uma solicitação de link:

1. Faça o login no site.
2. No painel **Hierarquia de sites federados**, clique com o botão direito do mouse no home site e clique em **Aceitar inclusão na hierarquia**.

   Se o site executa a versão XProtect Expert, clique com o botão direito no site no painel **Navegação do site**.

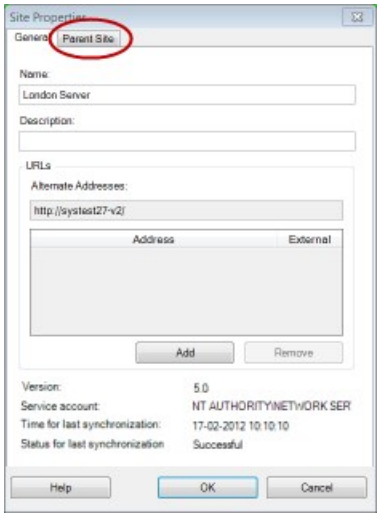
3. Clique em **Sim**.
4. O novo link pai/filho é estabelecido e o painel **Hierarquia de sites federados** é atualizado com o ícone  de site normal para o site selecionado.

> Alterações feitas nos sites filho localizados longe do site pai podem levar algum tempo para serem mostrados no painel **Hierarquia de Sites Federados**.

Configurar propriedades do site

Você pode visualizar e, possivelmente, editar as propriedade de seu home site e dos sites filhos dele.

1. No Management Client, no painel **Hierarquia de sites federados**, escolha o site relevante, clique com o botão direito e selecione **Propriedades**.



2. Se necessário, mude o seguinte:

   Guia **Geral** (consulte Guia Geral na página 606)

   Guia **Site pai** (consulte Guia Site Pai na página 607) **(disponível somente em sites filhos)**

> Devido a problemas de sincronização, qualquer alteração realizada no filho remoto pode levar algum tempo para ser refletida no painel de **Navegação do site**.

Atualizar hierarquia de site

O sistema faz a sincronização automática regularmente da hierarquia através de todos níveis de sua configuração pai/filho. Você pode atualizá-la manualmente se deseja ver as alterações refletidas instantaneamente na hierarquia, e não quer esperar pela próxima sincronização automática.

É necessário ter feito login em um site para realizar uma atualização manual. Somente alterações salvas por esse site desde a última sincronização serão mostradas na atualização. Isso significa que alterações feitas mais para baixo na hierarquia talvez não sejam refletidas pelo atualização manual, se as alterações ainda não tiverem atingido o site.

1. Faça login no site relevante.
2. Clique com o botão direito no site principal no painel **Hierarquia de Sites Federados** e clique em **Atualizar hierarquia do site**.

   Isso levará alguns segundos.

Faça login em outros sites na hierarquia

Você pode se conectar a outros sites e administrá-los. O site ao qual você está logado é o seu home site.

1. No painel da **Hierarquia de Sites Federados**, clique com o botão direito no site em que deseja fazer login.
2. Clique **Login no Site**.

   O Management Client desse site é aberto.
3. Digite as informações de login e clique em **OK**.
4. Feito o login, você está pronto para fazer suas tarefas administrativas nesse site.

Atualizar informações de sites filho.

> Esta seção só é relevante se você usa o XProtect Corporate ou XProtect Expert 2014 ou mais recente.

Em uma configuração maior do Milestone Federated Architecture com muitos sites filho, é fácil perder a visão geral e pode ser difícil encontrar as informações de contato para os administradores de cada site filho.

Portanto, você pode adicionar informações adicionais a cada site filho e essas informações estarão disponíveis para os administradores da central de controle.

Você pode ler as informações sobre o site, se passar o mouse sobre o nome do site no painel **Hierarquia de sites federados**. Para atualizar Informações sobre o site:

1. Faça o login no site.
2. Clique no painel **Navegação do site** e selecione **Informações do site**.
3. Clique em **Editar** e adicione as informações relevantes em cada categoria.

Desanexar site da hierarquia

Quando você desanexa um site do site pai, o link entre os sites é quebrado. Você pode desanexar sites a partir da central de controle, do próprio site ou do site pai.

1. No painel **Hierarquia de Sites Federados**, clique com o botão direito do mouse no home site e clique em **Desanexar site da hierarquia**.
2. Clique **Sim** para atualizar o painel **Hierarquia de sites federados**.

   Se o site desanexado tem sites filhos, este se torna o novo site de topo para este ramo da hierarquia, e o ícone de site normal muda para um ícone de site de topo.
3. Clique em **OK**.

As mudanças na hierarquia são mostradas após uma atualização manual ou uma sincronização automática.

Milestone Interconnect

Adicione uma base remota para o seu site central Milestone Interconnect

Adicione bases remotas à central de controle com o assistente **Adicionar Hardware**.
Requisitos

- Licenças de câmera Milestone Interconnect suficientes (consulte Milestone Interconnect e licenciamento na página 96).
- Outro sistema XProtect configurado e funcionando incluindo uma conta de usuário (usuários básicos, usuário local do Windows ou usuário do Active Directory do Windows) com permissões para os dispositivos que o sistema XProtect Corporate central deve poder acessar
- Conexão de rede entre a central de controle XProtect Corporate e bases remotas com acesso ou porta encaminhando para as portas usadas em bases remotas

Para adicionar uma base remota:

1. Na central de controle, expanda **Servidores** e selecione **Servidores de gravação**.
2. No painel **Visão geral**, expanda o servidor de gravação relevante e clique com o botão direito do mouse.
3. Selecione **Adicionar funções** para iniciar um assistente.
4. Na primeira página, selecione **Varredura de intervalo de endereços** ou **Manual** e clique em **Avançar**.
5. Especifique os nomes e senhas do usuário. A conta do usuário deve ser predefinida no sistema remoto. Você pode adicionar quantos nomes e senhas de usuários forem necessários clicando em **Adicionar**. Quando tiver concluído, clique em **OK**.
6. Selecione quais drivers usar ao fazer a varredura. Nesse caso, escolha entre os drivers Milestone. Clique em **Avançar**.
7. Especifique os endereços IP e os números de porta sobre os quais deseja fazer a varredura. O padrão é a porta 80. Clique em **Avançar**.

   Aguarde enquanto o sistema detecta as bases remotas. Um indicador de status mostra o processo de detecção. Em caso de êxito da detecção, será exibida uma mensagem de **Sucesso** na coluna **Status**. Se você não conseguir adicionar, clique na mensagem de erro **Falha** para saber o motivo.
8. Escolha habilitar ou desabilitar sistemas detectados com sucesso. Clique em **Avançar**.
9. Aguarde enquanto o sistema detecta o hardware e recolhe informações específicas do dispositivo. Clique em **Avançar**.
10. Escolha habilitar ou desabilitar hardware e dispositivos detectados com sucesso. Clique em **Avançar**.
11. Selecione um grupo padrão. Clique em **Concluir**.
12. Após a instalação, você pode ver o sistema e seus dispositivos no painel **Visão Geral**.

    Dependendo das permissões do usuário selecionado na base remota, a central de controle tem acesso a todas as câmeras e funções ou a um subconjunto delas.

Atribua permissões de usuário

Você configura as permissões do usuário para uma câmera interconectada como faz com outras câmeras, criando uma função e atribuindo acesso a funções.

1. No site central, no painel **Navegação do site**, expanda **Segurança** e selecione **Funções**.
2. No painel Visão geral, clique com o botão direito na função de administrador integrada e selecione **Adicionar função** (consulte Adicionar e gerenciar uma função).
3. Dê um nome para a função e defina as configurações na guia **Dispositivo** (consulte a guia Dispositivo (funções)) e a guia **Gravações remotas** (consulte Guia Gravações remotas (funções)).

Atualizar o hardware da base remota

Se a configuração foi alterada em uma base remota, como câmeras e eventos adicionados ou removidos, por exemplo, você deve atualizar as configurações na central de controle para que a nova configuração seja refletida na base remota.

1. Na central de controle, expanda **Servidores** e selecione **Servidores de gravação**.
2. No painel **Visão geral**, expanda o servidor de gravação desejado, selecione o sistema remoto relevante. Clique com o botão direito do mouse.
3. Selecione **Atualizar hardware**. Isso abre a caixa de diálogo **Atualizar hardware**.
4. A caixa de diálogo lista todas as alterações (dispositivos removidos, atualizados e adicionados) no sistema remoto desde o último estabelecimento ou atualização da configuração do Milestone Interconnect. Clique em **Confirmar** para atualizar sua central de controle com essas alterações.

Permitir a reprodução diretamente da câmera da base remota

Se a sua central de controle estiver continuamente conectada com as bases remotas da própria central, você pode configurar o seu sistema para que os usuários reproduzam as gravações diretamente das bases remotas. Para obter mais informações, consulte Configurações Milestone Interconnect (explicado) na página 96.

1. Na central de controle, expanda **Servidores** e selecione **Servidores de gravação**.
2. No painel **Visão geral**, expanda o servidor de gravação desejado, selecione o sistema remoto relevante. Selecione a câmera remota relevante.
3. No painel Propriedades, selecione a guia **Gravar** e selecione a opção **Reproduzir gravações da base remota**.
4. Na barra de ferramentas, clique em **Salvar**.

Em uma configuração Milestone Interconnect, a central de controle desconsidera as máscaras de privacidade definidas em uma base remota. Se você deseja aplicar as mesmas máscaras de privacidade, você deve redefini-las na central de controle.

Recuperar gravações remotas da câmera da base remota

Se a sua central de controle **não** estiver conectada de forma contínua com as bases remotas da própria central, você pode configurar o seu sistema para centralizar o armazenamento de gravações remotas e também para recuperar as gravações remotas quando a conexão de rede for ideal. Para obter mais informações, consulte Configurações Milestone Interconnect (explicado) na página 96.

Para permitir que os usuários realmente recuperem gravações, você deve ativar essa permissão para a função relevante (consulte Funções (Segurança)).

Para configurar o seu sistema:

1. Na central de controle, expanda **Servidores** e selecione **Servidores de gravação**.
2. No painel **Visão geral**, expanda o servidor de gravação desejado, selecione o sistema remoto relevante. Selecione o servidor remoto.
3. No painel Propriedades, selecione a guia **Recuperação remota** e atualize as configurações (consulte Guia Recuperação remota na página 444).

Caso a rede falhe por algum motivo, a central de controle omite sequências de gravação. Você pode configurar o seu sistema para que a base remota recupere automaticamente as gravações remotas a fim de cobrir o período de inatividade, depois que a rede tiver sido restabelecida.

1. Na central de controle, expanda **Servidores** e selecione **Servidores de gravação**.
2. No painel **Visão geral**, expanda o servidor de gravação desejado, selecione o sistema remoto relevante. Selecione a câmera relevante.
3. No painel Propriedades, selecione a guia **Gravar**, e selecione a opção **Recuperar automaticamente as gravações remotas quando a conexão estiver restaurada** (consulte Salvar e recuperar gravação remota).
4. Na barra de ferramentas, clique em **Salvar**.

Como alternativa, você pode usar regras ou iniciar as recuperações da gravação remota do XProtect Smart Client, quando necessário.

Em uma configuração Milestone Interconnect, a central de controle desconsidera as máscaras de privacidade definidas em uma base remota. Se você deseja aplicar as mesmas máscaras de privacidade, você deve redefini-las na central de controle.

Configure a sua central de controle para responder aos eventos de bases remotas

Você pode usar eventos definidos em bases remotas para disparar alarmes e regras na sua central de controle e, assim, responder imediatamente a eventos de bases remotas. Isso exige que as bases remotas estejam conectadas e on-line. O número e o tipo de eventos dependem dos eventos configurados nos sistemas remotos.

A lista de eventos compatíveis está disponível no website Milestone (https://www.milestonesys.com/).

Você não pode excluir eventos predefinidos.

Requisitos:

- Se você desejar usar eventos manuais/definidos pelos usuários como eventos desencadeadores a partir de bases remotas, você deve primeiro criar tais eventos nas bases remotas
- Certifique-se de que você tem uma lista atualizada dos eventos a partir de bases remotas (consulte Atualizar o hardware da base remota na página 326).

Adicione um evento manual/definido pelo usuário a partir de uma base remota:

1. Na central de controle, expanda **Servidores** e selecione **Servidores de gravação**.
2. No painel de Visão Geral, selecione o servidor remoto e a **Guia de eventos**.
3. A lista contém os eventos predefinidos. Clique em **Adicionar** para incluir na lista eventos definidos pelo usuário ou manuais a partir da base remota.

Use um evento em uma base remota para acionar um alarme na central de controle:

1. Na central de controle, expanda **Alarmes** e selecione **Definições de Alarme**.
2. No painel Visão geral, clique com o botão direito do mouse em **Definições de Alarme** e clique em **Adicionar Novo**.
3. Insira os valores conforme a necessidade.
4. No campo **Desencadeamento de evento**, você pode selecionar entre os eventos predefinidos suportados e os definidos pelo usuário.
5. No campo **Fontes**, selecione o servidor remoto que representa a base remota da qual você deseja que os alarmes venham.
6. Quando terminado, salve as configurações.

Use um evento em uma base remota para acionar uma regra de ação baseada na central de controle:

1. Na central de controle, expanda **Regras e Eventos** e selecione **Regras**.
2. No Painel de visão geral, clique com o botão direito do mouse no item **Regras** e clique em **Adicionar Regra**.
3. No assistente exibido, selecione **Executar uma ação em <evento>**.
4. Na área **Editar a descrição da regra**, clique em **evento** e selecione entre os eventos predefinidos suportados e os definidos pelo usuário. Clique em **OK**.
5. Clique em **dispositivos/servidor de gravação/servidor de gerenciamento** e selecione o servidor remoto que representa a base remota para a qual você deseja que a central de controle inicie uma ação. Clique em **OK**.
6. Clique em **Avançar** para ir para a próxima página do assistente.

7. Selecione as condições que pretende aplicar para esta regra. Se você não selecionar nenhuma condição, a regra sempre aplicará. Clique em **Avançar**.
8. Selecione uma ação e especifique os detalhes na área **Editar a descrição da regra**. Clique em **Avançar**.
9. Selecione um critério de parada, se necessário. Clique em **Avançar**.
10. Selecione uma ação de paragem se necessário. Clique em **Concluir**.

Serviços de conexão remota

Serviços de conexão remota (explicado)

> As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

O recurso Serviços de conexão remota contém a tecnologia de conexão de câmera Axis One-click desenvolvida pela Axis Communications. Isso permite que o sistema recupere vídeo (e áudio) de câmeras externas, onde firewalls e/ou a configuração de rede de roteador normalmente impedem iniciar conexões a tais câmeras. A comunicação real ocorre através de servidores de túnel seguros (servidores ST). Servidores ST usam VPN. Somente dispositivos que tenham uma chave válida funcionam dentro de uma VPN. Isso oferece um túnel seguro onde redes públicas podem compartilhar dados de forma segura.

Os Serviços de conexão remota permitem que você

- Editar credenciais dentro do Axis Dispatch Service
- Adicionar, editar e remover servidores ST
- Registrar/cancelar registro e editar câmeras Axis One-click
- Ir para o hardware relacionado à câmera Axis One-Click

Instale o ambiente de servidor de túnel seguro para a conexão da câmera One-click

Antes que você possa usar a conexão da câmera Axis One-click, você deve primeiro instalar um ambiente adequado de servidor ST. Para trabalhar com ambientes de servidor de túnel seguro (servidor ST) e com câmeras Axis One-click, você deve primeiro falar com seu provedor do sistema para obter o nome de usuário e senha necessários para os serviços Axis Dispatch.

Requisitos

- Fale com o administrador do sistema para obter o nome de usuário e senhas necessários para Axis Dispatch Services
- Assegure-se de que a sua câmera é compatível com o Axis Video Hosting System. Vá para o site da web

da Axis para ver os dispositivos suportados (https://www.axis.com/products/axis-guardian)

- Se necessário, atualize suas câmeras Axis com o firmware mais recente. Vá para o site da web da Axis para o download do firmware (https://www.axis.com/support/firmware)

1. Na página inicial de cada câmera, vá para **Configurações básicas**, **TCP/IP**, e selecione **Ativar AVHS** e **Sempre**.
2. A partir do seu servidor de gerenciamento, vá para a Milestone página de download (https://www.milestonesys.com/downloads/) e faça o download do software **AXIS One-Click**. Execute o programa para configurar uma framework adequada de túnel seguro Axis.

Adicione ou edite servidores de túnel seguros

A comunicação para serviços de conexão remota ocorre por meio de servidores de túnel seguro (servidores ST).

1. Faça um dos seguintes:
   - Para adicionar um servidor ST, clique com o botão direito no nó superior **Servidores de túnel seguros Axis** e selecione **Adicionar servidor de túnel seguro Axis**
   - Para editar um servidor ST, clique com o botão direito e selecione **Editar servidor de túnel seguro Axis**
2. Na janela que aparece, preencha as informações relevantes.
3. Se optar por usar as credenciais usadas na instalação do **Componente Axis One-Click Connection**, selecione a caixa de seleção **Usar credenciais** e preencha o mesmo nome de usuário e senha usados para o **Componente Axis One-Click Connection**.
4. Clique em **OK**.

Registrar nova câmera Axis One-Click

1. Para registrar uma câmera em um servidor ST, clique nela com o botão direito e selecione **Registrar câmera Axis One-Click**.
2. Na janela que aparece, preencha as informações relevantes.
3. Clique em **OK**.
4. A câmera agora aparece embaixo do servidor ST relevante.

A câmera pode ter a seguinte codificação por cores:

Cor	Descrição
Vermelho	Estado inicial. Registrada, mas não conectada ao servidor ST.
Amarelo	Registrada. Conectada ao servidor ST, mas não adicionada como hardware.
Verde	Adicionada como hardware. Pode estar ou não conectada ao servidor ST.

Quando você adiciona uma nova câmera, seu status está sempre verde. O status da conexão é refletido por **Dispositivos** em **Servidores de gravação** no painel **Visão geral**. No painel **Visão geral**, você pode agrupar suas câmeras para uma visão geral mais fácil. Se optar por **não** registrar sua câmera no Axis dispatch service neste ponto, poderá fazê-lo posteriormente, a partir do menu por clique com botão direito (selecione **Editar câmera Axis One-Click**).

Mapas inteligentes

Fundos geográficos (explicado)

Antes que um usuário do XProtect Smart Client possa selecionar um fundo geográfico, primeiro você precisa configurar os fundos geográficos no XProtect Management Client.

- **Mapa-múndi básico** – usa o fundo geográfico padrão fornecido em XProtect Smart Client. Isso não requer configuração. Este mapa deve ser usado como referência geral e não contém elementos como fronteiras de países, cidades ou outros detalhes. No entanto, como os outros fundos geográficos, ele contém dados de georreferência
- **Bing Maps** – conecte-se ao Bing Maps
- **Google Maps** – conecte-se ao Google Maps
- **Milestone Map Service** - conectar a um provedor de mapa gratuito. Após ativar o Milestone Map Service, nenhuma outra etapa é necessária.

  Consulte Ativar o Milestone Map Service

- **OpenStreetMap** - conectar a:
  - Um servidor de bloco comercial de sua preferência.
  - O seu próprio servidor de blocos, online ou local

  Consulte Especificar servidor de blocos no OpenStreetMap

> As opções Bing Maps e Google Maps exigem acesso à Internet e você deverá adquirir uma chave da Microsoft ou do Google.
>
> Milestone Map Service requer acesso à internet.
>
> A não ser que você esteja usando o seu próprio servidor de blocos local, o OpenStreetMap exigirá o acesso à Internet.

Se desejar que o sistema tenha uma instalação em conformidade com a EU GDPR, os seguintes serviços não podem ser usados:

- Bing Maps
- Google Maps
- Milestone Map Service

Para obter mais informações sobre proteção de dados e coleta de dados de uso, consulte o guia de privacidade do GDPR.

Por padrão, Bing Maps e Google Maps exibem imagens de satélite (Satélite). Você pode mudar as imagens em XProtect Smart Client, por exemplo, para aéreas e terrestres, para ver detalhes diferentes.

Ativar Bing Maps ou Google Maps no Management Client

Você pode disponibilizar uma chave para vários usuários introduzindo-a em um perfil do Smart Client no Management Client. Todos os usuários que atribuídos ao perfil irão utilizar esta chave.

Etapas:

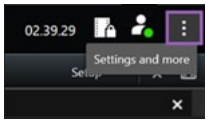
1. Em Management Client, no painel de **Navegação do Site**, clique em **Perfis Smart Client**.
2. No painel **Smart Client Perfis**, selecione o perfil Smart Client relevante.
3. No painel **Propriedades**, clique na aba **Mapa inteligente**:
   - Para o Bing Maps, insira a sua chave básica ou corporativa no campo **Chave Bing Maps**
   - Para Google Maps, insira a sua chave API estática de mapas no campo **Chave privada para Google Maps**
4. Para evitar que os operadores XProtect Smart Client usem uma chave diferente, selecione a caixa de verificação **Bloqueado**.

Ativar Bing Maps ou Google Maps no XProtect Smart Client

Para permitir que os operadores XProtect Smart Client usem uma chave diferente da chave do perfil Smart Client, é preciso inserir a chave nas configurações em XProtect Smart Client.

Etapas:

1. No XProtect Smart Client, abra a janela **Configurações**.



2. Clique em **Mapa inteligente**.

3. Dependendo do serviço de mapa que deseja usar, proceda de uma das seguintes maneiras:
   - Para o Bing Maps, digite a sua chave no campo **Bing Maps chave**. Consulte também Integração do mapa inteligente com o Bing Maps (explicado) na página 92.
   - Para o Google Maps, insira a sua chave no campo **Chave privada para Google Maps**. Consulte também Integração do mapa inteligente com o Google Maps (explicado) na página 91.

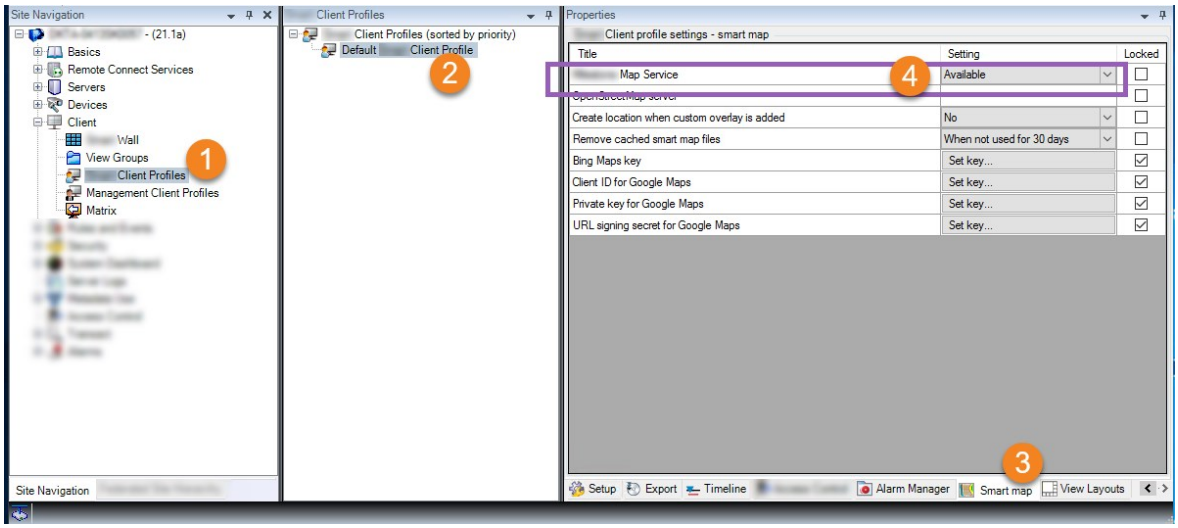
Ativar Milestone Map Service

Milestone Map Service é um serviço online que permite que você se conecte ao servidor de blocos do Milestone Systems. Este servidor de blocos usa um serviço de mapas gratuito, comercialmente disponível.

Após você ativar o Milestone Map Service no seu mapa inteligente, o mapa inteligente usará o Milestone Map Service como seu fundo geográfico.

Etapas:

1. No painel **Navegação do Site**, expanda o nó **Cliente** e clique em **Smart Client Perfis**.
2. No painel Visão geral, selecione o perfil Smart Client relevante.
3. No painel **Propriedades**, clique na aba **Mapa inteligente**.



4. No campo **Milestone Map Service**, selecione **Disponível**.
5. Para aplicar essa configuração no XProtect Smart Client, marque a caixa de seleção **Bloqueado**. Em seguida, os operadores do XProtect Smart Client não poderão ativar ou desativar o Milestone Map Service.
6. Salve as alterações.

Você também pode ativar o Milestone Map Service na janela **Configurações** em XProtect Smart Client.

Milestone Map Service requer acesso à internet.

Se você tiver um firewall restritivo ativado, é importante permitir acesso aos domínios usados. Você pode ter que permitir o tráfego de saída para Milestone Map Service usando maps.milestonesys.com em cada máquina em que o Smart Client esteja em funcionamento.

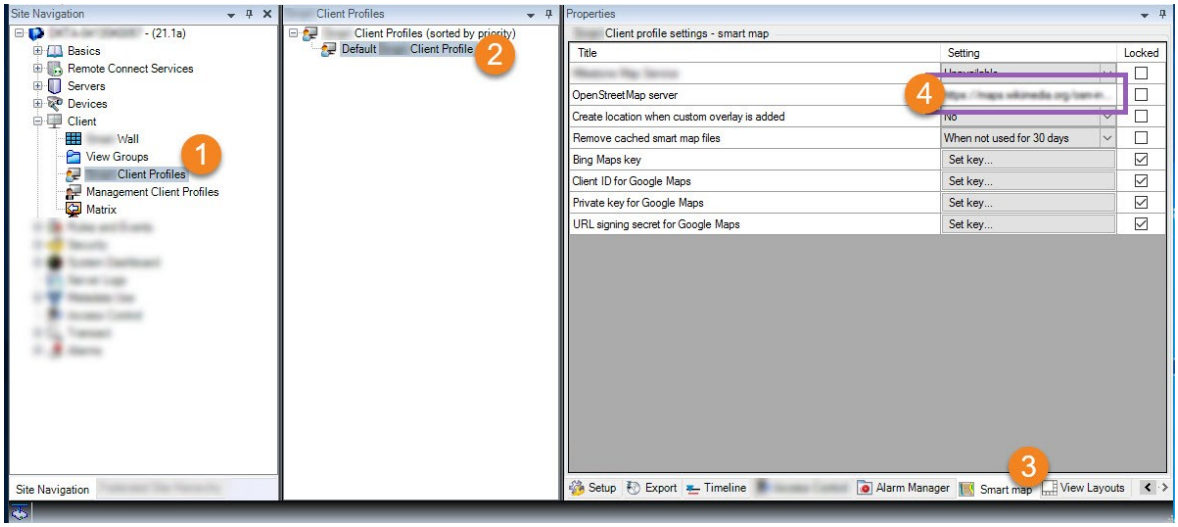
Specifique o servidor de blocos do OpenStreetMap

Se você usa a opção **OpenStreetMap** como fundo geográfico para o seu mapa inteligente, você deve especificar a origem da recuperação das imagens em bloco. Você faz isso especificando o endereço do servidor do bloco, ou um servidor de blocos comercial ou um servidor de blocos local, por exemplo, se a sua organização possui os seus próprios mapas para áreas como aeroportos ou portos.

Você também pode especificar o endereço do servidor de blocos na janela **Configurações** no XProtect Smart Client.

Etapas:

1. No painel **Navegação do Site**, expanda o nó **Cliente** e clique em **Smart Client Perfis**.
2. No painel Visão geral, selecione o perfil Smart Client relevante.
3. No painel **Propriedades**, clique na aba **Mapa inteligente**.



4. No campo **Servidor OpenStreetMap**, insira o endereço do servidor de blocos.

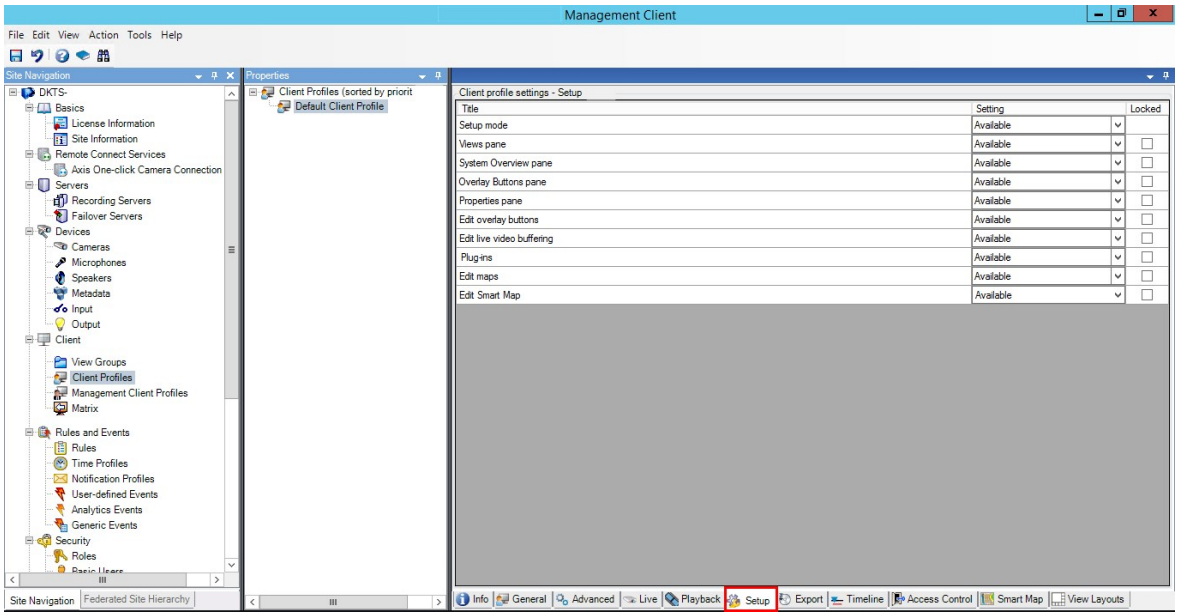
5. Para aplicar essa configuração no XProtect Smart Client, marque a caixa de seleção **Bloqueado**. Então, os operadores do XProtect Smart Client não podem alterar o endereço.
6. Salve as alterações.

Ativar a edição do mapa Inteligente

Os operadores podem editar mapas inteligentes no XProtect Smart Client no modo de configuração somente se a edição estiver ativada no Management Client. Se ainda não estiver ativada, você precisa ativar a edição para cada perfil relevante do Smart Client.

Etapas:

1. No painel **Navegação do Site**, expanda o nó **Cliente**.
2. Clique em **Perfis Smart Client**.



3. No painel Visão geral, selecione o perfil Smart Client relevante.
4. No painel **Propriedades**, clique na aba **Configuração**.
5. Na lista **Editar mapa inteligente**, selecione **Disponível**.
6. Repita essas etapas para cada perfil Smart Client relevante.
7. Salve suas alterações. Da próxima vez que os usuários atribuídos ao perfil Smart Client que você selecionou efetuarem o login no XProtect Smart Client, eles serão capazes de editar os mapas inteligentes.

Para desativar a edição, na lista **Editar mapa inteligente**, selecione **Indisponível**.

Ativar a edição de dispositivos no mapa inteligente

Você deve ativar a edição de dispositivos por função para permitir aos operadores, por exemplo:

- Posicione um dispositivo de entrada ou um microfone em um mapa inteligente.
- Ajuste o campo de visão de uma câmera em um mapa inteligente.

Operadores podem obter a permissão para editar os seguintes tipos de dispositivos em mapas inteligentes:

- Câmeras
- Dispositivos de entrada
- Microfones

Requisitos

Antes de iniciar, certifique-se de que a edição do mapa inteligente foi ativada (consulte Ativar a edição do mapa Inteligente na página 335). Você faz isso no perfil do Smart Client ao qual a função do operador está associada.

Etapas:

1. Expanda o **Nó de** segurança > **Funções**.
2. No painel de **Funções**, selecione a função com a qual o seu operador está associado.
3. Para dar permissões de edição à função:
    - Selecione a guia **Segurança geral**, e no painel **Configurações de função**, selecione o tipo de dispositivo (por exemplo **Câmeras** ou **Entrada**)
    - Na coluna **Permitir**, selecione a caixa de seleção **Controle total** ou **Editar**
4. Salve as alterações.

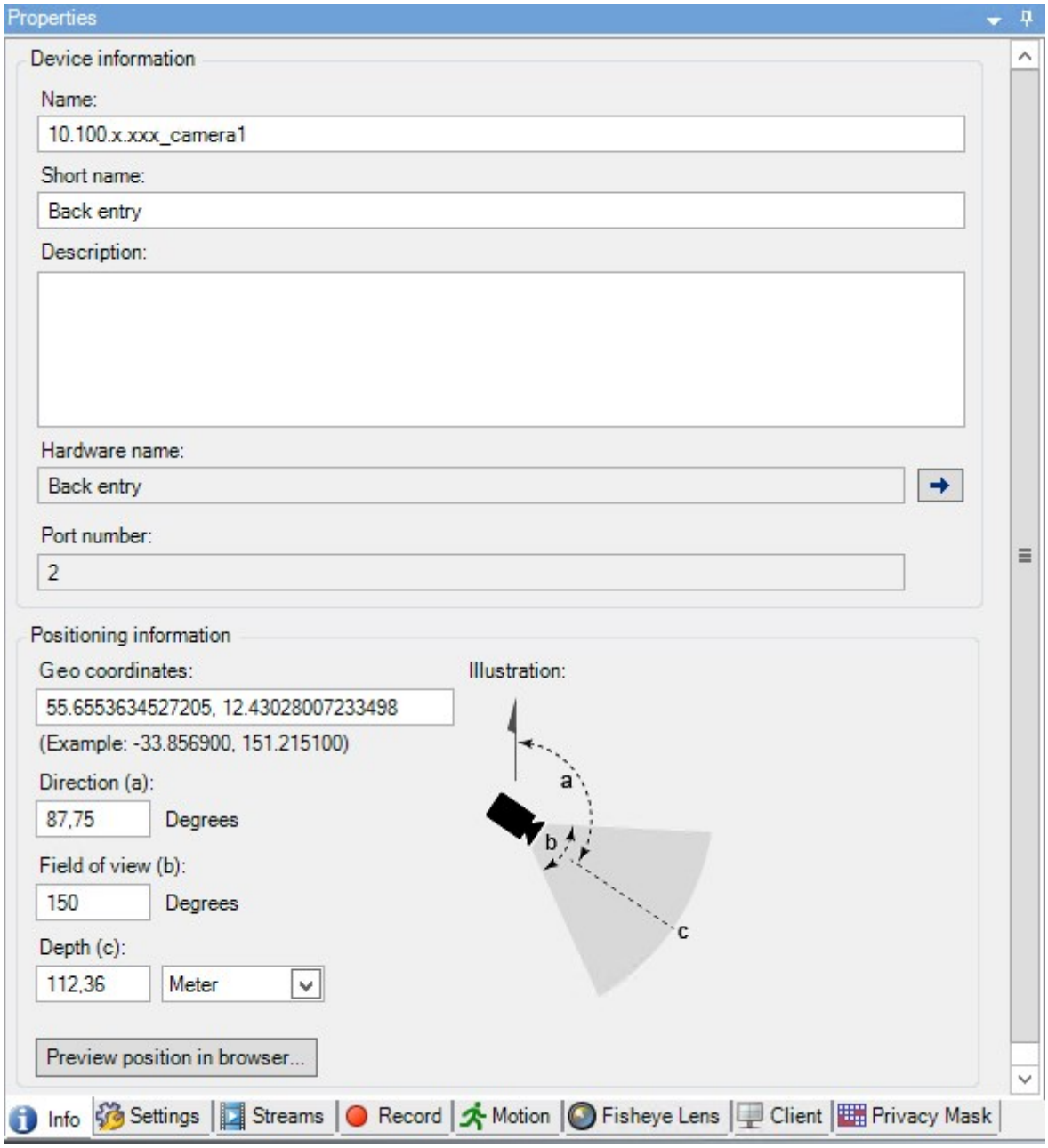
Para ativar a edição de dispositivo individuais, vá para a guia **Dispositivo** e selecione o dispositivo relevante.

Defina a posição do dispositivo e a direção da câmera, campo de visão, profundidade (mapa inteligente)

Para garantir que o dispositivo esteja posicionado corretamente no mapa inteligente, você pode definir as coordenadas geográficas do dispositivo. Para câmeras, você também pode definir a direção, o campo de visão e a profundidade da visualização. A configuração de qualquer das opções acima, adicionará o dispositivo automaticamente ao mapa inteligente na próxima vez que um operador carregar um mapa inteligente no XProtect Smart Client.

Etapas:

1. No Management Client, expanda o nó **Dispositivos** e selecione o tipo de dispositivo (por exemplo, **Câmeras** ou **Entrada**).
2. No painel **Dispositivos**, selecione o dispositivo relevante.
3. Na guia **Informações**, role para baixo para encontrar as **Informações de posicionamento**.



4. No campo **Coordenadas geográficas**, especifique as coordenadas de latitude e longitude, nessa ordem. Use um ponto como separador decimal e use uma vírgula pata separar a latitude e longitude.

- Para câmeras:
    1. No campo **Direção**, digite um valor no intervalo de 0 a 360 graus.
    2. No campo **Campo de visão**, digite um valor no intervalo de 0 a 360 graus.
    3. No campo **Profundidade**, insira a profundidade da exibição em metros ou em pés.

5. Salve as alterações.

Você também pode definir as propriedades nos servidores de gravação.

Configurar mapa inteligente com Milestone Federated Architecture

Quando você usa um mapa inteligente em um Milestone Federated Architecture, todos os dispositivos dos sites conectados aparecem no mapa inteligente. Siga as etapas abaixo para configurar o mapa inteligente em uma arquitetura federada.

Para informações gerais sobre o Milestone Federated Architecture, consulte Configurando Milestone Federated Architecture na página 97.

1. Antes de conectar os locais superiores com os secundários, assegure-se de que as coordenadas geográficas tenham sido especificadas em todos os dispositivos e todos os locais. Coordenadas geográficas são adicionadas automaticamente quando um dispositivo é posicionado no mapa inteligente através do XProtect Smart Client, mas você também pode adicioná-las manualmente no Management Client, nas propriedades do dispositivo. Para obter mais informações, consulte Defina a posição do dispositivo e a direção da câmera, campo de visão, profundidade (mapa inteligente) na página 336.
2. Você deve adicionar os operadores de Smart Client como usuários do Windows no site principal e em todos os sites federados. Pelo menos no site principal, os usuários do Windows devem ter permissões de edição no mapa inteligente. Isto permite aos usuários editar o mapa inteligente para o site principal e todos os sites filho. Em seguida, você precisa determinar se os usuários do Windows nos sites filho precisam de permissões de edição de mapa inteligente. Em Management Client, primeiro você cria os usuários do Windows em **Funções** e depois você ativa a edição do mapa inteligente. Para obter mais informações, consulte Ativar a edição do mapa Inteligente na página 335.
3. No site principal, adicione os sites filho como usuários do Windows a uma função com direitos de administrador. Quando você especificar o tipo de objeto, selecione a caixa de seleção **Computadores**.
4. Em cada um dos sites filho, adicione o site principal como um usuário do Windows à mesma função de administrador que é usada no site principal. Quando você especificar o tipo de objeto, selecione a caixa de seleção **Computadores**.

5. No site principal, certifique-se de que você possa visualizar a janela **Hierarquia de sites federados**. Em Management Client, vá para **Visualizar** e selecione **Hierarquia de site federado**. Adicione cada um dos sites filho ao site principal. Para obter mais informações, consulte Adicionar site à hierarquia na página 321.
6. Agora você pode testar se o Milestone Federated Architecture funciona no XProtect Smart Client. Faça o login no site principal como administrador ou como operador, e abra uma visualização que contenha o mapa inteligente. Se a configuração foi feita corretamente, todos os dispositivos do site principal e de todos os sites filho aparecerão no mapa inteligente. Se você fizer login em um dos sites filho, você verá somente os dispositivos daquele site e de seus sites filho.

Para editar dispositivos em um mapa inteligente, por exemplo, a posição e o ângulo da câmera, os usuários precisam de permissões de edição de dispositivo. Para obter mais informações, consulte Ativar a edição de dispositivos no mapa inteligente na página 336.

Manutenção

Fazendo backup e restauração da configuração do sistema

A Milestone recomenda que você faça backups regulares do a sua configuração de sistema como medida de recuperação de desastres.

Apesar de ser raro perder a sua configuração, isso pode acontecer sob as circunstâncias infelizes. É importante que você proteja seus backups, por meio de medidas técnicas ou organizacionais.

Backup e restauração da configuração do seu sistema (explicado)

O sistema oferece um recurso incorporado que faz o backup de toda a configuração do sistema definida no Management Client. O banco de dados do servidor de registros e os arquivos de registro, inclusive os arquivos de registro de auditoria, não estão incluídos neste backup.

Se o seu sistema é grande, a Milestone recomenda que você defina backups agendados. Isto é feito com a ferramenta de terceiros: Microsoft® SQL Server Management Studio. Esse backup inclui os mesmos dados que um backup manual.

Durante um backup seu sistema permanece on-line.

Fazer backup da configuração do seu sistema pode levar algum tempo. A duração do backup depende:

- Configuração do seu sistema
- Seu hardware
- Não importa se você instalou o SQL Server, o Event Server e os componentes do Management Server em um ou em vários servidores

Sempre que você fizer um backup manual ou programado, o arquivo de registro de transações do banco de dados SQL Server será liberado. Para obter informações adicionais sobre como eliminar o arquivo de registro de transações, consulte Registro de transações do banco de dados SQL Server (explicado) na página 140.

Certifique-se de saber as configurações de senha de seu sistema ao criar um backup.

Para sistemas compatíveis com FIPS 140-2, com exportações e bancos de dados de mídia arquivados de versões anteriores à 2017 R1 do XProtect VMS que são criptografados com cifras não compatíveis com FIPS, é necessário arquivar os dados em um local onde ainda possam ser acessados após a ativação do FIPS. Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

Selecionar a pasta de backup compartilhada

Antes de fazer backup e restauração de qualquer configuração de sistema, você precisa definir a pasta de backup para este propósito.

1. Clique com o botão direito no ícone de serviço Management Server na área de notificação e selecione **Escolher pasta de backup compartilhada**.
2. Na janela que aparece, pesquise o local do arquivo desejado.
3. Clique em **OK** duas vezes.
4. Se for perguntado se você deseja excluir os arquivos da pasta de backup atual, clique em **Sim** ou **Não**, dependendo de suas necessidades.

Faça Backup manual da Configuração do Sistema

1. Na barra de menu, escolha **Arquivo** > **Configuração de backup**.
2. Leia a nota na caixa de diálogo e clique em **Backup**.
3. Indique um nome de arquivo para o arquivo .cnf.
4. Indique um destino de pasta e clique em **Salvar**.
5. Aguarde até que o backup seja concluído e clique em **Fechar**.

> Todos os arquivos de configuração do sistema relevantes serão combinados em um único arquivo .cnf, salvo em um local especificado. Durante o backup, todos os arquivos de backup são exportados primeiro para uma pasta temporária de backup do sistema no servidor de gestão. Para selecionar outra pasta temporária, clique com o botão direito no ícone do serviço Management Server da área de notificação e escolha Selecionar pasta de backup compartilhada.

Restaurar a configuração do sistema a partir de um backup manual

Informação importante

- Tanto o usuário que instala quanto o usuário que restaura precisam ser administradores locais do banco de dados SQL Server da configuração do sistema no servidor de gerenciamento **e** no SQL Server
- Exceto para seus servidores de gravação, o sistema será completamente desligado durante o período da restauração, o que pode levar algum tempo
- Um backup só pode ser restaurado na instalação do sistema onde foi criado. Certifique-se de que a configuração seja o mais parecida possível com aquela do momento da realização do backup. Caso contrário, a restauração pode falhar

- Se for solicitada uma senha de configuração do sistema durante uma restauração, você deve fornecer a senha de configuração do sistema que era válida no momento em que o backup foi criado. Sem essa senha, você não pode restaurar sua configuração do backup
- Se você fizer um backup do banco de dados SQL Server e restaurá-lo em um SQL Server limpo, os erros abertos no banco de dados do SQL Server não funcionarão e você só receberá uma mensagem de erro genérica do SQL Server. Para evitar isso, primeiro reinstale o seu sistema XProtect usando o SQL Server e depois restaure o backup sobre ele
- Se a restauração falhar durante a fase de validação, será possível iniciar a configuração antiga novamente porque nenhuma alteração foi feita
  Se a restauração falhar em qualquer outra parte do processo, não é possível voltar à configuração antiga
  Desde que o arquivo de backup esteja corrompido, será, no entanto, possível fazer outra restauração
- A restauração substitui a configuração atual. Isso significa que qualquer alteração da configuração feita desde o último backup será perdida
- Nenhum registro é restaurado, inclusive os registros de auditoria
- Uma vez que a restauração é iniciada, não pode ser cancelada

Restaurando

1. Clique com o botão direito no ícone do serviço Management Server da área de notificação e selecione **Restaurar a configuração**.
2. Leia a nota importante e clique em **Restaurar**.
3. Na caixa de diálogo para abrir arquivo, navegue até o local do arquivo de backup de configuração do sistema, escolha-o e clique em **Abrir**.

   > O arquivo de backup está localizado no computador Management Client. Se o Management Client estiver instalado em um servidor diferente, copie o arquivo de backup para esse servidor antes de selecionar o destino.

4. A janela **Restaurar configuração** será aberta. Espere a restauração finalizar e clique em **Fechar**.

Configurações de senha do sistema (explicado)

Você pode escolher proteger a configuração geral do sistema atribuindo uma senha de configuração do sistema. Depois de atribuir uma senha de configuração do sistema, os backups são protegidos por essa senha. As configurações de senha são armazenadas no computador que está executando o servidor de gerenciamento em uma pasta segura. Você precisará desta senha para:

- Restaure a configuração de um backup de configuração que tenha sido criado com configurações de senha diferentes das configurações de senha atuais
- Mover ou instalar o servidor de gerenciamento em outro computador devido a uma falha de hardware (recuperação)
- Configure um servidor de gerenciamento adicional em um sistema com clustering

A senha de configuração do sistema pode ser atribuída durante ou após a instalação. A senha deve atender aos requisitos de complexidade do Windows, que são definidos pela política do Windows para senhas.

É importante que os administradores do sistema salvem esta senha e a mantenham em segurança. Se você atribuiu uma senha de configuração do sistema e está restaurando um backup, poderá ser solicitado o fornecimento da senha de configuração do sistema. Sem essa senha, você não pode restaurar sua configuração do backup.

Configurações de senha do ajuste do sistema

As configurações de senha do ajuste do sistema podem ser alteradas. Nas definições de senha de configuração do sistema, você tem estas opções:

- Escolher proteger a configuração do sistema atribuindo uma senha de configuração do sistema
- Alterar uma senha de configuração do sistema
- Escolha não proteger com senha a configuração do sistema removendo quaisquer senhas de configuração do sistema atribuídas

Modificar as configurações de senha do ajuste do sistema

Ao alterar a senha, é importante que os administradores do sistema salvem as senhas associadas aos diferentes backups e mantenham as senhas em segurança. Se estiver restaurando um backup, pode ser solicitado que você forneça a senha de configuração do sistema que era válida no momento em que o backup foi criado. Sem essa senha, você não pode restaurar sua configuração do backup.

Depois de alterar a senha, e se o servidor de gerenciamento e o servidor de eventos estiverem instalados em computadores separados, você também deve inserir a senha de configuração do site atual no servidor de eventos. Para obter mais informações, consulte Digite a senha de configuração do sistema atual (servidor de eventos).

Para aplicar as mudanças, é preciso reiniciar os serviços do servidor de gerenciamento.

1. Localize o ícone da bandeja do servidor de gerenciamento e certifique-se de que o serviço esteja em execução.
2. Clique com o botão direito no ícone do serviço Management Server da área de notificação e selecione **Alterar definições da senha de configuração do sistema**.
3. A janela para modificar as configurações de senha de ajuste do sistema é exibida.

Atribuir uma senha

1. Digite a nova senha no campo **Nova senha**.
2. Digite novamente a senha no campo **confirmar nova senha** e selecione **Enter**.
3. Leia a notificação e clique em **sim** sim para aceitar a alteração.
4. Aguarde a confirmação da mudança e selecione **Fechar**.
5. Para aplicar as mudanças, é preciso reiniciar os serviços do servidor de gerenciamento.
6. Depois de reiniciar, certifique-se de que o servidor de gerenciamento esteja sendo executado.

Remover a proteção de senha

Se você não precisa de proteção por senha, pode optar por sair:

1. Selecione a caixa de seleção: **Eu escolho não usar uma senha de configuração do sistema e entendo que a configuração do sistema não será criptografada** e clicar em **Enter**.
2. Leia a notificação e clique em **sim** para aceitar a alteração.
3. Aguarde a confirmação da mudança e selecione **Fechar**.
4. Para aplicar as mudanças, é preciso reiniciar os serviços do servidor de gerenciamento.
5. Depois de reiniciar, certifique-se de que o servidor de gerenciamento esteja sendo executado.

Digite as configurações de senha do ajuste do sistema (recuperação)

Se o arquivo que contém as configurações de senha for excluído devido a uma falha de hardware ou outros motivos, você precisará fornecer as configurações de senha do sistema para acessar o banco de dados que contém a configuração do sistema. Durante a instalação em seu novo computador, será solicitado que você

insira as configurações de senha do sistema.

Mas se o arquivo que contém as configurações de senha for excluído ou estiver corrompido e o computador que estiver executando o servidor de gerenciamento não tiver outros problemas, você terá a opção de inserir as configurações de senha do sistema:

1. Localize o ícone da bandeja do servidor de gerenciamento.
2. Clique com o botão direito no ícone do serviço Management Server da área de notificação e selecione **Inserir a senha de configuração do sistema**.
3. A janela para inserir as configurações de senha de ajuste do sistema é exibida.

A configuração do sistema é protegida por senha

1. Digite a senha no campo **senha** e selecione **Enter**.
2. Aguarde até que a senha seja aceita. Selecione **Fechar**.
3. Certifique-se de que o servidor de gerenciamento esteja sendo executado.

A configuração do sistema não é protegida por senha

1. Selecione a caixa de seleção: **Este sistema não usa uma senha de configuração do sistema** e selecione **Enter**.
2. Aguarde até que a configuração seja aceita. Selecione **Fechar**.
3. Certifique-se de que o servidor de gerenciamento esteja sendo executado.

Fazendo backup manual da configuração de seu sistema (explicado)

Quando você quiser fazer um backup manual do banco de dados do servidor de gerenciamento que contém a configuração do seu sistema, assegure-se de que o seu sistema permaneça on-line. O nome padrão do banco de dados do servidor de gerenciamento é **Surveillance**.

Alguns pontos a considerar antes de iniciar o backup:

- Você não pode usar um backup do banco de dados SQL Server para copiar configurações do sistema para outros sistemas
- Pode demorar algum tempo para fazer o backup do banco de dados SQL Server. Isso vai depender da configuração do sistema, do seu hardware, e se o seu SQL Server, servidor de gerenciamento e Management Client estão instalados no mesmo computador
- Registros, incluindo os registros de auditoria, são armazenados no banco de dados do servidor de registros e, portanto, **não** fazem parte do backup do banco de dados do servidor de gerenciamento. O nome padrão do banco de dados do servidor de registros é **SurveillanceLogServerV2**. Você faz o backup de ambos os bancos de dados SQL Server da mesma forma.

Fazendo backup e restauração da configuração do servidor de eventos (explicado)

O conteúdo da sua configuração de servidor de evento é incluído quando você faz o backup e restaura a configuração do sistema.

A primeira vez que você executar o servidor de eventos, todos os arquivos de configuração são automaticamente movidos para o banco de dados SQL Server. Você pode aplicar a configuração restaurada ao servidor de evento sem precisar reiniciar o servidor de evento e o servidor de evento é capaz de iniciar e interromper todas as comunicações externas enquanto a restauração da configuração está sendo carregada.

Backup e restauração agendados da configuração do sistema (explicado)

O servidor de gerenciamento armazena a configuração do seu sistema em um banco de dados SQL Server. A Milestone recomenda que você faça backups agendados regularmente desse banco de dados como uma medida de recuperação de desastres. Apesar de ser raro perder a sua configuração, isso pode acontecer sob as circunstâncias infelizes. Felizmente, a realização dos backups exige apenas um minuto e os backups também oferecem o benefício de liberar o registro de transações do banco de dados do SQL Server.

Se sua configuração é pequena e você não sente a necessidade de backup agendado regularmente, é possível fazer o backup manualmente. Para obter instruções, consulte Fazendo backup manual da configuração de seu sistema (explicado) na página 345.

Ao fazer backup/restauração do seu servidor de gerenciamento, assegure-se de que o banco de dados SQL Server com a configuração do sistema, seja incluído no backup/restauração.

Requisitos para o uso do backup e restauração agendados

Microsoft® SQL Server Management Studio, uma ferramenta que pode ser baixada gratuitamente no site deles (https://www.microsoft.com/downloads/).

Além de gerenciar o SQL Server e seus bancos de dados, a ferramenta tem recursos de backup e restauração fáceis usar. Baixe e instale a ferramenta em seu servidor de gerenciamento.

Backup da configuração do sistema com backup agendado

1. No menu Iniciar do Windows, inicialize Microsoft® SQL Server Management Studio.
2. Quando conectando, especifique o nome do SQL Server desejado. Use a conta na qual o banco de dados SQL Server foi criado.
    1. Localize o banco de dados SQL Server, contendo toda a configuração do sistema, inclusive o servidor de eventos, os servidores de gravação, câmeras, entradas, saídas, os usuários, as regras, os perfis de patrulhamento etc. O nome padrão deste banco de dados SQL é Surveillance.
    2. Faça um backup do banco de dados SQL Server e assegure que:

- Verifique se o banco de dados SQL Server é o correto
- Verifique se o tipo de backup **completo**.
- Defina o agendamento para o backup recorrente. Você pode ler mais sobre backups automáticos e agendados no site da Microsoft (https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017
- Verifique que o caminho sugerido é satisfatório ou escolha um caminho alternativo
- Selecione **verificar backup quando finalizado** e **realizar verificação antes de gravar em mídia**

3. Siga as instruções na ferramenta ao final.

Também considere fazer o backup do banco de dados do servidor de registros com seus registros usando mesmo método. O nome padrão do banco de dados do SQL Server no servidor de registros é **SurveillanceLogServerV2**.

Restaurar a configuração do sistema a partir do backup agendado

Requisitos
Para evitar que alterações da configuração sejam feitas enquanto você restaura o banco de dados, interrompa o:

- Management Server serviço (consulte Gerenciar serviços de servidor na página 360)
- Serviço Event Server (pode ser feito a partir de **Serviços** do Windows (pesquisar **services.msc** em sua máquina. Dentro de **Serviço**, localizar **Milestone XProtect Event Server**))
- World Wide Web Publishing Service, também conhecido como Internet Information Service (IIS). Saiba como interromper o IIS (https://technet.microsoft.com/library/cc732317(WS.10).aspx/)

Abra Microsoft® SQL Server Management Studio a partir do menu **Iniciar** do Windows.

Na ferramenta faça o seguinte:

1. Ao estabelecer conexão, especifique o nome do seu SQL Server. Use a conta de usuário sob a qual o banco de dados SQL Server foi criado.
2. Encontre o banco de dados SQL Server (o nome padrão é **Surveillance**) que contém toda a configuração do seu sistema, incluindo o servidor de eventos, servidores de gravação, câmeras, entradas, saídas, usuários, regras, perfis de patrulha, etc.
3. Faça uma restauração do banco de dados do SQL Server e garanta que:
   - Selecionar o backup **a partir** do dispositivo
   - Selecione tipo de **arquivo** de mídia de backup
   - Encontre e selecione seu arquivo de backup (**.bak**)
   - Escolha **substituir o banco de dados existente**
4. Siga as instruções na ferramenta ao final.

Use o mesmo método para restaurar o banco de dados SQL Server do servidor de registros com seus registros. O nome padrão do banco de dados do SQL Server no servidor de registros é **SurveillanceLogServerV2**.

> O sistema não trabalha enquanto o serviço Management Server estiver interrompido. É importante lembrar-se de reiniciar todos os serviços depois de concluir a restauração do banco de dados.

Fazer backup do banco de dados do servidor de registros

Processe o banco de dados do servidor de registros usando o método empregado ao processar a configuração do sistema conforme descrito anteriormente. O banco de dados do servidor de registros contém todos os seus registros do sistema, incluindo erros relatados por servidores de gravação e câmeras. O nome padrão do banco de dados do servidor de registros é **SurveillanceLogServerV2**.

O banco de dados SQL Server está localizado no servidor de registros do SQL Server. Normalmente, o servidor de registros e o servidor de gerenciamento têm seus bancos de dados SQL Server no mesmo SQL Server. A realização de um backup do banco de dados do servidor de registros não é vital, pois ele não contém nenhuma configuração do sistema, mas talvez você queira ter acesso aos registros do sistema anteriores ao backup/restauração do servidor de gerenciamento.

Falhas e cenários de problema em backup e restauração (explicado)

- Se, após o último backup da configuração do sistema, você tiver movido o servidor de eventos ou outros serviços registrados, como o servidor de registros, você deve selecionar a configuração do serviço registrada que deseja para o novo sistema. Neste caso, é possível manter a nova configuração depois do sistema ter sido restaurado para a versão antiga. Escolha clicando no nomes dos hosts dos serviços.
- Se a restauração da configuração do sistema falhar porque o servidor de eventos não estiver localizado no destino especificado (p.ex., se você escolheu a configuração anterior registrada do serviço), refaça a restauração.
- Se você estiver restaurando um backup de configuração e inserindo uma senha de configuração do sistema que esteja incorreta, deverá fornecer a senha de configuração do sistema que era válida no momento em que o backup foi criado.

Mover o servidor de gestão

O servidor de gerenciamento armazena a configuração do seu sistema em um banco de dados do SQL Server. Se você estiver movendo o servidor de gerenciamento de um servidor físico para outro, é vital que você certifique-se de que seu novo servidor de gerenciamento também acessa este banco de dados SQL Server. O banco de dados de configuração do sistema pode ser armazenado de duas maneiras diferentes:

- **Rede SQL Server**: Se estiver armazenando a configuração do sistema em um banco de dados existente do SQL Server em um SQL Server na sua rede, você pode apontar para a localização do banco de dados nesse SQL Server ao instalar o software do servidor de gerenciamento no seu novo servidor de gerenciamento. Nesse caso, apenas o parágrafo a seguir sobre endereço IP e nome do host do servidor de gerenciamento é aplicado, e você deve ignorar o resto deste tópico:

  Nome do host e endereço IP do servidor de gerenciamento: Quando você mover o servidor de gerenciamento de um servidor físico para um outro servidor físico, é muito mais fácil atribuir ao novo servidor o mesmo nome de host e endereço IP do servidor antigo. Isso se deve ao fato de que o servidor de gravação conecta-se ao nome do host e endereço IP do antigo servidor de gerenciamento. Se você atribuir um novo nome de host e/ou endereço IP ao novo servidor de gerenciamento, o servidor de gravação não conseguirá encontrar o servidor de gravação e você precisará interromper manualmente cada serviço do Recording Server no seu sistema, alterar o URL do servidor de gerenciamento deles, registrar o servidor de gravação novamente e, quando concluído, iniciar o serviço Recording Server.

- **Local SQL Server**: Se você estiver armazenando a configuração do seu sistema em um banco de dados do SQL Server em um SQL Server no próprio servidor de gerenciamento, é importante que você faça backup do banco de dados da configuração do sistema do servidor de gerenciamento existente antes da mudança. Fazendo o backup do banco de dados SQL Server e subsequentemente restaurando-o em um SQL Server no novo servidor de gerenciamento, você evitará a necessidade de reconfigurar suas câmeras, regras, perfis de tempo etc. após a mudança

> Se você mover o servidor de gerenciamento, precisará da senha de configuração do sistema atual para restaurar o backup, consulte Configurações de senha do sistema (explicado) na página 342.

Requisitos

- **Seu arquivo de instalação do software para instalação no novo servidor de gerenciamento**
- **Seu arquivo de licença de software (.lic)**, que você recebeu quando comprou seu sistema e o instalou inicialmente. Você não deve usar o arquivo de licença de software ativado recebido após a ativação manual de licença off-line. Um arquivo de licença ativado contém informações sobre o servidor específico no qual o sistema está instalado. Assim, um arquivo de licença de software ativado não pode ser reutilizado na mudança para um novo servidor

Se você também está atualizando o software do seu sistema em conexão com a mudança, você terá recebido um novo arquivo de licença de software. Basta usar este.

- **Somente para usuários Locais SQL Server: Microsoft® SQL Server Management Studio**
- Servidores de gerenciamento indisponíveis (explicado) na página 350O que acontece enquanto o servidor de gerenciamento não está disponível?
- Copiar banco de dados do servidor de registro (consulte Fazer backup do banco de dados do servidor de registros na página 348)

Servidores de gerenciamento indisponíveis (explicado)

- Os **servidores de gravação ainda podem gravar**: Quaisquer servidores de gravação trabalhando atualmente receberam como cópia de suas próprias configurações do servidor de gerenciamento, portanto serão capazes de trabalhar e armazenar gravações por conta própria enquanto o servidor de gerenciamento estiver indisponível. A gravação por ativação de movimento e a gravação agendada, portanto, funcionarão e a gravação ativada por eventos também funcionará a menos que seja baseada em eventos relacionados ao servidor de gerenciamento ou qualquer outro servidor de gravação uma vez que estes passam pelo servidor de gerenciamento
- **Servidores de gravação armazenarão temporariamente os registros de dados localmente**: Eles enviarão automaticamente dados de registro para o servidor de gerenciamento quando se tornar novamente disponível:
  - **Clientes não conseguem efetuar o login**: O acesso do cliente é autorizado através do servidor de gerenciamento. Sem o servidor de gerenciamento, os clientes não conseguem efetuar o login
  - **Clientes que já tiverem acessado podem continuar assim por até quatro horas**: Quando acessam, os clientes são autorizados pelo servidor de gerenciamento e podem se comunicar com os servidores de gravação por quatro horas. Se conseguir definir e executar o novo servidor de gerenciamento dentro de quatro horas, muitos de seus usuários não serão afetados
  - **Sem habilidade de configurar o sistema**: Sem o servidor de gerenciamento, você não será capaz de alterar a configuração do sistema

A Milestone recomenda que você informe seus usuários sobre o risco de perda de contato com o sistema de monitoramento enquanto o servidor de gerenciamento estiver fora do ar.

Mover a configuração do Sistema

Mover sua configuração de sistema é um processo de três etapas:

1. Faça um backup da configuração do sistema. Isso é idêntico a fazer um backup agendado. Consulte também Backup da configuração do sistema com backup agendado na página 346.
2. Instale o novo servidor de gestão no novo servidor. Veja backup agendado, etapa 2.
3. Restaure a configuração do sistema para o novo sistema. Consulte também Restaurar a configuração do sistema a partir do backup agendado na página 347.

Substituir um servidor de gravação

Se um servidor de gravação não funciona corretamente e você quer substituí-lo com um novo servidor que herda as configurações do servidor de gravação antigo:

1. Recupere o ID do servidor de gravação do antigo servidor de gravação:
   1. Selecione **Servidores de gravação**, em seguida, no painel **Visão Geral**, selecione o servidor de gravação antigo.
   2. Selecione a guia **Armazenamento**.

3. Pressione e segure a tecla CTRL no seu teclado enquanto seleciona a guia **Informações**.
4. Copie o número de ID do servidor de gravação na parte inferior da guia **Informações**. Não copie o termo *ID*, apenas o número em si.

2. Substitua o ID do servidor de gravação no novo servidor de gravação:
   1. Pare o serviço do Recording Server no servidor de gravação antigo e, em seguida, em **Serviços** do Windows, defina o **Tipo de inicialização** do serviço para **Desativada**.

      > É muito importante que você não inicie dois servidores de gravação com IDs idênticos aos mesmo tempo.

   2. No novo servidor de gravação, abra o explorer e acesse `C:\ProgramData\Milestone\XProtect Recording Server` ou o caminho onde o servidor de gravação está localizado.
   3. Abra o arquivo `RecorderConfig.xml`.
   4. Apague o ID que aparece entre as marcas *<id>* e *</id>*.

   5. Cole o ID do servidor de gravação copiado entre as marcas *<id>* e *</id>*. Salve o arquivo *RecorderConfig.xml*.
   6. Vá para o registro: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation`.
   7. Abra **RecorderIDOnMachine** e altere o ID do servidor de gravação antigo com o novo ID.
3. Registre o novo servidor de gravação no servidor de gerenciamento. Para fazer isso, clique com o botão direito no ícone da bandeja Recording Server Manager e clique em **Registrar**. Para obter mais informações, consulte Registrar um servidor de gravação na página 202.
4. Reinicializar o serviço Recording Server. Quando o novo serviço Recording Server iniciar, ele herda todas as configurações do antigo servidor de gravação.

Mover hardware

É possível mover hardware entre servidores de gravação que pertencem ao mesmo site. Depois de movidos, o hardware e os seus dispositivos serão executados no novo servidor de gravação e novas gravações são armazenadas neste servidor. A mudança é transparente para os usuários clientes.

As gravações no servidor de gravação antigo permanecem lá até que:

- O sistema os exclua quando expirar o tempo de retenção. Gravações que alguém tenha protegido com Proteção de evidências (consulte Sobre proteção de evidências na página 77) não são excluídas até que o tempo de retenção da proteção expire. Você define o tempo de retenção da proteção de evidências quando as cria. Potencialmente, o tempo de retenção nunca expira
- Você os exclui de cada novo servidor de gravação na guia **Gravação**

Se tentar remover um servidor de gravação que ainda contém gravações, você receberá um aviso.

Se mover hardware para um servidor de gravação que não tem hardware adicionado a ele, os usuários do cliente devem fazer logout e novo login para receber dados de dispositivos.

Você pode usar o recurso de mover hardware para:

- **Balanceamento de carga**: Se, por exemplo, o disco em um servidor de gravação está sobrecarregado, você pode adicionar um novo servidor de gravação e mover parte do seu hardware
- **Atualização**: Se você, por exemplo, tem que substituir o servidor que hospeda o servidor de gravação por um modelo mais novo, você pode instalar um novo servidor de gravação e mover o hardware do servidor antigo para o novo
- **Substituir um servidor de gravação defeituoso**: Se, por exemplo, o servidor estiver off-line não consegue retornar ao estado on-line novamente, é possível mover o hardware para outros servidores de gravação e, desta forma, manter o sistema em execução. Você não pode acessar as gravações antigas. Para obter mais informações, consulte Substituir um servidor de gravação na página 350.

Gravações remotas

Quando hardware é movido para outro servidor de gravação, o sistema cancela consultas em curso ou programadas a partir de sites interligados ou armazenamentos no dispositivo em câmeras. As gravações não são excluídas, mas os dados não são recuperados e guardados nas bases de dados conforme esperado. Se este for o caso, você receberá mensagem de aviso. A recuperação iniciada por um usuário do XProtect Smart Client acusa falha quando você inicia a movimentação do hardware. O usuário do XProtect Smart Client é notificado e pode tentar novamente mais tarde.

Se alguém mudou hardware em um site remoto, é necessário sincronizar manualmente o site central com a opção de **Atualização de hardware** para refletir a nova configuração do site remoto. Se você não sincronizar, as câmeras movidas permanecem como desconectadas no site central.

Mover hardware (assistente)

Para mover hardware de um servidor de gravação para outro, execute o **assistente de movimentação de hardware**. O assistente leva você pelas etapas necessárias para completar um movimento para um ou mais dispositivos de hardware.

Requisitos
Antes de você iniciar o assistente:

- Certifique-se de que o novo servidor de gravação pode acessar a câmera física através da rede
- Instale um servidor de gravação para o qual você deseja mover o hardware (consulte Instalando através do Download Manager (explicado) na página 170 ou Instalar silenciosamente um servidor de gravação na página 179)
- Instale a mesma versão do pacote de dispositivos que você executa no servidor existente no novo servidor de gravação (consulte Drivers de dispositivos (explicado) na página 150)

Para executar o assistente:

1. No painel **Navegação do site**, selecione **Servidores de gravação**.
2. No painel **Visão geral**, clique com o botão direito do mouse no servidor de gravação que você desejar mover.
3. Selecione **Mover hardware**.

> Se o servidor de gravação a partir do qual você quer mover hardware estiver desconectado, uma mensagem de erro é mostrada. Você só deve escolher mover hardware a partir de um servidor de gravação desconectado se tem certeza que ele nunca vai ficar on-line novamente. Se você mover hardware e mesmo assim o servidor voltar a ficar on-line, há o risco de um comportamento inesperado do sistema devido a se ter o mesmo hardware executando em dois servidores de gravação por um período. Problemas possíveis são, por exemplo, erros de licença ou eventos não enviados para o servidor de gravação correto.

4. Se você iniciou o assistente no nível do servidor de gravação, é mostrada a página **Selecionar o hardware que quer mover**. Selecione os dispositivos de hardware que deseja mover.
5. Na página **Selecione o servidor de gravação para o qual deseja mover o hardware**, selecione na lista de servidores de gravação instalados neste site.
6. Na página **Selecione o armazenamento que você deseja usar para futuras gravações**, a barra de utilização de armazenamento indica o espaço livre no banco de dados de gravação apenas para gravações ao vivo, não os arquivamentos. O tempo total de retenção é o período de retenção, tanto para o banco de dados de gravações quanto para os arquivos.
7. O sistema processa o seu pedido.

8. Se a mudança foi bem-sucedida, clique em **Fechar**. Se selecionar o novo servidor de gravação no Management Client, você poderá ver o hardware mudado e agora as gravações são armazenadas neste servidor.

   Se a mudança falhou, você pode solucionar o problema abaixo.

   > Em um sistema interligado, é necessário sincronizar manualmente o site central depois de mover o hardware em um site remoto para refletir as alterações que você ou outro administrador do sistema fez no site remoto.

Solução de problemas de mover hardware

Se a mudança não teve sucesso, uma das seguintes razões podem ser a causa:

Tipo de Erro	Solução de problemas
O servidor de gravação não está conectado ou em modo de recuperação de falhas (failover).	Certifique-se de que o servidor de gravação está on-line. Pode ser preciso registrá-lo. Se o servidor está no modo de recuperação de falhas (failover), espere e tente novamente.
O servidor de gravação não é a versão mais recente.	Atualize o servidor de gravação para a mesma versão do servidor de gerenciamento.
O servidor de gravação não pode ser encontrado na configuração.	Certifique-se de que o servidor de gravação não foi removido.
Atualizar a configuração ou a comunicação com o banco de dados de configuração falhou.	Assegure-se de que o SQL Server e o banco de dados estão conectados e em execução.
Houve falha ao parar o hardware no servidor de gravação atual	Talvez outro processo tenha bloqueado o servidor de gravação ou o servidor de gravação está em modo de erro. Certifique-se de que o servidor de gravação está em operação e tente novamente.
O hardware não existe.	Certifique-se de que o hardware que está tentando mover não tenha sido simultaneamente removido do sistema por outro usuário. O cenário é bastante improvável.

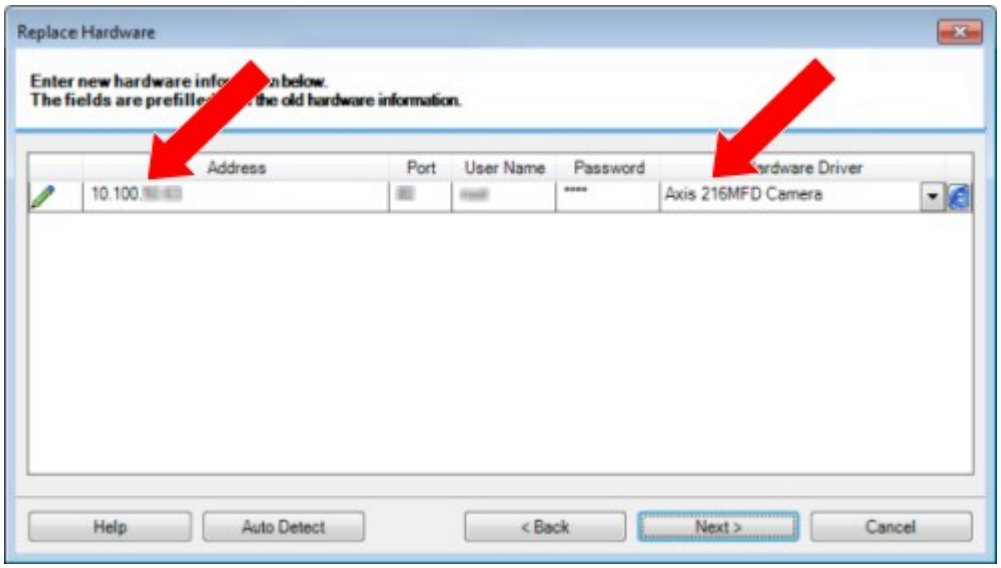
Tipo de Erro	Solução de problemas
O servidor de gravação do qual foi transferido o hardware está de volta on-line, mas você optou por ignorá-lo quando estava off-line.	Muito provavelmente, você achou que o servidor de gravação antigo nunca ficaria on-line novamente quando você iniciou o assistente **Mover hardware**, mas, durante a movimentação, o servidor voltou a ficar on-line. Reinicie o assistente e selecione **Não** quando lhe for pedido para confirmar se o servidor estará online novamente.
O armazenamento de gravação de origem está indisponível.	Você está tentando mover hardware com dispositivos configurados com um armazenagem de gravação que está atualmente off-line. Um armazenamento de gravação está off-line se o disco está off-line ou indisponível. Certifique-se de que o armazenamento de gravação está on-line e tente novamente.
Todos os armazenamentos de gravação no servidor de gravação de destino devem estar disponíveis.	Você está tentando mover hardware para um servidor de gravação onde um ou mais armazenamentos de gravação estão off-line atualmente. Certifique-se de que todos os armazenamentos de gravação no servidor de gravação alvo estão on-line. Um armazenamento de gravação está off-line se o disco está off-line ou indisponível.

Substituir hardware

Quando você substitui um dispositivo de hardware na sua rede de trabalho por outro dispositivo de hardware, você deve conhecer o endereço IP, porta, nome do usuário e senha do novo dispositivo de hardware.

Se você não habilitou a ativação automática da licença (consulte Ativação automática de licença (explicado) na página 121) e tiver utilizado todas as alterações do dispositivo sem ativação (consulte Alterações do dispositivo sem ativação (explicado) na página 122), você deve ativar manualmente as suas licenças **depois** de substituir os dispositivos de hardware. Se o novo número de dispositivos de hardware exceder o número total de licenças de dispositivo, você precisará comprar novas licenças de dispositivo.

1. Expanda o servidor de gravação desejado, clique com o botão direito do mouse no hardware que desejar substituir.
2. Selecione **Substituir hardware**.
3. O assistente **Substituir hardware** aparecerá. Clique em **Avançar**.
4. No assistente, no campo **Endereço** (marcado pela seta vermelha na imagem), entre com o endereço IP para o novo hardware. Se conhecido, selecione o driver relevante da lista suspensa **Driver de hardware**. Senão, selecione **Detecção Automática**. Se a porta, nome do usuário ou senha forem diferentes para o novo hardware, corrija isso **antes de iniciar o processo de auto detecção (se necessário)**.



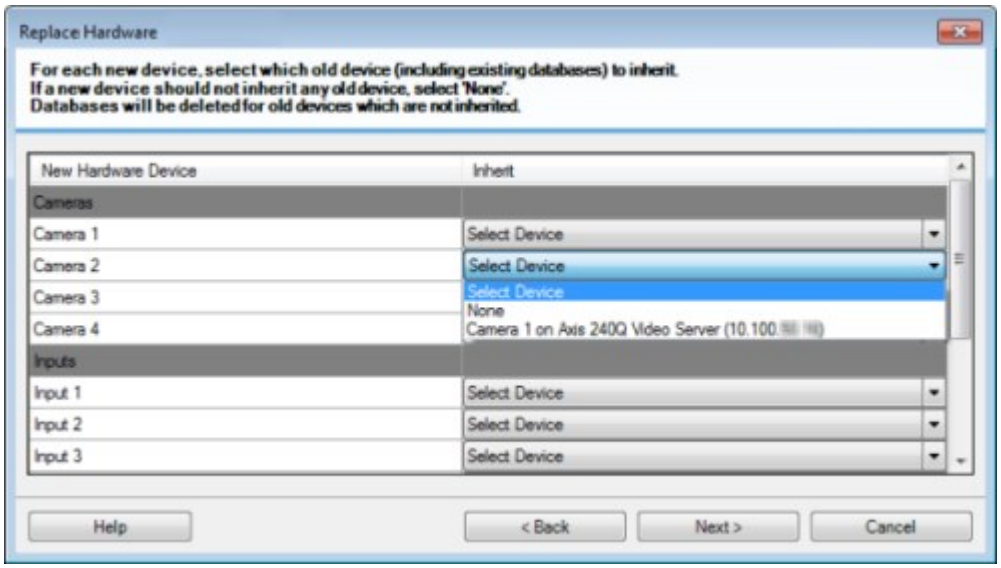
O assistente foi previamente preenchido com os dados do hardware existente. Se você substituí-lo com um dispositivo de hardware similar, você poderá reutilizar alguns desses dados - por exemplo, informações de porta e driver.

5. Faça um dos seguintes:
   - Se você selecionar o driver do dispositivo de hardware desejado diretamente da lista, clique em **Avançar**
   - Se você tiver selecionado **Detecção automática** na lista, clique em **Detecção automática**, espere que esse processo seja concluído com sucesso (marcado por um ✔ no lado esquerdo) e clique em **Próximo**

     Essa etapa é designada para lhe ajudar a mapear dispositivos e seus bancos de dados, dependendo do número de câmeras, microfones individuais, microfones, entradas, saídas, e assim por diante, anexados ao dispositivo de hardware antigo e novo respectivamente.

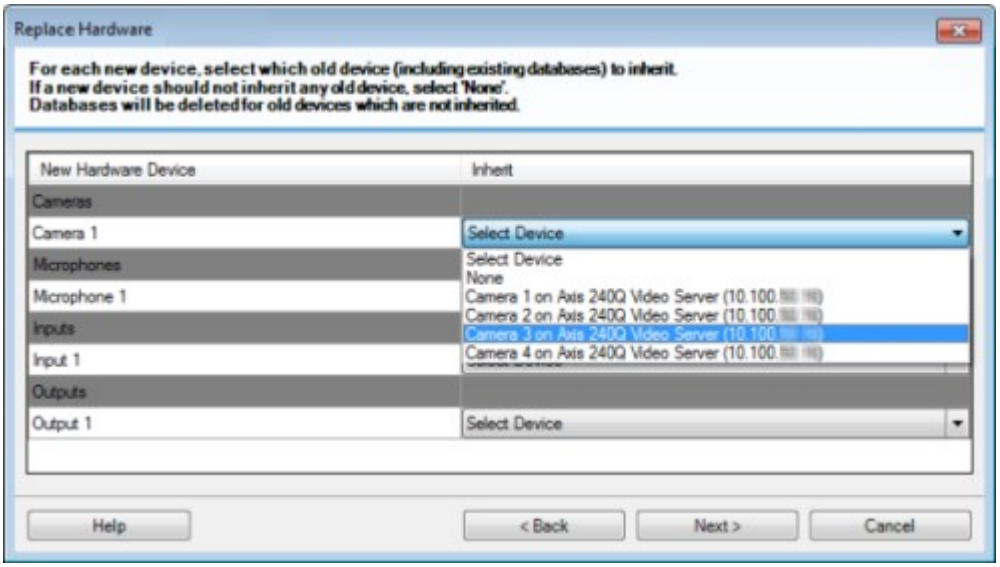
     É importante considerar **como** mapear bancos de dados a partir de um dispositivo de hardware antigo para bancos de dados de um dispositivo de hardware novo. Você faz um mapeamento real de dispositivos individuais, selecionando uma câmera, microfone, entrada, saída correspondente ou **Nenhum** na coluna do lado direito.

     > ⚠ Certifique-se de mapear **todas** as câmeras, microfones, entradas, saídas, e assim por diante. Conteúdos mapeados para **Nenhum**, são **perdidos**.



Exemplo de um dispositivo de hardware antigo que tem mais dispositivos individuais do que os

novos:



Clique em **Avançar**.

6. Uma lista de hardware a ser adicionado, substituído ou removido é apresentada. Clique em **Confirmar**.
7. A etapa final é um resumo dos dispositivos adicionados, substituídos e herdados e suas configurações. Clique em **Copiar para área de transferência** para copiar conteúdo à área de transferência do Windows ou/e **Fechar** para finalizar o assistente.

Atualize os dados do seu hardware

Para certificar-se de que seu dispositivo de hardware e o sistema estão usando a mesma versão de firmware, você precisa atualizar manualmente os dados de hardware para o dispositivo de hardware no Management Client. A Milestone recomenda que você atualize os dados de hardware após cada atualização de firmware para seu dispositivo de hardware.

Para obter os dados de hardware mais recentes:

1. No painel **Navegação do site**, selecione **Servidores de gravação**.
2. Expanda o servidor de gravação necessário e selecione o hardware para o qual deseja obter as informações mais recentes.
3. No painel **Propriedades**, na guia **Informações**, clique no botão **Atualizar** no campo **Dados de hardware atualizados pela última vez**.

4. O assistente verifica se o sistema está executando o firmware mais recente para o hardware.

   Selecione **Confirmar** para atualizar as informações no Management Client. Quando a atualização for concluída, a versão atual do firmware do dispositivo de hardware detectado pelo sistema aparecerá no campo **Versão do firmware** na guia **Informações**.

Alterar a localização e o nome de um banco de dados do SQL Server

O servidor de gerenciamento, servidor de eventos, servidor de registros, Identity Provider e XProtect Incident Manager se conectam a diferentes bancos de dados do SQL Server usando cadeias de caracteres de conexão. Essas cadeias de caracteres de conexão são armazenadas no registro do Windows. Se você tiver alterado o local ou o nome de um banco de dados do SQL Server, precisará editar todas as cadeias de caracteres de conexão que apontam para esse banco de dados do SQL Server.

Banco de dados	Utilizado por
Banco de dados de vigilância	• Serviço Management Server • Serviço Event Server • Pool de aplicativos do Management Server do VideoOS • Pool de aplicativos do Report Server do VideoOS
Surveillance_IDP	• Pool de aplicativos de IDP do VideoOS
Surveilance_IM	• Pool de aplicativos de IM do VideoOS
Surveillance_LogServerV2	• Serviço Log Server

Antes de continuar:

- Faça backup dos bancos de dados do SQL Server e do registro do Windows.
- Verifique se o usuário que executa os serviços e pools de aplicativos relacionados é o proprietário do banco de dados.
- Conclua a migração de conteúdo do antigo banco de dados do SQL Server para o novo.

Para atualizar as cadeias de conexão com a nova localização e nome de um banco de dados do SQL Server:

1. Interrompa todos os serviços e pools de aplicativos do XProtect VMS que usem o banco de dados do SQL Server.

   > Dependendo da arquitetura do seu sistema, os serviços e pools de aplicativos podem ser executados em computadores diferentes. Você precisa interromper todos os serviços e pools de aplicativos que se conectem ao mesmo banco de dados do SQL Server.

2. No editor de registro, acesse `HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString`.
3. Atualize as cadeias de caracteres de conexão com a nova localização e nome de um banco de dados do SQL Server.

   As cadeias de caracteres de conexão padrão para todos os banco de dados do SQL Server são:

   - **ManagementServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **EventServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ServerService**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ReportServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IDP**: `Data Source=localhost;Initial Catalog=Surveillance_IDP;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IncidentManager**: `Data Source=localhost;Initial Catalog=Surveillance_IM;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **LogServer**: `Data Source=localhost;Initial Catalog=SurveillanceLogServerV2;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
4. Inicie todos os serviços e pools de aplicativos do XProtect que você interrompeu na etapa 1.

Gerenciar serviços de servidor

No computador que executa serviços do servidor, você encontra os ícones da bandeja do gerenciador do servidor na área de notificação. Por meio destes ícones, você pode obter informações sobre os serviços e executar certas tarefas. Isso inclui, por exemplo, verificar o estado dos serviços, visualizar registros ou mensagens de status e iniciar ou interromper os serviços.

Ícones de bandeja do gerenciador do servidor (explicado)

Os ícones de bandeja na tabela mostram os diferentes estados dos serviços em execução no servidor de gerenciamento, servidor de gravação, servidor do sistema de gravação ininterrupta e servidor de eventos. Eles estão visíveis nos computadores com os servidores instalados, na área de notificação:

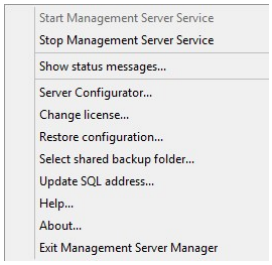
Management Server Manager ícone da bandeja	Recording Server Manager ícone da bandeja	Event Server Manager ícone da bandeja	Failover Recording Server Manager ícone da bandeja	Descrição
				**Executando** Aparece quando um serviço de servidos está ativado e iniciado. Se o serviço Failover Recording Server estiver em execução, ele pode assumir se o servidor de gravação padrão falhar.
				**Parado** Aparece quando um serviço de servidor tiver parado. Se o serviço Failover Recording Server parar, ele não pode assumir se o servidor de gravação padrão falhar.

Management Server Manager ícone da bandeja	Recording Server Manager ícone da bandeja	Event Server Manager ícone da bandeja	Failover Recording Server Manager ícone da bandeja	Descrição
				**Iniciando** Aparece quando um serviço de servidor está em processo de inicialização. Sob circunstâncias normais, o ícone de bandeja muda, após um breve período, para **Executando**.
				**Parando** Aparece quando um serviço de servidor está em processo de interrupção. Sob circunstâncias normais, o ícone de bandeja muda, após um breve período, para **Interrompido**.
				**Em estado indeterminado** Aparece quando o serviço do servidor é carregado inicialmente e até a primeira informação ser recebida, após o que o ícone de bandeja, sob circunstâncias normais muda para **Iniciando** e depois, para **Executando**.
				**Executando offline** Aparece normalmente, quando o servidor de gravação ou o serviço de gravação Failover está em execução, mas o serviço Management Server não.

Iniciar ou interromper o serviço Management Server

O ícone da bandeja Management Server Manager indica o estado do serviço Management Server, por exemplo **Executando**. Por meio desse ícone, você pode iniciar ou interromper o serviço Management Server. Se você interromper o serviço Management Server, você não poderá usar o Management Client.

1. Na área de notificação, clique com o botão direito no ícone da bandeja Management Server Manager. Um menu de contexto aparece.



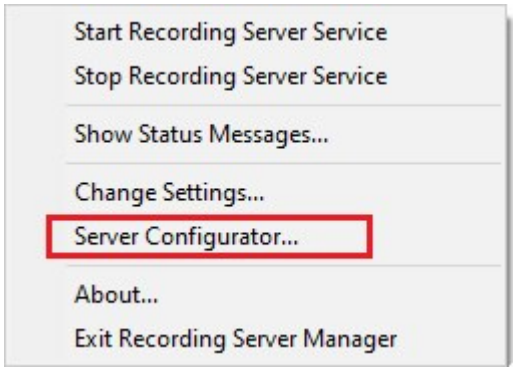
2. Se o serviço tiver sido interrompido, clique em **Iniciar serviço Management Server** para iniciá-lo. O ícone da bandeja muda, refletindo o novo status.
3. Para parar o serviço, clique em **Parar serviço Management Server**.

Para obter mais informações sobre os ícones de bandeja, consulte Ícones de bandeja do gerenciador do servidor (explicado) na página 361.

Iniciar ou interromper o serviço Recording Server

O ícone da bandeja Recording Server Manager indica o estado do serviço Recording Server, por exemplo **Executando**. Por meio desse ícone, você pode iniciar ou interromper o serviço Recording Server. Se você interromper o serviço Recording Server, seu sistema não poderá interagir com dispositivos conectados ao servidor. Isto significa que você não pode visualizar o vídeo ao vivo ou gravar vídeos.

1. Na área de notificação, clique com o botão direito no ícone da bandeja Recording Server Manager. Um menu de contexto aparece.

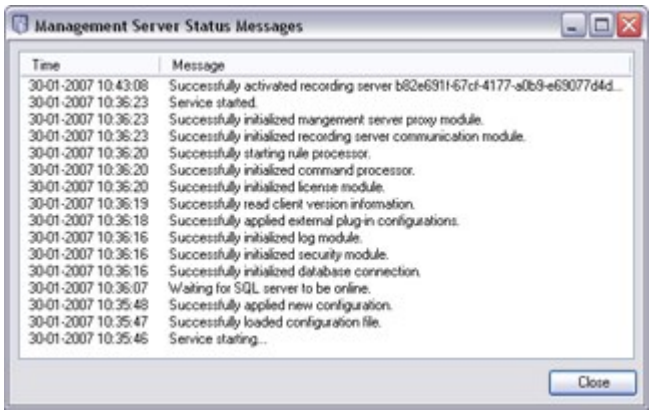


2. Se o serviço tiver sido interrompido, clique em **Iniciar serviço Recording Server** para iniciá-lo. O ícone da bandeja muda, refletindo o novo status.
3. Para parar o serviço, clique em **Parar serviço Recording Server**.

> Para obter mais informações sobre os ícones de bandeja, consulte Ícones de bandeja do gerenciador do servidor (explicado) na página 361.

Visualizar mensagens de status para o Servidor de gerenciamento ou para o Servidor de gravação

1. Na área de notificações, clique com o botão direito no ícone relevante da bandeja. Um menu de contexto aparece.
2. Selecione **Exibir mensagens de status**. Dependendo tipo de servidor, ou a janela **Mensagens de status do servidor de gerenciamento** ou **Mensagens de status do servidor de gravação** aparece, listando mensagens de status com carimbo de horário:



Gerenciar a criptografia com o Server Configurator

Use o Server Configurator para selecionar certificados em servidores locais para a comunicação criptografada e registrar serviços do servidor para torná-los qualificados a se comunicar com os servidores.

Abrir o Server Configurator no menu iniciar do Windows, do ícone de bandeja do servidor de gerenciamento ou do ícone da bandeja do servidor de gravação. Consulte Server Configurator (Utilidade) na página 414.

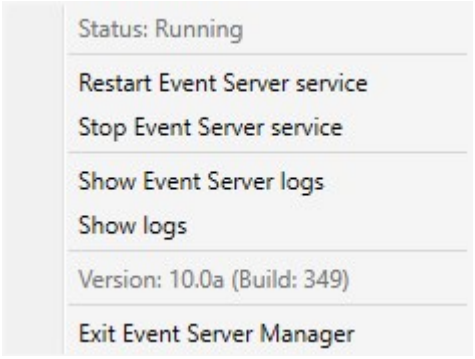
Para obter mais informações, consulte o guia de certificados sobre como proteger suas XProtect VMS instalações.

Iniciar, parar ou reiniciar o serviço Event Server

O ícone da bandeja Event Server Manager indica o estado do serviço Event Server, por exemplo **Executando**. Por meio desse ícone, você pode iniciar, interromper ou reiniciar o serviço Event Server. Se você interromper o serviço, partes do sistema não funcionarão, incluindo eventos e alarmes. Contudo, você ainda poderá

visualizar e gravar vídeos. Para obter mais informações, consulte Parando o serviço Event Server na página 365.

1. Na área de notificação, clique com o botão direito no ícone da bandeja Event Server Manager. Um menu de contexto aparece.



2. Se o serviço tiver sido interrompido, clique em **Iniciar serviço Event Server** para iniciá-lo. O ícone da bandeja muda, refletindo o novo status.
3. Para reiniciar ou interromper o serviço, clique em **Reiniciar serviço Event Server** ou **Parar serviço Event Server**.

> Para obter mais informações sobre os ícones de bandeja, consulte Ícones de bandeja do gerenciador do servidor (explicado) na página 361.

Parando o serviço Event Server

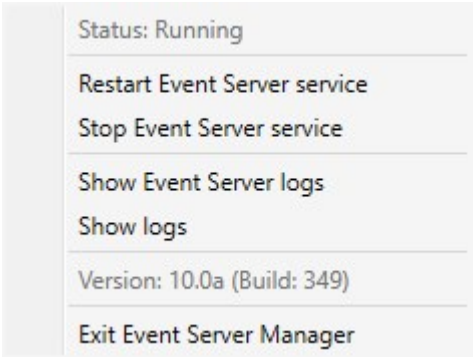
Ao instalar os plug-ins do MIP no servidor de eventos, você precisa primeiro interromper o serviço Event Server e, depois, reiniciá-lo. Enquanto o serviço estiver parado, muitas áreas do sistema VMS não funcionarão:

- Nenhum evento ou alarme será armazenado no Servidor de eventos. Ainda assim, os eventos do sistema e do dispositivo ainda ativarão ações, como, por exemplo, iniciar gravações
- Extensões do XProtect não funcionam no XProtect Smart Client e não podem ser configuradas usando o Management Client.
- Eventos analíticos não funcionam
- Eventos genéricos não funcionam
- Nenhum alarme é disparado
- No XProtect Smart Client, itens de visualização de mapa, itens de visualização de lista de alarme e o espaço de trabalho do Gerenciador de alarmes não funcionam.
- Os plug-ins do MIP no servidor de eventos não podem ser executados.
- Os plug-ins do MIP no Management Client e XProtect Smart Client não funcionam corretamente

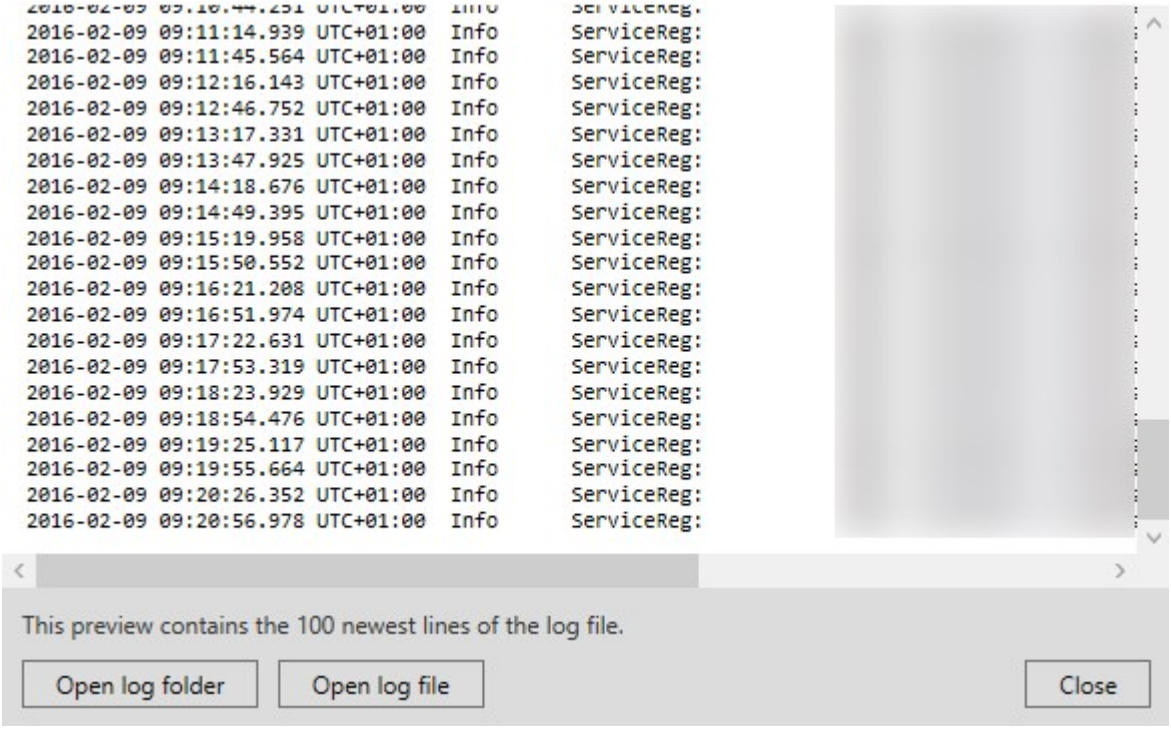
Visualizar registros do Event Server ou do MIP

Você pode visualizar informações com carimbo de data/hora sobre as atividades do Servidor de eventos no registro do Servidor de eventos. Informações sobre integrações de terceiros são registradas no registro do MIP, em uma subpasta na pasta **Servidor de eventos**.

1. Na área de notificação, clique com o botão direito no ícone da bandeja Event Server Manager. Um menu de contexto aparece.



2. Para visualizar as 100 linhas mais recentes no registro do Event Server, clique em **Mostrar registros do Servidor de eventos**. Um visualizador de registro é exibido.



    1. Para visualizar o arquivo de registro, clique em **Abrir arquivo de registro**.
    2. Para abrir a pasta de registro, clique em **Abrir pasta de registro**.

3. Para visualizar as 100 linhas mais recentes do registro do MIP, volte ao menu de contexto e clique em **Mostrar registros do MIP**. Um visualizador de registro é exibido.

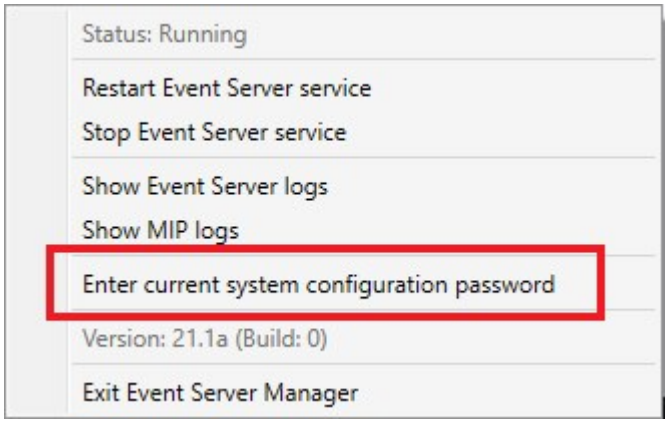
> Se alguém remove o arquivo de registro do diretório de registros, os itens do menu ficam indisponíveis. Para abrir o visualizador de registro, você precisa antes copiar o arquivo de registro de volta em sua pasta: `C:\ProgramData\Milestone\XProtect Event Server\logs` ou `C:\ProgramData\Milestone\XProtect Event Server\logs\MIP Logs`.

Digite a senha de configuração do site atual

Se a senha de configuração do sistema foi alterada no servidor de gerenciamento, você também deve inserir a senha de configuração do sistema atual no servidor de eventos.

> Se você não inserir a senha atual no servidor de eventos, os componentes do sistema, como o controle de acesso, deixarão de funcionar.

1. Na área de notificação, clique com o botão direito no ícone da bandeja Event Server Manager. Um menu de contexto aparece.



2. Para inserir a senha de configuração do sistema atual, clique em **Inserir a senha de configuração do sistema atual**. Uma janela aparece.
3. Insira a mesma senha de configuração do site que foi inserida no servidor de gerenciamento.

Gerenciar serviços registrados

Ocasionalmente, você tem servidores e / ou serviços que devem poder comunicar-se com o seu sistema, mesmo se eles não forem diretamente parte do seu sistema de monitoramento. Alguns serviços, mas não todos, podem registar-se automaticamente no sistema. Serviços que podem ser automaticamente registrados são:

- Serviço Event Server
- Serviço Log Server

Serviços registrados automaticamente são mostrados na lista de serviços registrados.

Você pode especificar servidores/serviços manualmente como serviços registrados no Management Client.

Adicionar e editar serviços registrados

1. Na janela **Adicionar/remover serviços registrados**, clique em **Adicionar** ou **Editar**, dependendo de suas necessidades.
2. Na janela **Adicionar serviço registrado** ou **Editar serviço registrado** (dependendo da sua seleção anterior), especifique ou edite as configurações.
3. Clique em **OK**.

Gerenciar configuração de rede

Com as definições de configuração de rede, você pode especificar os endereços LAN e WAN do servidor de gerenciamento de modo que o servidor de gerenciamento e os servidores de confiança possam se comunicar.

1. Na janela **Adicionar/remover serviços registrados**, clique **Serviço de rede**.
2. Especifique o endereço IP LAN e/ou WAN do servidor de gerenciamento.

   Se todos os servidores envolvidos (tanto o servidor de gerenciamento quanto os servidores de confiança) estiverem na sua rede local, você pode simplesmente especificar o endereço LAN. Se um ou mais servidores envolvidos acessar o sistema através de uma conexão da internet, você também deve especificar o endereço WAN.

3. Clique em **OK**.

Propriedades de serviços registrados

Na janela **Adicionar serviço registrado** ou **Editar serviço registrado**, especifique o seguinte:

Componente	Exigência
Tipo	Campo pré-preenchido.
Nome	Nome do serviço registrado. O nome é usado apenas para fins de exibição no Management Client.
URLs	Clique em **Adicionar** para adicionar o endereço IP ou nome de host do serviço registrado. Se especificar um nome de host como parte de uma URL, o host deve existir e estar disponível na rede. URLs devem começar com *http://* ou *https://* e não devem conter qualquer tipo dos seguintes caracteres especiais: < > & ' " * ? | [ ] ". **Exemplo** de um formato de URL típico: *http://ipaddress:port/directory* (onde porta e diretório são opcionais). Você pode adicionar mais de um URL se desejado.
Confiável	Selecione se o serviço registrado deve ser certificado imediatamente (este é um caso frequente, mas a opção lhe dá flexibilidade par adicionar serviços registrados e então marcar como certificados editando o serviço registrado posteriormente). A alteração do estado de confiança também alterará o estado de outros serviços registrados compartilhando um ou mais dos URLs definidos para o serviço registrado relevante.
Descrição	Descrição do serviço registrado. O nome é usado apenas para fins de exibição no Management Client.
Avançado	Quando um serviço é avançado, ele tem esquemas URI específicos (por exemplo, HTTP, HTTPS, TCP ou UDP) que precisam ser configurados para cada endereço de host que você definir. Portanto, um endereço de host tem vários terminais, cada um com seu próprio esquema, endereço de host e porta IP para esse esquema.

Remoção de drivers de dispositivos (explicada)

Se não precisar mais de drivers de dispositivos em seu computador, você poderá excluir os pacotes de dispositivos de seu sistema. Para isso, siga o procedimento padrão do Windows para remover programas.

Se tiver vários pacotes de dispositivos instalados e tiver problemas ao excluir os arquivos, você poderá usar o script na pasta de instalação dos pacotes de dispositivos para excluí-los completamente.

Se você remover os drivers de dispositivos, o servidor de gravação e os dispositivos de câmeras não poderão mais se comunicar. Não remova pacotes de dispositivo quando atualizar, porque você poderá instalar uma nova versão em cima de uma antiga. Você só poderá remover o Device Pack se desinstalar todo o sistema.

Remover um servidor de gravação

> ⚠ Se você remover um servidor de gravação, toda a configuração especificada no Management Client será removida do servidor de gravação, incluindo **todo** o hardware associado ao servidor de gravação (câmeras, dispositivos de entrada e assim por diante).

1. Clique com o botão direito do mouse no servidor de gravação que você desejar remover no painel **Visão geral**.
2. Selecione **Remover servidor de gravação**.
3. Se tiver certeza, clique no botão **Sim**.
4. O servidor de gravação e todos os seus hardware associados são removidos.

Excluir todos o hardware em um servidor de gravação

> ⚠ Quando você exclui hardware, todos os dados gravados relacionados ao hardware são excluídos permanentemente.

1. Clique com o botão direito do mouse no servidor de gravação no qual você desejar excluir todo o hardware.
2. Selecione **Excluir todo o hardware**.
3. Confirme a exclusão.

Alterar o nome do host do computador servidor de gerenciamento

Se o servidor de gerenciamento estiver endereçado por seu nome de domínio totalmente qualificado (FQDN) ou seu nome do host, uma alteração ao nome do host do computador, terá implicações dentro do XProtect que devem ser consideradas e resolvidas.

> ⚠ Em geral, uma alteração do nome do host de um servidor de gerenciamento deve ser planejada cuidadosamente, devido à quantidade de limpezas necessárias depois.

Nas seções a seguir, você pode obter uma visão geral de algumas das implicações de uma alteração de um nome de host.

A validade dos certificados

Os certificados são usados para criptografar a comunicação entre serviços, e os certificados são instalados em todos os computadores que executam um ou mais dos serviços XProtect.

Dependendo de como os certificados são criados, eles podem ser relacionados ao computador em que estão instalados e só serão válidos enquanto o nome do computador permanecer o mesmo.

Para obter mais informações sobre como criar certificados, consulte Introdução a certificados.

Se o nome de um computador for alterado, os certificados em uso podem se tornar inválidos e o XProtect VMS não poderá ser inicializado. Para que o sistema volte a funcionar, execute estas etapas:

- Crie novos certificados e reinstale-os em todos os computadores do ambiente.
- Aplique os novos certificados, usando o Server Configurator, em cada um dos computadores para habilitar a criptografia com os novos certificados.

Isso acionará o registro dos novos certificados e fará com que o sistema volte a funcionar.

Perda de propriedades de dados do cliente para serviços registrados

Se você concluiu um registro usando o Server Configurator depois, por exemplo, uma alteração ao endereço do servidor de gerenciamento, qualquer edição aos serviços registrados serão substituídas. Portanto, se você alterou as informações para os serviços registrados, as alterações devem ser aplicadas novamente para todos os serviços que estão registrados no servidor de gerenciamento no computador com o nome alterado.

As informações que podem ser editadas para serviços registrados estão localizadas em **Ferramentas** > **Serviços registrados** > **Editar**:

- Confiável
- Avançado
- Sinalizador externo
- Qualquer URL adicionado manualmente

Em Milestone Customer Dashboard, o nome do host aparecerá inalterado

Milestone Customer Dashboard é uma ferramenta online gratuita para parceiros e revendedores do Milestone e usuários do XProtect VMS gerenciarem e monitorarem instalações de software e licenças do Milestone.

Uma mudança no nome do servidor de gerenciamento em um site que está conectado ao Milestone Customer Dashboard não será refletido automaticamente em Milestone Customer Dashboard.

O nome do host antigo aparecerá no Milestone Customer Dashboard até que uma nova ativação de licença seja concluída. A mudança de nome, no entanto, não interromperá nada no Milestone Customer Dashboard e, uma vez que uma nova ativação ocorra, o registro é atualizado no banco de dados com o novo nome de host. Para mais informações sobre o Milestone Customer Dashboard, consulte Milestone Customer Dashboard (explicado).

Uma mudança no nome do host pode desencadear a mudança do endereço SQL Server

Se o SQL Server estiver no mesmo computador que o servidor de gerenciamento e o nome desse computador for alterado, o endereço do SQL Server também será alterado. Isto significa que será necessário atualizar o endereço do SQL Server para os componentes localizados em diferentes computadores, assim como para componentes no computador local que usem o nome do computador, em vez do localhost para estabelecer conexão com o SQL Server. Isto, especificamente, se aplica ao Event Server que usa o mesmo banco de dados que o Management Server. Isto também pode ser aplicável ao Log Server, que usa um banco de dados diferente, mas muito provavelmente no mesmo SQL Server.

Consulte Alterar a localização e o nome de um banco de dados do SQL Server na página 359.

Mudanças de nome de host em um Milestone Federated Architecture

Alterações ao nome de um computador que resida dentro de uma configuração do Milestone Federated Architecture terão as seguintes implicações e, isto se aplica a quando os sites estiverem conectados dentro de grupos de trabalho e através de domínios.

O host do site é o nó raiz na arquitetura

Se você alterar o nome do computador no qual o site central da arquitetura está sendo executado, todos os nós filhos serão reconectados automaticamente ao novo endereço. Assim, neste caso, uma renomeação não exigirá nenhuma ação.

O host do site é um nó filho na arquitetura

Para evitar problemas de conexão ao alterar o nome de um computador, no qual um ou mais sites federados estão sendo executados, você deve adicionar um endereço alternativo ao site afetado, antes de renomear o computador. O site afetado sendo o nó cujo computador host será renomeado. Para mais informações sobre questões de conexão devido a alterações não preparadas ou imprevistas ao nome do host e sobre como resolver os problemas, consulte Problema: Um nó parente em uma configuração do Milestone Federated Architecture não pode ser conectar a um nó filho.

O endereço alternativo deve ser adicionado no painel **Propriedades** na **Navegação do site** ou no painel **Hierarquia de sites federados**. Os seguintes pré-requisitos devem ser atendidos:

- O endereço alternativo deve ser adicionar para estar disponível antes que o computador host seja renomeado.
- O endereço alternativo deve refletir o nome futuro do computador host (quando renomeado)

Consulte Definir propriedades do site para obter informações sobre como acessar o painel **Propriedades**.

Para assegurar uma atualização mais suave possível, pare o Management Client no nó que serve como nó parente para aquele cujo nome do host será alterado. Caso contrário, pare e reinicie o cliente após o computador ter sido renomeado. Para obter mais informações, consulte Iniciar ou parar o serviço Management Server.

Além disso, assegure-se de que o endereço alternativo fornecido, seja refletido no painel **Hierarquia de sites federados** na sua central de controle e, se não, pare e reinicie o Management Client.

Após o host ter sido renomeado, e você ter reiniciado o computador, o site federado mudará automaticamente para o novo endereço.

Gerenciar registros de servidor

A seguir estão os tipos de registros do servidor:

- Registro do sistema
- Registro de auditoria
- Registros acionados por regras

Eles são usados para registrar o uso do sistema. Esses registros estão disponíveis no Management Client em **Registros do servidor**.

Para obter informações sobre os registros usados para solucionar problemas e investigar erros de software, consulte Registros de depuração (explicado) na página 378.

Identificar atividades, eventos, ações e erros de usuário.

Use os registros para obter um registro detalhado da atividade dos usuários, eventos, ações e erros no sistema.

Para ver registros no Management Client, acesse o painel **Navegação do site** e selecione **Registros do servidor**.

Tipos de registro	O que é registrado?
Registros do sistema	Informações relacionadas ao sistema

Tipos de registro	O que é registrado?
Registros de auditoria	Atividade do usuário
Registros acionados por regras	Regras nas quais os usuários tenham especificado a ação **Fazer nova <entrada de registro>**. Para mais informações sobre a ação <entrada de registro>, consulte Ações e ações de parada.

Para ver os registros em um idioma diferente, consulte Guia Geral (opções) na página 394 em **Opções**.

Para exportar registros como arquivos com valores separados por vírgula (.csv), consulte Exportar registros.

Para modificar as configurações de registro, consulte Guia Registros do servidor (opções) na página 397.

Filtrar registros

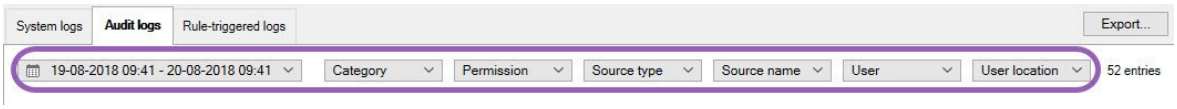
Em cada janela de registro, você pode aplicar filtros para ver entradas de registro, por exemplo, de um intervalo de tempo, dispositivo ou usuário específico.

> Os filtros são gerados a partir das entradas de registro atualmente visíveis na interface do usuário.

1. No painel **Navegação do site**, selecione **Registros do servidor**. Por padrão, a guia **Registros do sistema** é exibida.

   Para navegar entre tipos de registro, selecione uma guia diferente.

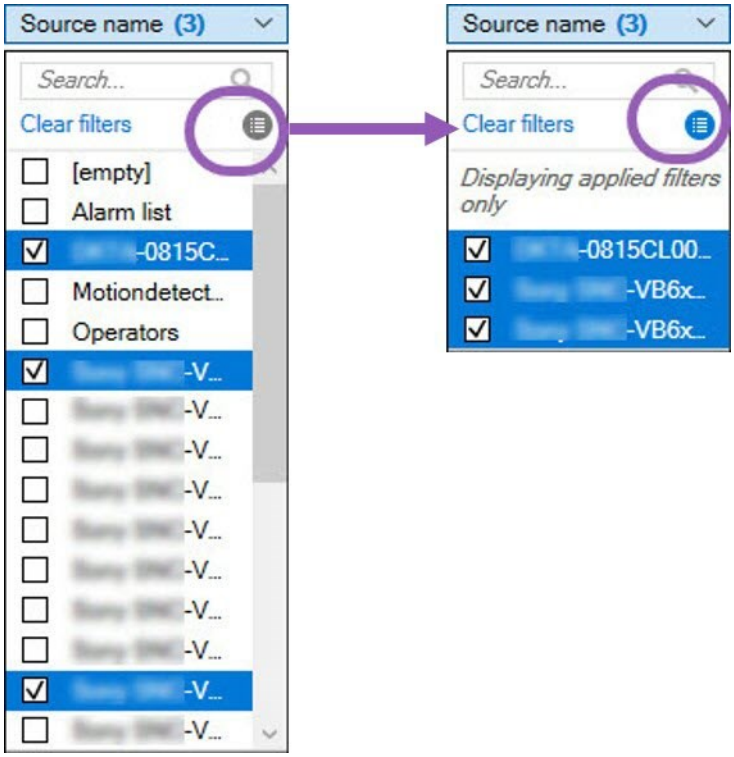
2. Sob as guias, selecione um grupo de filtros, por exemplo, **Categoria**, **Tipo de fonte** ou **Usuário**.



   Uma lista de filtros aparece. Uma lista de filtros exibe no máximo 1000 filtros.

3. Selecione um filtro para aplicá-lo. Selecione o filtro novamente para removê-lo.

   Opcional: Em uma lista de filtros, selecione **Exibir apenas filtros aplicados** para ver apenas os filtros que você aplicou.



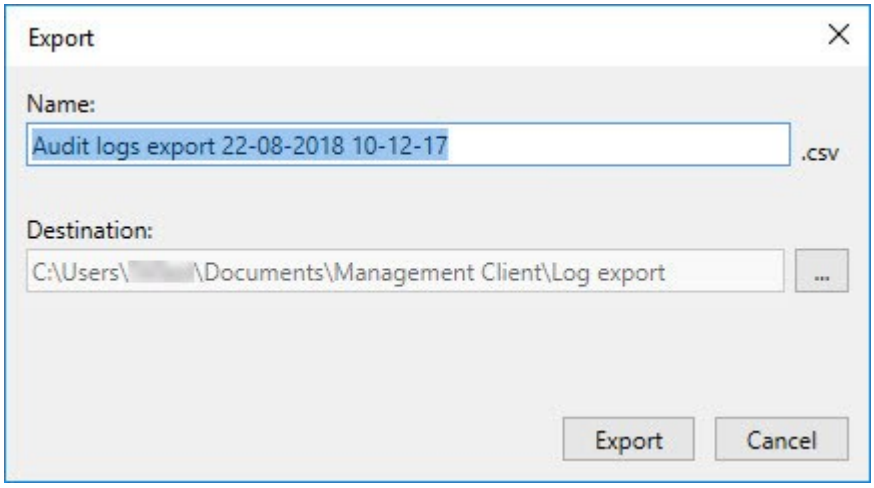
Quando você exporta registros, o conteúdo de sua exportação muda dependendo dos filtros que você aplicar. Para informações sobre sua exportação, consulte Exportar registros.

Exportar registros

A exportação de registros ajuda você a, por exemplo, salvar entradas de registros além do período de retenção do registro. Você pode exportar registros como arquivos com valores separados por vírgula (.csv).

Para exportar um registro:

1. Selecione **Exportar** no canto superior direito. A janela de **Exportação** aparece.



2. Na janela **Exportação**, no campo **Nome**, especifique um nome para o arquivo de registro.
3. Por padrão, arquivos de registro exportados são salvos em sua pasta **Exportação de registros**. Para especificar um local diferente, selecione ... à direita do campo **Destino**.
4. Selecione **Exportar** para exportar o registro.

> O conteúdo de sua exportação muda dependendo dos filtros que você aplicar. Para informações sobre sua exportação, consulte Filtrar registros.

Pesquisar registros

Para pesquisar um registro, use os **Critérios de pesquisa** na parte superior do painel de registro:

1. Especifique seus critérios de pesquisa nas listas.
2. Clique em **Atualizar** para fazer a página de registro refletir seus critérios de pesquisa. Para limpar seus critérios de pesquisa e voltar a visualizar todo o conteúdo do registro, clique em **Limpar**.

Você pode clicar duas vezes em qualquer linha para que todos os detalhes sejam apresentados em uma janela de **Detalhes de registro**. Dessa forma, você também pode ler as entradas de registro que contêm mais texto do que pode ser exibido em uma única linha.

Modificar idioma do registro

1. Na parte inferior do painel de registro, na lista **Mostrar login**, selecione o idioma desejado.

2. O registro é exibido no idioma selecionado. Da próxima vez que você abrir o registro, ele é redefinido para o idioma padrão.

Permitir que 2018 R2 e componentes anteriores escrevam registros

A versão 2018 R3 do servidor de registros introduz autenticação para segurança adicional. Isso impede que os componentes 2018 R2 e anteriores gravem registros no servidor de registros.

Componentes afetados:

- XProtect Smart Client
- Plug-in do XProtect LPR
- LPR Server
- Plug-in de controle de acesso
- Servidor de eventos
- Plug-in de alarme

Se estiver usando a versão 2018 R2 ou anterior de qualquer um dos componentes listados acima, você deverá decidir se permitirá ou não que o componente grave registros no novo servidor de registros:

1. Selecione **Ferramentas** > **Opções**.
2. Na caixa de diálogo **Opções**, na parte inferior da guia **Registros do servidor** encontre a caixa de seleção **Permitir que 2018 R2 e componentes anteriores gravem registros**.
    - Selecione a caixa de seleção para permitir que 2018 R2 e componentes anteriores gravem registros
    - Desmarque a caixa de seleção para não permitir que 2018 R2 e componentes anteriores gravem registros

Solução de problemas

Registros de depuração (explicado)

Os registros de depuração são usados para identificar defeitos e falhas no site.

Para obter informações sobre os registros usados para uso do site, consulte Gerenciar registros de servidor na página 373.

A seguir estão os locais dos arquivos de log na instalação do XProtect:

- `C:\ProgramData\Milestone\IDP\Logs`

  > Isso só pode ser acessado por usuários e administradores do IIS. Se o usuário IIS for alterado, essas permissões deverão ser atualizadas.

- `C:\ProgramData\Milestone\MIPSDK`
- `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
- `C:\ProgramData\Milestone\XProtect Event Server\Logs`
- `C:\ProgramData\Milestone\XProtect Log Server`
- `C:\ProgramData\Milestone\XProtect Management Server\Logs`
- `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
- `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
- `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`

Problema: A alteração da localização do SQL Server e do banco de dados impede o acesso ao banco de dados

Se a localização do SQL Server e dos bancos de dados de VMS tiverem mudado, por exemplo, pela alteração no nome do host do computador que executa o SQL Server, o servidor de gravação perderá o acesso ao banco de dados.

Solução: Altere as cadeias de caracteres de conexão para corresponder à alteração do SQL Server e do banco de dados. Consulte Alterar a localização e o nome de um banco de dados do SQL Server na página 359.

Problema: Falha do servidor de gravação devido à conflito de porta

Este problema só pode aparecer se o serviço do Protocolo SMTP (Simple Mail Transfer Protocol) estiver sendo executado, pois ele usa a porta 25. Se a porta 25 já estiver em uso, pode não ser possível inicializar o serviço Recording Server. É importante que a porta número 25 esteja disponível para o serviço de SMTP do servidor.

Serviço de SMTP: Verificação e soluções

Para verificar se o Serviço de SMTP está instalado:

1. No menu **Iniciar** do Windows, selecione **Painel de Controle**.
2. No **Painel de controle**, dê um clique duplo em **Adicionar ou remover programas**.
3. No lado esquerdo da janela **Adicionar ou Remover Programas**, clique em **Adicionar ou Remover Componentes do Windows**.
4. No assistente **Componentes do Windows**, selecione **Serviços de Informações da Internet (IIS)**, e clique em **Detalhes**.
5. Na janela **Serviços de Informações da Internet (IIS)**, verifique se a caixa de seleção **Serviço SMTP** está selecionada. Se estiver, o Serviço SMTP está instalado.

Se o serviço SMTP estiver instalado, selecione uma das seguintes soluções:

Solução 1: Desative o serviço SMTP ou configure-o para inicialização manual

Esta solução permite que você inicialize o servidor de ravação, se ter que sempre interromper o Serviço SMTP:

1. No menu **Iniciar** do Windows, selecione **Painel de Controle**.
2. No **Painel de controle**, dê um clique duplo em **Ferramentas administrativas**.
3. Na janela **Ferramentas administrativas**, dê um clique duplo em **Serviços**.
4. Na janela **Serviços**, dê um clique duplo em **Protocolo SMTP**.
5. Na janela **Propriedades de SMTP**, clique em **Parar**, em seguida, defina **Tipo de inicialização** para **Manual** ou **Desativada**.

   Quando definido para **Manual**, o Serviço SMTP pode ser iniciado manualmente, a partir da janela **Serviços** ou de um prompt de comando, usando o comando *net start SMTPSVC*.
6. Clique em **OK**.

Solução 2: Remover o serviço de SMTP

A remoção do Serviço SMTP pode afetar outros aplicativos usando o Serviço SMTP.

1. No menu **Iniciar** do Windows, selecione **Painel de Controle**.
2. Na janela **Painel de controle**, dê um clique duplo em **Adicionar ou remover programas**.
3. No lado esquerdo da janela **Adicionar ou Remover Programas**, clique em **Adicionar ou Remover Componentes do Windows**.
4. No assistente **Componentes do Windows**, selecione o item **Serviços de Informações da Internet (IIS)** e

clique em **Detalhes**.

5. Na janela **Serviços de Informações da Internet (IIS)**, limpe a caixa de seleção **Serviço SMTP**.
6. Clique em **OK**, **Avançar** e **Concluir**.

Problema: Recording Server fica offline na mudança do nó de cluster do Management Server

Se você definir um cluster da Microsoft para Management Server redundância, o Recording Server ou Recording Servers podem ficar offline ao alterna o Management Server entre os nós de cluster.

Para corrigir isso, faça o seguinte:

> Ao fazer alterações na configuração do Gerenciador do Cluster de Failover da Microsoft, pause o controle e monitoramento do serviço para que o Server Configurator possa fazer as alterações e iniciar e/ou parar o serviço Management Server. Se você mudar o tipo de inicialização do serviço de cluster de emergência para manual, isso não deve resultar em conflitos com o Server Configurator.

Nos computadores Management Server:

1. Inicie o Server Configurator em cada um dos computadores que possuem um servidor de gerenciamento instalado.
2. Ir para a página de **Registro**.
3. Clique no símbolo de lápis ( ) para tornar o endereço do servidor de gerenciamento editável.
4. Altere o endereço do servidor de gerenciamento para a URL do grupo, por exemplo `http://MeuGrupo`.
5. Clique em **Registrar**.

Em computadores que possuem componentes que usam o Management Server (por exemplo, Recording Server, Mobile Server, Event Server, API Gateway):

1. Inicie o Server Configurator em cada um dos computadores.
2. Ir para a página de **Registro**.
3. Altere o endereço do servidor de gerenciamento para a URL do grupo, por exemplo `http://MeuGrupo`.
4. Clique em **Registrar**.

Problema: Um nó parente em uma configuração do Milestone Federated Architecture não pode ser conectar a um nó filho.

Se você tiver renomeado o computador host de um site que atua como nó filho em um Milestone Federated Architecture, um nó parente não poderá se conectar a ele.

Para restabelecer a conexão entre o nó pai e o site

- Desanexe o site afetado de seu pai. Para obter mais informações, consulte Desanexar um site da hierarquia.
- Anexe o site novamente usando o novo nome de seu host. Para mais informações, consulte Adicionar site à hierarquia.

> Para assegurar que as alterações estejam em vigor, pode ser bom parar e reiniciar o Management Client no nó que serve como nó parente àquele cujo nome do host foi alterado. Para obter mais informações, consulte Iniciar ou parar o serviço Management Server.

Para obter mais informações sobre as implicações de uma mudança de nome de host em uma configuração do Milestone Federated Architecture, consulte Mudanças de nome de host em um Milestone Federated Architecture.

Problema: O serviço Banco de dados SQL do Azure não está disponível

Se você usar o Banco de dados SQL do Azure e tiver um problema de conexão durante a instalação ou durante o funcionamento normal, pode ser que o serviço Banco de dados SQL do Azure esteja temporariamente indisponível.

O Banco de dados SQL do Azure é um serviço no qual a maior parte da manutenção tradicional do banco de dados é feita pela Microsoft. O serviço pode ficar indisponível por curtos períodos e foi projetado para se recuperar até certo ponto sem a necessidade de interação do usuário.

Os erros do banco de dados são gravados nos arquivos de registro XProtect VMS com uma ID de incidente relacionada, que pode ser fornecida ao suporte da Microsoft no caso de indisponibilidade prolongada do Banco de dados SQL do Azure.

Para obter mais informações, consulte Resolução de problemas de conexão comuns no Banco de dados SQL do Azure.

Atualizar

Atualização (explicada)

Quando você atualiza, todos os componentes instalados atualmente no computador são atualizados. Não é possível remover componentes instalados durante uma atualização. Se desejar remover componentes instalados, use a funcionalidade **Adicionar e remover programas** do Windows, antes ou depois de uma atualização. Durante a atualização, todos os componentes, exceto o banco de dados do servidor de gerenciamento, são automaticamente removidos e substituídos. Isto inclui os drivers de seu pacote de dispositivos.

O banco de dados do servidor de gerenciamento contém toda a configuração do sistema (configurações do servidor de gravação, configurações de câmera, regras, e assim por diante). Contanto que você não remova o banco de dados do servidor de gerenciamento, não é necessário reconfigurar o sistema, embora você possa querer configurar alguns dos novos recursos na nova versão.

A compatibilidade com versões XProtect de servidores de gravação anteriores à versão atual é limitada. Você ainda pode acessar gravações em tais servidores de gravação com versões mais antigas, mas para alterar a configuração deles, é necessário que eles sejam da mesma versão que a atual. A Milestone recomenda a atualização de todos os servidores de gravação em seu sistema.

Ao atualizar incluindo os servidores de gravação, você será perguntado se deseja atualizar ou manter os drivers do dispositivo de vídeo. Se optar por atualizar, pode levar alguns minutos para os dispositivos do hardware fazerem contato com os novos drivers de dispositivo de vídeo depois de reiniciar o sistema. Isto acontece devido a muitas verificações internas nos novos drivers instalados.

Se você atualizar da versão 2017 R3 ou anterior para a versão 2018 R1 ou posterior e se seu sistema tiver câmeras mais antigas, você deve fazer o download manual do pacote de dispositivos com drivers obsoletos da página de download em nosso site (https://www.milestonesys.com/downloads/). Para ver se você possui câmeras que usam drivers no Legacy Device Pack, visite esta página em nosso site (https://www.milestonesys.com/community/business-partner-tools/device-packs/).

Se você fizer a atualização da versão 2018 R1 ou anterior/posterior à versão 2018 R2, é importante que atualize todos os servidores de gravação em seu sistema com um patch de segurança antes de fazer a atualização. Atualizar sem o patch de segurança causará a falha dos servidores de gravação.

As instruções para instalar o patch de segurança nos seus servidores de gravação estão disponíveis em nosso site https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/.

Se desejar criptografar a conexão entre o servidor de gerenciamento e os servidores de gravação, todos os servidores de gravação deverão ser atualizados para a versão 2019 R2 ou superior.

Para obter uma visão geral da sequência de atualização recomendada, consulte Melhores práticas de atualização na página 386

Requisitos para atualização

- Tenha seu arquivo de licença de software (consulte Licenças (explicadas) na página 119) (.lic) pronto:
  - **Atualização do pacote de serviços**: Durante a instalação do servidor de gerenciamento, o assistente pode te pedir para especificar a localização do arquivo de licença de software. Você pode usar tanto o arquivo de licença de software que obteve após a compra do seu sistema (ou da última atualização) e o arquivo ativado de licença de software que você obteve após a sua última ativação da licença
  - **Atualização de versão**: Após você ter adquirido a nova versão, você receberá um novo arquivo de licença de software. Durante a instalação do servidor de gerenciamento, o assistente pede que você especifique a localização do novo arquivo de licença de software

  O sistema verifica o arquivo de licença de software antes que você possa continuar. Dispositivos de hardware já adicionados e outros dispositivos que requerem licenças entram em um período de carência. Se você não tiver habilitado a ativação automática de licença (consulte Habilitar ativação automática de licença na página 126), lembre-se de ativar suas licenças manualmente antes da expiração do período de gratuidade. Se você não tiver o arquivo de licença de software, entre em contato com o fornecedor da XProtect.
- Tenha seu software com a **nova versão do produto** pronto. É possível baixá-lo na página de download no site Milestone.

- Certifique-se de ter feito um backup da configuração do sistema (consulte Backup e restauração da configuração do seu sistema (explicado) na página 340)

  O servidor de gerenciamento armazena a configuração do sistema em um banco de dados do SQL Server. O banco de dados do SQL Server pode estar em uma instância do SQL Server na própria máquina do servidor de gerenciamento ou em uma instância do SQL Server na rede.

  Se você usar um banco de dados do SQL Server em uma instância do SQL Server na sua rede, o servidor de gerenciamento precisará ter permissões de administrador na instância do SQL Server sempre que você quiser criar, mover ou atualizar o banco de dados do SQL Server. Para o uso e manutenção regulares do banco de dados do SQL Server, o servidor de gerenciamento só precisa ser o proprietário do banco de dados.

- Se você planeja ativar a criptografia durante a instalação,você precisa ter os certificados adequados instalados e confiáveis em todos os computadores relevantes. Para obter mais informações, consulte Comunicação segura (explicado) na página 151.

Quando você estiver pronto para iniciar a atualização, siga os procedimentos em Melhores práticas de atualização na página 386.

Atualize o XProtect VMS para executar no modo compatível com FIPS 140-2

A partir da versão 2020 R3, o XProtect VMS está configurado para ser executado de modo que use apenas as instâncias de algoritmo certificadas pelo FIPS 140-2.

Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

> ⚠ Para sistemas compatíveis com FIPS 140-2, com exportações e bancos de dados de mídia arquivados de versões anteriores à 2017 R1 do XProtect VMS que são criptografados com cifras não compatíveis com FIPS, é necessário arquivar os dados em um local onde ainda possam ser acessados após a ativação do FIPS.

O processo a seguir descreve o que é necessário configurar o XProtect VMS para executar no modo compatível com FIPS 140-2:

1. Desative a política de segurança FIPS do Windows em todos os computadores que integram o VMS, incluindo o computador que hospeda o SQL Server.

   Ao atualizar, você não pode instalar o XProtect VMS quando o FIPS estiver ativado no sistema operacional Windows.

2. Certifique-se de que integrações independentes de terceiros possam ser executadas em um sistema operacional Windows habilitado para FIPS.

   Se uma integração autônoma não for compatível com FIPS 140-2, ela não poderá ser executada depois de configurar o sistema operacional Windows para operar no modo FIPS.

   Para evitar isto:

   - Faça um inventário de todas as suas integrações autônomas para XProtect VMS
   - Entre em contato com os fornecedores dessas integrações e pergunte se as integrações são compatíveis com FIPS 140-2
   - Implante as integrações autônomas em conformidade com FIPS 140-2

3. Certifique-se de que os drivers e, portanto, a comunicação com os dispositivos, estejam em conformidade com o FIPS 140-2.

   XProtect VMS é garantido e pode impor o modo de operação compatível com FIPS 140-2 se os seguintes critérios forem atendidos:

   - Os dispositivos usam apenas drivers compatíveis para se conectar ao XProtect VMS

     Consulte a seção de conformidade FIPS 140-2 no guia de proteção para obter mais informações sobre os drivers que podem garantir e impor conformidade.

   - Os dispositivos usam o pacote de dispositivos versão 11.1 ou superior

     Os drivers dos pacotes de dispositivos de driver herdados não podem garantir uma conexão compatível com FIPS 140-2.

   - Os dispositivos são conectados por HTTPS e em protocolo de transporte seguro em tempo real (Secure Real-Time Transport Protocol, SRTP) ou protocolo de transmissão em tempo real (Real Time Streaming Protocol, RTSP) por HTTPS para o fluxo de vídeo

     > Módulos de driver não podem garantir conformidade FIPS 140-2 de uma conexão sobre HTTP. A conexão pode ser compatível, mas não há garantia de que seja de fato compatível.

   - O computador que está executando o servidor de gravação executa o sistema operacional Windows com o modo FIPS ativado

4. Certifique-se de que os dados no banco de dados de mídia sejam criptografados com cifras compatíveis com FIPS 140-2.

   Isso é feito executando a ferramenta de atualização do banco de dados de mídia. Para obter informações detalhadas sobre como configurar seu XProtect VMS para ser executado no modo compatível com FIPS 140-2, consulte a seção de conformidade com FIPS 140-2 no guia de proteção.

5. Antes de habilitar o FIPS no sistema operacional Windows e depois de configurar seu sistema XProtect VMS e garantir que todos os componentes e dispositivos possam ser executados em um ambiente habilitado para FIPS, atualize suas senhas de hardware existentes no XProtect Management Client.

   Para fazer isso, no Management Client, a partir do servidor de gravação selecionado no nó **Servidores de gravação**, clique com o botão direito do mouse e selecione **Adicionar Hardware**. Siga em frente com o assistente **Adicionar hardware**. Isso atualizará todas as credenciais atuais e criptografá-las para serem compatíveis com FIPS.

Você pode habilitar o FIPS somente depois de atualizar todo o VMS, incluindo todos os clientes.

Melhores práticas de atualização

Antes de iniciar a atualização, leia mais sobre os requisitos de atualização (consulte Requisitos para atualização na página 383), incluindo backup dos banco de dados do SQL Server.

> Os drivers de dispositivos estão agora divididos em dois pacotes: o pacote de dispositivos regular, com drivers mais recentes, e um pacote de dispositivos herdados com drivers mais antigos. O pacote de dispositivos regular sempre é instalado automaticamente com uma atualização ou melhoria. Se você tiver câmeras mais antigas que usam drivers de dispositivos do pacote de dispositivos herdados, e você não possuir um pacote de dispositivos herdados já instalado, o sistema não instala automaticamente o pacote de dispositivo herdado.

> Se o seu site tiver câmeras mais antigas, a Milestone recomenda que você verifique se as câmeras usam drivers do Legacy Device Pack nesta página (https://www.milestonesys.com/community/business-partner-tools/device-packs/). Para verificar se você já possui o pacote herdado instalado, procure nas pastas do sistema XProtect. Se você precisar fazer o download do pacote de dispositivos obsoletos, vá para a página de download (https://www.milestonesys.com/downloads/).

Se o seu sistema for um sistema de um **Computador único**, você pode instalar o novo software sobre a instalação existente.

Em um sistema Milestone Interconnect ou Milestone Federated Architecture, você deve iniciar atualizando a central de controle e, depois, os sites remotos.

Em um sistema distribuído, realize a atualização nesta ordem:

1. Atualize o servidor de gerenciamento com a opção **Personalizado** no instalador (consulte Instale o seu sistema – opção Personalizado na página 163).
    1. Na página do assistente onde você escolher os componentes, todos os componentes do servidor de gerenciamento são pré-selecionados.
    2. Especifique o SQL Server e o banco de dados. Decida ser quer manter o banco de dados SQL Server que já está usando e manter os dados existentes no banco de dados.

    > Quando você iniciar a instalação, a funcionalidade do servidor do sistema de gravação ininterrupta será perdida (consulte Servidor do sistema de gravação ininterrupta (explicado) na página 39).

    > Se você ativou a criptografia no servidor de gerenciamento, os servidores de gravação estarão off-line até serem atualizados e você ter ativado a criptografia ao servidor de gerenciamento (consulte Comunicação segura (explicado) na página 151).

2. Atualizar servidores do sistema de gravação ininterrupta. Na página web de download do servidor de gerenciamento (controlado por Download Manager), instale o Recording Server.

    > Se você planeja ativar a criptografia nos servidores do sistema de gravação ininterrupta e desejar reter a funcionalidade ininterrupta, atualize o servidor do sistema de gravação ininterrupta sem criptografia e ative-o depois que atualizar os servidores de gravação.

    Nesse ponto, a funcionalidade do servidor de failover funciona novamente.

3. Se você planeja ativar a criptografia dos servidores de gravação ou nos servidores do sistema de gravação ininterrupta para clientes e for importante que os clientes possam recuperar dados durante a atualização, atualize todos os clientes e serviços que recuperam fluxos de dados dos servidores de gravação antes de atualizar os servidores de gravação. Esses clientes e serviços são:
    - XProtect Smart Client
    - Management Client
    - Management Server
    - Servidor XProtect Mobile
    - XProtect Event Server
    - DLNA Server Manager

- Milestone Open Network Bridge
- Sites que recuperam os fluxos de dados do servidor de gravação por meio de Milestone Interconnect
- Algumas integrações de terceirizadas MIP SDK

4. Atualize os servidores de gravação. Você pode instalar servidores de gravação usando o assistente de instalação (consulte Instalar um servidor de gravação através de Download Manager na página 171) ou silenciosamente (consulte Instalar silenciosamente um servidor de gravação na página 179). A vantagem de uma instalação silenciosa é que você pode fazê-la remotamente.

> ⚠ Se você ativa a criptografia, e o certificado de autenticação de servidor selecionado não é confiável em todos os computadores relevantes executando clientes e serviços que recuperam fluxos de dados do servidor de gravação, eles perderão conexão. Para obter mais informações, consulte Comunicação segura (explicado) na página 151.

Continue essas instruções para os outros sites em seu sistema.

Atualizar em um grupo

Certifique-se de ter um backup do banco de dados antes de atualizar o grupo.

1. Pare o serviço Management Server em todos os servidores de gerenciamento no grupo.
2. Desinstale o servidor de gerenciamento em todos os servidores do grupo.
3. Use o procedimento para instalar vários servidores de gerenciamento em um grupo, como descrito para instalar em um grupo. Consulte Instale em um grupo na página 186.

> ⚠ Durante a instalação, não se esqueça de reutilizar o SQL Server existente e o banco de dados existente do SQL Server que armazena a configuração do sistema. A configuração do sistema é atualizada automaticamente.

Detalhes da interface de usuário

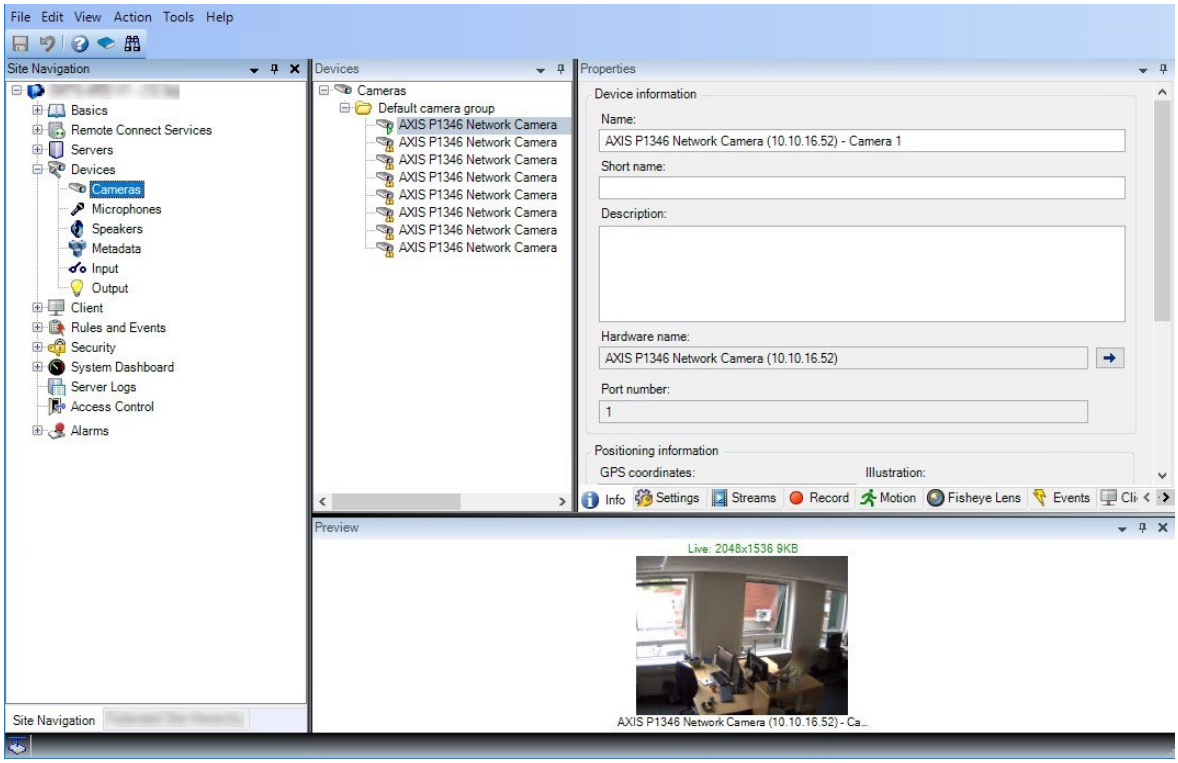
Janela principal e painéis

A janela do Management Client é dividida em paineis. O número de painéis e layout depende de:

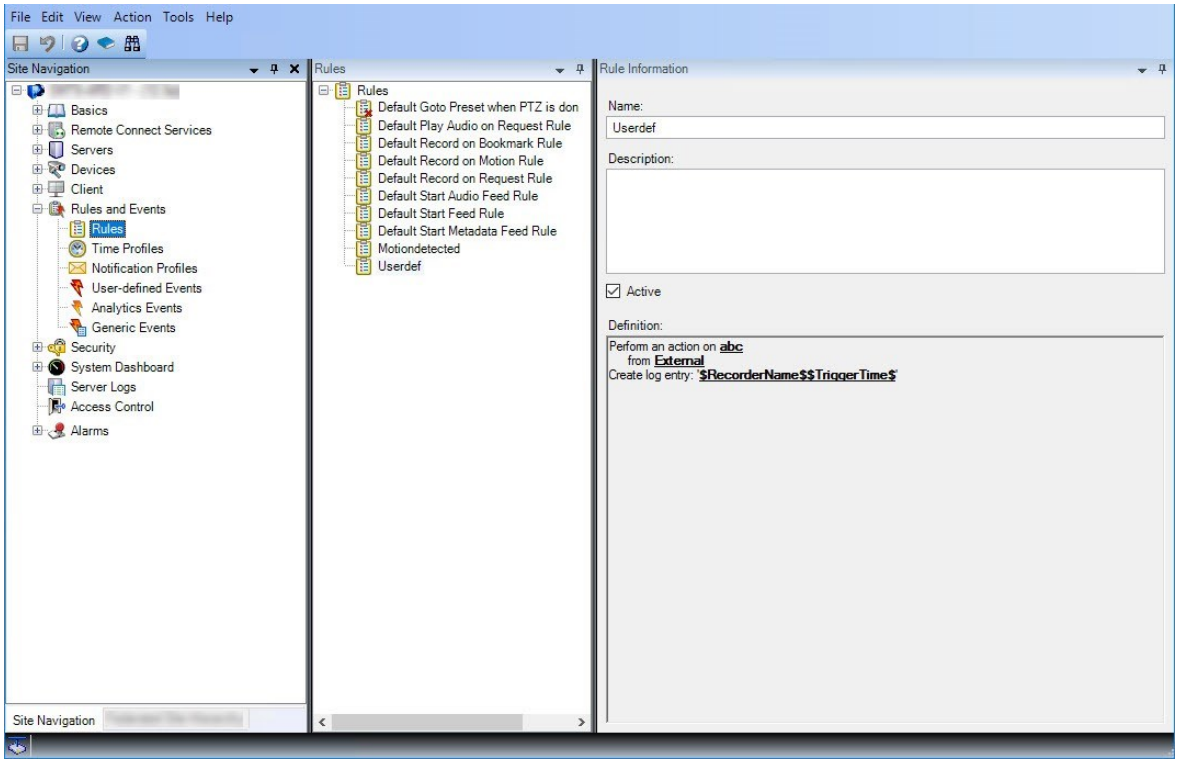
- Configuração do sistema
- Tarefa
- Funções disponíveis

Abaixo estão alguns exemplos de layouts típicos:

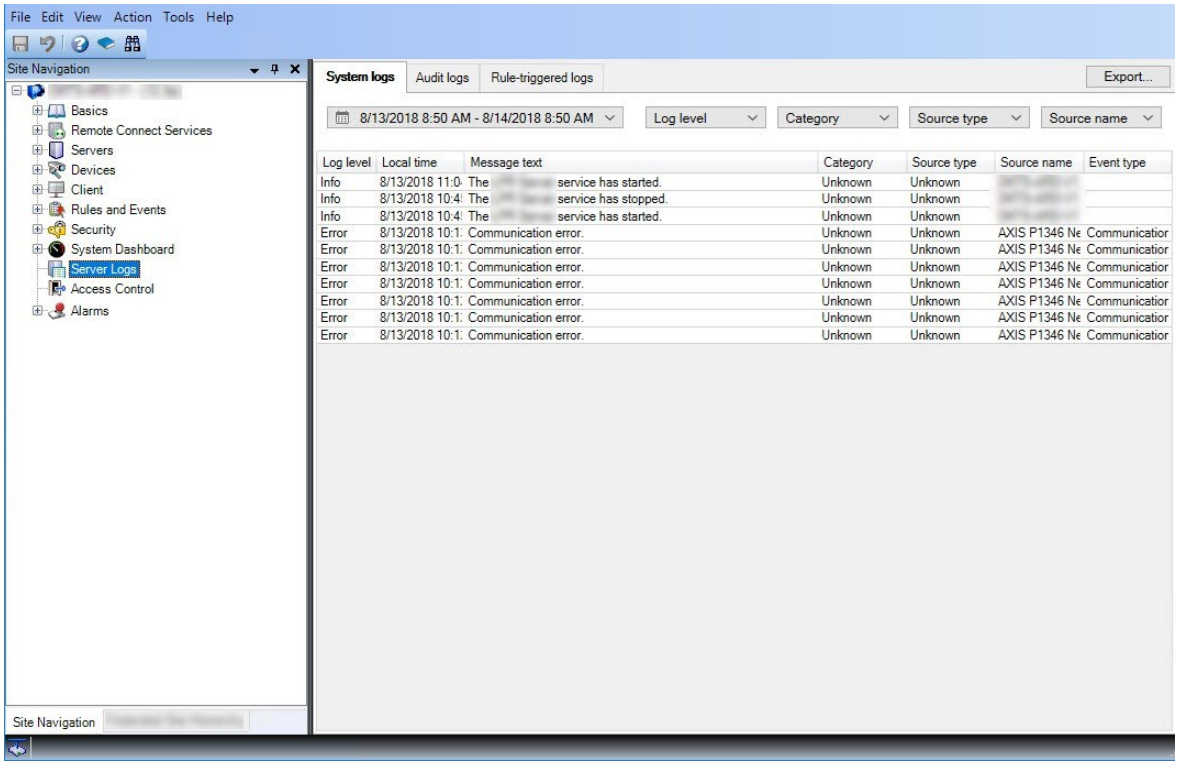
- Quando você trabalha com dispositivos e servidores de gravação:



- Quando você trabalha com regras, perfis de tempo e de notificação, usuários, funções:

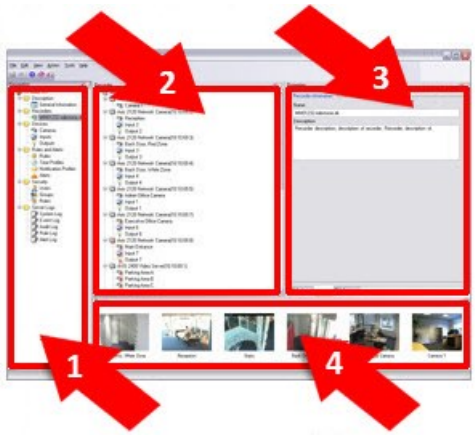


- Quando você exibir registros:



Layout de painéis

A ilustração descreve o layout de uma janela típica. Você pode personalizar o layout para que ele possa ter uma aparência diferente no seu computador.



1. Painel de Navegação do Site e painel de Hierarquia de Site Federados
2. Painel Visão geral
3. Painel Propriedades
4. Painel de Visualização

Painel navegação do site

Este é o elemento principal de navegação no Management Client. Ele reflete o nome, os ajustes e as configurações do site em que você efetuou o login. O nome do site é visível na parte superior do painel. As funções são agrupadas em categorias que refletem a funcionalidade do software.

No painel **Navegação do site**, você pode configurar e gerenciar seu sistema para que ele corresponda às suas necessidades. Se seu sistema não é um sistema de site único, mas inclui sites federados, note que você gerencia esses sites no painel **Hierarquia de sites federados**.

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Painel da hierarquia de sites federados

Este é o elemento de navegação que exibe todos os sites Milestone Federated Architecture em uma hierarquia de sites pai/filho.

Você pode selecionar qualquer site, fazer o login e o Management Client daquele site é inicializado. O servidor pai em que você está logado está sempre no topo da hierarquia de sites.

Painel Visão geral

Fornece uma visão geral do elemento selecionado no painel **Navegação do site**, por exemplo, como uma lista detalhada. Quando você seleciona um elemento no painel **Visão geral**, ele normalmente exibe as propriedades no painel **Propriedades**. Ao clicar com o botão direito do mouse em elementos no painel **Visão geral** você obtém acesso aos recursos de gerenciamento.

Painel Propriedades

Exibe as propriedades do elemento selecionado no painel **Visão Geral**. As propriedades aparecem em várias guias dedicadas:

Painel de Visualização

O painel **Visualização** aparece quando você trabalha com dispositivos e servidores de gravação. Ele mostra imagens de visualização das câmeras ou exibe informações sobre o estado do dispositivo. O exemplo mostra uma imagem de visualização de uma câmera com informação sobre a resolução e taxa de dados da transmissão ao vivo da câmera:

Por padrão, as informações mostradas com as imagens de visualização da câmera referem-se às transmissões ao vivo. Isso é exibido em texto verde acima da visualização. Se você quiser gravar informações de transmissão em vez disso (texto em vermelho), selecione **Exibir** > **Mostrar transmissões de gravação** no menu.

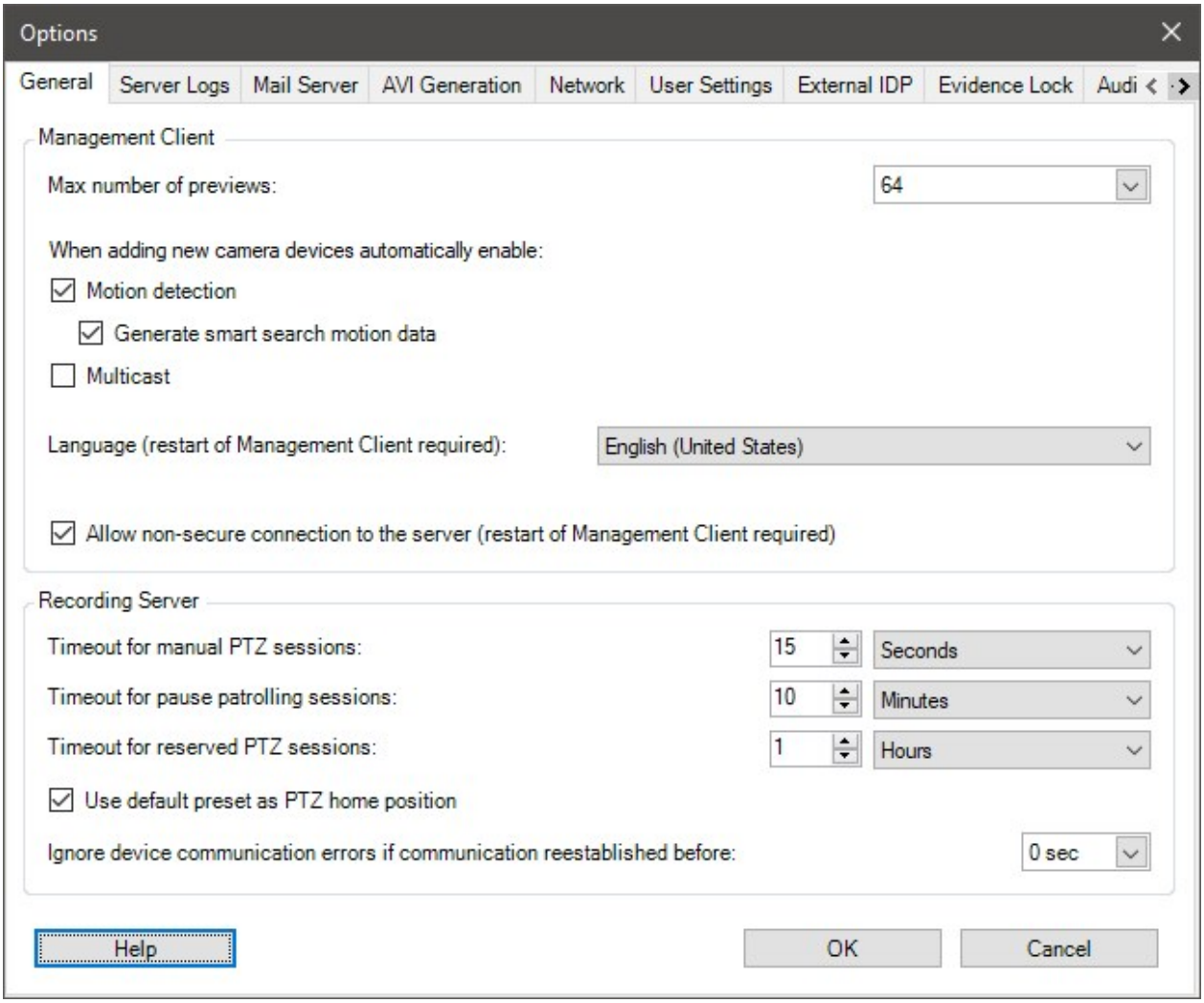
O desempenho pode ser afetado se o painel **Visualização** exibir imagens de visualização de várias câmeras em uma alta taxa de quadros. Para controlar o número de imagens de visualização e a taxa de quadros, selecione **Opções** > **Geral** no menu.

Configurações do sistema (caixa de diálogo Opções)

Na caixa de diálogo **Opções**, você pode especificar um número de definições relacionadas com a aparência geral e a funcionalidade do sistema.

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Para acessar a caixa de diálogo, selecione **Ferramentas** > **Opções**.



Guia Geral (opções)

Na guia Geral, você pode especificar as configurações gerais para o Management Client e o servidor de gravação.

Management Client

Nome	Descrição
Número máximo de visualizações	Selecione o número máximo de imagens em miniatura exibidas no painel **Visualização**. O padrão é 64 imagens em

Nome	Descrição
	miniatura. Selecione **Ação** > **Atualizar** no menu para que a alteração tenha efeito. Um grande número de imagens em miniatura em conjunto com uma alta taxa de quadros pode reduzir a velocidade do sistema.
Ao adicionar novos dispositivos de câmera automaticamente, ativar: Detecção de movimento	Marque a caixa de seleção para ativar a detecção de movimento em novas câmeras quando você adicioná-las ao sistema com o assistente **Adicionar hardware**. Essa configuração não afeta as configurações de detecção de movimento em câmeras existentes. Você ativa e desativa a detecção de movimento de uma câmera na guia **Movimento** para o dispositivo da câmera.
Ao adicionar novos dispositivos de câmera automaticamente, ativar: Gerar dados de movimento para pesquisa inteligente	A geração de dados para pesquisa de movimento inteligente requer que a detecção de movimento seja habilitada para a câmera. Marque a caixa de seleção para ativar a geração de dados de movimento em novas câmeras quando você adicioná-las ao sistema com o assistente **Adicionar hardware**. Essa configuração não afeta as configurações de detecção de movimento em câmeras existentes. Você ativa e desativa a geração de dados de movimento de pesquisa inteligente de uma câmera na guia **Movimento** para o dispositivo da câmera.
Ao adicionar novos dispositivos de câmera automaticamente, ativar: Multicast	Marque a caixa de seleção para ativar multicast em novas câmeras quando você adicioná-las com o assistente **Adicionar hardware**. Essa configuração não afeta as configurações de multicast em câmeras existentes. Você ativa e desativa o multicasting ao vivo para uma câmera na guia **Cliente** para o dispositivo da câmera.

Nome	Descrição
Idioma	Selecione o idioma do Management Client. Reinicie o Management Client para usar o novo idioma.
Permitir conexão não segura ao servidor	Marque a caixa de seleção para permitir conexões não seguras do servidor, por protocolo HTTP. (Nenhum usuário é solicitado a permitir conexões de servidor não seguras). Reinicie o Management Client para usar esta configuração.

Servidor de gravação

Nome	Descrição
Limite de tempo para sessões PTZ	Usuários de cliente com as permissões de usuário necessárias pode interromper manualmente o patrulhamento de câmeras PTZ. Selecione quanto tempo deve passar antes de o patrulhamento regular ser retomado após uma interrupção manual. A configuração se aplica a todas as câmeras PTZ no seu sistema. A configuração padrão é 15 segundos. Se quiser tempos limite individuais para as câmeras, especifique isso na guia **Predefinições** da câmera.
Limite de tempo para pausa de sessões de patrulha	Usuários clientes com prioridade PTZ suficiente podem pausar uma patrulha em câmera PTZ. Selecione quanto tempo deve passar antes da patrulha regular ser retomada após uma pausa. A configuração se aplica a todas as câmeras PTZ no seu sistema. A configuração padrão é 10 minutos. Se quiser tempos limite individuais para as câmeras, especifique isso na guia **Predefinições** da câmera.
Limite de tempo para sessões PTZ reservadas	Defina o limite de tempo para sessões PTZ reservadas. Quando um usuário executa uma sessão PTZ reservada, a câmera PTZ não pode ser usada por outras pessoas antes de ser liberada manualmente ou quando o período limite expirou. A configuração padrão é 1 hora. Se quiser tempos limite individuais para as câmeras, especifique isso na guia **Predefinições** da câmera.

Nome	Descrição
Usar predefinida padrão como posição inicial PTZ	Marque esta caixa de seleção para usar a posição predefinida padrão em vez da posição inicial de câmeras PTZ ao ativar o botão **Início** em um cliente. Uma posição predefinida padrão precisa ser definida para a câmera. Se não houver uma posição predefinida estabelecida, nada acontecerá ao ativar o botão **Início** em um cliente. Por padrão, esta caixa de seleção está desmarcada. Para atribuir uma posição predefinida padrão, consulte Atribuir uma posição predefinida da câmera como padrão na página 254
Ignore os erros de comunicação de dispositivos se a comunicação for restabelecida antes	O sistema registra todos os erros de comunicação no hardware e nos dispositivos, mas aqui você seleciona por quanto tempo um erro de comunicação deve existir antes que o mecanismo dispare o evento **Erro de comunicação**.

Guia Registros do servidor (opções)

Na guia **Registros do servidor**, você pode especificar as configurações de registros do servidor de gerenciamento do sistema.

Para obter mais informações, consulte Identificar atividades, eventos, ações e erros de usuário.

Nome	Descrição
Registros	Selecione o tipo de registro que deseja configurar: • Registros do sistema • Registros de auditoria • Registros acionados por regras
Configurações	Desativar ou ativar os registros e especificar o período de retenção. Permitir que 2018 R2 e componentes anteriores escrevam registros. Para obter mais

Nome	Descrição
	informações, consulte Permitir que 2018 R2 e componentes anteriores escrevam registros. Para registros do **Sistema**, especifique o nível de mensagens que você desejar registrar: • Tudo - inclui mensagens indefinidas • Informações, avisos e erros • Avisos e erros • Erros (configuração padrão) Para registros de **Auditoria**, ativar o registro de acesso do usuário, se você desejar que o sistema registre todas as ações do usuário em XProtect Smart Client. Essas são, por exemplo, exportações, ativação das saídas, visualização das câmeras ao vivo ou em reprodução. Especifique: • A duração de uma sequência de reprodução Isso significa que, enquanto o usuário reproduz dentro deste período, o sistema gera apenas uma entrada no registro. Ao reproduzir fora do período, o sistema cria uma nova entrada de registro. • O número de registros (quadros) que um usuário viu antes que o sistema criasse uma entrada de registro.

Guia Servidor de correio (opções)

Na guia **Servidor de e-mail**, você pode especificar as configurações para o servidor de e-mail do seu sistema. Para mais informações, consulte Perfis de notificação (explicado).

Nome	Descrição
Endereço de e-mail do remetente	Digite o endereço de e-mail que você quer que apareça como remetente da notificação para todos os perfis de notificação. Exemplo: **sender@organization.org**.

Nome	Descrição
Endereço do servidor de e-mail	Digite o endereço do servidor de e-mail SMTP que envia notificações por e-mail. Exemplo: **mailserver.organization.org**.
Porta do servidor de e-mail	A porta TCP usada para conectar ao servidor de e-mail. A porta padrão é 25 para conexões não criptografadas. Conexões criptografas normalmente usam a porta 465 ou 587.
Criptografe a conexão ao servidor	Se desejar proteger a comunicação entre o servidor de gerenciamento e o servidor de e-mail SMTP, selecione esta caixa de verificação. A conexão é protegida usando o comando do protocolo de e-mail STARTTLS. Neste modo, a sessão começa em uma conexão não criptografada , então um comando STARTTLS é emitido pelo servidor de correio SMTP para o servidor de gerenciamento para alternar para comunicação segura usando SSL.
O servidor requer login	Se ativada, você deve especificar um nome de usuário e senha para que os usuários efetuem o login ao servidor de e-mail.

Guia Geração AVI (opções)

Na guia **Geração AVI**, você pode especificar as configurações de compactação para a geração de clipes de vídeo AVI. As configurações são necessárias se você quiser incluir arquivos AVI em notificações por e-mail enviadas por perfis de notificação acionados por regras.

Consulte também Acionar notificações por e-mail com regras.

Nome	Descrição
Compactador	Selecione o codec (tecnologia de compactação / descompactação) que você deseja aplicar. Para ter mais codecs disponíveis na lista, instale-os no servidor de gerenciamento. Nem todas as câmeras suportam todos os codecs.
Qualidade de compactação	(Não está disponível para todos os codecs). Usar o controle deslizante para selecionar o grau de compactação (**0**-**100**) a ser realizado pelo codec.

Nome	Descrição
	0 significa sem compressão, geralmente resultando em imagens de altas qualidade e arquivos de grande tamanho. **100** significa compactação máxima, geralmente resultando em imagens de baixa qualidade e arquivos de pequeno tamanho. Se o controle deslizante não estiver disponível, a qualidade de compactação é determinada inteiramente pelo codec selecionado.
Quadro-chave cada	(Não está disponível para todos os codecs). Se você quiser usar quadros-chave, marque a caixa de seleção e especifique o número necessário de quadros entre os quadros-chave. Uma chave de quadro é um único quadro armazenado em intervalos específicos. O quadro chave contém a visão inteira da câmera, enquanto os quadros seguintes gravam apenas os pixels que mudam. Isso ajuda muito a reduzir o tamanho dos arquivos. Se a caixa de seleção não estiver disponível, ou não for selecionado, cada quadro contém toda a visão da câmera.
Taxa de dados	(Não está disponível para todos os codecs). Se você quiser usar uma taxa de dados específica, selecione a caixa de seleção e especifique o número de kilobytes por segundo. A taxa de dados especifica o tamanho do arquivo AVI anexado. Se a caixa de seleção não estiver disponível, ou não estiver selecionada, a taxa de dados é determinada pelo codec selecionado.

Guia Rede (opções)

Na guia **Rede**, você pode especificar os endereços IP dos clientes locais, se os clientes irão se conectar ao servidor de gravação pela internet. O sistema de monitoramento, em seguida, os reconhece como vindo da rede local.

Você também pode especificar a versão do IP do sistema: IPv4 ou IPv6. O valor padrão é IPv4.

Guia Marcadores (opções)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Na guia **Marcadores**, você pode especificar configurações para marcadores, suas identificações e função no XProtect Smart Client.

Nome	Descrição
Prefixo ID do marcador	Especifique um prefixo para todos os marcadores feitos pelos usuários do XProtect Smart Client.
Hora padrão do marcador	Especificar o início e o fim do tempo padrão de um marcador definido no XProtect Smart Client. Esta definição tem de estar alinhada com: • Regra de marcador padrão, consulte Regras (nó Regras e eventos). • Período de pré-buffer para cada câmera, consulte Gerenciar pré-buffering.

Para especificar as permissões de marcador de uma função, consulte Guia Dispositivos (funções) na página 559.

Guia Configurações do usuário (opções)

Na guia **Configurações do usuário**, você pode especificar as configurações de preferências do usuário, por exemplo, se uma mensagem deve ser exibida quando a gravação remota estiver ativada.

Guia IDP externo (opções)

Na guia **IDP externo** no Management Client, você pode adicionar e configurar um IDP externo e registrar alegações dele.

Nome	Descrição
Ativado	O IDP externo é ativado por padrão.
Nome	O nome do IDP externo. O nome que você insere aqui aparece no campo **Autenticação** na janela de login do seu cliente.
Autoridade de autenticação	O URL do IDP externo.
Adicionar	Adicionar e configurar um IDP externo. Ao selecionar **Adicionar**, a caixa de diálogo **IDP externo** é aberta e você pode inserir as informações para a configuração, consulte **Configurar um IDP externo** abaixo da tabela.
Editar	Edite a configuração do IDP externo.
Remover	Remova a configuração do IDP externo.  Se você remover uma configuração de IDP externo, os usuários que são autenticados por meio deste IDP externo não serão capazes de fazer login no VMS do XProtect. Se você adicionar o IDP externo novamente, novos usuários serão criados no login porque o ID do IDP externo mudou.

Configurou um IDP externo

- Para adicionar um IDP externo, selecione **Adicionar** na seção **IDP externo** e insira as informações na tabela abaixo:

Nome	Descrição
Nome	O nome do IDP externo que você insere aqui aparece no campo **Autenticação** na janela de login do seu cliente.
ID do cliente e **Segredo do cliente**	Deve ser obtido do IDP externo. O ID do cliente e o segredo do cliente são necessários para se comunicar com segurança com o IDP externo.

Nome	Descrição
Caminho de retorno	Parte de uma URL para o fluxo de redirecionamento de autenticação para conectar usuários. Os usuários são conectados a partir de uma página de login hospedada pelo IDP externo. Quando o processo de autenticação é concluído, esse caminho é invocado e o usuário é redirecionado para o VMS do XProtect. O valor padrão é “/signin-oidc”. O formato de redirecionamento O caminho de retorno de chamada do URI é construído pelo servidor de gerenciamento FQID junto com /idp/ e o caminho de retorno de chamada configurado no provedor externo. Exemplos: • Formato de redirecionamento URI para o XProtect Smart Client e o XProtect Management Client: [schema]://[management server address]/idp/[callback path] • Formato de redirecionamento do URI para o XProtect Web Client e o cliente XProtect Mobile: [redirect Uri without “/index.html”]/idp/[callback path] Observe que a parte "idp" do caminho de retorno de chamada diferencia maiúsculas de minúsculas e deve ser inserida em letras minúsculas.
Solicitar login	Especifique ao IDP externo se o usuário deve permanecer conectado ou se é necessária uma verificação do usuário. Dependendo do IDP externo, a verificação pode incluir uma verificação de senha ou um login completo.
Reivindicação de uso para criar nome de usuário	Opcionalmente, especifique qual alegação do IDP externo deve ser usada para gerar um nome de usuário exclusivo para o usuário provisionado automaticamente no VMS. Para obter mais informações sobre nomes de usuários exclusivos criados por alegações, consulte Nomes de usuários exclusivos para usuários de IDP externo.
Escopos	Alternativamente, use escopos para limitar o número de alegações que você obtém de um IPD externo. Se você sabe que as alegações relevantes para seu VMS estão em um escopo específico, você pode usar o escopo para limitar o número de alegações que obtém do IDP externo.

Registrar reivindicações

Ao registrar alegações do IDP externo, você pode mapear as alegações para funções no VMS para determinar os privilégios do usuário no VMS. Para obter mais informações, consulte Alegações de mapa de um IDP externo.

- Para registrar alegações de um IDP externo, selecione **Adicionar** na seção **Alegações registradas** e insira as informações na tabela abaixo:

Nome	Descrição
IDP externo	O nome do IDP externo.
Nome da reivindicação	Nome da reivindicação em texto livre. O nome estará disponível ao selecionar uma função.
Nome de exibição	O nome de exibição de uma reivindicação.
Reconhecer maiúsculas e minúsculas	Indica se o valor de uma reivindicação diferencia maiúsculas de minúsculas. Exemplos de valores que normalmente diferenciam maiúsculas de minúsculas: - Representações textuais de IDs, como um guia: F951B1F0-2FED-48F7-88D3-49EB5999C923 ou OadFgrDesdFesff= Exemplos de valores que normalmente não diferenciam maiúsculas de minúsculas: - Endereços de e-mail - Nomes da função - Nomes do grupo .
Adicionar, **Editar**, **Remover**	Registre e mantenha reivindicações. Se você modificar uma alegação no site do IDP externo, um novo login no cliente XProtect será exigido pelos usuários. Digamos que um usuário, Bob, precise ser, por exemplo, Operador. A alegação é então adicionada a Bob no site do IDP externo, mas se Bob já estiver conectado ao XProtect, ele deverá realizar um novo login para que a alteração tenha efeito.

Adicionar URIs redirecionados para clientes da web

O URI redirecionado é a localização para onde o usuário é redirecionado depois do sucesso no login. Os URIs redirecionados precisam ser uma correspondência exara dos endereços dos clientes da web. Por exemplo, não será possível fazer login por meio de um IDP externo se você abrir XProtect Web Client a partir de **https://localhost:8082/index.html** e o URI redirecionado para os clientes da web que você adicionou for **https://127.0.0.1:8082/index.html**.

Nome	Descrição
URI	O URI do XProtect Web Client no formato **https://[mobile server]:[port]/index.html**. Os URIs redirecionados não diferenciam maiúsculas de minúsculas.
Adicionar, **Editar**, **Remover**	Registrar e manter URIs redirecionados. Ao remover URIs, é preciso manter pelo menos um URI redirecionado para o sistema funcionar.

Guia Painel de Controle do Cliente (opções)

Na guia **Customer Dashboard (Painel de Controle do Cliente)**, você pode ativar ou desativar Milestone Customer Dashboard.

O Painel de Controle do Cliente é um serviço de monitoramento on-line que fornece uma visão geral gráfica do estado atual de seu sistema, inclusive possíveis problemas técnicos (tais como falhas de câmera), para os administradores do sistema ou outras pessoas que têm acesso a informações sobre a instalação do sistema.

Marque ou desmarque a caixa de seleção para alterar as configurações do Painel de Controle do Cliente.

Guia Proteção de evidências (opções)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Na guia **Proteção de evidências** são definidos e editados os perfis de proteção de evidências e o tempo que os usuários clientes podem escolher para manter os dados protegidos.

Nome	Descrição
Perfis de proteção de evidências	Uma relação com perfis definidos de proteção de evidências. Você pode adicionar e remover perfis de proteção de evidências existentes. Não é possível remover o perfil de proteção de evidências padrão, mas você pode alterar suas opções de tempo e nome.
Opções de tempo de proteção	O tempo que os usuários do cliente podem escolher para proteger evidências. As opções disponíveis são hora(s), dia(s), semana(s), mês(es), ano(s), indefinido ou definido pelo usuário.

Para especificar as permissões de proteção de evidências de uma função, consulte Guia Dispositivos (funções) na página 559 para configurações da função.

Guia de mensagens de áudio (opções)

Na guia **Mensagens de áudio**, você pode fazer o upload dos arquivos com mensagens de áudio que são usados para a transmissão de mensagens, ativadas por regras.

O número máximo de arquivos cujo upload foi feito é 50, e o tamanho máximo permitido para cada arquivo é de 1 MB.

Nome	Descrição
Nome	Fornece o nome de uma mensagem. Você digita o nome quando você adiciona uma mensagem. Para fazer o upload de uma mensagem no sistema, clique em **Adicionar**.
Descrição	Fornece uma descrição da mensagem. Você digita a descrição quando adiciona uma mensagem. Você pode usar o campo de descrição para descrever o propósito ou a própria mensagem.
Adicionar	Adicione você mesmo mensagens de áudio ao sistema. Formatos compatíveis são arquivos de áudio padrão do Windows: • .wav • .wma

Nome	Descrição
	• .flac
Editar	Modifique você mesmo o nome e a descrição, ou você pode substituir o arquivo em questão.
Remover	Delete a mensagem de áudio da lista.
Reproduzir	Clique neste botão para ouvir a mensagem de áudio do computador que executa o Management Client.

Para criar uma regra que dispara a reprodução de mensagens de áudio, consulte Adicionar uma regra.

Para saber mais sobre as ações em geral que você pode usar nas regras, consulte Ações e ações de interrupção.

Guia de configurações de privacidade

Na guia **Configurações de privacidade**, é possível ativar ou desativar o uso da coleta de dados no XProtect Mobile Server, cliente XProtect Mobile, XProtect Web Client e XProtect Smart Client. Em seguida, clique em **OK**.

Ao ativar a coleta de dados de uso, você consente ao Milestone Systems o uso da tecnologia pelo Google como provedor terceirizado, com o qual o processamento de dados nos EUA não pode ser excluído. Para obter mais informações sobre proteção de dados e coleta de dados de uso, consulte o guia de privacidade do GDPR.

Guia Configurações do controle de acesso (opções)

O uso de XProtect Access requer que você tenha adquirido uma licença básica que lhe permita acessar este recurso.

Nome	Descrição
Mostrar o painel de propriedade de desenvolvimento	Se selecionado, são mostradas informações adicionais do desenvolvedor para **Controle de Acesso** > **Configurações Gerais**. Esta definição só deve ser usada por desenvolvedores de integrações de sistemas de controle de acesso.

Guia Eventos analíticos (opções)

Na guia **Eventos analíticos**, você pode ativar e especificar o recurso de eventos analíticos.

Nome	Descrição
Ativar	Especifique se você quer usar os eventos analíticos. Como padrão, o recurso está desativado.
Porta	Especifique a porta usada por este recurso. A porta padrão é 9090. Certifique-se de que os fornecedores de ferramenta VCA relevante também usem este número de porta. Se você alterar o número da porta, lembre-se de mudar o número da porta dos provedores.
Todos os endereços de rede ou **Endereços de rede especificados**	Especifique se os eventos de todos os endereços IP / nomes de host são permitidos, ou apenas eventos de endereços IP / nomes de host que estão especificados na **Lista de endereços** (veja abaixo).
Lista de endereços	Especifique uma lista de endereços IP / nomes de host de confiança. A lista filtra os dados de entrada, de modo que somente os eventos de determinados endereços IP / nomes de host são permitidos. Você pode usar ambos os formatos de endereço Domain Name System (DNS), IPv4 e IPv6. Você também pode adicionar endereços à sua lista ao inserir manualmente cada endereço IP ou nome do host ou ao importar uma lista externa de endereços. • **Inserção manual**: Digite o endereço IP/nome de host na lista de endereços. Repita para cada endereço desejado • **Importar**: Clique em **Importar** para procurar a lista externa de endereços. A lista externa deve ter um arquivo .txt, e cada endereço IP ou nome do host deve estar em uma linha separada

Guia Alarmes e Eventos (opções)

Na guia **Alarmes e Eventos**, você pode especificar as definições para alarmes, eventos e registros. Sobre essas configurações, consulte também Tamanho limite do banco de dados na página 134.

Nome	Descrição
Manter alarmes fechados para	Especifique o número de dias para armazenar alarmes com o status **Fechado** no banco de dados. Se definir o valor como **0**, o alarme será excluído depois de ser fechado. Os alarmes sempre têm carimbos de data/hora. Se o alarme for acionado por uma câmera, o carimbo de data/hora terá uma imagem do momento do alarme. A própria informação de alarme é armazenada no servidor de eventos, ao passo que as gravações de vídeo correspondentes à imagem associada são armazenadas no servidor do sistema de monitoramento relevante. Para poder ver as imagens de seus alarmes, mantenha as gravações de vídeo por, pelo menos, o tempo que você pretende deixar os alarmes no servidor de eventos.
Manter todos os outros alarmes para	Especifique o número de dias para armazenar alarmes com o status **Novo**, **Em andamento** ou **Suspenso**. Se definir o valor como 0, o alarme aparecerá no sistema, mas não será armazenado. Os alarmes sempre têm carimbos de data/hora. Se o alarme for acionado por uma câmera, o carimbo de data/hora terá uma imagem do momento do alarme. A própria informação de alarme é armazenada no servidor de eventos, ao passo que as gravações de vídeo correspondentes à imagem associada são armazenadas no servidor do sistema de monitoramento relevante. Para poder ver as imagens de seus alarmes, mantenha as gravações de vídeo por, pelo menos, o tempo que você pretende deixar os alarmes no servidor de eventos.
Manter os registros para	Especifique o número de dias para manter os registros do servidor de eventos. Se mantiver os registros por períodos mais longos, certifique-se de que a máquina em que o servidor de eventos está instalada tem espaço em disco suficiente.
Ativar registro	Para manter um registro mais detalhado de comunicação do servidor de eventos,

Nome	Descrição
detalhado	selecione a caixa. Ele será armazenado pelo número de dias especificado no campo **Manter registros por**.
Tipos de evento	Especifique o número de dias para armazenar eventos no banco de dados. Há duas maneiras de fazer isso: • Você pode especificar o tempo de retenção para um grupo de eventos inteiro. Tipos de eventos com o valor **Seguir grupo** herdarão o valor do grupo de eventos • Mesmo que defina um valor para um grupo de eventos, você pode especificar o tempo de retenção para tipos de evento individuais.  Se o valor for **0**, os eventos não serão armazenados no banco de dados.  Os eventos externos (eventos definidos pelo usuário, eventos genéricos e eventos de entrada) são definidos como **0** por padrão e você não pode mudar esse valor. A razão pela qual esses tipos de eventos ocorrem tão frequentemente é que armazená-los no banco de dados pode causar problemas de desempenho.

Guia Eventos genéricos (opções)

Na guia **Eventos genéricos**, você pode especificar os eventos genéricos e as configurações relacionadas à fonte de dados.

Para mais informações sobre como configurar os eventos genéricos reais, consulte Eventos genéricos (explicados).

Nome	Descrição
Fonte de dados	Você pode escolher entre duas fontes de dados padrão e definir uma fonte de dados

Nome	Descrição
	personalizada. O que escolher depende do seu programa de terceiros e/ou do software ou hardware do qual você quer fazer a interface: **Compatível**: Configurações padrão de fábrica são ativadas, ecos a todos os bytes, TCP e UDP, somente IPv4, porta 1234, sem separador, apenas o host local, atual codificação de página de código (ANSI). **Internacional**: Configurações padrão de fábrica são ativadas, estatísticas ecos apenas, apenas TCP, IPv4+6, porta 1235, <CR><LF> como separador, apenas o host local, codificação UTF-8. (<CR><LF> = 13,10). [Fontes de dados A] [Fontes de dados B] e assim por diante.
Novo	Clique para definir uma nova fonte de dados.
Nome	Nome da fonte de dados.
Ativado	Fontes de dados são desabilitadas por padrão. Marque a caixa de seleção para ativar a fonte de dados.
Redefinir	Clique para restaurar todas as configurações da fonte de dados selecionada. O nome fornecido no campo **Nome** permanece.
Porta	O número da porta da fonte de dados.
Seletor de tipo de protocolo	Os protocolos que o sistema deve ouvir e analisar, a fim de detectar eventos genéricos: **Qualquer**: TCP bem como UDP. **TCP**: Somente TCP. **UDP**: Somente UDP. Pacotes TCP e UDP utilizados para eventos genéricos podem conter caracteres especiais, como @, #, +, ~, etc.
Seletor de tipo IP	Tipos selecionáveis de endereço IP: IPv4, IPv6 ou ambos.

Nome	Descrição
Bytes separadores	Selecione os bytes de separadores para separar registros individuais de eventos genéricos. Padrão para o tipo de fonte de dados **internacional** (veja **Fontes de dados** anterior) é **13,10**. (13,10 = <CR><IF>).
Seletor de tipo eco	Formatos de retorno de echo disponíveis: • **Estatísticas de eco**: Ecoa o seguinte formato: **[X],[Y],[Z],[Nome do evento genérico]** **[X]** = número do pedido. **[Y]** = número de caracteres. **[Z]** = número combina com um evento genérico. **[Nome de evento genérico]** = nome digitado no campo **Nome**. • **Ecoar todos os bytes**: Ecoa todos os bytes • **Sem eco**: Suprimir todos os ecos
Seletor de tipo codificação	Por padrão, a lista somente exibe as opções mais relevantes. Selecione a caixa de seleção **Mostrar todos** para exibir todas as codificações disponíveis.
Endereços IPv4 externos permitidos	Especifique os endereços IP com os quais o servidor de gerenciamento deve poder comunicar-se a fim de gerenciar eventos externos. Você também pode usar isso para excluir endereços IP dos quais você não deseja dados.
Endereços IPv6 externos permitidos	Especifique os endereços IP com os quais o servidor de gerenciamento deve poder comunicar-se a fim de gerenciar eventos externos. Você também pode usar isso para excluir endereços IP dos quais você não deseja dados.

Menus de componente

Management Client menus

Menu Arquivo

Você pode salvar as alterações na configuração e sair do aplicativo. Você também pode fazer backup de sua configuração, consulte Backup e restauração da configuração do seu sistema (explicado) na página 340.

Menu Editar

Você pode desfazer as alterações.

Menu Visualizar

Nome	Descrição
Redefinir layout do aplicativo	Redefina o layout dos diferentes painéis no Management Client para suas configurações padrão.
Janela de visualização	Alterne o painel **Visualização** ao trabalhar com dispositivos e servidores de gravação.
Exibir transmissões de gravação	Por padrão, as informações mostradas com imagens de visualização no painel **Visualização** referem-se a transmissões ao vivo das câmeras. Em vez disso se você quer informação sobre transmissões de gravação, selecione **Exibir transmissões de gravação**.
Hierarquia de sites federados	Por padrão, o painel **Hierarquia federada do site** está habilitado.
Navegação no site	Por padrão, o painel **Navegação do site** está habilitado.

Menu Ação

O conteúdo do menu **Ação** varia de acordo com o elemento selecionado no painel **Navegação do site**. As ações que você pode escolher são as mesmas de quando você clica com o botão direito no elemento.

Período de pré-buffer para cada câmera, consulte Gerenciar pré-buffering.

Nome	Descrição
Atualizar	Está sempre disponível e recarrega as informações solicitadas a partir do servidor de gerenciamento.

Menu de ferramentas

Nome	Descrição
Serviços registrados	Gerencie serviços registrados. Consulte Gerenciar serviços registrados na página 367.
Funções efetivas	Veja todas as funções de um usuário ou grupo selecionado.
Opções	Abre a caixa de diálogo Opções, que permite definir e editar configurações globais do sistema. Para obter mais informações, consulte Configurações do sistema (caixa de diálogo Opções) na página 393.

Menu Ajuda

Você pode acessar o sistema de ajuda e informações sobre a versão do Management Client.

Server Configurator (Utilidade)

Propriedades da guia Criptografia

Essa guia permite especificar as seguintes propriedades:

> Em um ambiente de cluster, você deve configurar seu cluster e certificar-se de que ele esteja em execução antes de criar certificados para todos os computadores no ambiente de cluster. Depois disso, você pode instalar os certificados e fazer o registro usando o Server Configurator para todos os nós do cluster. Para obter mais informações, consulte o guia de certificados sobre como proteger suas XProtect VMS instalações.

Nome	Descrição	Tarefa
Certificado do servidor	Selecione o certificado a ser usado para criptografar a conexão de duas vias entre o servidor de gerenciamento, coletores de dados, servidores de registros e servidores de gravação.	Ativar criptografia para e do servidor de gerenciamento Habilitar a criptografia do servidor para servidores de gravação ou servidores

Nome	Descrição	Tarefa
		remotos
Servidor de eventos e extensões	Selecione o certificado a ser usado para criptografar a conexão bidirecional entre o servidor de eventos e os componentes que se comunicam com o servidor de eventos , incluindo o LPR Server.	Ativar criptografia do servidor de eventos na página 314
Certificado de mídia de streaming	Selecione o certificado a ser usado para criptografar a comunicação entre os servidores de gravação e todos os clientes, e as integrações que recuperam fluxos de dados dos servidores de gravação.	Ative a criptografia para cliente e serviços
Certificado de mídia de streaming móvel	Selecione o certificado a ser usado para criptografar a comunicação entre o servidor móvel e os clientes móveis e da web que recuperam fluxos de dados do servidor móvel.	Ativar criptografia no servidor móvel

Servidores de registro

Nome	Descrição	Tarefa
Endereço do servidor de gerenciamento	O endereço do servidor de gerenciamento normalmente inclui o nome do host ou o nome do domínio totalmente qualificado (FQDN) do computador. Por padrão, este endereço fica ativo apenas em um computador no XProtect VMS em que o servidor de gerenciamento não esteja instalado. Como regra geral, o endereço do servidor de gerenciamento não deve ser alterado em um computador que tenha o servidor de gerenciamento instalado.	Clique para obter mais informações sobre as implicações de alterar o endereço do servidor de gerenciamento de um computador que possua o servidor de gerenciamento instalado: Alterar o nome do host do computador servidor de gerenciamento

Nome	Descrição	Tarefa
	No entanto, se, por exemplo, você usar o Server Configurator em uma configuração de failover, pode ser necessário alterar o endereço no computador do servidor de gerenciamento. Isso pode ser em um ambiente de failover de cluster ou em outro cenário de configuração de failover. • Para ativar o campo **Endereço do servidor de gerenciamento**, a partir de um computador com o servidor de gerenciamento instalado, clique no ícone da caneta ( ). Se você atualizar o endereço do servidor de gerenciamento, você precisará acessar cada um dos computadores que têm componentes instalados e atualize o servidor de gerenciamento com as novas informações de endereço.	
Registrar	Registra os servidores que estão sendo executados no computador com o servidor de gerenciamento designado.	Registrar um servidor de gravação

Seleção de idioma

Use esta guia para selecionar o idioma para o Server Configurator. O conjunto de idiomas para o Server Configurator corresponde ao conjunto de idiomas para o Management Client.

Nome	Descrição
Escolher idioma	Escolher o idioma da interface de usuário.

Se trabalhar em um ambiente com cluster de emergência, recomenda-se que você pause o cluster, antes de iniciar tarefas no Server Configurator. Isto é porque o Server Configurator pode precisar interromper serviços enquanto aplica as alterações e o ambiente de cluster de emergência pode interferir com esta operação.

Status do ícone de bandeja

Os ícones da bandeja na tabela mostram os diferentes estados dos serviços em execução nos servidores no XProtect VMS. Os ícones estão disponíveis em computadores com os servidores instalados:

Management Server Manager ícone da bandeja	Recording Server Manager ícone da bandeja	Event Server Manager ícone da bandeja	Failover Recording Server Manager ícone da bandeja	Descrição
				**Executando** Aparece quando um serviço de servidos está ativado e iniciado. Se o serviço Failover Recording Server estiver em execução, ele pode assumir se o servidor de gravação padrão falhar.
				**Parado** Aparece quando um serviço de servidor tiver parado.

Management Server Manager ícone da bandeja	Recording Server Manager ícone da bandeja	Event Server Manager ícone da bandeja	Failover Recording Server Manager ícone da bandeja	Descrição
				Se o serviço Failover Recording Server parar, ele não pode assumir se o servidor de gravação padrão falhar.
				**Iniciando** Aparece quando um serviço de servidor está em processo de inicialização. Sob circunstâncias normais, o ícone de bandeja muda, após um breve período, para **Executando**.
				**Parando** Aparece quando um serviço de servidor está em processo de interrupção. Sob circunstâncias normais, o ícone de bandeja muda, após um breve período, para **Interrompido**.
				**Em estado indeterminado** Aparece quando o serviço do servidor é carregado inicialmente e até a primeira informação ser recebida, após o que o ícone de bandeja, sob circunstâncias normais muda para **Iniciando** e depois, para **Executando**.

Management Server Manager ícone da bandeja	Recording Server Manager ícone da bandeja	Event Server Manager ícone da bandeja	Failover Recording Server Manager ícone da bandeja	Descrição
				**Executando offline** Aparece normalmente, quando o servidor de gravação ou o serviço de gravação Failover está em execução, mas o serviço Management Server não.

Iniciar e interromper serviços a partir dos ícones da bandeja

Clique com o botão direito do mouse no ícone da bandeja na área de notificação onde é possível iniciar e interromper serviços.

- Iniciar ou interromper o serviço Management Server
- Iniciar ou interromper o serviço Recording Server

Management Server Manager (ícone de bandeja)

Use os itens de menu no ícone da bandeja do Management Server Manager para executar tarefas do Management Server Manager.

Nome	Descrição
Iniciar Management Server e **Parar Management Server**	Clique no item de menu apropriado para iniciar ou interromper o serviço Management Server. Se você interromper o serviço Management Server, não poderá usar o Management Client. O estado do serviço é refletido pelo ícone da bandeja. Para mais informações sobre os estados dos ícones de bandeja, consulte Ícones da bandeja do gerenciador de servidores (explicado).
Exibir mensagens de status	Visualize uma lista de mensagens de status com registro de data e hora.

Nome	Descrição
Alterar as configurações de senha de configuração do site	Atribua ou altere uma senha de configuração do sistema. Você também pode optar por não proteger a configuração do sistema com senha, removendo quaisquer senhas de configuração do sistema atribuídas. Modificar as configurações de senha do ajuste do sistema
Insira a senha de configuração do site	Insira uma senha. Isso se aplica se, por exemplo, o arquivo que contém as configurações de senha for excluído ou corrompido. Para obter mais informações, consulte Digitar as configurações de senha de configuração do sistema.
Configurar servidor de gerenciamento de failover	Inicie o assistente de configuração para o servidor de gerenciamento de failover ou abra a página **Gerenciar sua configuração** para gerenciar sua configuração existente. Para obter mais informações sobre o cluster de failover, consulte XProtect Management Server Failover na página 38.
Server Configurator	Abre o **Server Configurator** para registrar servidores e gerenciar criptografia. Para obter mais informações sobre como gerenciar criptografia, consulte Gerenciar criptografia com o Server Configurator.
Modificar a licença	No computador do servidor de gerenciamento, altere o código de licença do software. Você precisaria inserir um novo código de licença para, por exemplo, atualizar seu sistema XProtect. Para obter mais informações, consulte Alterar o código da licença de software.
Restaurar configuração	Abre uma caixa de diálogo de onde é possível restaurar a configuração do sistema. Certifique-se de ler as informações na caixa de diálogo antes de clicar em **Restaurar**. Para obter mais informações, consulte Restaurar a configuração do sistema a partir de um backup manual.
Selecionar a pasta de backup compartilhada	Defina uma pasta de backup para armazenar seu backup, antes de fazer backup de qualquer configuração do sistema. Para obter mais informações, consulte Selecionar pasta de backup compartilhada.
Atualizar endereço SQL	Abra um assistente para alterar o endereço do SQL Server. No caso raro de uma mudança de nome de host, talvez o endereço do SQL Server possa ter de ser alinhado com as mudanças. Para obter mais informações, consulte Uma mudança no nome do host pode desencadear a mudança do endereço do servidor SQL.

Nó básico

Informações da licença (nó Fundamentos)

Na janela **Informações da licença**, você pode acompanhar todas as licenças que compartilham o mesmo arquivo de licença de software tanto neste site como em todos os outros sites, suas assinaturas Milestone Care e decidir como deseja ativar as suas licenças.

Para saber mais sobre os vários recursos e informações disponíveis na janela **Informações da licença**, consulte Janela Informações da licença na página 130.

Informações do site (nó Fundamentos)

Em uma configuração maior do Milestone Federated Architecture com muitos sites filho, é fácil perder a visão geral e pode ser difícil encontrar as informações de contato para os administradores de cada site filho.

Portanto, você pode adicionar informações adicionais a cada site filho e essas informações estarão disponíveis para os administradores da central de controle.

É possível acrescentar as seguintes informações:

- Nome do site
- Endereço / localização
- Administrador(es)
- Informações adicionais

Nó de serviços de conexão remota

Conexão de câmera Axis One-click (Nó de serviços de conexão remota)

Essas são as propriedades de conexão da câmera Axis One-Click.

Nome	Descrição
Senha da câmera	Inserir/editar. Fornecida com a sua câmera na compra. Para mais detalhes, veja o manual da sua câmera ou acesse o site da Axis (https://www.axis.com/).
Usuário da câmera	Veja os detalhes para a **Senha da câmera**.

Nome	Descrição
Descrição	Insira/edite uma descrição para a câmera.
Endereço externo	Insira/edite o endereço da web do servidor ST ao qual a câmera(s) está conectada.
Endereço interno	Insira/edite o endereço da web do servidor ST ao qual o servidor de gravação se conecta.
Nome	Se necessário, edite o nome do item.
Chave de autenticação do proprietário	Veja **Senha da câmera**.
Senhas (para Dispatch Server)	Insira a senha. Deve ser idêntica àquela recebida do seu provedor do sistema.
Senhas (para servidor ST)	Insira a senha. Deve ser idêntico àquele inserido quando o Componente Axis One-Click Connection foi instalado.
Registrar/cancelar registro no Axis Dispatch Service	Indica se você deseja registrar sua câmera Axis com o Axis dispatch service. Pode ser feito no momento da configuração ou posteriormente.
Número de série	Número de série do hardware especificado pelo fabricante. O número de série é frequentemente, mas não sempre, idêntico ao endereço MAC.
Usar credenciais	Selecione a caixa de seleção se decidir usar credenciais durante a instalação no servidor ST.
Nome de usuário (para Dispatch Server)	Insira um nome de usuário. O nome de usuário deve ser idêntico àquele recebido do seu provedor do sistema.
Nome de usuário (para servidor ST)	Insira um nome de usuário. Deve ser idêntico àquele inserido quando o **Componente Axis One-Click Connection** foi instalado.

Nó de servidores

Servidores (nó)

Esta seção descreve como instalar e configurar servidores de gravação e servidores do sistema de gravação ininterrupta. Você também vai aprender como adicionar novo hardware ao sistema e interconectar outros sites.

- Servidores de gravação (nó Servidores) na página 423
- Servidores de failover (nó Servidores) na página 437

Servidores de gravação (nó Servidores)

O sistema usa servidores de gravação para gravação de feeds de vídeo e para comunicação com câmeras e outros dispositivos. Um sistema de monitoramento é tipicamente constituído por vários servidores de gravação.

Os servidores de gravação são computadores em que você instalou o software Recording Server e o configurou para se comunicar com o servidor de gerenciamento. É possível ver os servidores de gravação do seu sistema no painel **Visão geral** quando você expande a pasta **Servidores** e seleciona **Servidores de Gravação**.

A compatibilidade com versões de servidores de gravação anteriores à versão atual do servidor de gerenciamento é limitada. Você ainda pode acessar gravações nesses servidores de gravação com versões mais antigas, mas se desejar alterar a sua configuração, certifique-se de que eles tenham a mesma versão do servidor de gerenciamento. A Milestone recomenda que você atualize todos os servidores de gravação no seu sistema para a mesma versão que o seu servidor de gerenciamento.

Janela Configurações do servidor de gravação

Ao clicar com o botão direito do mouse no ícone do Recording Server Manager da bandeja e selecionar **Alterar configurações**, você pode especificar o seguinte:

Nome	Descrição
Endereço	Endereço IP (exemplo: 123.123.123.123) ou o nome do host do servidor de gerenciamento (exemplo: nossoservidor) para o qual o servidor de gravação deve ser conectado. Essas informações são necessárias para que o servidor de gravação possa se comunicar com o servidor de gerenciamento.
Porta	Número da porta a ser utilizada na comunicação com o servidor de gerenciamento. O padrão é a porta 9000. Você pode mudar isso, caso precise.
Porta do servidor web	Número da porta a ser usado para lidar com solicitações de servidor web, por exemplo, para lidar com comandos de controle de câmera PTZ e para navegar e solicitações ao vivo do XProtect Smart Client. O padrão é a porta 7563. Você pode mudar isso, caso precise.
Porta do servidor de alertas	Número da porta a ser usado quando o servidor de gravação escuta as informações de TCP (alguns dispositivos usam TCP para enviar mensagens de eventos). O padrão é a porta 5432 (desativada por padrão). Você pode mudar isso, caso precise.
Porta do servidor SMTP	Número da porta a ser usado quando o servidor de gravação escuta as informações do Simple Mail Transfer Protocol (SMTP). SMTP é um padrão para enviar mensagens de e-mail entre servidores. Alguns dispositivos usam SMTP para enviar mensagens de eventos ou imagens ao servidor do sistema de vigilância por e-mail. O padrão é a porta 25, que você pode ativar e desativar. Você pode mudar o número da porta, caso seja necessário.
Criptografe conexões do servidor de gerenciamento para o servidor de gravação	Antes de habilitar a criptografia e selecionar um certificado de autenticação do servidor na lista, certifique-se de habilitar a criptografia no servidor de gerenciamento primeiro e de que o certificado do servidor de gerenciamento é confiável no servidor de gravação. Para obter mais informações, consulte Comunicação segura (explicado) na página 151.
Criptografe conexões para clientes e serviços que realizam fluxo de dados	Antes de ativar a criptografia e selecionar o certificado de autenticação da lista, certifique-se de que o certificado é confiável em todos os computadores executando clientes e serviços que recuperam fluxos de dados do servidor de gravação. XProtect Smart Client e todos os serviços que recuperam fluxos de dados do servidor de gravação devem ser atualizados para a versão 2019 R1 ou superior. Algumas soluções de terceiros criadas usando versões do MIP SDK anteriores à 2019 R1 podem precisar ser atualizadas.

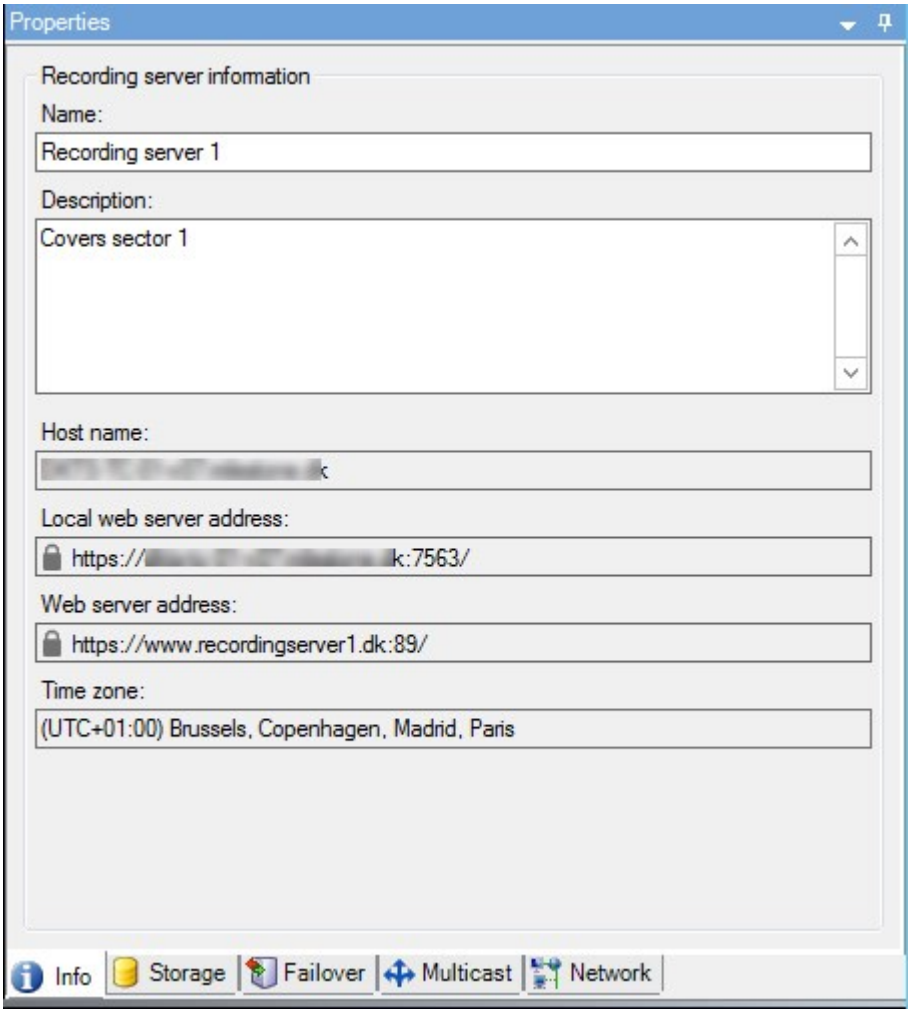
Nome	Descrição
	Para obter mais informações, consulte Comunicação segura (explicado) na página 151. Para verificar se seu servidor de gravação usa criptografia, consulte Visualizar status de criptografia para clientes na página 300.
Detalhes	Visualizar informações do Repositório de certificados do Windows sobre o certificado selecionado.

Propriedades de servidores de gravação

Guia informações (servidor de gravação)

Na guia **Informações**, você pode verificar ou editar o nome e a descrição do servidor de gravação.

Você pode visualizar o nome do host e endereços. O ícone de cadeado na frente do endereço do servidor de web indica a comunicação criptografa com os clientes e serviços que recuperam fluxos de dados desse servidor de gravação.



Nome	Descrição
Nome	É possível escolher inserir um nome para o servidor de gravação. O nome é usado no sistema e nos clientes quando o servidor de gravação estiver listado. O nome não tem que ser único. Quando você renomeia um servidor de gravação, o nome é alterado globalmente no Management Client.
Descrição	É possível escolher inserir uma descrição que aparece em uma série de listas dentro do sistema. Uma descrição não é obrigatória.
Nome do	Mostra o nome do host do servidor de gravação.

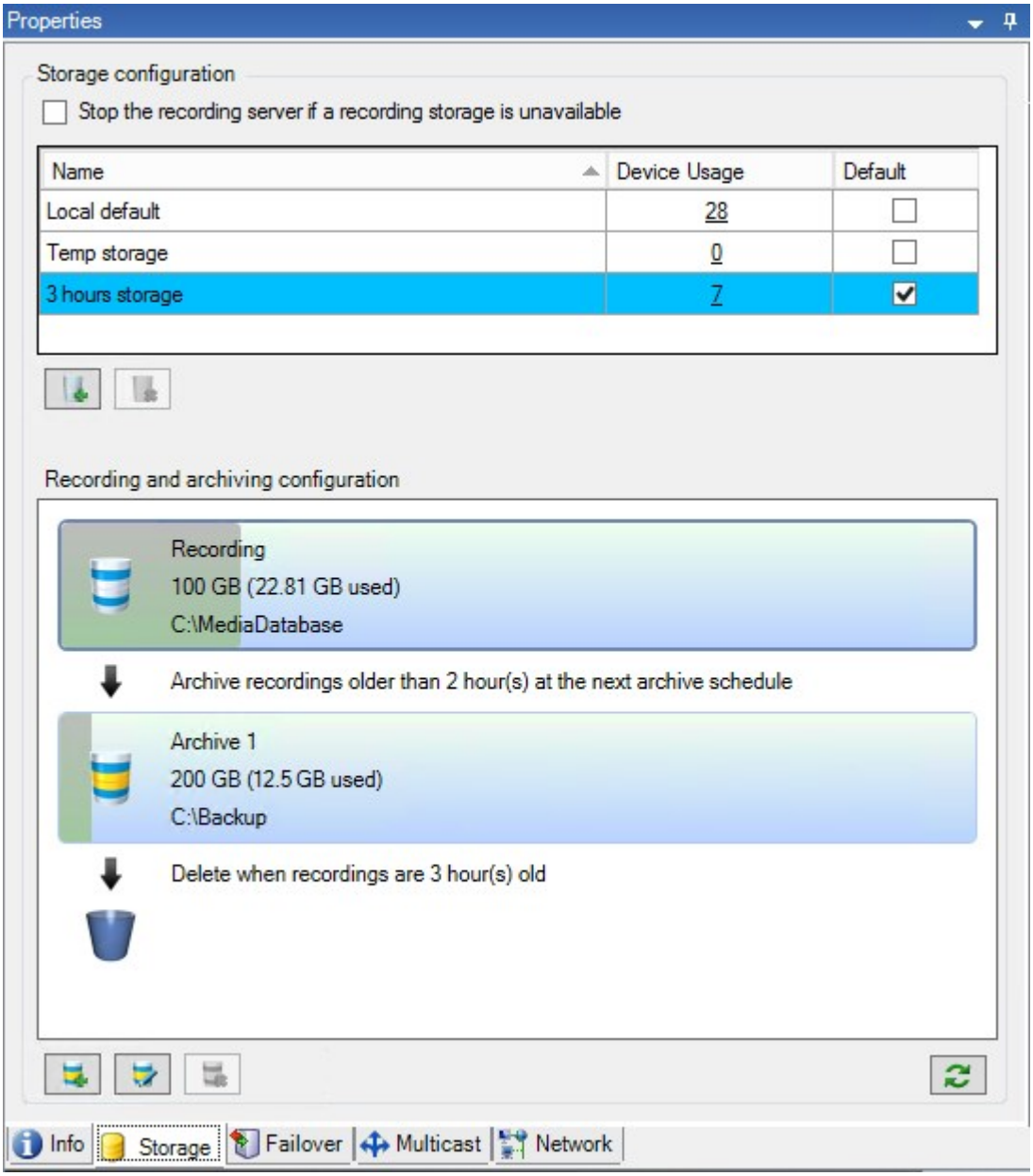
Nome	Descrição
host	
Endereço do servidor de web local	Exibe o endereço local do servidor de web do servidor de gravação. Use o endereço local, por exemplo, para lidar com os comandos de controle da câmera PTZ e para lidar com solicitações de navegação e exibição ao vivo do XProtect Smart Client. O endereço inclui o número da porta que é usado para comunicação do servidor de web (geralmente porta 7563). Se você ativar a criptografia para clientes e servidores que recuperam fluxos de dados do servidor de gravação, um ícone de cadeado aparecerá, e o endereço incluirá **https** em vez de **http**.
Endereço do servidor de web	Exibe o endereço público do servidor de web do servidor de gravação na Internet. Se sua instalação usar um firewall ou roteador NAT, insira o endereço do firewall ou roteador NAT para que os clientes que acessam o sistema de monitoramento na internet possam se conectar ao servidor do sistema de gravação. Especifique o endereço público e o número da porta na guia **Rede**. Se você ativar a criptografia para clientes e servidores que recuperam fluxos de dados do servidor de gravação, um ícone de cadeado aparecerá, e o endereço incluirá **https** em vez de **http**.
Fuso horário	Exibe o fuso horário em que o servidor de gravação está localizado.

Guia Armazenamento (servidor de gravação)

Na guia **Armazenamento**, você pode configurar, gerenciar e visualizar armazenamentos para os servidores de gravação selecionados.

Para armazenamento e arquivos de gravação, a barra horizontal mostra a quantidade atual de espaço livre. Você pode especificar o comportamento do servidor de gravação no caso de armazenamento de gravações ficar disponível. Isso é principalmente relevante se seu sistema inclui servidores de emergência.

Se estiver usando a **Proteção de evidências**, haverá uma linha vermelha vertical mostrando o espaço usado para filmagens de proteção de evidências.



Propriedades das definições de armazenamento e gravação

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Na caixa de diálogo **Definições de Armazenamento e Gravação**, especifique o seguinte:

Nome	Descrição
Nome	Mude o nome do armazenamento, se necessário. Os nomes devem ser únicos.
Caminho	Especifique o caminho para o diretório no qual você salva as gravações neste armazenamento. O armazenamento não precisa estar necessariamente localizado no computador do servidor de gravação. Se o diretório não existir, você pode criá-lo. As unidades de rede devem estar especificadas usando o formato UNC (Convenção de nomeação universal), exemplo: `\\server\volume\directory\`.
Tempo de retenção	Especifique por quanto tempo as gravações longas devem ficar no arquivo antes de serem excluídas ou movidas para o próximo arquivo (dependendo das configurações de arquivo). O período de retenção deve sempre ser maior do que o período de retenção do arquivo anterior ou banco de dados de gravação padrão. Isso é porque o número de dias de retenção especificados por um arquivo inclui todos os períodos de retenção em mencionados anteriormente no processo.
Tamanho máximo	Selecione o número máximo de gigabytes dos dados de gravação a ser salvo no banco de dados de gravação. Dados de gravação que excedam o um número especificado de gigabytes são movidos automaticamente ao primeiro arquivo da lista – se algum for especificado – ou apagados. ⚠ Quando há menos de 5 GB de espaço livre, o sistema sempre autoarquiva (ou exclui se não foi definido o arquivo próximo) os dados mais antigos em um banco de dados. Se houver menos de 1GB de espaço livre, os dados são excluídos. Um banco de dados sempre requer 250MB de espaço livre. Se você atinge este limite (se os dados não forem apagados rápido o suficiente), nenhum dado a mais é escrito no banco de dados até que se tenha liberado espaço suficiente. O tamanho máximo real de seu banco de dados é a quantidade de gigabytes especificada, menos 5GB.
Assinando	Permite uma assinatura digital nas gravações. Isso significa, por exemplo, que o sistema confirma que o vídeo exportado não sofreu modificações ou adulterações quando reproduzido.

Nome	Descrição
	O sistema usa o algoritmo SHA-2 para assinatura digital.
Criptografia	Selecione o nível de criptografia das gravações: • Nenhum • Leve (menos uso da CPU) • Forte (mais uso da CPU) O sistema usa o algoritmo AES-256 para criptografia. Se você selecionar **Leve**, uma parte da gravação será criptografada. Se você selecionar **Forte**, a gravação inteira será criptografada. Se escolher habilitar a criptografia, deve especificar também uma senha abaixo.
Senha	Insira uma senha para os usuários cuja visualização dos dados criptografados é permitida. Milestone recomenda que você use senhas fortes. Senhas fortes não contêm palavras que podem ser encontradas em um dicionário nem são parte do nome do usuário. Elas incluem oito ou mais caracteres alfa-numéricos, letras maiúsculas e minúsculas e caracteres especiais.

Propriedades de configurações de arquivamento

Na caixa de diálogo **Configurações de Arquivo**, especifique o seguinte:

Nome	Descrição
Nome	Mude o nome do armazenamento, se necessário. Os nomes devem ser únicos.
Caminho	Especifique o caminho para o diretório no qual você salva as gravações neste armazenamento. O armazenamento não precisa estar necessariamente localizado no computador do servidor de gravação. Se o diretório não existir, você pode criá-lo. As unidades de rede devem estar especificadas usando o formato UNC (Convenção de nomeação universal), exemplo:

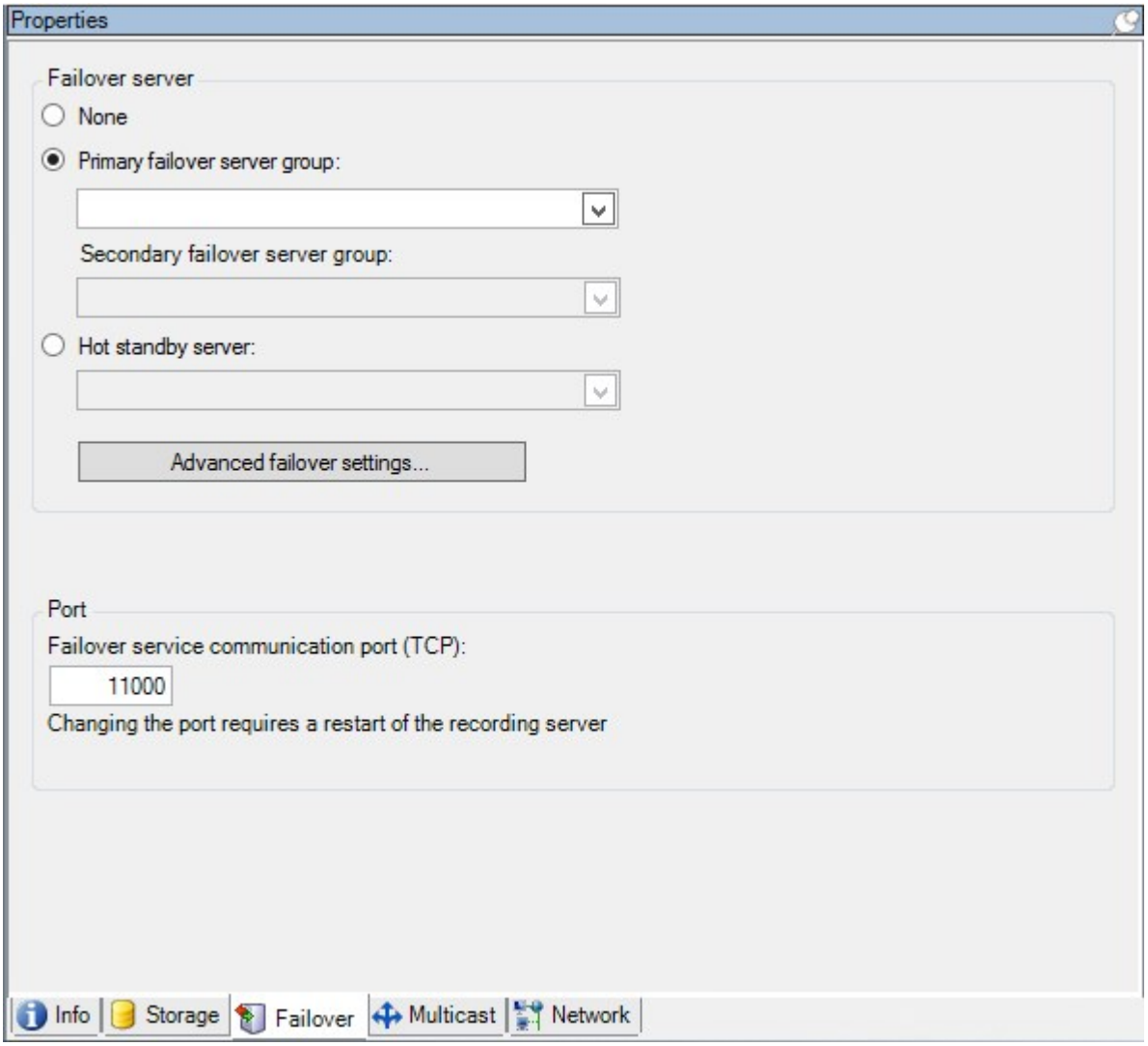
Nome	Descrição
	`\\server\volume\directory\`.
Tempo de retenção	Especifique por quanto tempo as gravações longas devem ficar no arquivo antes de serem excluídas ou movidas para o próximo arquivo (dependendo das configurações de arquivo). O período de retenção deve sempre ser maior do que o período de retenção do arquivo anterior ou banco de dados de gravação padrão. Isso é porque o número de dias de retenção especificados por um arquivo inclui todos os períodos de retenção em mencionados anteriormente no processo.
Tamanho máximo	Selecione o número máximo de gigabytes dos dados de gravação a ser salvo no banco de dados de gravação. Dados de gravação que excedam o um número especificado de gigabytes são movidos automaticamente ao primeiro arquivo da lista – se algum for especificado – ou apagados. ⚠ Quando há menos de 5 GB de espaço livre, o sistema sempre autoarquiva (ou exclui se não foi definido o arquivo próximo) os dados mais antigos em um banco de dados. Se houver menos de 1GB de espaço livre, os dados são excluídos. Um banco de dados sempre requer 250MB de espaço livre. Se você atinge este limite (se os dados não forem apagados rápido o suficiente), nenhum dado a mais é escrito no banco de dados até que se tenha liberado espaço suficiente. O tamanho máximo real de seu banco de dados é a quantidade de gigabytes especificada, menos 5GB.
Programação	Especifique uma programação de arquivamento que descreva os intervalos com os quais o processo de arquivamento deve começar. Você pode arquivar muito frequentemente (em princípio, a cada hora durante todo o ano) ou muito raramente (por exemplo, cada primeira segunda-feira a cada 36 meses).
Reduzir taxa de quadros	Para reduzir FPS ao arquivar, marque caixa de seleção **Reduzir taxa de quadros** e configure um quadro por segundo (FPS). A redução das taxas de quadros por um determinado número de FPS faz suas gravações ocuparem menos espaço no arquivo, mas também reduz a qualidade do

Nome	Descrição
	seu arquivo. MPEG-4/H.264/H.265 reduz automaticamente para quadros-chave como um mínimo de. 0.1 = 1 quadro por 10 segundos.

Aba Failover (servidor de gravação)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Se a sua organização usa servidores de gravação de failover, use a aba **Failover** para atribuir servidores de failover aos servidores de gravação, consulte Propriedades da aba Failover.



Para obter detalhes sobre servidores do sistema de gravação ininterrupta, instalação e configurações, grupos de failover e suas configurações, consulte Servidor do sistema de gravação ininterrupta (explicado) na página 39.

Propriedades da aba Failover

Nome	Descrição
Nenhum	Selecione uma configuração sem servidores de gravação de failover.
Grupo do servidor de	Selecione uma configuração de failover regular com um primário e

Nome	Descrição
emergência primário/Grupo do servidor de emergência secundário	possivelmente um grupo do servidor de failover secundário.
Servidor em hot standby	Selecione uma configuração de espera ativa com um servidor de gravação dedicado como servidor em espera ativa.
Configurações avançadas de failover	Abre a janela **Configurações avançadas de failover**: • **Suporte Completo**: Ativa o suporte de failover completo para o dispositivo • **Apenas Ao vivo**: Ativa apenas o suporte de failover para transmissões ao vivo no dispositivo • **Desativado**: Desativa o suporte de failover para o dispositivo
Porta de comunicação do serviço de failover (TCP)	Por padrão, o número de porta é 11000. Você usa esta porta para comunicação entre servidores de gravação e servidores de gravação de failover. Se você alterar a porta, o servidor de gravação **deve** estar em execução e **deve** estar conectado ao servidor de gerenciamento.

Guia Multicast (servidor de gravação)

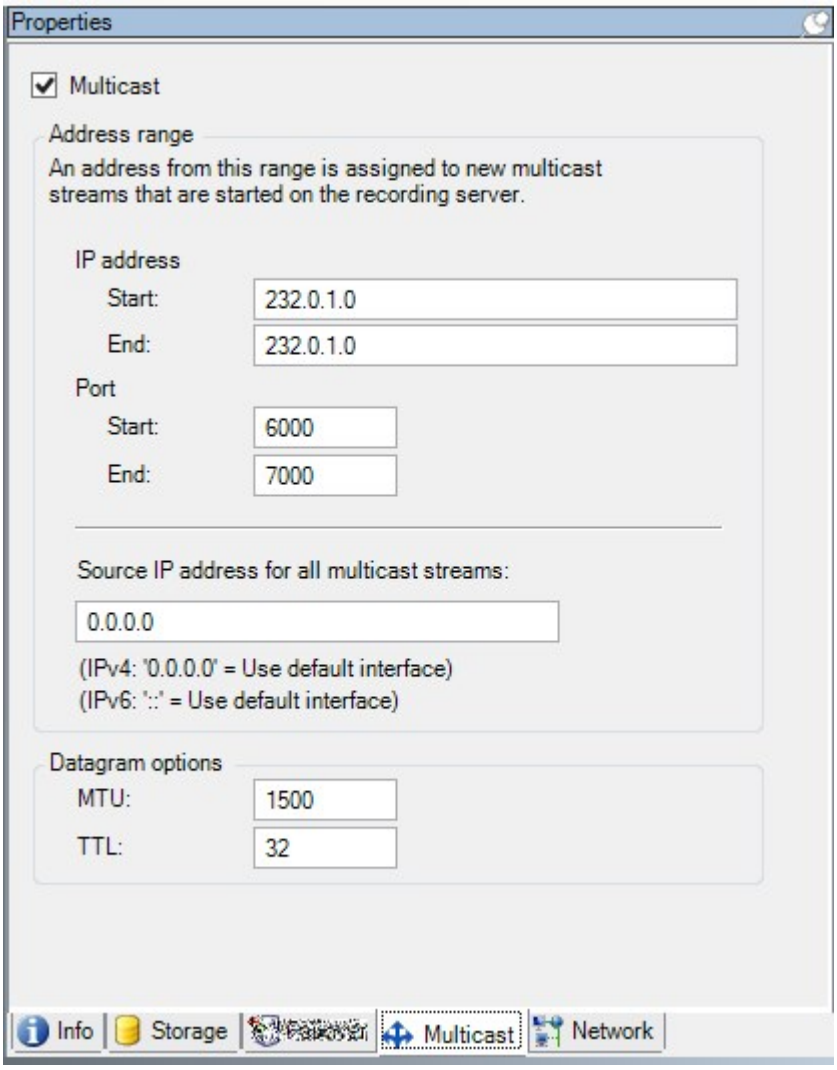
Seu sistema suporta multicasting de transmissões ao vivo de servidores de gravação. Se muitos usuários do XProtect Smart Client quiserem ver o vídeo ao vivo da mesma câmera, o multicasting ajuda a poupar recursos consideráveis do sistema. A multicasting é especialmente útil se você usar a funcionalidade do Matrix, onde múltiplos clientes necessitam de vídeo ao vivo da mesma câmera.

Multicasting somente é possível para fluxos ao vivo, não para vídeo/áudio gravados.

Se um servidor de gravação tem mais que uma placa de interface de rede, somente é possível usar multicasting em uma delas. Através do Management Client, você pode especificar qual delas usar.

Se você estiver usando servidores de failover, lembre-se de também especificar o endereço IP da placa de interface de rede nos servidores de failover (consulte Guia Multicast (servidor de emergência) na página 441).

A implantação de multicasting bem sucedida também requer que você configure seu equipamento de rede para retransmitir pacotes de dados para somente o grupo de destinatários solicitados. Senão, o multicasting pode não ser diferente de emissão, que pode significativamente desacelerar a comunicação de rede.



Atribuir intervalo de endereços IP

Especifique o intervalo que você quer atribuir como endereços para transmissões de multicast do servidor de gravação selecionado. Os clientes se conectam a esses endereços quando os usuários visualizam o vídeo multicast a partir do servidor de gravação.

Para cada alimentação de câmera de multicast, a combinação endereço e porta IP deve ser única (IPv4 exemplo: 232.0.1.0:6000). Você pode usar um endereço IP e muitas portas, ou muitos endereços IP e menos portas. Por padrão, o sistema sugere um único endereço IP e uma variedade de 1.000 portas, mas você pode mudar isso, conforme necessário.

Endereços IP para multicasting devem estar dentro do intervalo definido para a alocação de host dinâmico pela IANA. IANA é a autoridade que supervisiona a atribuição de endereços IP globais.

Nome	Descrição
Endereço IP	No campo **Iniciar**, especifique o primeiro endereço IP no intervalo desejado. Então especifique o último endereço IP do intervalo no campo **Fim**.
Porta	No campo **Iniciar**, especifique o primeiro número da porta no intervalo desejado. Em seguida, especifique o último número da porta do intervalo no campo **Fim**.
Endereço IP de fonte para todas as transmissões de multicast	Você só pode fazer transmissão multicast em um cartão de interface de rede, portanto este campo é relevante se seu servidor de gravação tem mais que um cartão de interface de rede ou se tem um cartão de interface de rede com mais de um endereço IP. Para usar a interface padrão do servidor de gravação, deixe o valor 0.0.0.0 (IPv4) ou: (IPv6) no campo. Se você quer usar outro cartão de interface de rede ou endereço de IP diferente no mesmo cartão de interface de rede, especifique o endereço IP da interface solicitada. • IPv4: 224.0.0.0 a 239.255.255.255. • IPv6, o intervalo é descrito no site da IANA (https://www.iana.org/).

Especificar opções de conjunto de dados

Especifique as configurações para pacotes de dados (datagramas) transmitidos através da multicast.

Nome	Descrição
MTU	Unidade de transmissão máxima, a maior tamanho do pacote de dados físico permitido (medidos em bytes). Mensagens maiores que o MTU especificado são divididas em pacotes menores antes de serem enviadas. O valor padrão é 1500, que também é o padrão na maioria dos computadores com Windows e redes Ethernet.
TTL	Time To Live (tempo para ao vivo), o maior número permitido de saltos que um pacote de dados deve ser capaz de se deslocar antes de ser descartado ou devolvido. Um salto é um ponto entre dois dispositivos de rede, tipicamente um roteador. O valor padrão é 128.

Guia Rede (servidor de gravação)

Se você precisar acessar o VMS com XProtect Smart Client por meio de uma rede pública ou não confiável, a Milestone recomenda que você use uma conexão segura por meio de VPN. Isso ajuda a garantir que a comunicação entre o XProtect Smart Client e o servidor VMS seja protegida.

Você define um endereço de servidor IP público do servidor de gravação na aba **rede de trabalho**.

Por que usar um endereço público?

Cliente podem conectar a partir de uma rede local bem como pela Internet e, em ambos os casos, o sistema de monitoramento deve fornecer endereços adequados para que os clientes possam acessar vídeos gravados ou em tempo real de seus servidores de gravação:

- Quando clientes conectam localmente, o sistema de monitoramento deve responder com endereços locais e número de portas
- Quando clientes se conectam pela internet, o sistema de monitoramento deve responder com o endereço público do servidor de gravação. Este é o endereço do firewall ou roteador NAT (Network Address Translation), e frequentemente também um número de porta diferente. O endereço e a porta podem então ser encaminhados para o endereço local e a porta do servidor.

Servidores de failover (nó Servidores)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Um servidor do sistema de gravação ininterrupta (failover) é um servidor de gravação extra que retoma a partir do servidor de gravação padrão se este se torna indisponível. Você pode configurar um servidor do sistema de gravação ininterrupta (failover) em dois modos, como um **servidor em cold standby** ou como um **servidor em hot standby**.

Você instala servidores do sistema de gravação ininterrupta (consulte Instale um servidor do sistema de gravação ininterrupta através do Download Manager na página 175). Depois de ter instalado os servidores de gravação ininterrupta (failover), eles são visíveis no Management Client. Milestone recomenda que você instale todos os servidores do sistema de gravação ininterrupta (failover) em computadores separados. Não deixe de configurar servidores do sistema de gravação ininterrupta com o endereço IP/nome do host do servidor de gerenciamento. As permissões de usuário para a conta de usuário sob a qual o serviço Failover Server é executado são fornecidas durante o processo de instalação. São eles:

- Permissões Iniciar/Parar para iniciar ou parar o servidor do sistema de gravação ininterrupta
- Permissões de acesso a gravação e leitura para ler ou gravar o arquivo RecorderConfig.xml

Se um certificado estiver selecionado para criptografia, o administrador deve conceder permissão de acesso ao usuário de failover na chave privada do certificado selecionado.

Se o servidor do sistema de gravação ininterrupta assumir a partir de um servidor de gravação que usa criptografia, o Milestone recomenda que você também prepare o servidor do sistema de gravação ininterrupta para o uso de criptografia. Para obter mais informações, consulte Comunicação segura (explicado) na página 151 e Instale um servidor do sistema de gravação ininterrupta através do Download Manager na página 175.

Você pode especificar que tipo de suporte de failover você quer no nível de dispositivo. Para cada dispositivo em um servidor de gravação, selecione completo, apenas ao vivo ou nenhum suporte de failover. Isso ajuda você a priorizar seus recursos de failover e, por exemplo, apenas configurar failover para vídeo e não para áudio, ou só ter failover em câmeras essenciais, e não em câmeras menos importantes.

Enquanto seu sistema estiver no modo de recuperação de falhas, não é possível substituir ou mover o hardware, atualizar o servidor de gravação ou alterar configurações do dispositivo, como configurações de armazenamento ou configurações de fluxo de vídeo.

Servidores de gravação de failover em cold standby

Em uma configuração do servidor do sistema de gravação ininterrupta (failover) em cold standby, você agrupa diversos servidores de gravação de failover em um grupo de failover. Todo o grupo de emergência é dedicado para assumir a partir de qualquer um dos diversos servidores de gravação pré-selecionados, se um destes se tornar indisponível. Você pode criar quantos grupos deseja (consulte Servidores de gravação de failover do grupo para cold standby na página 218).

Agrupamento tem um benefício claro: quando você posteriormente especifica quais os servidores do sistema de gravação ininterrupta (failover) devem assumir o controle de um servidor de gravação, você seleciona um grupo de servidores do sistema de gravação ininterrupta (ailover). Se o grupo selecionado contiver mais de um servidor do sistema de gravação ininterrupta (failover), isto lhe dará a segurança de ter mais do que um servidor do sistema de gravação ininterrupta (failover) pronto para assumir o controle caso um servidor de gravação fique indisponível. Você pode especificar um grupo de servidor de failover secundário que assume a partir do grupo primário se todos os servidores de gravação no grupo primário estiverem ocupados. Um servidor do sistema de gravação ininterrupta (failover) só pode ser membro de um grupo de cada vez.

Os servidores de gravação de failover em um grupo de failover são ordenados em uma sequência. A sequência determina a ordem em que os servidores de gravação de failover assumirão a partir de um servidor de gravação. Por padrão, a sequência reflete a ordem na qual você tem incorporado os servidores de gravação de failover no grupo de failover: o primeiro a entrar é o primeiro na sequência. Você pode mudar isso, caso precise.

Servidores de gravação de failover de espera ativa

Em uma configuração do servidor do sistema de gravação ininterrupta (failover) em hot standby, você dedica um servidor do sistema de gravação ininterrupta (failover) para assumir a partir de apenas **um** servidor de gravação. Por isso, o sistema pode manter este servidor do sistema de gravação ininterrupta (failover) em um modo de "espera", o que significa que ele é sincronizado com a configuração correta/atual que o servidor de gravação é dedicado e pode assumir muito mais rápido do que um servidor do sistema de gravação ininterrupta (failover) em cold standby. Conforme mencionado, você atribui servidores em espera ativa para apenas um servidor de gravação e não pode agrupá-lo. Você não pode atribuir os servidores de failover que já fazem parte de um grupo de failover como servidores de gravação em hot standby.

Validação do servidor do sistema de gravação ininterrupta

Para validar uma fusão de dados de vídeo do servidor de emergência para o servidor de gravação, você deve tornar o servidor de gravação indisponível, parando o serviço do servidor de gravação ou desligando o computador do servidor de gravação.

Qualquer interrupção manual da rede que você possa causar removendo o cabo de rede ou bloqueando a rede usando uma ferramenta de teste não é um método válido.

Propriedades da guia Informações (servidor de emergência)

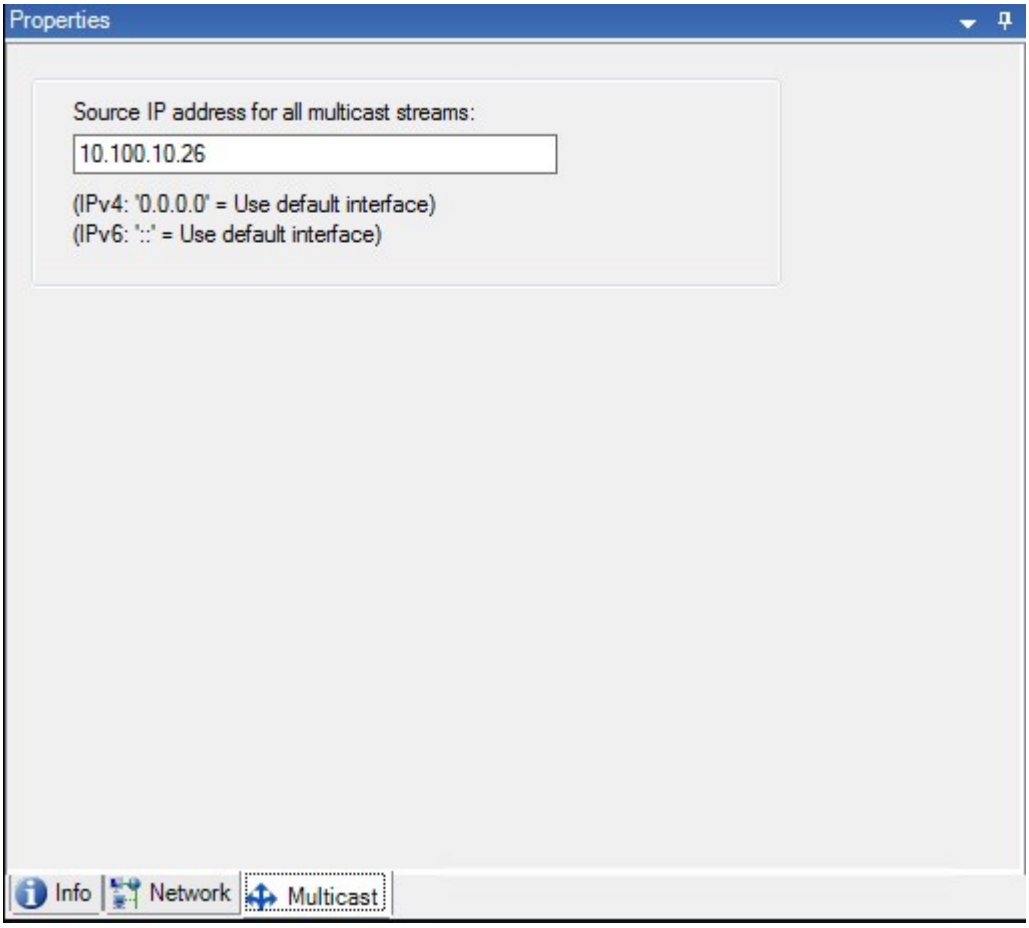
Especifique as seguintes propriedades do servidor de gravação de failover:

Nome	Descrição
Nome	O nome do servidor de gravação de failover conforme aparece no Management Client, registros e muito mais.
Descrição	Um campo opcional que você pode usar para descrever o servidor de gravação de failover, por exemplo, de qual servidor de gravação ele assume o controle.
Nome do host	Mostra o nome do host do servidor do sistema de gravação ininterrupta. Você não pode mudar isso.
Endereço do servidor de web local	Exibe o endereço local do servidor de web do servidor do sistema de gravação ininterrupta. Use o endereço local, por exemplo, para lidar com os comandos de controle da câmera PTZ e para lidar com solicitações de navegação e exibição ao vivo do XProtect Smart Client. O endereço inclui o número da porta que é usado para comunicação do servidor de web (geralmente porta 7563). Se o servidor do sistema de gravação ininterrupta assume um servidor de gravação que usa criptografia, você também precisa preparar o servidor do sistema de gravação ininterrupta para usar criptografia. Se você ativar a criptografia para clientes e servidores que recuperam fluxos de dados do servidor de gravação, um ícone de cadeado aparecerá, e o endereço incluirá **https** em vez de **http**.
Endereço do servidor de web	Exibe o endereço público do servidor de web do servidor do sistema de gravação ininterrupta na internet. Se sua instalação usar um firewall ou roteador NAT, insira o endereço do firewall ou roteador NAT para que os clientes que acessam o sistema de monitoramento na internet possam se conectar ao servidor do sistema de gravação ininterrupta. Especifique o endereço público e o número da porta na guia **Rede**. Se você ativar a criptografia para clientes e servidores que recuperam fluxos de dados do servidor de gravação, um ícone de cadeado aparecerá, e o endereço incluirá **https** em vez de **http**.
Porta UDP	O número da porta usado para a comunicação entre servidores de gravação de failover. A porta padrão é 8844.

Nome	Descrição
Local do banco de dados	Especifique o caminho para o banco de dados usado pelo servidor de gravação de failover para armazenar as gravações. Você não pode mudar o caminho do banco de dados enquanto o servidor de gravação de failover estiver assumindo um servidor de gravação. O sistema aplica as alterações quando o servidor de gravação de failover não estiver mais assumindo um servidor de gravação.
Ativar este servidor de recuperação de falha	Desmarque para desativar o servidor de gravação de failover (selecionado por padrão). Desative os servidores do sistema de gravação ininterrupta antes que eles possam assumir o lugar dos servidores de gravação.

Guia Multicast (servidor de emergência)

Se você estiver usando servidores de emergência e tiver habilitado multicast de streaming ao vivo, será necessário especificar o endereço IP da placa de interface de rede que você estiver usando, tanto nos servidores de gravação quanto nos servidores de emergência.



Para obter mais informações sobre multicast, consulte Ativar multicasting para o servidor de gravação na página 213.

Propriedades da guia Informações (grupo de emergência)

Campo	Descrição
Nome	O nome do grupo de failover conforme aparece no Management Client, nos registros e outros lugares.
Descrição	Uma descrição opcional, por exemplo, o local físico do servidor.

Propriedades da guia Sequência (grupo de emergência)

Campo	Descrição
Especificar a sequência de recuperação de falha	Clique em **Para cima** e **Para baixo** para definir a sequência desejada dos servidores de gravação de failover regulares no grupo.

Servidor remoto para Milestone Interconnect

Milestone Interconnect™ permite que você integre várias instalações menores, fragmentadas fisicamente e remotas do XProtect com uma central de controle XProtect Corporate. Você pode instalar esses sites menores, chamados de bases remotas, em unidades móveis, por exemplo, barcos, ônibus ou trens. Isto significa que esses sites não precisam estar permanentemente conectados a uma rede.

Guia informações (servidor remoto)

Nome	Descrição
Nome	O sistema usa o nome sempre que o servidor remoto estiver listado no sistema e clientes. O nome não tem que ser único. Quando você renomeia um servidor, o nome é alterado globalmente no Management Client.
Descrição	Digite uma descrição do sistema remoto (opcional). A descrição aparece em uma série de listas dentro do sistema. Por exemplo, ao pausar o ponteiro do mouse sobre o nome do hardware no painel **Visão Geral**.
Modelo	Mostra o produto XProtect instalado na base remota.
Versão	Mostra a versão do sistema remoto.
Código da licença de software	O código de licença de software do sistema remoto.

Nome	Descrição
Driver	Identifica o driver que trata da conexão ao servidor remoto.
Endereço	O endereço IP ou nome do host do hardware.
IE	Abre a página inicial padrão do fornecedor de hardware. Você pode usar esta página para a administração do hardware ou do sistema.
ID do sistema remoto	A ID do sistema único do site remoto usada por XProtect para, por exemplo, gerenciar licenças.

Guia Configurações (servidor remoto)

Na guia **Configurações**, é possível ver o nome do sistema remoto.

Guia Eventos (servidor remoto)

Você pode adicionar eventos do sistema remoto ao site central, a fim de criar regras e, assim, responder imediatamente a eventos do sistema remoto. O número de eventos depende dos eventos configurados no sistema remoto. Você não pode excluir eventos padrão.

Se a lista parece estar incompleta:

1. Clique com o botão direito do mouse no servidor remoto relevante no painel **Visão geral** e selecione **Atualizar hardware**.
2. A caixa de diálogo lista todas as alterações (dispositivos removidos, atualizados e adicionados) no sistema remoto desde que você estabeleceu ou atualizou por último a configuração Milestone Interconnect. Clique em **Confirmar** para atualizar sua central de controle com essas alterações.

Guia Recuperação remota

Na guia **Recuperação remota**, você pode lidar com as configurações de recuperação de gravação remota para a base remota em uma configuração do Milestone Interconnect:

Especifique as seguintes propriedades:

Nome	Descrição
Recuperar	Determina a largura de banda máxima em Kbits/s para ser usada para recuperar

Nome	Descrição
gravações no máximo	gravações de um site remoto. Selecione a caixa de seleção para ativar as limitações de recuperações.
Recuperar gravações entre	Determina que a recuperação de gravações de um site remoto é limitada a um intervalo de tempo específico. Trabalhos inacabados na hora de fim continua até a conclusão, por isso, se a hora de fim é fundamental, você precisa configurá-lo mais cedo para permitir que os trabalhos inacabados sejam concluídos. Se o sistema recebe uma recuperação automática ou uma solicitação para recuperação a partir do XProtect Smart Client fora do intervalo de tempo, ele é aceito, mas não iniciado até que o intervalo de tempo selecionado seja atingido. Você pode ver os trabalhos pendentes de recuperação de gravação remota iniciados pelos usuários do **Painel do sistema** -> **Tarefas atuais**.
Recuperar em dispositivos em paralelo	Determina o número máximo de dispositivos de onde as gravações são recuperadas simultaneamente. Altere o valor padrão se você precisar de maior ou menor capacidade dependendo das capacidades do seu sistema.

Quando você altera as configurações, pode demorar alguns minutos até que as alterações sejam refletidas no sistema.

> Nenhuma das opções acima se aplica a reprodução direta de gravações remotas. Todas as câmeras definidas para serem reproduzidas diretamente estão disponíveis para reprodução direta e uso da largura de banda, conforme necessário.

Nó de dispositivos

Dispositivos (nó Dispositivos)

Os dispositivos aparecem no Management Client quando você adiciona hardware com o assistente **Adicionar hardware**. Consulte Adicionar hardware na página 221.

Você pode gerenciar os dispositivos através dos grupos de dispositivos se eles tiverem as mesmas propriedades, consulte Grupos de dispositivos (explicado) na página 58.

Você também pode gerenciar os dispositivos individualmente.

A ativação/desativação, bem como mudança de nome de dispositivos individuais ocorre no hardware do servidor de gravação. Consulte Ativar/desativar dispositivos através de grupos de dispositivos.

Para todas as demais configurações e gerenciamento de câmeras, expanda **Devices** no painel de Navegação do site e então selecione um dispositivo:

- **Câmeras**
- **Microfones**
- **Alto-falantes**
- **Metadados**
- **Entradas**
- **Saídas**

No painel Visão geral, você pode agrupar suas câmeras para uma visão geral fácil de suas câmeras. O agrupamento inicial é feito como parte do **Assistente para adicionar hardware**.

> Para obter informações sobre o hardware suportado, consulte a página de suporte de hardware no site da Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Ícones de status de dispositivos

Quando você seleciona um dispositivo, informações sobre o estado atual são exibidas no painel **Visualização**. Os seguintes ícones indicam o status dos dispositivos:

Câmera	Microfone	Alto-falante	Metadados	Entrada	Saída	Descrição
						**Dispositivo ativado e recuperando dados**: O dispositivo é ativado e você recupera uma transmissão ao vivo.
						**Dispositivo em gravação**: O dispositivo está gravando dados no sistema.

Câmera	Microfone	Alto-falante	Metadados	Entrada	Saída	Descrição
						**Dispositivo interrompido temporariamente ou sem alimentação**: Quando interrompido, nenhuma informação é transferida para o sistema. Se for uma câmera, você não pode ver ao vivo. Um dispositivo parado pode ainda se comunicar com o servidor de gravação para a recuperação de eventos, configurações etc, ao contrário de quando um dispositivo está desativado.
						**Dispositivos desativados**: Não pode ser iniciado automaticamente através de uma regra e não pode se comunicar com o servidor de gravação. Se uma câmera estiver desativada, você não pode ver o vídeo ao vivo ou gravado.
						**Banco de dados do dispositivo que está sendo reparado**.
						**Dispositivo requer**

Câmera	Microfone	Alto-falante	Metadados	Entrada	Saída	Descrição
						atenção: O aparelho não funciona corretamente. Coloque o ponteiro do mouse sobre o ícone do dispositivo para obter uma descrição do problema na dica de ferramentas.
						**Status desconhecido**: O status do dispositivo é desconhecido, por exemplo, se o servidor de gravação está desligado.
						Alguns ícones podem ser combinados, como neste exemplo, onde o **Dispositivo ativado e recuperando dados** é combinado com **Dispositivo em gravação**.

Câmeras (nó Dispositivos)

Dispositivos de câmera são acrescentados automaticamente e são, por padrão, habilitados, quando você adiciona o hardware ao sistema.

O sistema vem com regra padrão de iniciar feed, garantindo que os feeds de vídeo de todas as câmeras conectadas são automaticamente enviados para o sistema. A regra padrão pode ser desativada e/ou modificada, se necessário.

Siga esta ordem de configuração para concluir as tarefas mais comuns relacionadas à configuração de um dispositivo de câmera:

1. Configure as propriedades da câmera, consulte a guia Configurações (dispositivos).
2. Configurar transmissões, consulte a guia Transmissões (dispositivos).
3. Configurar movimento, consulte a guia Movimento (dispositivos).
4. Configure a gravação, consulte a guia Gravar (dispositivos) e Monitorar os bancos de dados para dispositivos.
5. Faça as configurações restantes, conforme necessário.

Microfones (nó Dispositivos)

Dispositivos de microfone são acrescentados automaticamente quando você adiciona o hardware ao sistema. Eles são por padrão desativados. Assim, você deve ativá-los antes do uso, seja durante o assistente para **Adicionar Hardware** ou posteriormente. Microfones não requerem licenças separadas. Você pode usar tantos microfones quantos solicitados em seu sistema.

Você pode usar microfones de forma completamente independente das câmeras.

O sistema vem com uma regra padrão que garante que as alimentações de áudio de todos os microfones e alto-falantes conectados sejam alimentados automaticamente ao sistema. A regra padrão pode ser desativada e/ou modificada, se necessário.

Você pode configurar os dispositivos de microfone nessas guias:

- Guia Informações, consulte guia Informações (dispositivos)
- Guia Configurações, consulte guia Configurações (dispositivos)
- Guia Gravar, consulte guia Gravar (dispositivos)
- Guia Eventos, consulte guia Eventos (dispositivos)

Alto-falantes (nó Dispositivos)

Dispositivos de alto-falante são acrescentados automaticamente quando você adiciona o hardware ao sistema. Eles são por padrão desativados. Assim, você deve ativá-los antes do uso, seja durante o assistente para **Adicionar Hardware** ou posteriormente. Alto-falantes não requerem licenças separadas. Você pode usar tantos alto-falantes quantos solicitados em seu sistema.

Você pode usar alto-falantes de forma completamente independente das câmeras.

O sistema vem com uma regra padrão de alimentação de áudio que inicia o dispositivo, deixando-o pronto para enviar áudio ativado pelo usuário para os alto-falantes. A regra padrão pode ser desativada e/ou modificada, se necessário.

Você pode configurar os dispositivos de alto-falante nessas guias:

- Guia Informações, consulte guia Informações (dispositivos)
- Guia Configurações, consulte guia Configurações (dispositivos)
- Guia Gravar, consulte guia Gravar (dispositivos)

Metadados (nó Dispositivos)

O sistema vem com regra padrão de iniciar feed, garantindo que os feeds de metadados de todo o hardware conectado são automaticamente enviados para o sistema. A regra padrão pode ser desativada e/ou modificada, se necessário.

Você pode configurar os dispositivos de metadados nessas guias:

- Guia Informações, consulte guia Informações (dispositivos)
- Guia Configurações, consulte guia Configurações (dispositivos)
- Guia Gravar, consulte guia Gravar (dispositivos)

Entrada (nó Dispositivos)

Você pode usar dispositivos de entrada de forma completamente independente das câmeras.

Antes de especificar o uso de unidades de entrada e de saída externas em um dispositivo, verifique se a operação do sensor foi reconhecida pelo dispositivo. A maioria dos dispositivos pode mostrar isso em suas interfaces de configuração ou através de comandos de script da Interface de passagem comum (CGI).

Dispositivos de entrada são acrescentados automaticamente quando você adiciona o hardware ao sistema. Eles são por padrão desativados. Assim, você deve ativá-los antes do uso, seja durante o assistente para **Adicionar Hardware** ou posteriormente. Dispositivos de entrada não requerem licenças separadas. Você pode usar tantos dispositivos de entrada quantos solicitados em seu sistema.

Você pode configurar os dispositivos de metadados nessas guias:

- Guia Informações, consulte guia Informações (dispositivos)
- Guia Configurações, consulte guia Configurações (dispositivos)
- Guia Eventos, consulte guia Eventos (dispositivos)

Saída (nó Dispositivos)

A saída também pode ser acionada manualmente a partir do Management Client e XProtect Smart Client.

Antes de especificar o uso de unidades de saída externas em um dispositivo, verifique se o dispositivo pode controlar o dispositivo ligado à saída. A maioria dos dispositivos pode mostrar isso em suas interfaces de configuração ou através de comandos de script da Interface de passagem comum (CGI).

Dispositivos de saída são acrescentados automaticamente quando você adiciona o hardware ao sistema. Eles são por padrão desativados. Assim, você deve ativá-los antes do uso, seja durante o assistente para **Adicionar Hardware** ou posteriormente. Dispositivos de saída não requerem licenças separadas. Você pode usar tantos dispositivos de saída quantos solicitados em seu sistema.

Você pode configurar os dispositivos de saída nessas guias:

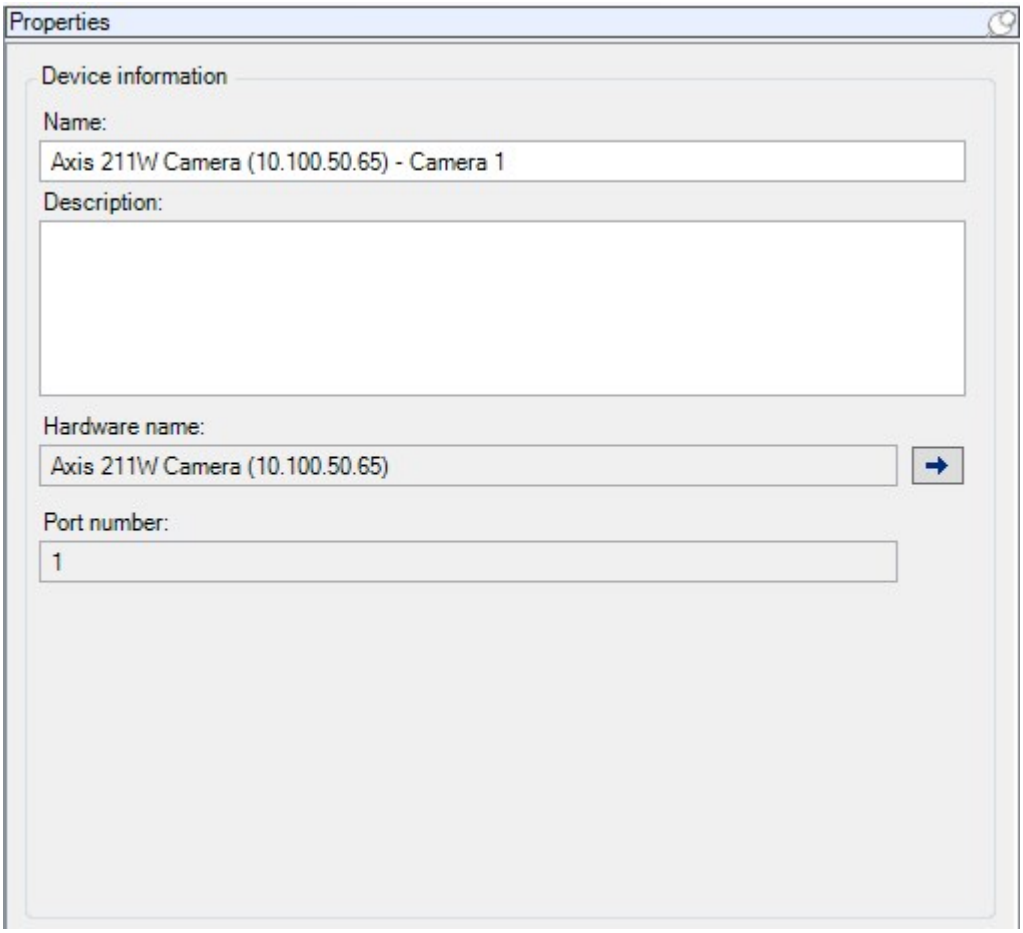
Guia Informações, consulte

- Guia Informações, consulte guia Informações (dispositivos)
- Guia Configurações, consulte guia Configurações (dispositivos)

Guias Dispositivos

Guia Informações (dispositivos)

Na guia **Informações**, você pode visualizar e editar as informações básicas sobre um dispositivo em diversos campos.
Todos os dispositivos têm uma guia **Informações**.



Propriedades da guia Informações

Nome	Descrição
Nome	O nome é usado sempre que o dispositivo estiver listado no sistema e nos clientes. Quando você renomeia um dispositivo, o nome é alterado globalmente no Management Client.
Descrição	Digite uma descrição do dispositivo (opcional). A descrição aparece em uma série de listas dentro do sistema. Por exemplo, quando você pausa o ponteiro do mouse sobre o nome no painel **Visão Geral**.
Nome do hardware	Exibe o nome do hardware, com o qual o dispositivo está conectado. O campo não é editável daqui, mas você pode alterá-lo clicando em **Ir para** ao lado dele. Isso o leva para informações de hardware, onde você pode mudar o nome.
Número da porta	Exibe a porta na qual o dispositivo está conectado no hardware. Para hardware de dispositivo único, o número da porta é geralmente **1**. Para hardware com diversos dispositivos, como servidores de vídeo com vários canais, o número da porta normalmente indica o canal no qual o dispositivo está conectado, por exemplo **3**.
Nome abreviado	Para aplicar um nome abreviado a uma câmera, digite aqui. O número máximo de caracteres é 128. Se estiver usando o mapa inteligente, o nome abreviado automaticamente será exibido com a câmera no mapa inteligente. Caso contrário, o nome complete será exibido.
Coordenadas geográficas	Digite a localização geográfica da câmera no formato **latitude, longitude**. O valor que você digita determina a posição do ícone da câmera no mapa inteligente no XProtect Smart Client e cliente XProtect Mobile. O campo serve principalmente para integrações de mapa inteligente e de terceiros.
Direção	Digite a direção visualizada na câmera medida em relação ao ponto norte devido em um eixo vertical. O valor que você digita determina a direção do ícone da câmera no mapa inteligente no XProtect Smart Client e cliente XProtect Mobile.

Nome	Descrição
	O valor padrão é 0.0.  O campo serve principalmente para integrações de mapa inteligente e de terceiros.
Campo de visão	Digite a amplitude do campo de visão em graus. O valor digitado determinará o ângulo do campo de visão para o ícone da câmera no mapa inteligente no XProtect Smart Client e cliente XProtect Mobile. O valor padrão é 0.0.  O campo serve principalmente para integrações de mapa inteligente e de terceiros.
Profundidade	Digite a profundidade do campo de visão da câmera em metros ou pés. O valor digitado determinará o comprimento do campo de visão para o ícone da câmera no mapa inteligente no XProtect Smart Client e cliente XProtect Mobile. O valor padrão é 0.0.  O campo serve principalmente para integrações de mapa inteligente e de terceiros.
Posição visualização no navegador	Para verificar se você inseriu as coordenadas geográficas corretas, clique no botão. O Google Maps abrirá no seu navegador de Internet padrão na posição que você especificar.  O campo serve principalmente para integrações de mapa inteligente e de terceiros.

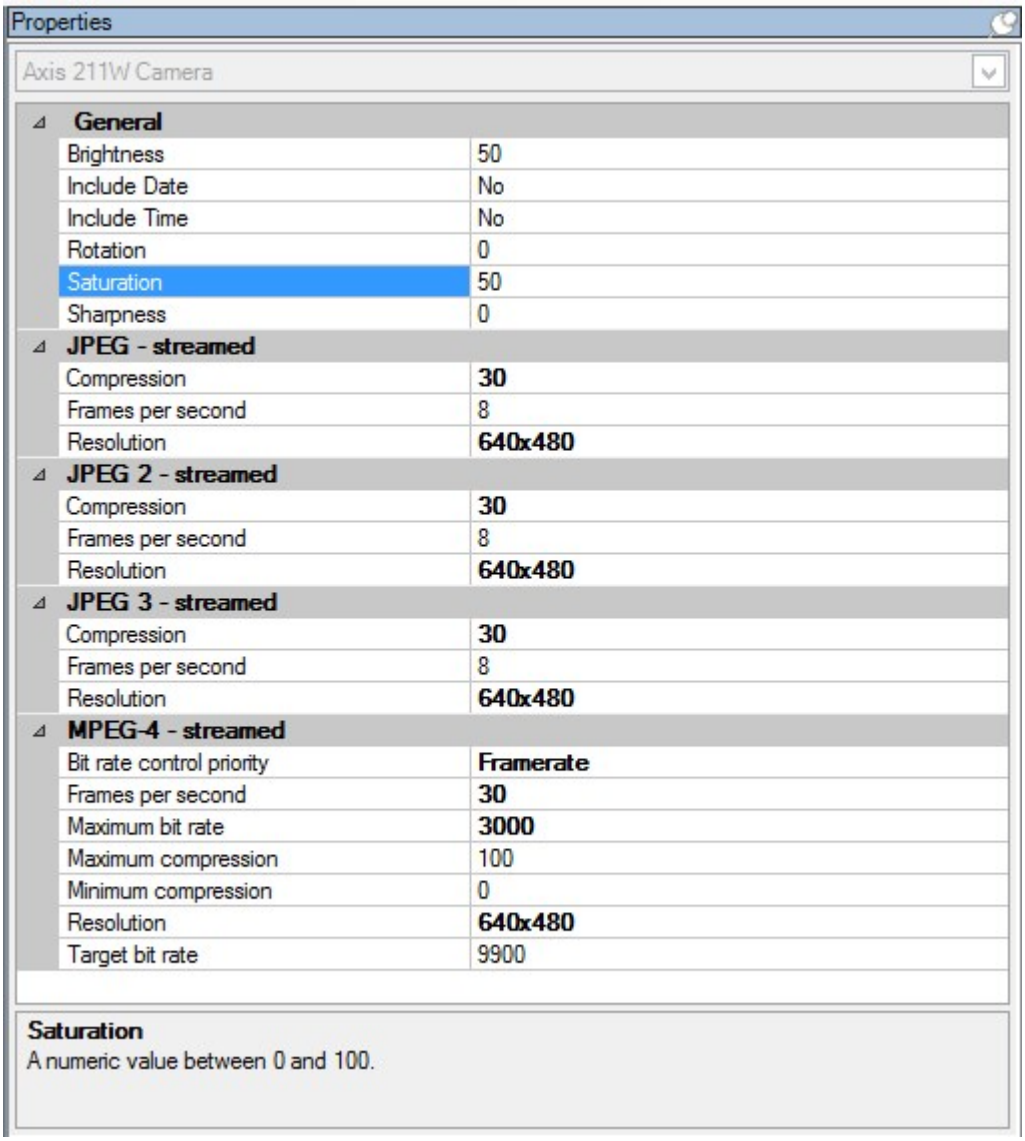
Guia Configurações (dispositivos)

Na guia **Configurações**, você pode visualizar e editar configurações de um dispositivo em diversos campos. Todos os dispositivos têm uma guia **Configurações**.

Os valores aparecem em uma tabela como sujeito à mudança ou somente leitura. Ao alterar uma configuração para um valor não-padrão, o valor é exibido em negrito.

O conteúdo da tabela depende do driver do dispositivo.

Intervalos permitidos aparecem na caixa de informações abaixo da tabela de configurações:



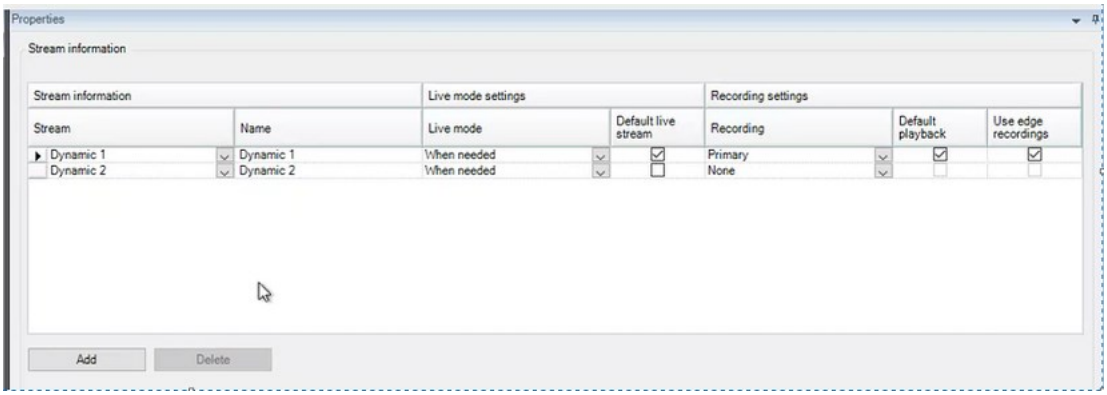
Para obter mais informações sobre as configurações da câmera, consulte Exibir ou editar as configurações da câmera.

Guia Fluxos (dispositivos)

Os seguintes dispositivos têm uma guia **Transmissões**:

- Câmeras

A guia **Transmissões** lista, por padrão, uma única transmissão. É a transmissão padrão da câmera selecionada, usada para vídeo ao vivo e gravado. Se você usar a reprodução adaptável, será preciso criar dois fluxos.



Tarefas na guia Transmissões

Nome	Descrição
Adicionar	Clique para adicionar uma transmissão à lista. Adicionar uma transmissão

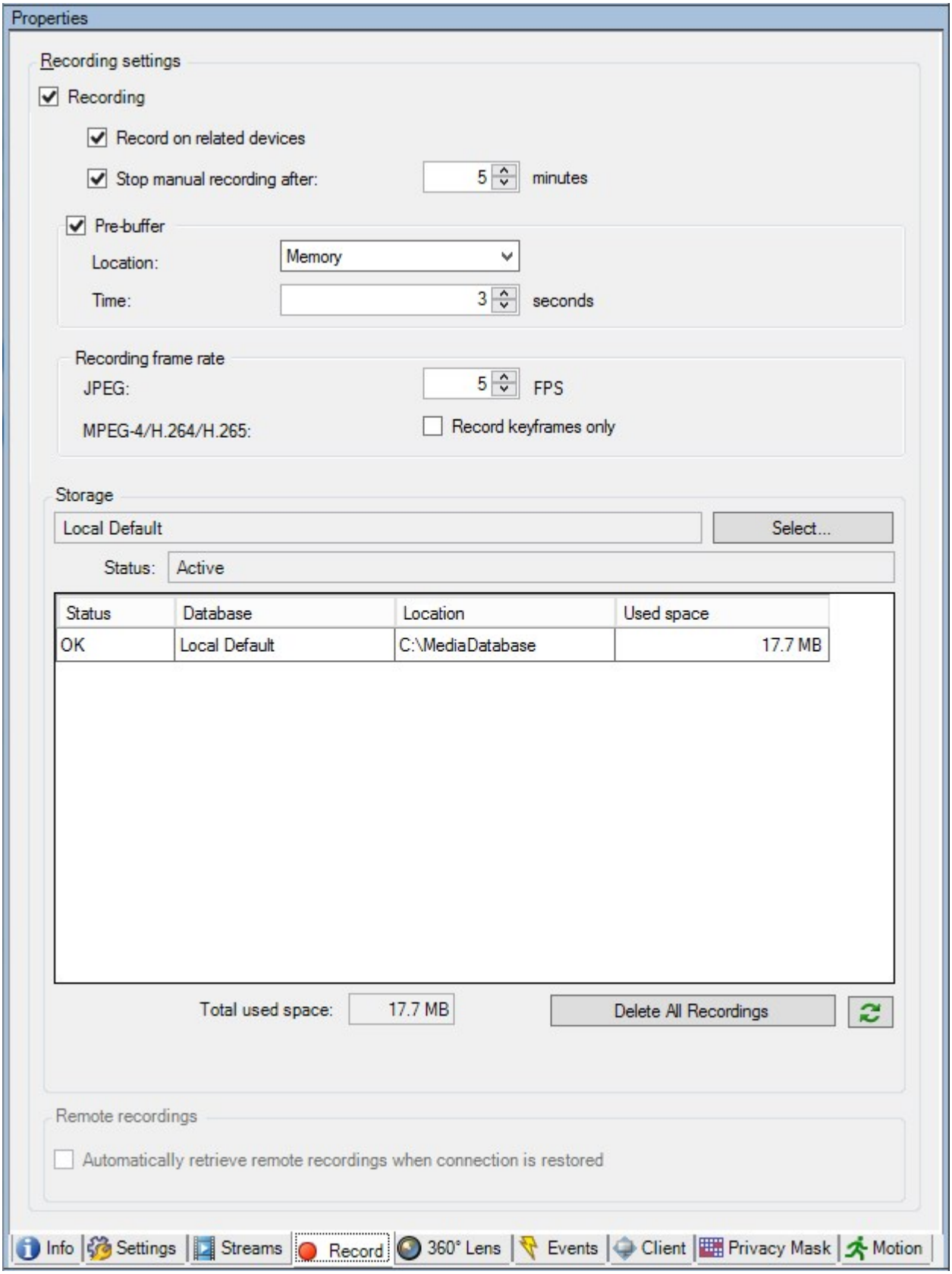
Guia Gravar (dispositivos)

Os seguintes dispositivos têm uma guia **Gravar**:

- Câmeras
- Microfones
- Alto-falantes
- Metadados

As gravações de um dispositivo só são salvas no banco de dados quando você tiver ativado a gravação e os critérios de regras relacionadas com gravação tiverem sido satisfeitos.

Os parâmetros que não podem ser configurados para um dispositivo são desativados.


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

Tarefas na guia Gravação

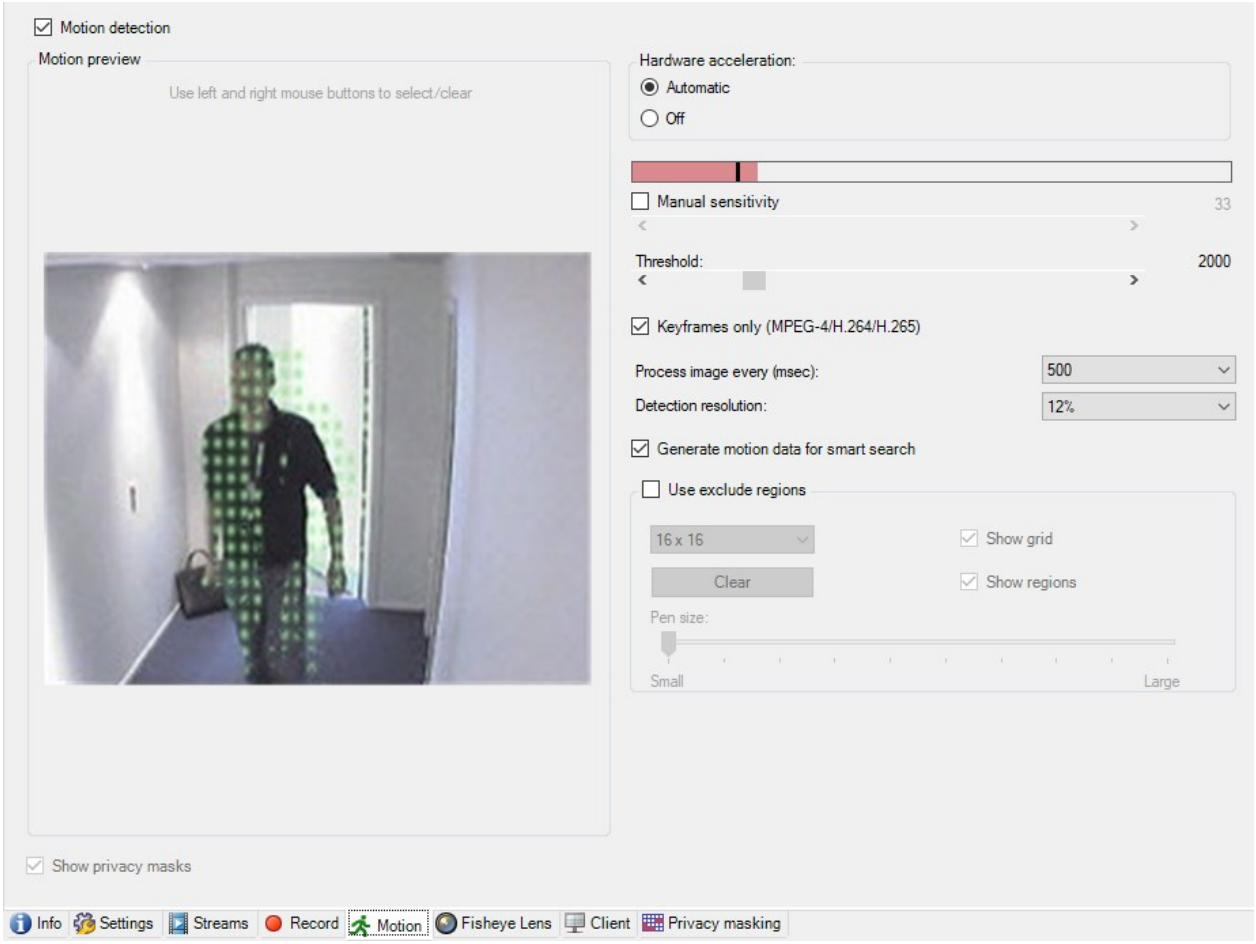
Nome	Descrição
Gravando	Ativar/desativar a gravação Habilitar gravação em dispositivos relacionados
Pré-buffer	Pré-buffer e armazenamento de gravações pré-buffer (explicado) Gerenciar pré-buffering Gerenciar gravação manual
Taxa de quadros de gravação	Especificar a taxa de quadros de gravação Ativar gravação de frame-chave
Armazenamento	Monitorar o status de bancos de dados para dispositivos
Selecionar	Mover dispositivos de um armazenamento a outro
Excluir todas as gravações	Use este botão se você adicionou todos os dispositivos do grupo ao mesmo servidor: Excluir gravações
Recuperar automaticamente as gravações remotas quando a conexão for restaurada	Salvar e recuperar gravações remotas

Guia Movimento (dispositivos)

Os seguintes dispositivos têm uma aba **Movimento**:

- Câmeras

Na aba **Movimento**, você pode ativar e configurar a detecção de movimento para a câmera selecionada.



Tarefas na guia Movimento

Nome	Descrição
Detecção de movimento	Ativar e desativar a detecção de movimento
Aceleração de hardware	Selecione **Automático** para ativar a aceleração de hardware ou selecione **Desligado** para desativar a configuração. Para obter mais informações, consulte Ativar ou desativar aceleração de hardware.
Máscaras de privacidade	Se você definiu áreas com máscaras de privacidade permanentes, pode marcar a caixa de seleção **Máscaras de privacidade** para exibir as máscaras de privacidade na guia **Movimento**. Você define áreas com máscaras de privacidade em Guia Máscara de privacidade (dispositivos) na página 472.

Nome	Descrição
	Não há detecção de movimento em áreas cobertas por máscaras de privacidade permanentes.
Sensibilidade manual	Determina **quanto cada pixel** na imagem precisa mudar antes de ser visto como movimento: Ativar sensibilidade manual para definir movimento
Limite	Determina **quantos pixels** na imagem devem mudar antes de ser visto como movimento: Especifique o limite para definir movimento
Apenas quadros-chave (MPEG-4/H.264/H.265)	Marque esta caixa de seleção para realizar detecção de em quadros-chave em vez de toda a transmissão de vídeo. Só se aplica a MPEG-4/H.264/H.265. A detecção de movimento em quadros-chave reduz a quantidade de poder de processamento utilizado para realizar a análise.
Processar imagem a cada (ms)	Selecione um intervalo de processamento de imagem nesta lista para determinar com que frequência o sistema realiza a análise de detecção de movimento. Por exemplo, cada 1000 milissegundos é uma vez a cada segundo. O valor padrão é a cada 500 milissegundos. O intervalo é aplicado se a taxa de quadros real é maior do que o intervalo definido aqui.
Método de detecção	Selecione uma resolução de detecção nesta lista para otimizar o desempenho da detecção de movimento. Apenas a porcentagem selecionada da imagem é analisada, por exemplo 25%. Ao analisar, por exemplo 25%, somente cada quarto pixel na imagem é analisado em vez de todos os pixels. Usar detecção otimizada reduz a quantidade de energia de processamento, mas também significa uma detecção de movimento menos precisa.
Gerar dados de movimento para pesquisa	Com esta caixa de seleção ativada, o sistema gera dados de movimento para as imagens usadas para detecção de movimento. Por exemplo, se você selecionar a detecção de movimento em apenas frames-chaves, os dados de movimento

Nome	Descrição
inteligente	também são produzidos para apenas frames-chaves. Os dados de movimento adicional permitem que o usuário do cliente, através da função de pesquisa inteligente, procure rapidamente as gravações relevantes com base em movimento na área selecionada da imagem. O sistema não gera dados de movimento em áreas cobertas por máscaras de privacidade permanentes, mas apenas para áreas com máscaras de privacidade removíveis, consulte Detecção de movimento (explicado). O limiar de detecção de movimento e as regiões de exclusão não influenciam os dados de movimento gerados. • Especifica a configuração padrão de gerar dados de pesquisa inteligente para câmeras em **Ferramentas** > **Opções** > **Geral**.
Usar regiões de exclusão	Excluir detecção de movimento de áreas específicas de uma visualização da câmera: Especificar regiões de exclusão para detecção de movimento

Guia Predefinições (dispositivos)

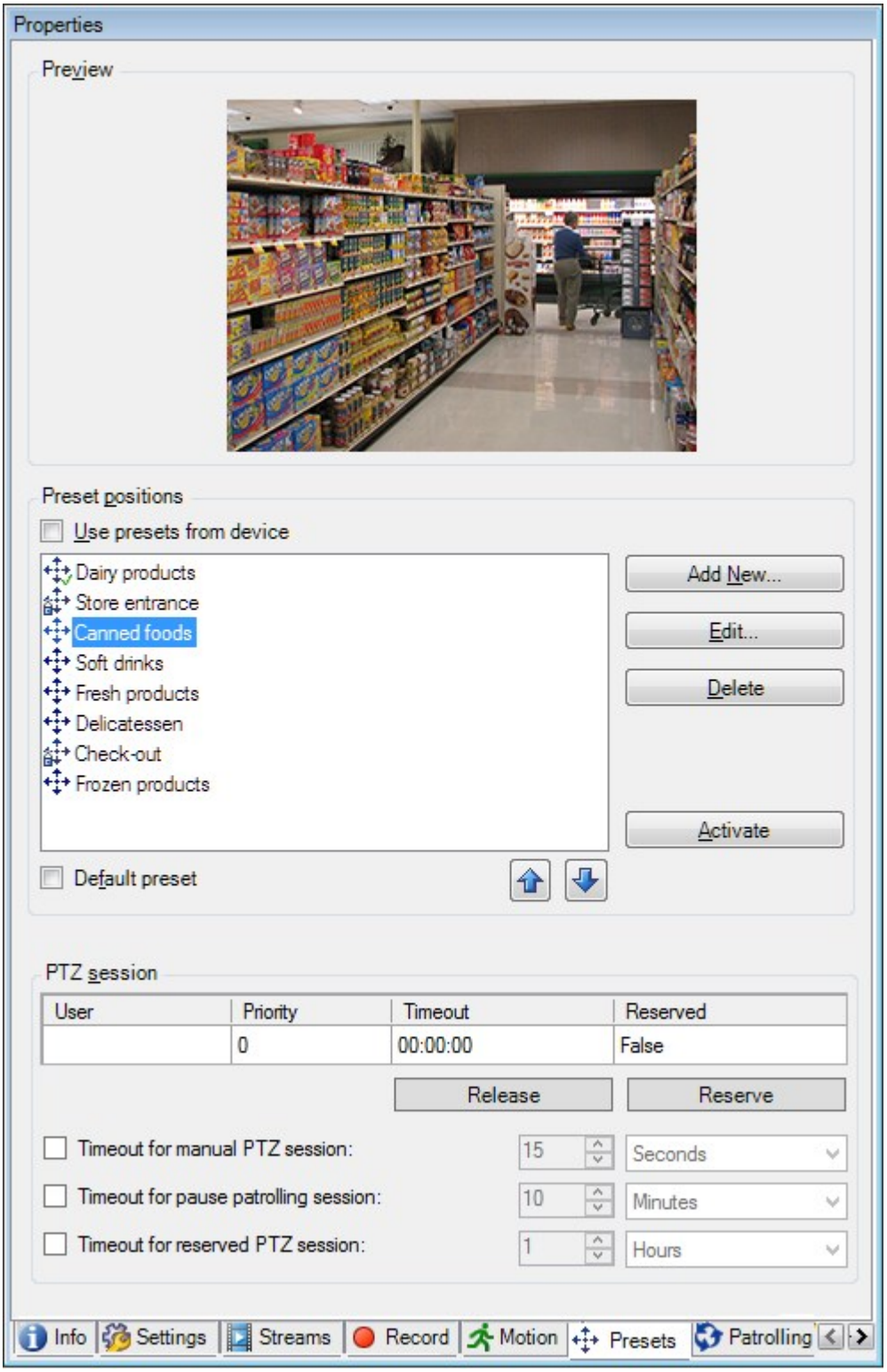
Os seguintes dispositivos têm uma guia **Predefinições**:

- Câmeras PTZ que suportam posições predefinidas

Na guia **Predefinições**, você pode criar ou importar posições predefinidas, por exemplo:

- Em regras para fazer uma câmera PTZ (pan / tilt / zoom) movimentar-se para uma posição predefinida específica' quando ocorre um evento
- Em patrulha, para o movimento automático de uma câmera PTZ entre um número de posições predefinidas
- Para a ativação manual pelos usuários do XProtect Smart Client

Você atribui permissão PTZ para funções na guia Segurança geral (consulte Guia Segurança Geral (funções) na página 528) ou a guia PTZ (consulte Guia PTZ (funções) na página 571).


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

Tarefas na guia Predefinições

Nome	Descrição
Novo	Adicionar uma posição predefinida para uma câmera no site: Adicionar uma posição predefinida (tipo 1)
Uso de predefinições do dispositivo	Adicionar uma posição predefinida para câmeras PTZ na própria câmera: Usar posições predefinidas da câmera (tipo 2)
Predefinição padrão	Atribua uma das posições predefinidas de uma câmera PTZ como posição predefinida padrão da câmera: Atribuir a posição predefinida padrão de uma câmera como padrão
Editar	Editar uma posição predefinida existente definida no sistema: Editar uma posição predefinida para uma câmera (somente tipo 1) Editar o nome de uma posição predefinida estabelecida na câmera: Alterar o nome de uma posição predefinida (somente tipo 2)
Bloqueado	Marque esta caixa de seleção para bloquear uma posição predefinida. Você pode bloquear uma posição predefinida se quiser impedir que usuários no XProtect Smart Client ou usuários com permissões de segurança limitadas atualizem ou excluam uma predefinição. Predefinições bloqueadas são assinaladas com este ícone  . Você trava predefinições como parte da inclusão (consulte Adicionar uma posição predefinida (tipo 1)) e edição (consulte Editar uma posição predefinida (tipo 1 somente)).

Nome	Descrição
Ativar	Clique neste botão para testar uma posição predefinida da câmera: Testar uma posição predefinida (somente tipo 1).
Reservar e **Liberar**	Evite que outros usuários assumam o controle da câmera e liberem a reserva. Administradores com direitos de segurança para executar uma sessão de PTZ reservada podem usar a câmera PTZ neste modo. Isso impede outros usuários de tomarem o controle sobre a câmera. Com permissões suficientes, você pode liberar as sessões PTZ reservadas de outros usuários: Reservar e liberar sessões PTZ.
Sessão PTZ	Monitorar se o sistema está patrulhando atualmente ou se um usuário tomou o controle: Propriedades da sessão PTZ na página 463. Visualize o status das câmeras PTZ e gerencie o tempo limite das câmeras: Especificar tempo limite das sessões PTZ.

Propriedades da sessão PTZ

A tabela **Sessão PTZ** mostra o estado atual da câmera PTZ.

Nome	Descrição
Usuário	Exibe o usuário que pressionou o botão **Reservado** e atualmente controla a câmera PTZ. Se uma sessão de patrulha é ativada pelo sistema, **Patrulha** é exibida.

Nome	Descrição
Prioridade	Exibe a prioridade PTZ do usuário. Você só pode assumir sessões PTZ de usuários com prioridade mais baixa do que a sua.
Tempo limite	Exibe o tempo restante da sessão PTZ atual.
Reservado	Indica se a sessão atual é uma sessão de PTZ reservada ou não: • **Verdadeiro**: Reservado • **Falso**: Não reservado

As caixas de seleção na seção da **Sessão PTZ** permitem que você altere os seguintes tempos limite para cada câmera PTZ.

Nome	Descrição
Limite de tempo para sessões PTZ manuais	Especifique o período de tempo limite para sessões PTZ manuais nesta câmera se você deseja que o tempo limite seja diferente do padrão. Você especifica o período padrão no menu **Ferramentas**, sob **Opções**.
Limite de tempo para pausa de sessões PTZ	Especifique o período de tempo limite para pausar sessões PTZ nesta câmera se você deseja que o tempo limite seja diferente do padrão. Você especifica o período padrão no menu **Ferramentas**, sob **Opções**.
Limite de tempo para sessões PTZ reservadas	Especifique o período de tempo limite para sessões PTZ reservadas nesta câmera se você deseja que o tempo limite seja diferente do padrão. Você especifica o período padrão no menu **Ferramentas**, sob **Opções**.

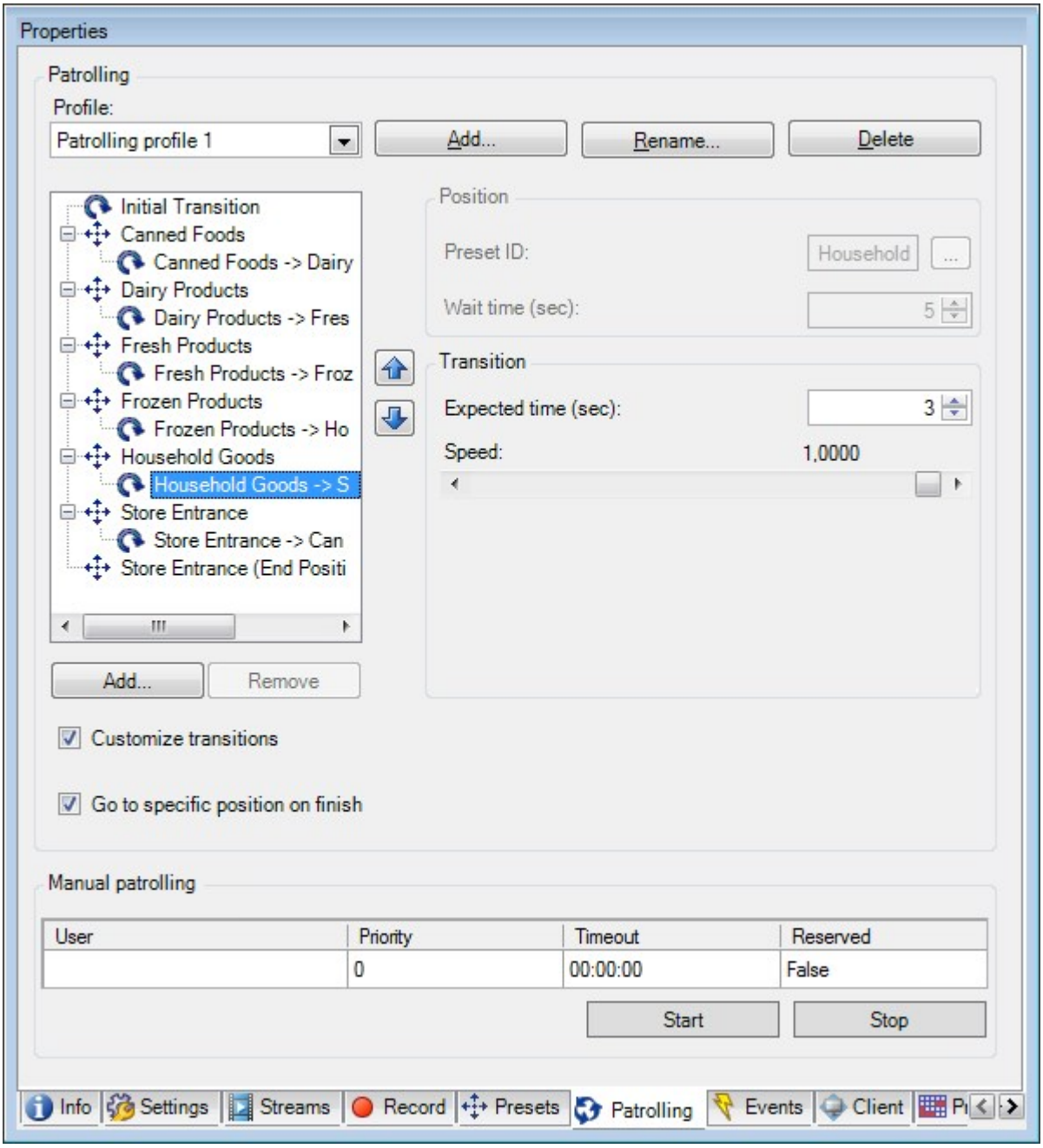
Guia Patrulha (dispositivos)

Os seguintes dispositivos têm uma guia **Patrulhamento**:

- Câmeras PTZ

Na guia **Patrulha**, você pode criar perfis da patrulha, o movimento automático de uma câmera PTZ (Pan/Tilt/Zoom) entre um número de posições predefinidas.
Antes que você possa trabalhar com o patrulhamento, especifique pelo menos duas posições predefinidas para a câmera na guia **Predefinições**, consulte Adicionar uma posição predefinida (type 1).

A guia **Patrulhamento** exibe um perfil de patrulhamento com transições personalizadas:



Tarefas na guia Patrulhamento

Nome	Descrição
Adicionar	Adicionar um perfil de patrulha
ID predefinido	Especificar posições predefinidas em um perfil de patrulha
Tempo de espera (segundos)	Especificar o tempo em cada posição predefinida
Personalizar transições	Personalizar transições (PTZ)
Ir para posição específica ao concluir	Especificar uma posição final em patrulha
Patrulha manual	Monitorar se o sistema está patrulhando atualmente ou se um usuário assumiu o controle.
Iniciar e **Parar**	Use os botões **Iniciar** e **Parar** para iniciar e interromper a patrulha manual. Consulte Especificar tempos limites das sessões PTZ para obter informações sobre como especificar quanto tempo deve passar antes que o patrulhamento regular seja retomado para todos ou para câmeras PTZ individuais.

Propriedades da patrulha manual

A tabela **Patrulha Manual** mostra o estado atual da câmera PTZ.

Nome	Descrição
Usuário	Exibe o usuário que reservou a sessão PTZ ou iniciou uma patrulha manual e atualmente controla a câmera.

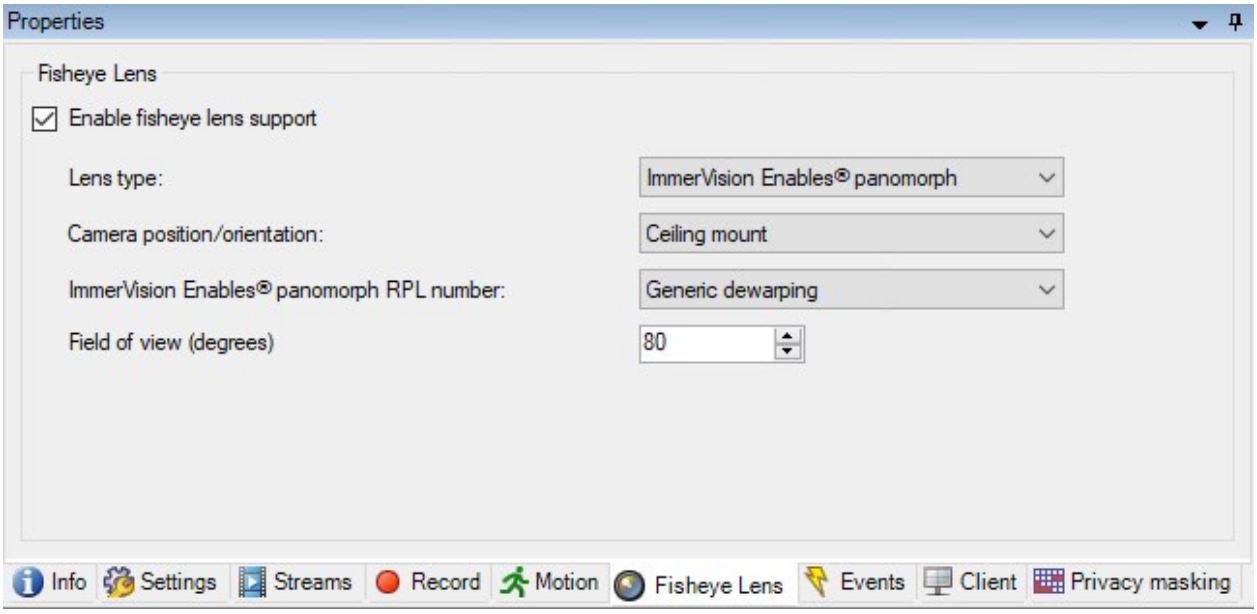
Nome	Descrição
	Se uma sessão de patrulha é ativada pelo sistema, **Patrulha** é exibida.
Prioridade	Exibe a prioridade PTZ do usuário. Você só pode assumir sessões PTZ de usuários ou perfis de patrulha com prioridade mais baixa do que a sua.
Tempo limite	Exibe o tempo restante da sessão PTZ atual, manual ou reservada.
Reservado	Indica se a sessão atual é uma sessão de PTZ reservada ou não. • **Verdadeiro**: Reservado • **Falso**: Não reservado

Guia Lentes olho de peixe (dispositivos)

Os seguintes dispositivos têm uma guia **Lentes olho de peixe**:

- Câmeras fixas com uma lente olho de peixe

Na guia **Lentes olho de peixe**, você pode ativar e configurar o suporte das lentes olho de peixe para a câmera selecionada.



Tarefa na guia da lente olho de peixe

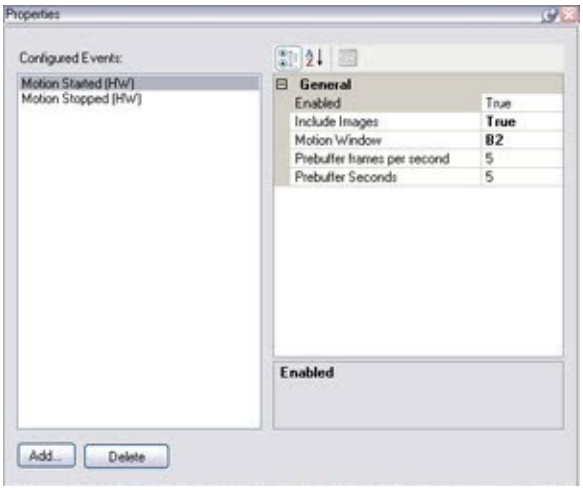
Nome	Descrição
Ativar suporte das lentes olho de peixe	Ativar e desativar o suporte das lentes olho de peixe

Guia Eventos (dispositivos)

Os seguintes dispositivos têm uma guia **Eventos**:

- Câmeras
- Microfones
- Entradas

Além do evento do sistema, algumas câmeras podem, elas mesmas, ser configuradas para disparar eventos. Estes eventos podem ser usados ao criar regras baseadas em eventos no sistema. Tecnicamente, eles ocorrem no dispositivo/hardware real ao invés de no sistema de monitoramento.



Tarefas na guia Eventos

Nome	Descrição
Adicionar e **Excluir**	Adicionar ou excluir um evento para um dispositivo

Guia Eventos (propriedades)

Nome	Descrição
Eventos configurados	Que eventos você pode selecionar e adicionar à lista de **Eventos configurados** é integralmente determinado pelo dispositivo e sua configuração. Para alguns tipos de hardware/dispositivo, a lista pode ser vazia.
Geral	A lista de propriedades depende do dispositivo e do evento. Para o evento funcionar como esperado, algumas ou todas as propriedades devem ser especificadas de forma idêntica no dispositivo e nesta guia.

Guia Cliente (dispositivos)

Os seguintes dispositivos têm uma guia **Cliente**:

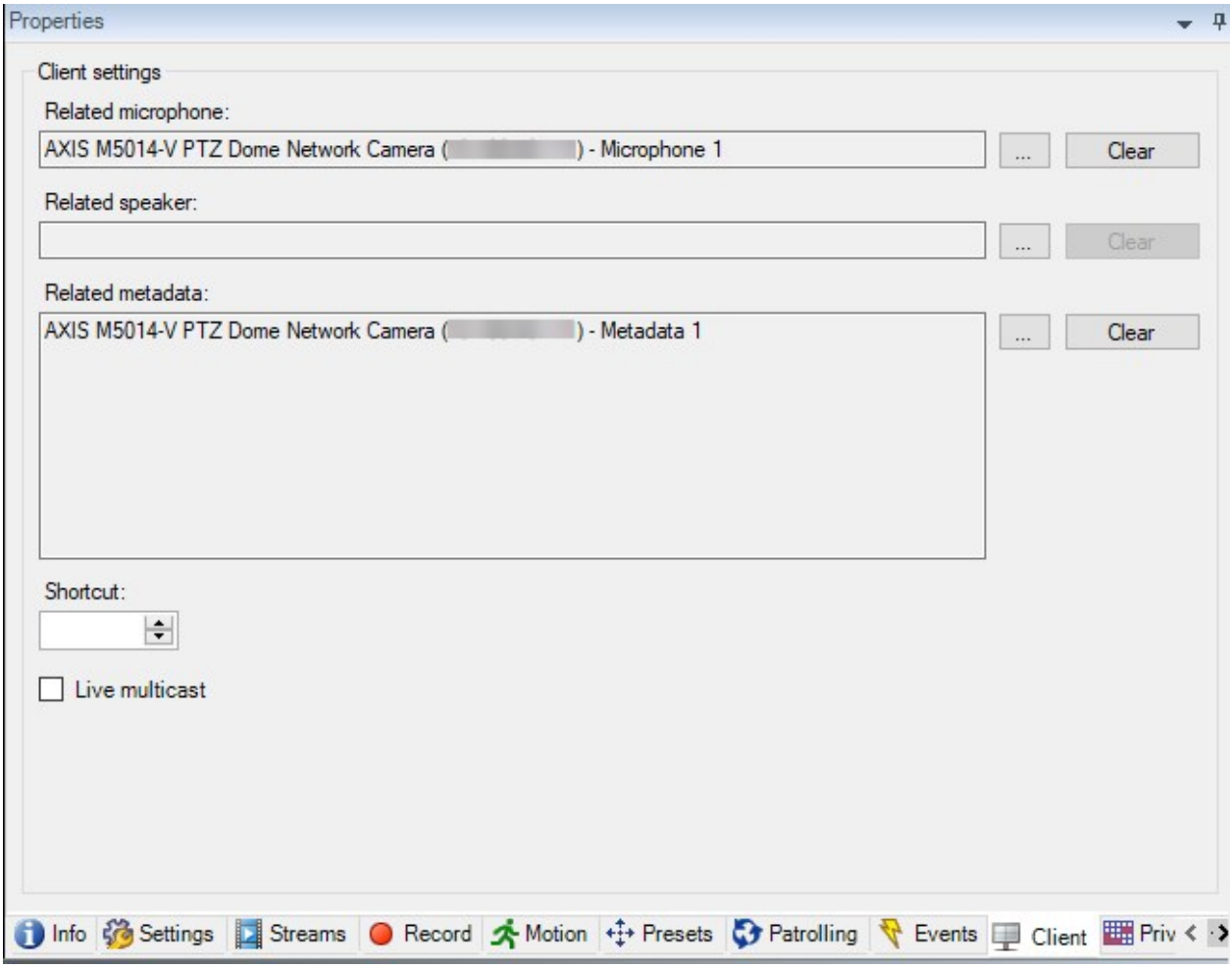
- Câmeras

Na guia **Cliente**, você pode especificar quais outros dispositivos são visualizados e ouvidos ao usar a câmera no XProtect Smart Client.

Os dispositivos de metadados relacionados são gravados quando a câmera grava, consulte Habilitar gravação em dispositivos relacionados na página 239.

Também é possível ativar **Multicast ao vivo** na câmera. Isso significa que a câmera exibe vários fluxos ao vivo para os clientes por meio do servidor de gravação.

As transmissões de multicast não são criptografadas, mesmo se o servidor de gravação usar criptografia.



Propriedades da aba Cliente

Nome	Descrição
Microfone relacionado	Especifique a partir de que microfone da câmera os usuários XProtect Smart Client recebem áudio por padrão. O usuário XProtect Smart Client pode selecionar manualmente para ouvir outro microfone, caso necessário. Especifique o microfone relacionado à câmera de Video Push para o fluxo de vídeo com áudio. Os microfones relacionados são gravados quando a câmera grava.

Nome	Descrição
Alto-falante relacionado	Especifique por quais alto-falantes na câmera os usuários XProtect Smart Client falam por padrão. O usuário XProtect Smart Client pode selecionar manualmente um outro alto-falante, caso necessário. Os microfones relacionados são gravados quando a câmera grava.
Metadados relacionados	Especifique um ou mais dispositivos de metadados da câmera, de onde os usuários XProtect Smart Client recebem dados. Os dispositivos de metadados relacionados são gravados quando a câmera grava.
Atalho	Para facilitar a seleção de câmeras para o usuários do XProtect Smart Client, defina atalhos de teclado para a câmera. • Crie cada atalho de modo a que ele identifique cada câmera • Um número do atalho da câmera não pode ter mais de quatro dígitos
Multicast ao vivo	O sistema suporta multidifusão de fluxos ao vivo do servidor de gravação para XProtect Smart Client. Para ativar multicast de fluxos ao vivo da câmera, marque a caixa de seleção. A multidifusão ao vivo só funciona no fluxo que você especificou como fluxo padrão da câmera na guia **Fluxos**. Você também deve configurar multicast para o servidor de gravação. Consulte Ativar multicasting para o servidor de gravação na página 213. As transmissões de multicast não são criptografadas, mesmo se o servidor de gravação usar criptografia.

Guia Máscara de privacidade (dispositivos)

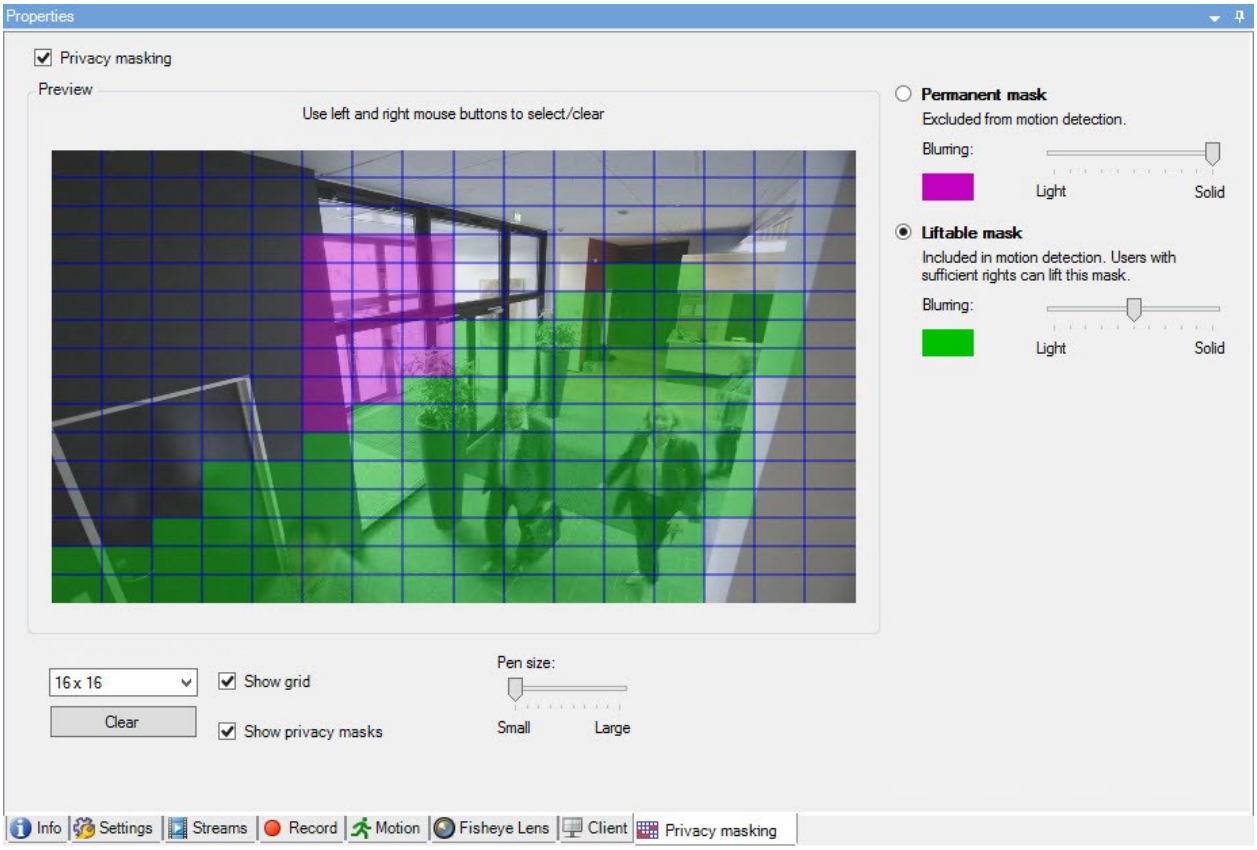
> As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

XProtect Essential+ 2018 R1 e versões seguintes não são compatíveis com a máscara de privacidade; portanto, se você atualizar um sistema com máscaras de privacidade aplicadas, as máscaras serão removidas.

Os seguintes dispositivos têm uma guia **Máscara de privacidade**:

- Câmeras

Na guia **Máscara de privacidade**, você pode ativar e configurar a proteção de privacidade para a câmera selecionada.



Tarefas na guia de Máscara de privacidade

Nome	Descrição
Máscara de privacidade	Ativar/desativar a máscara de privacidade Máscara de privacidade (explicado)
Máscara permanente e **Máscara removível**	Defina se você deseja uma máscara de privacidade permanente ou removível: Definir máscaras de privacidade

Tarefas relacionadas a máscara de privacidade

Tarefa	Descrição
Alterar o tempo limite para máscaras de privacidade removidas para o perfil Smart Client associado à função que tenha a permissão para remover máscaras de privacidade.	Alterar o tempo limite para máscaras de privacidade removidas
Ativar ou desativar permissão para remover máscaras de privacidade para uma função.	Dar aos usuários permissão para remover máscaras de privacidade
Crie um relatório de dispositivos com informações sobre as configurações atuais de máscara de privacidade das câmeras.	Gere um relatório da configuração da máscara de privacidade

Guia Máscara de privacidade (propriedades)

Nome	Descrição
Tamanho da grade	O tamanho da grade selecionado determina a densidade da grade, independentemente de a grade estar visível na visualização ou não. Escolha entre os valores 8×8, 16×16, 32×32 ou 64×64.
Limpar	Limpa **todas** as máscaras de privacidade que você especificou.
Mostrar grade	Marque a caixa de seleção **Mostrar grade** para tornar a grade visível.
Exibir máscaras de privacidade	Quando você marca a caixa de seleção **Exibir máscaras de privacidade** (padrão), as máscaras de privacidade permanentes aparecem em roxo na visualização e as máscaras de privacidade removíveis, em verde. A Milestone recomenda que você mantenha a caixa **Exibir máscaras de privacidade** selecionada para que você e seus colegas possam ver a configuração de proteção de privacidade atual.
Tamanho da caneta	Use o controle deslizante **Tamanho da caneta** para indicar o tamanho das seleções que você deseja fazer ao clicar e arrastar a grade para selecionar regiões. O padrão é pequeno, que é equivalente a um quadrado da grade.
Máscara permanente	Aparece em roxo na visualização nesta guia e na guia **Movimento**. As máscaras de privacidade permanentes são sempre visíveis no XProtect Smart Client e não podem ser removidas. Podem ser usadas para cobrir áreas do vídeo que nunca requerem vigilância, como áreas públicas ou onde a vigilância não for permitida. A detecção de movimento é excluída de máscaras permanentes. Você pode especificar a cobertura de máscaras de privacidade como sólidas ou com algum nível de desfoque. As configurações de cobertura se aplicam a vídeo ao vivo e a vídeo gravado.
Máscara removível	Aparece em verde na visualização nesta guia. Máscaras de privacidade removíveis podem ser levantadas no XProtect Smart Client por usuários com permissões de usuário suficientes. Por padrão, as máscaras de privacidade são removidas por 30 minutos ou até que o usuário as aplique novamente. Esteja ciente de que as máscaras de privacidade são removidas no vídeo de todas as câmeras às quais o usuário tenha acesso.

Nome	Descrição
	Se o usuário XProtect Smart Client não tiver permissão para levantar máscaras de privacidade, o sistema solicitará um usuário com permissão para autorizar o levantamento. Você pode especificar a cobertura de máscaras de privacidade como sólidas ou com um nível de desfoque. As configurações de cobertura se aplicam a vídeo ao vivo e a vídeo gravado.
Desfoque	Use o controle deslizante para selecionar o nível de desfoque das máscaras de privacidade nos clientes ou definir a cobertura como sólida. Por padrão, a cobertura de áreas com máscaras de privacidade permanentes são sólidas (não transparentes). Por padrão, as máscaras de privacidade removíveis possuem nível de desfoque médio. Você pode informar os usuários do cliente sobre a aparência das máscaras de privacidade permanentes e removíveis, para que possam distingui-las.

Janela de propriedades de hardware

Você tem várias opções para adicionar hardware para cada servidor de gravação em seu sistema.

> Se seu hardware está localizado atrás de um roteador ou um firewall habilitado para NAT, você pode precisar especificar um número de porta diferente e configurar o roteador/firewall para que ele mapeie a porta e os endereços IP que o hardware utiliza.

O assistente **Adicionar hardware** ajuda você detectar hardware como câmeras e codificadores de vídeo na sua rede e adicioná-los ao servidor de gravações no seu sistema. O assistente também ajuda a adicionar servidores de gravação remotos para configurações Milestone Interconnect. Só adicione hardware para **um servidor de gravação** de cada vez.

Guia Informações (hardware)

Para obter informações sobre a guia **Informações** para servidores remotos, consulte Guia informações (servidor remoto) na página 443.

Nome	Descrição
Nome	Digite um nome. O sistema usa o nome sempre que o hardware estiver listado no sistema e nos clientes. O nome não tem que ser único. Quando você renomeia o hardware, o nome é alterado globalmente no Management Client.
Descrição	Digite uma descrição do hardware (opcional). A descrição aparece em uma série de listas dentro do sistema. Por exemplo, ao mover o ponteiro do mouse sobre o nome do hardware no painel **Visão Geral**: 
Modelo	Identifica o modelo de hardware.
Número de série	Número de série do hardware especificado pelo fabricante. O número de série é frequentemente, mas não sempre, idêntico ao endereço MAC.
Driver	Identifica o driver que trata da conexão ao hardware.
IE	Abre a página inicial padrão do fornecedor de hardware. Você pode usar esta página para a administração do hardware.
Endereço	O endereço IP ou nome do host do hardware.
Endereço MAC	Especifica o Endereço do Controle de Acesso de Mídia (MAC) do hardware do sistema. Um endereço MAC é um número hexadecimal de 12 caracteres que identifica exclusivamente cada dispositivo de hardware na rede.
Versão do firmware:	A versão do firmware do dispositivo de hardware. Para garantir que o sistema exiba a versão atual, execute o assistente **Atualizar dados de hardware** após cada atualização de firmware.
Última alteração de senha	O campo **Última alteração de senha** mostra o carimbo de hora da alteração de senha mais recente, com base nas configurações de hora locais do computador a partir do qual a senha foi alterada.

Nome	Descrição
Dados de hardware atualizados pela última vez:	Hora e data da última atualização dos dados de hardware.

Guia Configurações (hardware)

Na guia **Configurações**, você pode verificar ou editar configurações para o hardware.

> O conteúdo da guia **Configurações** é determinado inteiramente pelo hardware selecionado, e pode variar dependendo do tipo de hardware. Para alguns tipos de hardware, a guia **Configurações** não exibe nenhum conteúdo ou conteúdo de somente leitura.

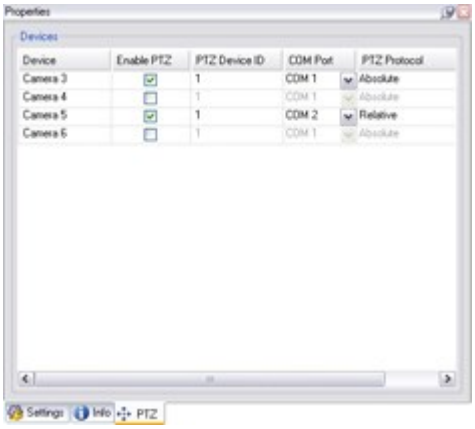
Para obter informações sobre a guia **Configurações** para servidores remotos, consulte a Guia Configurações (servidor remoto) na página 444.

Guia PTZ (codificadores de vídeo)

Na guia **PTZ**, você pode ativar o PTZ (Pan/Tilt/Zoom) para codificadores de vídeo. A guia está disponível se o dispositivo selecionado for um codificador de vídeo ou se o driver suportar tanto câmeras PTZ quanto câmeras não-PTZ.

Você deve habilitar o uso de PTZ separadamente para cada um dos canais de codificador de vídeo na guia **PTZ** antes que você possa usar os recursos PTZ das câmeras PTZ anexadas ao codificador de vídeo.

> Nem todos os codificadores de vídeo suportam o uso de câmeras PTZ. Mesmo os codificadores de vídeo que suportam o uso de câmeras PTZ podem exigir uma configuração antes das câmeras PTZ poderem ser utilizadas. É tipicamente a instalação de drivers adicionais através de uma interface de configuração baseada em navegador no endereço IP do dispositivo.



A guia **PTZ**, com PTZ ativado para dois canais em um codificador de vídeo.

Nó de cliente

Clientes (nó)

Este artigo descreve como personalizar a interface do usuário para operadores no XProtect Smart Client e para administradores do sistema no Management Client.

Smart Wall (Nó Cliente)

Propriedades Smart Wall

Guia Informações

Na guia **Informações** de uma definição de Smart Wall, você pode adicionar e editar propriedades de Smart Wall.

Nome	Descrição
Nome	O nome da definição do Smart Wall. É exibido no XProtect Smart Client como o nome do grupo de visualização do Smart Wall.
Descrição	Uma descrição da definição do Smart Wall. A descrição é usada apenas internamente no XProtect Management Client.
Texto de	Exibe informações do status da câmera e do site em itens de visualização da câmera.

Nome	Descrição
status	
Sem barra de título	Oculte a barra de título em todos os itens de visualização no videowall.
Barra de título	Exiba a barra de título em todos os itens de visualização no videowall.

Guia Predefinições

Na guia **Predefinições** de uma definição do Smart Wall, você pode adicionar e editar predefinições[1] do Smart Wall.

Nome	Descrição
Adicionar Novo	Adicionar uma predefinição para a definição do seu Smart Wall. Insira um nome e a descrição da predefinição.
Editar	Edita o nome ou a descrição de uma predefinição.
Excluir	Excluir uma predefinição.
Ativar	Aplique a predefinição nos monitores Smart Wall que estão configurados para usar a predefinição. Para aplicar uma predefinição automaticamente, você deve criar uma regra que use a predefinição.

Guia Layout

Na guia **Layout** para uma definição de Smart Wall, você posiciona os monitores de forma que suas posições se assemelhem à montagem dos monitores físicos no videowall. O layout também é utilizado no XProtect Smart Client.

[1]Layout predefinido para um ou mais monitores Smart Wall no XProtect Smart Client. As predefinições determinam quais câmeras são exibidas e como o conteúdo é estruturado em cada monitor no videowall.

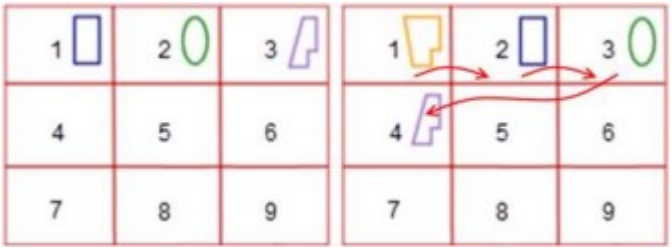
Nome	Descrição
Editar	Ajustar o posicionamento dos monitores.
Movimento	Para mover uma monitor para uma posição nova, selecione o monitor e arraste-o para a posição escolhida ou clique nos botões de seta para mover o monitor na direção desejada.
Botões de zoom	Dê zoom in/out na pré-visualização do layout do Smart Wall para garantir que posicionou os monitores corretamente.
Nome	O nome do monitor. O nome é exibido no XProtect Smart Client.
Tamanho	Tamanho físico do monitor no rack de vídeos.
Proporção do vídeo	A relação altura/largura do monitor no rack de vídeos.

Propriedades do Monitor

Guia Informações

Na guia **Informações** para um monitor em uma predefinição Smart Wall, é possível adicionar monitores e editar suas configurações.

Nome	Descrição
Nome	O nome do monitor. O nome é exibido no XProtect Smart Client.
Descrição	Uma descrição do monitor. A descrição é usada apenas internamente no XProtect Management Client.
Tamanho	Tamanho físico do monitor no rack de vídeos.
Proporção do vídeo	A relação altura/largura do monitor no rack de vídeos.

Nome	Descrição
Predefinição vazia	Define o que deve ser exibido em um monitor com um layout predefinido vazio quando uma nova predefinição Smart Wall for disparada ou selecionada em XProtect Smart Client: • Selecione **Preservar** para manter o conteúdo atual no monitor. • Selecione **Limpar** para limpar todos os conteúdos de modo que nada seja exibido no monitor.
Item predefinido vazio	Define o que deve ser exibido em uma predefinição vazia quando uma nova predefinição do Smart Wall for disparada ou selecionada em XProtect Smart Client: • Selecione **Preservar** para manter o conteúdo atual no item de layout. • Selecione **Limpar** para limpar todos os conteúdos de modo que nada seja exibido no item de layout.
Inserção de elementos	Define de que maneira as câmeras são inseridas no layout do monitor quando vistas no XProtect Smart Client: • **Independente** – somente os conteúdos do layout afetado mudam. O restante dos conteúdos permanece como estava. • **Relacionado** – o conteúdo dos itens de layout são empurrados a partir da esquerda para a direita. Se, por exemplo, uma câmera for inserida na posição 1, a câmera anterior da posição 1 será enviada para a posição 2, a câmera anterior da posição 2 será enviada para a posição 3 e assim por diante. Ilustrado neste exemplo: 

Guia Predefinições

Na guia **Predefinições** de um monitor em uma predefinição Smart Wall, é possível editar o layout e conteúdo do monitor da predefinição Smart Wall selecionada.

Nome	Descrição
Predefinido	Uma lista de predefinições do Smart Wall para a definição do Smart Wall selecionada.
Editar	Clique em **Editar** para editar o layout e o conteúdo do monitor selecionado. Clique duas vezes em uma câmera para removê-la. Clique em **Limpar** para definir um novo layout ou para excluir o monitor da predefinição de Smart Wall de modo que o monitor fique disponível para outros conteúdos não controlados pela predefinição de Smart Wall. Clique em  para selecionar o layout que você deseja usar com o seu monitor em clique em **OK**.

Smart Client Perfis (nó de Cliente)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Nas guias a seguir, você pode especificar as propriedades de cada perfil do Smart Client. Você pode bloquear as configurações no Management Client, se necessário, para que os usuários do XProtect Smart Client não possam alterá-las.

Para criar ou editar perfis Smart Client, expanda **Cliente** e selecione **Smart ClientPerfis**.

Guia informações (perfis do Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Informações	Nome e descrição, prioridade de perfis existentes e uma visão geral de quais funções usar o perfil. Se um usuário é membro de mais de uma função, cada um com seu perfil individual do Smart Client, o usuário receberá o perfil de Smart Client com a prioridade mais alta.

Guia Geral (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Geral	Configurações, tais como mostrar/ocultar, mini/maximizar o menu, efetuar login/sair, inicialização, tempo de espera, informação e opções de mensagem, além de ativar ou desativar determinadas guias no XProtect Smart Client. As configurações **Mensagens de erro da câmera**, **Mensagens de erro do servidor** e **Mensagem de erro ao vivo** permitem controlar se essas mensagens de erro serão exibidas como sobreposição ou se ficarão ocultas. A **Mensagem de vídeo ao vivo parado** é exibida no XProtect Smart Client quando a alimentação ao vivo da câmera for interrompida. Por exemplo, se a câmera parou de enviar imagens mesmo estando conectada. ⚠ Se você **Ocultar** as mensagens de erro da câmera, há um risco de o operador não perceber que a conexão à câmera foi perdida. A configuração **Câmeras permitidas durante a pesquisa** permitem que você controle quantas câmeras os operadores podem adicionar a pesquisas no XProtect Smart Client. A configuração de um limite de câmeras pode ajudá-lo a evitar a sobrecarga do sistema. A configuração da **Ajuda online** permite desativar o sistema de ajuda no XProtect Smart Client. A configuração dos **Tutoriais de vídeo** permite desativar o botão **Tutoriais de vídeo** no XProtect Smart Client. O botão redireciona os operadores para a página de tutoriais de vídeo: https://www.milestonesys.com/support/help-yourself/video-tutorials/

Guia Avançado (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Avançado	Configurações avançadas, como decodificação máxima, desentrelaçar e configurações de

Guia	Descrição
	fuso horário. **Máximo de threads de descodificação** controla quantas threads de decodificação são usadas para decodificar fluxos de vídeo. Isso pode ajudar a melhorar a performance em computadores multi-núcleos nos fluxos em tempo real bem como em modo reprodução. A melhora de performance exata depende da transmissão do fluxo de vídeo. É relevante principalmente se estiver usando fluxos de vídeo de alta resolução fortemente codificados como o H.264/H.265, para o qual o potencial de melhoria de desempenho pode ser significativo, e menos relevante se estiver usando, por exemplo, JPEG ou MPEG-4. Com o **desentrelaçamento**, você converte vídeo em um formato não interlaçado. Entrelaçamento determina como uma imagem é atualizada na tela. A imagem é atualizada pela primeira varredura de linhas ímpares na imagem, então varrendo as linhas pares. Isso permite uma taxa de atualização mais rápida, porque menos informação deve ser processada durante cada escaneamento. Todavia, entrelaçamento pode ser oscilante ou as mudanças na metade das linhas da imagem pode ser notável. **Streaming adaptável** permite que o XProtect Smart Client selecione automaticamente os fluxos de vídeo ao vivo com a melhor correspondência na resolução para os fluxos solicitados pelo item de visualização. Isso reduz a carga na CPU e GPU e, assim, melhora a capacidade de descodificação e desempenho do computador. Isso requer que streaming múltiplo ou fluxos de vídeo ao vivo com diferentes resoluções sejam configurados, consulte Gerenciar streaming múltiplo. O fluxo adaptável pode ser aplicado aos modos ao vivo e de reprodução. No modo de reprodução, o fluxo adaptável é chamado de reprodução adaptável. Na reprodução adaptável, é preciso configurar dois fluxos para a gravação. Para obter mais informações sobre como adicionar fluxos para fluxos adaptáveis no modo ao vivo e na reprodução adaptável, consulte Adicionar uma transmissão na página 241.

Guia Ao vivo (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Ao vivo	A disponibilidade do modo ao vivo e outros recursos ao vivo, reprodução de câmera e botões sobrepostos e caixas delimitadoras além de MIP plugins relacionados ao vivo.

Guia Reprodução (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Reprodução	A disponibilidade do modo de reprodução e outros recursos de reprodução, layout de relatórios de impressão, reprodução independente, marcadores e caixas delimitadoras além de MIP plugins relacionados à reprodução.

Guia Configuração (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Configuração	Disponibilidade de configuração geral/painéis/botões, MIP plug-in relacionado à configuração e permissões para editar um mapa e editar buffer de vídeo ao vivo.

Guia Exportar (perfis do Smart Client

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Exportar	Caminhos, máscaras de privacidade, formatos de vídeo e de imagem estática e o que incluir ao exportá-los, formatos de exportação para XProtect Smart Client – Player e muito mais.

Guia Linha do tempo (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Linha do tempo	Se desejar incluir áudio ou não, a visibilidade de indicação de tempo e de movimento, e, por fim, como lidar com as lacunas de reprodução. Você também pode selecionar se deseja mostrar dados adicionais ou marcadores adicionais a partir de outras fontes.

Guia Controle de acesso (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Controle de acesso	Selecione se as notificações de solicitação de acesso devem ser mostradas na tela do XProtect Smart Client quando acionadas por eventos.

Guia Gerenciador de Alarmes (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Gerente de alarmes	Especifique se:

Guia	Descrição
	• As notificações da área de trabalho para alarmes devem ser exibidas nos computadores em que o XProtect Smart Client está instalado. As notificações aparecem apenas se o XProtect Smart Client estiver em execução - mesmo se minimizado Notificações na área de trabalho para alarmes aparecem somente quando os alarmes tiverem determinadas prioridades, por exemplo **Média** ou **Alta**. Para configurar as prioridades de alarme que disparam notificações, vá para **Alarmes** > **Configurações de dados de alarme** > **Níveis dos dados de alarme**. Para cada prioridade de alarme necessária, selecione a caixa de verificação **Ativar notificações na área de trabalho**. Consulte Configurações de dados de alarmes (nó Alarmes). • Alarmes devem tocar notificações sonoras nos computadores em que o XProtect Smart Client está instalado. As notificações sonoras tocam apenas se o XProtect Smart Client estiver em execução - mesmo se minimizado As notificações sonoras para alarmes são reproduzidas apenas quando um som está associado ao alarme. Para associar sons a alarmes, acesse **Alarmes** > **Configurações de dados de alarme** > **Níveis de dados de alarmes**. Para cada prioridade de alarme necessária, selecione o som a ser associado com o alarme. Consulte Configurações de dados de alarmes (nó Alarmes).

Guia Mapa inteligente (perfis Smart Client)

Essa guia permite especificar as seguintes propriedades:

Guia	Descrição
Mapa inteligente	Especifique configurações para o recurso de mapa inteligente. Você pode especificar se: • Milestone Map Service está disponível para o uso como fundo geográfico • O OpenStreetMaps está disponível para o uso como fundo geográfico • XProtect Smart Client criará locais automaticamente quando um usuário adicionar uma sobreposição personalizada ao mapa inteligente. Você também pode especificar a frequência com que você deseja que o sistema exclua dados relacionados a mapas inteligentes do seu computador. Para ajudar o XProtect Smart Client a exibir o mapa inteligente mais rapidamente, o cliente salva os dados do mapa no cache do seu computador. Com o passar do tempo, isso pode tornar o seu computador mais lento. O armazenamento em cache não se aplica ao Google Maps. Se desejar usar Bing Maps ou Google Maps como fundos geográficos, insira uma chave do Bing Maps API, ou uma chave API estática de mapas do Google.

Management Client Perfis (nó de Cliente)

Essa funcionalidade só está disponível no XProtect Corporate.

Guia Informações (perfis do Management Client)

Na guia **Informações**, você pode definir o seguinte nos perfis Management Client:

Componente	Exigência
Nome	Dar um nome ao perfil do Management Client.
Prioridade	Use as setas para cima e para baixo para definir uma prioridade para o

Componente	Exigência
	perfil do Management Client.
Descrição	Digite uma descrição para o perfil. Isto é opcional.
Funções usando o perfil do Management Client	Este campo mostra as funções que você associou ao perfil do Management Client. Você não pode editar este campo.

Guia perfil (perfis Management Client)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Na guia **Perfil**, você pode ativar ou desativar a visibilidade dos seguintes elementos na interface de usuário do Management Client:

Navegação

Nesta seção, decida se um usuário administrador associado ao perfil do Management Client tem permissão para ver os vários recursos e funcionalidades localizados no painel de **Navegação**.

Elemento de navegação	Descrição
Fundamentos	Permite que o usuário administrador associado ao perfil do Management Client acesse as **Informações da licença** e **Informações do site**.
Serviços de Conexão Remota	Permite que o usuário administrador associado ao perfil do Management Client acesse a **Conexão da Câmera Axis One-click**.
Servidores	Permite que o usuário administrador associado ao perfil do Management Client acesse os **Servidores de gravação** e **Servidores de emergência**.

Elemento de navegação	Descrição
Dispositivos	Permite que o usuário administrador associado ao perfil do Management Client acesse **Câmeras**, **Microfones**, **Alto-falantes**, **Metadados**, **Entradas** e **Saídas**.
Client	Permite que o usuário administrador associado ao perfil do Management Client acesse **Smart Wall**, **Grupos de visualização**, **Perfis Smart Client**, **Perfis Management Client** e **Matrix**.
Regras e Eventos	Permite que o usuário administrador associado ao perfil do Management Client acesse **Regras**, **Perfis de Tempo**, **Perfis de Notificação**, **Eventos Definidos pelo Usuário**, **Eventos Analíticos** e **Eventos Genéricos**.
Segurança	Permite que o usuário administrador associado ao perfil do Management Client acesse **Funções** e **Usuários Básicos**.
Painel do sistema	Permite que o usuário administrador associado ao perfil do Management Client veja **Monitor do sistema**, **Limites do monitor do sistema**, **Proteção de evidência**, **Tarefas atuais** e **Relatórios de configuração**.
Registros de servidor	Permite que o usuário administrador associado ao perfil do Management Client veja o registro do sistema, o registro de auditoria e os registros disparados por regras.
Controle de acesso	Permite que o usuário administrador associado ao perfil do Management Client veja recursos do **Controle de acesso**, caso integrações ou plug-ins de controle de acesso tenham sido adicionados ao sistema.

Detalhes

Nesta seção, decida se um usuário administrador associado ao perfil do Management Client tem permissão para ver as várias guias de um canal específico de dispositivo, p. ex., as guias **Configurações** ou **Gravação** das câmeras.

Canal de dispositivos	Descrição
Câmeras	Permite que o usuário administrador associado ao perfil do Management Client veja

Canal de dispositivos	Descrição
	todas ou algumas abas e configurações relacionadas a câmeras.
Microfones	Permite que o usuário administrador associado ao perfil do Management Client veja todas ou algumas abas e configurações relacionadas a microfones.
Alto-falantes	Permite que o usuário administrador associado ao perfil do Management Client veja todas ou algumas abas e configurações relacionadas a alto-falantes.
Metadados	Permite que o usuário administrador associado ao perfil do Management Client veja todas ou algumas abas e configurações relacionadas a metadados.
Entrada	Permite que o usuário administrador associado ao perfil do Management Client veja todas ou algumas abas e configurações relacionadas a entradas.
Saída	Permite que o usuário administrador associado ao perfil do Management Client veja todas ou algumas abas e configurações relacionadas a saídas.

Menu de ferramentas

Nesta seção, decida se um usuário administrador associado ao perfil do Management Client tem permissão para ver os elementos que compõem o menu **Ferramentas**.

Opção do Menu Ferramentas	Descrição
Serviços registrados	Permite que o usuário administrador associado ao perfil do Management Client acesse **Serviços Registrados**.
Funções efetivas	Permite que o usuário administrador associado ao perfil do Management Client acesse **Funções eficazes**.
Opções	Permite que o usuário administrador associado ao perfil do Management Client acesse as **Opções**.

Sites em Conjunto

Nesta seção, decida se um usuário administrador associado ao perfil do Management Client tem permissão para ver o painel **Hierarquia de Sites Federados**.

Nó de regras e eventos

Regras (nó Regras e eventos)

O sistema inclui uma série de regras predefinidas que você pode usar para recursos básicos sem configurar nada. Você pode desativar ou modificar as regras padrão conforme suas necessidades. Se você modificar ou desativar as regras padrão, o sistema pode não funcionar conforme desejaria, nem garante que as alimentações de vídeo ou alimentações de áudio sejam alimentadas automaticamente para o sistema.

Regra padrão	Descrição
Ir para Predefinição quando PTZ tiver terminado	Garante que as câmeras PTZ vão para suas respectivas posições predefinidas padrão depois de terem operado manualmente. Esta regra não está ativada por padrão. Mesmo que você ative a regra, você deve definir posições predefinidas padrão para as câmeras PTZ relevantes para que a regra funcione. Você pode fazer isso na guia **Predefinições**.
Reproduzir áudio mediante pedido	Garante que o vídeo seja gravado automaticamente quando há uma solicitação externa. O pedido é sempre acionado por um sistema de integração externa com o seu sistema, e a regra é usada principalmente por integradores de sistemas externos ou plug-ins.
Gravar no marcador	Garante que o vídeo seja gravado automaticamente quando um operador define um marcador no XProtect Smart Client. Isto é desde que você tenha ativado a gravação para as câmeras relevantes. A gravação está ativada por padrão. O tempo de gravação padrão para esta regra é de três segundos antes do marcador ser definido e 30 segundos depois do indicador ser definido. Você pode editar os tempos de gravação padrão na regra. O pré-buffer que você definir na guia Gravar deve corresponder ou ser maior que o tempo de pré-gravação.
Gravar em movimento	Garante que, enquanto o movimento for detectado em vídeo das câmeras, o vídeo será gravado, contanto que a gravação esteja ativada para as câmeras relevantes. Gravação é ativada por padrão.

Regra padrão	Descrição
	Enquanto a regra padrão especifica a gravação baseada em detecção de movimento, ela não garante que o sistema grava vídeo, porque você pode ter gravação desativada de câmeras individuais para uma ou mais câmeras. Mesmo que você ativou a gravação, lembre-se que a qualidade das gravações pode ser afetada por configurações de gravação da câmera individual.
Gravar a pedido	Garante que o vídeo seja gravado automaticamente quando ocorrer um pedido externo, contanto que a gravação esteja ativada para as câmeras relevantes. A gravação está ativada por padrão. O pedido é sempre acionado por um sistema de integração externa com o seu sistema, e a regra é usada principalmente por integradores de sistemas externos ou plug-ins.
Começar a alimentação de áudio	Garante que as alimentações de áudio de todos os microfones e alto-falantes conectados sejam alimentadas automaticamente para o sistema. Enquanto a regra padrão permite o acesso a alimentações de áudio dos microfones e alto-falantes conectados imediatamente após a instalação do sistema, ela não garante que o áudio seja gravado, porque você deve especificar as configurações de gravação separadamente.
Começar a alimentação	Garante que as alimentações de vídeo de todas as câmeras conectadas são alimentadas automaticamente para o sistema. Enquanto a regra padrão permite o acesso a alimentações de vídeo de câmeras conectadas imediatamente após a instalação do sistema, ela não garante que o vídeo seja gravado, porque as configurações de gravação das câmeras devem ser especificadas separadamente.
Começar a alimentação de metadados	Garante que as alimentações de dados de todas as câmeras conectadas sejam alimentadas automaticamente para o sistema. Enquanto a regra padrão permite o acesso a alimentações de dados de câmeras conectadas imediatamente após a instalação do sistema, ela não garante que os dados sejam gravados, porque as configurações de gravação das câmeras devem ser especificadas separadamente.
Mostrar notificação de solicitação de acesso	Garante que todos os eventos de controle de acesso classificados como "Solicitação de Acesso" mostrarem uma notificação de pedido de acesso no XProtect Smart Client, a menos que a função de notificação esteja desativada no perfil do Smart Client.

Recriar regras padrão

Se você acidentalmente excluir qualquer uma das regras padrão, poderá recriá-las, digitando o seguinte conteúdo:

Regra padrão	Texto a inserir
Voltar ao Padrão quando o PTZ estiver concluído	Realize uma ação em Sessão PTZ manual interrompido para todas as câmeras Mude imediatamente para a predefinição padrão no dispositivo em que o evento ocorreu
Reproduzir áudio mediante pedido	Executar uma ação a Pedido de reprodução de mensagem de áudio externo Reproduzir mensagem de áudio dos metadados nos dispositivos dos metadados com prioridade 1
Gravar no marcador	Execute uma ação no marcador Referência solicitada de todas as câmeras, todos os microfones, todos os alto-falantes para começar a gravar três segundos antes do dispositivo no qual ocorreu o evento Execute a ação de 30 segundos após parar a gravação imediatamente
Gravar em movimento	Execute uma ação em Movimento iniciado de todas as câmeras para começar a gravar três segundos antes do dispositivo no qual ocorreu o evento Execute uma ação de parada em Movimento interrompido de todas as câmeras para a gravação três segundos após o movimento
Gravar a pedido	Realize uma ação em Solicitar o início da gravação da gravação de início externo imediatamente nos dispositivos a partir de metadados Realize ação para parar em Solicitar a interrupção da gravação de gravação de interrupção externa imediatamente
Começar a alimentação de áudio	Realizar uma ação em um intervalo de tempo sempre inicia alimentação em todos os microfones e todos os alto-falantes Realizar uma ação quando um intervalo de tempo termina interrompe a alimentação imediatamente
Começar a alimentação	Realizar uma ação em um intervalo de tempo sempre inicia alimentação em todas as câmeras

Regra padrão	Texto a inserir
	Realizar uma ação quando um intervalo de tempo termina interrompe a alimentação imediatamente
Começar a alimentação de metadados	Realizar uma ação em um intervalo de tempo sempre inicia alimentação em todos os metadados Realizar uma ação quando um intervalo de tempo termina interrompe a alimentação imediatamente
Mostrar notificação de solicitação de acesso	Executar uma ação no pedido de acesso (Categorias de Controle de Acesso) dos sistemas [+ unidades] Mostrar notificação de solicitação de acesso embutida

Perfis de notificação (nó Regras e eventos)

Especifique as seguintes propriedades para os perfis de notificação:

Componente	Exigência
Nome	Digite um nome descritivo para o perfil de notificação. O nome aparece mais tarde sempre que você selecionar o perfil de notificação durante o processo de criação de uma regra.
Descrição (opcional)	Digite uma descrição para o perfil de notificação. A descrição aparece quando você pausa o ponteiro do mouse sobre o perfil de notificação no painel Visão geral na lista de **Perfis de notificação**.
Destinatário	Digite os endereços de e-mail aos quais a notificação do e-mail do perfil de notificações devem ser enviadas. Para digitar mais de um endereço de e-mail, separe os endereços por ponto-e-vírgula. Exemplo: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
Assunto	Digite o texto que você quer que apareça no assunto da notificação de e-mail. Você pode inserir variáveis de sistema, como **Nome do dispositivo**, no campo de texto de assunto e mensagem. Para inserir variáveis, clique nos links variáveis desejados na

Componente	Exigência
	caixa abaixo do campo.
Texto da mensagem	Digite o texto que você quer que apareça no corpo dos e-mails de notificações. Além do texto da mensagem, o corpo de cada notificação por e-mail automaticamente contém esta informação: • O que aciona o e-mail de notificação • A fonte de qualquer imagem estática anexada ou videoclipes AVI
Tempo entre emails	Especifique o tempo mínimo (em segundos) desejado entre o envio de cada e-mail de notificação. Exemplos: • Se for especificado um valor de **120**, um mínimo de 2 minutos se passará entre o envio de cada email de notificação, mesmo se o perfil de notificação for acionado novamente por uma regra antes que 2 minutos tenham se passado • Se for especificado um valor **0**, emails de notificações serão enviados a cada vez que o perfil de notificação for acionado por uma regra. Isto pode, potencialmente, resultar em um número muito grande de emails de notificação sendo enviados. Se usar o valor **0**, você deve, portanto, considerar cuidadosamente se quer usar o perfil de notificação nas regras que você aciona com frequência
Número de imagens	Especifique o número máximo de imagens estáticas que você quer incluir em cada notificação de perfil de e-mails de notificação. O padrão é cinco imagens.
Tempo entre imagens (ms)	Especifique o número de milissegundos que você quer entre as gravações apresentadas nas imagens incluídas. Exemplo: Com o valor padrão de 500 milissegundos, as imagens incluídas mostram gravações com meio segundo entre elas.
Tempo antes do evento (seg)	Esta configuração é usada para especificar o início de um arquivo AVI. Por padrão, o arquivo AVI contém gravações de 2 segundos antes que o perfil de notificação seja disparado. Você pode mudar isso para o número de segundos que você necessitar.
Tempo após o evento (seg)	Esta configuração é usada para especificar o término de um arquivo AVI. Por padrão, o arquivo AVI terminará 4 segundos depois que o perfil de notificação for disparado. Você pode mudar isso para o número de segundos que você necessitar.
Taxa de quadros	Especifique a número de quadros por segundo que você deseja que o arquivo AVI contenha. O padrão é cinco quadros por segundo. Quanto maior a taxa de quadros,

Componente	Exigência
	maior a qualidade da imagens e o tamanho do arquivo AVI.
Inserir imagens no e-mail	Se selecionado (padrão), imagens são inseridas no corpo dos e-mails de notificações. Se não, imagens são incluídas nos e-mails de notificações como arquivos anexados.

Visão geral de Eventos

Ao adicionar uma regra com base em um evento no assistente **Gerenciar regra**, você pode escolher entre uma série de tipos de eventos diferentes. Para que você tenha uma boa visão geral, eventos selecionáveis são relacionados em grupos de acordo com o que são:

Hardware:

Alguns hardware podem criar eventos eles mesmos, por exemplo, para detectar movimento. Você pode usá-los como eventos, mas deve configurá-los no hardware antes de poder usá-los no sistema. Só é possível usar os eventos relacionados em alguns hardwares já que nem todos os tipos de câmeras podem detectar adulteração ou mudanças de temperatura.

Hardware - Eventos configuráveis:

Eventos configuráveis por hardware são importados automaticamente dos drivers de dispositivos. Isto significa que variam de hardware para hardware e não são documentados aqui. Eventos configuráveis não são acionados até terem sido adicionados ao sistema e configurados na guia **Eventos** de hardware. Alguns dos eventos configuráveis também exigem que você configure a câmera (hardware) em si.

Hardware - Eventos pré-definidos:

Evento	Descrição
Erro de comunicação (hardware)	Ocorre quando uma conexão com um hardware é perdida.
Comunicação iniciada (hardware)	Ocorre quando a comunicação com um dispositivo é estabelecida com sucesso.
Comunicação interrompida (hardware)	Ocorre quando a comunicação com um dispositivo é interrompida com sucesso.

Dispositivos - Eventos configuráveis:

Os eventos configuráveis dos dispositivos são importados automaticamente dos drivers respectivos. Isto significa que variam de dispositivo para dispositivo e não são documentados aqui. Eventos configuráveis não são acionados até terem sido adicionados ao sistema e configurados na guia **Eventos** do dispositivo.

Dispositivos - Eventos pré-definidos:

Evento	Descrição
Referência de marcador solicitada	Ocorre quando um marcador é feito nos clientes no modo ao vivo. Além disso, um requisito para usar a Regra de gravação padrão em marcador.
Erro de comunicação (dispositivo)	Ocorre quando se perde conexão com um dispositivo ou quando há tentativa de comunicação com um dispositivo e essa tentativa não obtém sucesso.
Comunicação iniciada (dispositivo)	Ocorre quando a comunicação com um dispositivo é estabelecida com sucesso.
Comunicação interrompida (dispositivo)	Ocorre quando a comunicação com um dispositivo é interrompida com sucesso.
Proteção de evidências alterado	Ocorre quando uma proteção de evidências é alterada em dispositivos por um usuário do cliente ou através do MIP SDK.
Evidência protegida	Ocorre quando uma proteção de evidências é criada em um dispositivo por um usuário do cliente ou através do MIP SDK.
Evidência desprotegida	Ocorre quando uma proteção de evidências é removida para dispositivos por um usuário do cliente ou através do MIP SDK.
Estouro de alimentação iniciado	Estouro de alimentação (estouro de mídia) ocorre quando um servidor de gravação não consegue processar o vídeo recebido tão rapidamente quanto especificado na configuração e, portanto, é forçado a descartar algumas gravações.

Evento	Descrição
	Se o servidor estiver saudável, estouro de alimentação normalmente acontece por uma baixa leitura do disco. Pode ser resolvido tanto reduzindo a quantidade de dados sendo gravados quanto melhorando a performance do armazenamento do sistema. Reduza a quantidade de dados gravados reduzindo a taxa de quadros, a resolução ou a qualidade da imagem nas câmeras, mas isso pode degradar a qualidade da gravação. Se você não estiver interessado em fazer isso, você pode melhorar a performance do armazenamento do sistema instalando drives extras para compartilhar o carregamento ou instalando controladores de disco mais rápidos. Esse evento pode ser usado para disparar ações que ajudem a evitar o problema, p. ex., reduzir a taxa de quadros de gravação.
Estouro de alimentação parado	Ocorre quando o estouro de feed termina (consulte Estouro de alimentação iniciado na página 498).
Alimentação ao vivo de cliente solicitada	Ocorre quando os usuários do cliente solicitam uma transmissão ao vivo de um dispositivo. O evento ocorre por solicitação, mesmo se a solicitação do usuário de cliente subsequentemente não ocorrer com sucesso, por exemplo, porque o usuário do cliente não tem as permissões necessárias para visualizar a alimentação em tempo real solicitada ou porque a alimentação por algum motivo foi interrompida.
Alimentação ao vivo de cliente encerrada	Ocorre quando os usuários do cliente não mais solicitam uma transmissão ao vivo de um dispositivo.
Gravação manual iniciada	Ocorre quando um usuário cliente inicia a sessão de gravação de uma câmera. O evento é acionado, mesmo se o dispositivo já esteja gravando por meio de regras.
Gravação manual parada	Ocorre quando um usuário cliente para a sessão de gravação de uma câmera. Se o sistema de regras também começou uma sessão de gravação, esta prosseguirá mesmo após a parada da gravação manual.
Referência de dados marcada solicitada	Ocorre quando uma proteção de evidências é feita em modo de reprodução no do cliente ou através o MIP SDK.

Evento	Descrição
	Um evento que pode ser usado em suas regras é criado.
Movimento iniciado	Ocorre quando o sistema detecta movimento em vídeo recebido de câmeras. Este tipo de evento requer que a detecção de movimento do sistema seja habilitada nas câmeras para as quais o evento está vinculado. Além da detecção de movimento do sistema, algumas câmeras podem detectar movimento por si próprias e acionar o evento **Movimento iniciado (HW)**, mas isso depende da configuração do hardware da câmera e no sistema. Consulte também Hardware - Eventos configuráveis: na página 497.
Movimento interrompido	Ocorre quando um movimento não é mais detectado em um vídeo recebido. Consulte também Movimento iniciado na página 500. Este tipo de evento requer que a detecção de movimento do sistema seja habilitada nas câmeras para as quais o evento está vinculado. Além da detecção de movimento do sistema, algumas câmeras podem detectar movimento por si próprias e acionar o evento Movimento Interrompido (HW), mas isso depende da configuração do hardware da câmera e no sistema. Consulte também Hardware - Eventos configuráveis: na página 497.
Saída ativada	Ocorre quando a porta de saída externa de um dispositivo é ativada. Este tipo de evento requer que pelo menos um dispositivo em seu sistema suporte portas de saída.
Saída alterada	Ocorre quando a porta de saída externa de um dispositivo é alterada. Este tipo de evento requer que pelo menos um dispositivo em seu sistema suporte portas de saída.
Saída desativada	Ocorre quando a porta de saída externa de um dispositivo é desativada. Este tipo de evento requer que pelo menos um dispositivo em seu sistema suporte portas de saída.
Sessão PTZ manual iniciada	Ocorre quando sessão PTZ operada manualmente (em oposição a uma sessão PTZ baseada em patrulha programada ou ativada automaticamente por um evento) é iniciada em uma câmera. Este tipo de evento exige que as câmeras à quais os eventos estarão conectados

Evento	Descrição
	sejam câmeras PTZ.
Sessão PTZ manual parada	Ocorre quando sessão PTZ operada manualmente (em oposição a uma sessão PTZ baseada em patrulha programada ou ativada automaticamente por um evento) é interrompida em uma câmera. Este tipo de evento exige que as câmeras à quais os eventos estarão conectados sejam câmeras PTZ.
Gravação iniciada	Ocorre sempre que a gravação é iniciada. Há um evento separado para o início de gravação manual.
Gravação parada	Ocorre sempre que a gravação é interrompida. Há um evento separado para a interrupção de gravação manual.
Configurações alteradas	Ocorre quando as configurações em um dispositivo são alteradas com sucesso.
Erro de alteração de configurações	Ocorre quando há tentativa de alterar as configurações em um dispositivo e essa tentativa não obtém sucesso.

Eventos externos - Eventos pré-definidos:

Evento	Descrição
Solicitar reprodução de mensagem de áudio	Ativado quando reproduzir mensagens de áudio são solicitadas por meio do MIP SDK. Através do MIP SDK, um fornecedor terceirizado pode desenvolver plug-ins personalizados (por exemplo, integração a sistemas de controle de acesso externo ou semelhante) para o seu sistema.
Solicitar início da gravação	Ativado quando o início da gravação é solicitado por MIP SDK. Através do MIP SDK, um fornecedor terceirizado pode desenvolver plug-ins personalizados (por exemplo, integração a sistemas de controle de acesso externo ou semelhante) para o seu sistema.

Evento	Descrição
Solicitar parada da gravação	Ativado quando a interrupção da gravação é solicitada por MIP SDK. Através do MIP SDK, um fornecedor terceirizado pode desenvolver plug-ins personalizados (por exemplo, integração a sistemas de controle de acesso externo ou semelhante) para o seu sistema.

Eventos externos - Eventos genéricos:

Os eventos genéricos permitem desencadear ações no sistema, enviando sequências simples através da rede IP para o sistema. O objetivo dos eventos genéricos é permitir que o maior número possível de fontes externas interaja com o sistema.

Eventos externos - Eventos definidos pelo usuário:

Um número de eventos personalizados feitos para adequar seu sistema podem também ser escolhidos. Você pode usar esses eventos definidos pelo usuário para:

- Tornar possível a usuários de clientes ativar manualmente eventos enquanto visualizando vídeo em tempo real no cliente
- Inúmeros outros propósitos. Por exemplo, você pode criar eventos definidos por usuário que ocorrerão se um tipo de dado em particular for recebido de um dispositivo

  Consulte também Eventos definidos pelo usuário (explicado) na página 85.

Servidores de gravação:

Evento	Descrição
Arquivo disponível	Ocorre quando um arquivo para o servidor de gravação fica disponível depois de ter ficado indisponível. Consulte também Arquivo indisponível na página 502.
Arquivo indisponível	Ocorre quando um arquivo para o servidor de gravação fica indisponível, por exemplo, se a conexão com um arquivo localizado em uma unidade de rede é perdida. Nesses casos, você não pode arquivar gravações. Você pode usar o evento para, por exemplo, ativar um perfil de notificação para ativar um alarme ou perfil de notificação seja automaticamente enviado para as

Evento	Descrição
	pessoas relevantes de sua organização.
Arquivo Não Finalizado	Ocorre quando um arquivo de um servidor de gravação não é finalizado com a última rodada de arquivamento quando a próxima está agendada para começar.
Banco de Dados Excluindo Gravações Antes de Configurar o Tamanho de Retenção	Ocorre quando o limite de tempo de retenção é atingido antes do limite de tamanho do banco de dados.
Banco de Dados Excluindo Gravações Antes de Configurar o Tempo de Retenção	Ocorre quando o limite de tamanho do banco de dados é atingido antes do limite de tempo de retenção.
Disco do banco de dados cheio - Autoarquivamento	Ocorre quando um disco de banco de dados está cheio. Um disco de banco de dados está cheio quando ele tem menos de 5GB de espaço livre: Os dados mais antigos no banco de dados sempre são auto-arquivados (ou excluídos se nenhum arquivamento seguinte for definido) quando houver menos de 5GB de espaço livre.
Disco do banco de dados cheio - Excluindo	Ocorre quando um disco de banco de dados está cheio e tem menos de 1GB de espaço livre. Os dados são excluídos mesmo se um próximo arquivo for definido. Um banco de dados sempre requer 250MB de espaço livre. Se este limite é atingido (se o dado não é apagado rápido o suficiente), nenhum dado a mais será escrito no banco de dados até que se tenha liberado espaço suficiente. O tamanho máximo real de seu banco de dados é a quantidade de gigabytes especificada, menos 5GB.
Banco de dados cheio - autoarquivamento	Ocorre quando um arquivo de um servidor de gravação está cheio e precisa auto arquivar para um arquivo na unidade de armazenamento.
Reparo do banco de dados	Ocorre se um banco de dados torna-se corrompido, nesse caso o sistema tentará automaticamente dois métodos diferentes de reparação do banco de dados: um reparo rápido e um reparo completo.
Armazenamento de	Ocorre quando um armazenamento para o servidor de gravação fica disponível

Evento	Descrição
banco de dados disponível	depois de ter ficado indisponível. Consulte também Armazenamento de banco de dados indisponível na página 504. Você pode, por exemplo, usar o evento para iniciar a gravação se tiver sido interrompida por um evento **Armazenamento de banco de dados indisponível**.
Armazenamento de banco de dados indisponível	Ocorre quando o armazenamento do servidor de gravação fica indisponível, por exemplo, se a conexão armazenamento localizado em uma unidade de rede é perdida. Nesses casos, você não pode arquivar gravações. Você pode usar o evento para, por exemplo, interromper gravação e ativar um alarme ou perfil de notificação para que uma notificação de email seja automaticamente enviada para as pessoas relevantes de sua organização.
Erro de comunicação criptografada de emergência	Ocorre quando há um erro de comunicação entre o servidor de emergência SSL e os servidores de gravação monitorados.
Recuperação de falha iniciada	Ocorre quando um servidor de gravação de failover assume o controle de um servidor de gravação. Consulte também Servidores de Failover (nó).
Recuperação de falha parada	Ocorre quando um servidor de gravação torna-se disponível novamente e é capaz de reassumir o controle de um servidor do sistema de gravação ininterrupta.

Eventos do monitor do sistema

Eventos do monitor do sistema são acionados pelos valores de limites excedidos configurados no nó **Limites do Monitor do Sistema**. Consulte também Ver estado atual do hardware e resolver problemas, se necessário na página 304.

Esta funcionalidade exige que o serviço Data Collector esteja sendo executado.

Monitor do Sistema - Servidor:

Evento	Descrição
Estado crítico do uso de CPU	Ocorre quando o uso de CPU excede o limite crítico de CPU.
Estado normal do uso de CPU	Ocorre quando o uso de CPU cai abaixo do limite de CPU de aviso.
Estado de advertência do uso de CPU	Ocorre quando o uso de CPU excede o limite de CPU de aviso ou cai abaixo do limite crítico de CPU.
Estado crítico do uso da memória	Ocorre quando o uso da memória excede o limite crítico da memória.
Estado normal do uso da memória	Ocorre quando o uso da memória cai abaixo do limite da memória de aviso.
Estado de advertência do uso da memória	Ocorre quando o uso da memória excede o limite da memória de aviso ou cai abaixo do limite crítico da memória.
Decodificação NVIDIA crítica	Ocorre quando o uso da decodificação NVIDIA excede o limite crítico da decodificação NVIDIA.
Decodificação NVIDIA normal	Ocorre quando o uso da decodificação NVIDIA cai abaixo do limite da decodificação NVIDIA de aviso.
Aviso de decodificação NVIDIA	Ocorre quando o uso da decodificação NVIDIA excede o limite da decodificação NVIDIA de aviso ou cai abaixo do limite crítico da decodificação NVIDIA.
Memória NVIDIA crítica	Ocorre quando o uso da memória NVIDIA excede o limite crítico da memória NVIDIA.
Memória NVIDIA normal	Ocorre quando o uso da memória NVIDIA cai abaixo do limite da memória de aviso NVIDIA.
Aviso de memória NVIDIA	Ocorre quando o uso da memória NVIDIA excede o limite da memória NVIDIA de aviso ou cai abaixo do limite crítico da memória NVIDIA.

Evento	Descrição
Renderização NVIDIA crítica	Ocorre quando o uso de renderização NVIDIA excede o limite crítico da renderização NVIDIA.
Renderização NVIDIA normal	Ocorre quando o uso da renderização NVIDIA cai abaixo do limite da renderização NVIDIA de aviso.
Aviso de renderização NVIDIA	Ocorre quando o uso da renderização NVIDIA excede o limite da renderização NVIDIA de aviso ou cai abaixo do limite crítico da renderização NVIDIA.
Estado crítico do serviço disponível	Ocorre quando um serviço de servidor para de ser executado. Não há valores-limite para este evento.
Estado normal do serviço disponível	Ocorre quando um serviço de servidor é alterado para execução. Não há valores-limite para este evento.

Monitor do Sistema - Câmera:

Evento	Descrição
Estado críticos de quadros por segundo ao vivo	Ocorre quando a taxa de FPS ao vivo cai abaixo do limite crítico de FPS ao vivo.
Estado Normal de Quadros por Segundo ao Vivo	Ocorre quando a taxa de FPS ao vivo excede o limite de aviso de FPS ao vivo.
Estado de advertência de quadros por segundo ao vivo	Ocorre quando a taxa de FPS ao vivo cai abaixo do limite de aviso de FPS ao vivo ou excede o limite crítico de FPS ao vivo.
Estado crítico de quadros por segundo	Ocorre quando a taxa de gravação FPS ao vivo cai abaixo do limite crítico de gravação FPS.

Evento	Descrição
Estado normal do registro de quadros por segundo	Ocorre quando a taxa de gravação FPS excede o limite de aviso de gravação FPS.
Estado de advertência do registro de quadros por segundo	Ocorre quando a taxa de gravação FPS cai abaixo do limite de aviso de gravação FPS ou excede o limite crítico de gravação FPS.
Estado crítico do espaço utilizado	Ocorre quando o armazenamento usado para gravações por uma câmera específica excede o limite de espaço crítico usado.
Estado normal do espaço utilizado	Ocorre quando o armazenamento usado para gravações por uma câmera específica cai abaixo do limite de espaço de aviso usado.
Estado de advertência do espaço utilizado	Ocorre quando o armazenamento usado para gravações por uma câmera específica excede o limite de espaço de aviso usado ou cai abaixo do limite de espaço crítico usado.

Monitor do Sistema - Disco:

Evento	Descrição
Estado crítico do espaço livre	Ocorre quando o uso do espaço no disco excede o limite crítico de espaço livre.
Estado normal do espaço livre	Ocorre quando o uso do espaço no disco cai abaixo do limite de espaço livre de aviso.
Estado de advertência do espaço livre	Ocorre quando o uso do espaço de disco excede o limite de espaço livre de aviso ou cai abaixo do limite crítico de espaço livre.

Monitor do Sistema - Armazenamento:

Evento	Descrição
Estado Crítico do Tempo de Retenção	Ocorre quando o sistema prevê que o armazenamento será preenchido de forma mais rápida do que o valor do limite crítico de tempo de retenção. Por exemplo, quando dados provenientes de fluxos de vídeo estão enchendo o armazenamento mais rápido do que o esperado.
Estado Normal do Tempo de Retenção	Ocorre quando o sistema prevê que o armazenamento será preenchido de forma mais lenta do que o valor do limite de aviso de tempo de retenção. Por exemplo, quando dados provenientes de fluxos de vídeo estão enchendo o armazenamento na taxa esperada.
Estado de advertência do tempo de retenção	Ocorre quando o sistema prevê que o armazenamento será preenchido de forma mais rápida do que o valor do limite de aviso de tempo de retenção ou mais lento do que o valor do limite crítico de tempo de retenção. Por exemplo, quando os dados dos fluxos de vídeo estão enchendo o armazenamento mais rápido do que o esperado devido a mais movimento detectado pelas câmeras configuradas para gravar em movimento.

Outros:

Evento	Descrição
A ativação automática da licença falhou	Ocorre quando a ativação da licença automática online falha. Não há valores-limite para este evento.
Alteração de senha agendada iniciada	Ocorre quando uma alteração de senha agendada inicia.
Alteração de senha agendada concluída com sucesso	Ocorre quando uma alteração de senha agendada é concluída sem erros.
Alteração de senha agendada concluída com erros	Ocorre quando uma alteração de senha agendada é concluída com erros.

Eventos de extensões e integrações do XProtect:

É possível usar eventos de extensões e integrações do XProtect no sistema de regras, por exemplo:

- Eventos analíticos também podem ser usados no sistema de regras

Ações e ações de interrupção

Um conjunto de ações e ações de parada estão disponíveis para a criação de regras no assistente **Gerenciar regra**. Você pode ter mais ações disponíveis se a instalação do sistema usar extensões XProtect ou plug-ins específicos do fornecedor. Para cada tipo de ação, informações da ação de parada estão relacionadas, caso sejam relevantes.

Assistente de gerenciamento de regras

Ação	Descrição
Iniciar gravação em <dispositivos>	Começa a gravar e salvar os dados no banco de dados dos dispositivos selecionados. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você especifique: Quando a gravação deve ter início. Imediatamente ou um número de segundos antes do evento/começo do intervalo de tempo de ativação, bem como em quais dispositivos a ação deve ser efetuada. Este tipo de ação requer que a gravação seja habilitada nos dispositivos aos quais a ação está conectada. Você só poderá salvar dados antes de um evento ou intervalo de tempo se você tiver habilitado o pré-buffer para os dispositivos relevantes. Você permite a gravação e especifica as configurações de pré-carregamento para um dispositivo na guia **Gravação**. **Interromper ação solicitada**: Esse tipo de ação requer um ou mais ações de parar. Em uma das seguintes etapas, o assistente automaticamente solicitará que você especifique a ação de parar: **Parar a gravação**. Sem esta ação de interrupção, a gravação continuaria por tempo indeterminado. Você também tem a opção de especificar mais ações de interrupção.
Iniciar alimentação em <dispositivos>	Comece a alimentação de dados a partir de dispositivos ao sistema. Quando a alimentação de um dispositivo é iniciada, os dados são transferidos do dispositivo ao sistema. Nesse caso, a visão e a gravação são possíveis dependendo do tipo de dados. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** pedirá que você

Ação	Descrição
	especifique. Seu sistema tem uma regra padrão que garante que as alimentações sejam sempre iniciadas em todas as câmeras. **Interromper ação solicitada**: Esse tipo de ação requer um ou mais ações de parar. Em uma das seguintes etapas, o assistente automaticamente solicitará que você especifique a ação de parar: **Parar a alimentação**. Você também pode especificar outras ações de parada. O uso da ação de interrupção obrigatória **Interromper alimentação** para interromper a ação de um dispositivo significa que os dados não serão mais transferidos do dispositivo para o sistema, nesse caso a visualização ao vivo e a gravação do vídeo, p. ex., não serão mais possíveis. Entretanto, um dispositivo em que você parou a alimentação ainda pode se comunicar com o servidor de gravação e você pode começar a alimentação do dispositivo automaticamente através de uma regra, ao contrário de quando o dispositivo foi desativado manualmente. ⚠ Embora este tipo de ação permita o acesso às alimentações de dados dos dispositivos selecionados, isso não garante que os dados sejam gravados porque as configurações de gravação devem ser especificadas separadamente.
Configurar <Smart Wall> para <predefinição>	Define o XProtect Smart Wall para uma predefinição selecionada. Especifique a predefinição na guia **Smart Wall Predefinições**. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Configurar o <monitor> de <Smart Wall> para exibir <câmeras>	Define um monitor específico XProtect Smart Wall para exibir vídeo ao vivo a partir das câmeras selecionadas neste site ou em qualquer site filho configurado em Milestone Federated Architecture. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Definir o <Smart Wall> <monitor> para exibir <mensagens> de	Define um monitor XProtect Smart Wall específico para exibir uma mensagem de texto definida pelo usuário de até 200 caracteres. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de

Ação	Descrição
texto	parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Remover <câmeras> do monitor <Smart Wall> <monitor>	Interromper a exibição de vídeo de uma câmera específica. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Definir taxa de quadros ao vivo em <dispositivos>	Fixa uma taxa de quadros particular para ser usada quando o sistema exibe vídeo em tempo real a partir de câmeras selecionadas que substituem a taxa de quadros padrão das câmeras. Especifique isso na guia **Configurações**. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você especifique a taxa de quadros e em quais dispositivos. Sempre verifique se a taxa de quadros que você especifica está disponível nas câmeras em questão. **Interromper ação solicitada**: Esse tipo de ação requer um ou mais ações de parar. Em uma das seguintes etapas, o assistente automaticamente solicitará que você especifique a ação de parar: **Restaurar a taxa de quadros em tempo real padrão**. Sem esta ação de interrupção, a taxa de quadros padrão nunca seria potencialmente restaurada. Você também tem a opção de especificar mais ações de interrupção.
Definir taxa de quadros de gravação em <dispositivos>	Fixa uma taxa de quadros específica para ser usada quando salvar vídeo gravado da câmera selecionada no banco de dados ao invés da taxa de quadros padrão das câmeras. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você especifique a taxa de quadros e em quais câmeras. Especificar taxa de quadros para gravação somente é possível para JPEG, um codec de vídeo que faz com que cada quadro seja comprimido separadamente em uma imagem JPEG. Este tipo de ação requer que a gravação esteja habilitada nos dispositivos aos quais a ação está conectada. Você permite a gravação para uma câmera na guia **Gravação**. A taxa de quadros máxima que pode ser especificada depende do tipo da câmera e da resolução de imagem selecionada. **Interromper ação solicitada**: Esse tipo de ação requer um ou mais ações de parar. Em uma das seguintes etapas, o assistente automaticamente solicitará que você especifique a ação de parar: **Restaurar a taxa de quadros de gravação padrão**. Sem esta ação de interrupção, a taxa de quadros de gravação padrão nunca seria

Ação	Descrição
	potencialmente restaurada. Você também tem a opção de especificar mais ações de interrupção.
Defina a taxa de quadros de gravação para todos os quadros para MPEG-4/H.264/H.265 em <dispositivos>	Define a taxa de quadros para gravar todos os frames quando o sistema salva o vídeo gravado a partir das câmeras selecionadas no banco de dados, em vez de apenas frames-chave. Habilitar a função gravação de frame-chave apenas na guia **Gravação**. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** pedirá que você especifique em quais dispositivos a ação deverá ser aplicada. Você só pode ativar a gravação de frames-chave para MPEG-4/H.264/H.265. Este tipo de ação requer que a gravação esteja habilitada nos dispositivos aos quais a ação está conectada. Você permite a gravação para uma câmera na guia **Gravação**. **Interromper ação solicitada**: Esse tipo de ação requer um ou mais ações de parar. Em uma das seguintes etapas, o assistente automaticamente solicitará que você especifique a ação de parar: **Restaurar padrão da taxa de quadros de gravação de frames-chave para MPEG-4/H.264/H.265** Sem esta ação de interrupção, a taxa de quadros padrão poderia nunca ser restaurada. Você também tem a opção de especificar mais ações de interrupção.
Iniciar patrulha no <dispositivo> usando <profile> com prioridade PTZ <prioridade>	Começa a patrulha PTZ de acordo com um perfil de patrulha específico em uma câmera PTZ específica com uma prioridade específica. Esta é a definição exata de como a patrulha deve ser realizada, incluindo a sequência de posições pré-definidas, configurações de tempo etc. Se o seu sistema foi atualizado de uma versão mais antiga, os valores antigos (**Muito baixo**, **Baixo**, **Médio**, **Alto** e **Muito alto**) foram ajustados como se segue: • Muito baixo = 1 000 • Baixo = 2 000 • Médio = 3 000 • Alto = 4 000 • Muito alto = 5 000 Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você selecione um perfil de patrulha. Somente pode ser selecionado um perfil de patrulha por dispositivo; não é possível selecionar diversos perfis de patrulha.

Ação	Descrição
	 Este tipo de evento exige que os dispositivos aos quais a ação estará conectada sejam dispositivos PTZ.  Pelo menos um perfil de patrulhamento deve ser definido para o(s) dispositivo(s). Você define os perfis de patrulhamento para uma câmera PTZ na guia **Patrulhamento**. **Interromper ação solicitada**: Esse tipo de ação requer um ou mais ações de parar. Em uma das seguintes etapas, o assistente automaticamente solicitará que você especifique a ação de parar: **Parar patrulha** Sem esta ação de interrupção, o patrulhamento nunca iria parar. Você também pode especificar outras ações de parada.
Pausar patrulha em <dispositivos>	Pausa a patrulha PTZ. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** pedirá que você especifique os dispositivos nos quais a patrulha deverá ser interrompida.  Este tipo de evento exige que os dispositivos aos quais a ação estará conectada sejam dispositivos PTZ.  Pelo menos um perfil de patrulhamento deve ser definido para o(s) dispositivo(s). Você define os perfis de patrulhamento para uma câmera PTZ na guia **Patrulhamento**. **Interromper ação solicitada**: Esse tipo de ação requer um ou mais ações de parar. Em uma das seguintes etapas, o assistente automaticamente solicitará que você especifique a ação de parar: **Continuar patrulha** Sem esta ação de interrupção, a patrulha iria pausar indefinidamente. Você também tem a opção de especificar mais ações de interrupção.

Ação	Descrição
Mover o <dispositivo> para a posição <predefinição> com prioridade PTZ <prioridade>	Mova uma câmera em particular para uma posição pré-definida – no entanto, sempre de acordo com a prioridade. Quando selecionar este tipo de ação, o assistente de **Regra de gerenciamento** solicitará que você selecione uma posição predefinida. Apenas uma posição predefinida pode ser selecionada para uma câmera. Não é possível selecionar diversas posições predefinidas.  Este tipo de evento exige que os dispositivos aos quais a ação estará conectada sejam dispositivos PTZ.  Esta ação requer pelo menos uma posição predefinida seja definida para os dispositivos. Você define as posições predefinidas para uma câmera PTZ na guia **Predefinições**. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Mover para predefinição padrão em <dispositivos> com prioridade PTZ <prioridade>	Mova uma ou mais câmeras em particular para suas respectivas posições padrão predefinidas – no entanto, sempre de acordo com a prioridade. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** pedirá que você especifique em quais dispositivos a ação deverá ser aplicada.  Este tipo de evento exige que os dispositivos aos quais a ação estará conectada sejam dispositivos PTZ. Esta ação requer pelo menos uma posição predefinida seja definida para os dispositivos. Você define as posições predefinidas para uma câmera PTZ na guia **Predefinições**. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Definir saída do dispositivo como <estado>	Define uma saída em um dispositivo para um estado particular (ativado ou desativado). Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você especifique o estado a ser configurado e em quais dispositivos.

Ação	Descrição
	Este tipo de ação requer que cada um dos dispositivos aos quais a ação está conectada tenha pelo menos uma unidade de saída externa conectada a uma porta de saída. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Criar marcador no <dispositivo>	Criar um marcador em uma transmissão em tempo real ou gravações de um dispositivo selecionado. Um marcador torna fácil a revisão de um certo evento ou período de tempo. As configurações de marcadores são controladas a partir da caixa de diálogo **Opções**. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você especifique detalhes de marcadores e selecione um dispositivo. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Reproduzir áudio <mensagem> nos <dispositivos> com <prioridade>	Reproduz uma mensagem de áudio em dispositivos selecionados ativados por um evento. A maioria dos dispositivos são alto-falantes ou câmeras. Este tipo de ação requer que você tenha feito o upload da mensagem no sistema em **Ferramentas** > **Opções** > na guia **Mensagens de áudio**. Você pode criar mais regras para o mesmo evento e enviar mensagens diferentes para cada dispositivo, mas sempre de acordo com a prioridade. As prioridades que controlam a sequência são aquelas definidas na regra e no dispositivo para uma função na guia **Discurso**: • Se uma mensagem é reproduzida e outra mensagem com a mesma prioridade é enviada ao mesmo alto-falante, a primeira mensagem será completada e, então, a segunda começa • Se uma mensagem for reproduzida e outra mensagem com uma prioridade mais alta for enviada ao mesmo alto-falante, a primeira mensagem será interrompida e a segunda começará imediatamente
Enviar notificação para <perfil>	Envia uma notificação, usando uma notificação de perfil particular. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você selecione um perfil de notificação e quais dispositivos a partir dos quais as imagens de pré-alarme serão incluídas. Somente pode ser selecionado um perfil de notificação; não é possível selecionar diversos perfis de notificação. Um único perfil de notificação

Ação	Descrição
	pode conter diversos destinatários. Você também pode criar mais regras para o mesmo evento e enviar notificações diferentes para cada um dos perfis da notificação. Clicando com o botão direito do mouse em uma regra na lista de **Regras** você pode copiar e usar novamente o conteúdo das regras. Este tipo de ação requer que pelo menos um perfil de notificação tenha sido definido. Imagens de pré-alarme só são incluídas se a opção **Incluir imagens** foi habilitada no perfil de notificação em questão. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Criar nova <entrada de registro>	Gera uma entrada no registro de regras. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você especifique um texto para a entrada de registro. Quando especificar o texto do log, você pode inserir variáveis, tais como **$DeviceName$**, **$EventName$**, na mensagem de log. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Iniciar plug-in em <dispositivos>	Inicia um ou mais plug-ins. Quando você seleciona esse tipo de ação, o assistente de **Gerenciamento de regra** solicita que você selecione os plug-ins necessários e em quais dispositivos iniciar os plug-ins. Este tipo de ação requer que um ou mais plug-ins estejam instalados em seu sistema. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Parar plug-in em <dispositivos>	Interrompe um ou mais plug-ins. Quando você seleciona esse tipo de ação, o assistente de **Gerenciamento de regra** solicita que você selecione os plug-ins necessários e em quais dispositivos interromper os plug-ins. Este tipo de ação requer que um ou mais plug-ins estejam instalados em seu sistema. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de

Ação	Descrição
	parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Aplicar novas configurações a <dispositivos>	Altera as configurações do dispositivo em um ou mais dispositivos. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você selecione os dispositivos relevantes e possa definir as configurações desejadas nos dispositivos que especificou.  Ao definir configurações para mais de um dispositivo você somente poderá mudar as configurações que estão disponíveis para todos os dispositivos especificados. **Exemplo**: Você pode especificar que a ação deve estar conectada ao dispositivo 1 e dispositivo 2. O Dispositivo 1 tem configurações A, B e C e o Dispositivo 2 tem configurações B, C e D. Neste caso você somente poderá mudar as configurações disponíveis para ambos os dispositivos, i.e., as configurações B e C. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Definir a Matrix para a visualização <dispositivos>	Faz o vídeo das câmeras selecionadas ser mostrado em um computador capaz de exibir o vídeo acionado por Matrix, isto é, um computador no qual o XProtect Smart Client estiver instalado. Quando seleciona este tipo de ação, o assistente **Gerenciar regra** pedirá para selecionar um destinatário Matrix e um ou mais dispositivos de onde mostrar o vídeo do destinatário Matrix selecionado. Este tipo de ação permite a você selecionar somente um único recipiente Matrix por vez. Se você deseja fazer com que um vídeo dos dispositivos selecionados apareça em mais de um destinatário Matrix, deve criar uma regra para cada destinatário Matrix desejado ou usar o recurso do XProtect Smart Wall. Clicando com o botão direito do mouse em uma regra na lista de **Regras** é possível copiar e usar novamente o conteúdo das regras. Desta forma você pode evitar a criação de regras quase idênticas a partir do zero.

Ação	Descrição
	Como parte da configuração dos próprios destinatários Matrix, os usuários devem especificar o número da porta e a senha desejada para a comunicação Matrix. Certifique-se de que os usuários têm acesso à essa informação. Os usuários precisam também definir os endereços IP dos hosts permitidos, i.e., hosts dos quais comandos de exibição de vídeo ativados pelo Matrix serão aceitos. Nesse caso, os usuários também devem conhecer o endereço IP do servidor de gerenciamento ou qualquer roteador ou firewall usado.
Enviar interceptação SNMP	Gera uma pequena mensagem que registra eventos nos dispositivos selecionados. A mensagem de intercepção de SNMP é autogerada e não pode ser personalizada. Pode conter o tipo de fonte e o nome do dispositivo em que o evento ocorreu. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Recuperar e armazenar gravações remotas de <dispositivos>	Recupera e armazena gravações remotas a partir de dispositivos selecionados (que suporta gravação interna) em um período especificado antes e depois do evento acionador. Esta regra é independente da configuração **Recuperar automaticamente as gravações remotas quando a conexão for restaurada**. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Recuperar e arquivar gravações remotas entre <horário de início e término> de <dispositivos>	Recupera e armazena gravações remotas em um período especificado dos dispositivos selecionados (que suportam gravações internas). Esta regra é independente da configuração **Recuperar automaticamente as gravações remotas quando a conexão for restaurada**. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Salvar imagens	Assegura que quando uma imagem for recebida do evento Imagens Recebidas

Ação	Descrição
anexas	(enviado de uma câmera por e-mail SMTP) seja salva para uso futuro. No futuro, outros eventos podem também ativar esta ação. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Ativar arquivamento em <arquivos>	Iniciar arquivamento em um ou mais arquivos. Ao selecionar este tipo de ação, o assistente **Gerenciar Regra** solicitará que você selecione os arquivos desejados. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Ativar <evento definido pelo usuário> no <site>	Relevante principalmente no Milestone Federated Architecture, mas você também pode usar esta configuração em uma única configuração de site. Use a regra para ativar um evento definido pelo usuário em um site, normalmente um site remoto dentro de hierarquia federada. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Mostrar <notificação de solicitação de acesso>	Permite que as notificações de solicitação de acesso sejam mostradas (pop-up) na tela do XProtect Smart Client quando os critérios de disparo de eventos são cumpridos. Milestone recomenda que você use eventos de controle de acesso como eventos desencadeadores para esta ação. Isso ocorre porque notificações de solicitação de acesso geralmente são configuradas para operar em comandos de controle relacionados a acesso e em câmeras. Este tipo de ação requer que pelo menos um plug-in de acesso esteja instalado em seu sistema. **Nenhuma ação de interrupção obrigatória**: Esse tipo de ação não requer uma ação de parar.É possível especificar ações de parar opcionais para serem realizadas tanto em um evento quanto período de tempo.
Alterar a senha em dispositivos de hardware	Altera a senha em todos os dispositivos de hardware selecionados, para uma senha gerada aleatoriamente, baseada nos requisitos de senhas para o dispositivo de hardware específico. Para obter uma lista de dispositivos de hardware suportados, consulte Encontrar hardware.

Ação	Descrição
	Esta ação só está disponível quando você define uma regra usando o tipo de regra **Executar uma ação em um <recurring time>**. Os seguintes eventos estão disponíveis para a ação: • Alteração de senha agendada iniciada na página 508 • Alteração de senha agendada concluída com sucesso na página 508 • Alteração de senha agendada concluída com erros na página 508 O tipo de ação não tem uma ação de parar. Você pode ver o progresso dessa ação no nó **Tarefas atuais**. Para obter mais informações, consulte Visualizar tarefas em andamento nos servidores de gravação na página 301. Para ver os resultados da ação - vá para o nó **Registros do servidor**, na guia **Registros do sistema**. Para obter mais informações, consulte Guia Registros do servidor (opções) na página 397. Para obter mais informações, consulte Registros do sistema (guia).

Testar Evento de Análise (propriedades)

Quando você testa os requisitos de um evento de análise, aparece uma janela que verifica quatro condições e fornece descrições de erro e soluções possíveis.

Condição	Descrição	Mensagens de erro e Soluções
Alterações salvas	Se o evento é novo, ele foi salvo? Ou se há mudanças para o nome do evento, estas mudanças foram salvas?	**Salvar alterações antes de testar evento analítico**. Solução/Explicação: Salve as alterações.
Eventos de Análise	O recurso Eventos analíticos está ativado?	**Os eventos analíticos não foram ativados**. Solução/Explicação: Ativar o recurso Eventos

Condição	Descrição	Mensagens de erro e Soluções
ativado		Analíticos. Para fazer isso, clique em **Ferramentas** > **Opções** > **Eventos de Análise** e selecione a caixa de seleção **Ativado**.
Endereço permitido	É o endereço IP / nome do host do computador que envia o(s) evento(s) permitido (listado na lista de endereços dos eventos de análise)?	**O nome do host local deve ser adicionado como endereço permitido para o serviço de eventos analíticos**. Solução/Explicação: Adicionar seu computador à lista de endereços IP ou nomes de host permitidos para eventos de análise. **Erro ao resolver o nome do host local**. Solução/Explicação: O endereço IP ou o nome do host do computador não pode ser encontrado ou é inválido.
Enviar evento analítico	O envio de um evento teste para o servidor de eventos teve êxito?	Ver a tabela abaixo.

Cada etapa é marcada com qualquer falha: ❌ ou bem-sucedido: ✓.

Mensagens de erro e soluções para a condição **Enviar eventos analíticos**:

Mensagens de erro	Solução
Servidor de eventos não encontrado	Não é possível localizar o servidor de eventos na lista de serviços registrados.
Erro ao conectar ao servidor de eventos	Não é possível conectar ao servidor de eventos na porta referida. O erro ocorre provavelmente devido a problemas de rede ou o serviço Event Server parou.
Erro ao enviar evento de análise	A conexão com o servidor de eventos é estabelecida, mas o evento não pode ser enviado. O erro provavelmente ocorre devido a problemas de rede, por exemplo, um tempo limite.
Erro ao receber resposta do servidor de	O evento foi enviado para o servidor de eventos, mas não recebeu resposta. O erro provavelmente ocorre devido a problemas de rede ou uma porta que está

Mensagens de erro	Solução
eventos	ocupada. Consulte o registro do servidor de eventos, normalmente localizado em `ProgramData\Milestone\XProtect Event Server\Logs\`.
Evento analítico desconhecido pelo servidor de eventos	O serviço do Event Server não conhece o evento. O erro provavelmente ocorre porque o evento ou alterações ao evento não foram salvas.
Evento analítico inválido recebido pelo servidor de eventos	O formato do evento está incorreto.
Remetente não autorizado pelo servidor de eventos	O mais provável é que sua máquina não esteja na lista de endereços IP ou nome de host autorizados.
Erro interno no servidor de eventos	Erro no servidor de eventos. Consulte o registro do servidor de eventos, normalmente localizado em `ProgramData\Milestone\XProtect Event Server\Logs\`.
Resposta inválida recebida do servidor de eventos	A resposta é inválida. Possivelmente a porta está ocupada ou há problemas de rede. Consulte o registro do servidor de eventos, normalmente localizado em `ProgramData\Milestone\XProtect Event Server\Logs\`.
Resposta desconhecida do servidor de eventos	A resposta é válida, mas não compreendida. O erro ocorre possivelmente devido a problemas de rede ou a porta está ocupada. Consulte o registro do servidor de eventos, normalmente localizado em `ProgramData\Milestone\XProtect Event Server\Logs\`.
Erro inesperado	Entre em contato com o suporte Milestone para obter ajuda.

Eventos genéricos e fontes de dados (propriedades)

Este recurso funciona apenas se você tiver o servidor de eventos XProtect instalado.

Evento genérico (propriedades)

Componente	Exigência
Nome	Nome único para o evento genérico. O nome deve ser único entre todos os tipos de eventos, como, por exemplo, eventos definidos pelo usuário, eventos analítico, e assim por diante.
Ativado	Eventos genéricos são habilitados por padrão. Desmarque a caixa para desativar o evento.
Expressão	A expressão que o sistema deve procurar quando analisa os pacotes de dados. Você pode usar os seguintes operadores: • `( )`: Usado para assegurar que os termos relacionados são processados em conjunto, como uma unidade lógica. Eles podem ser usados para forçar uma determinada ordem de processamento na análise **Exemplo**: O critério de pesquisa `(Usuário001 OR Porta053) AND Domingo` processa primeiro os dois termos dentro dos parênteses e então combina o resultado com a última parte da cadeia de caracteres. Assim, o sistema procura primeiro os pacotes que contenham qualquer um dos termos `Usuário001` ou `Porta053`, em seguida, leva os resultados para executá-los, a fim de ver quais pacotes contêm também o termo `Domingo`. • `E`: Com um operador `AND`, você especifica que os termos nos dois lados do operador `AND` precisam estar presentes **Exemplo**: O critério de pesquisa `Usuário001 AND Porta053 AND Domingo` só retorna um resultado se os termos `Usuário001`, `Porta053` e `Domingo` estiverem todos incluídos na sua expressão. Não é suficiente só um ou dois dos termos estarem presentes. Quanto mais termos você reunir com E, menos resultados você recupera. • `OU`: Com um operador `OR`, você especifica que um ou outro termo precisa estar presente **Exemplo**: O critério de pesquisa `“Usuário001” OR “Porta053” OR “Domingo”` retorna qualquer resultado contendo `Usuário001`, `Porta053` ou `Domingo`. Quanto mais termos você combinar com `OR`, mais resultados você recuperará.
Tipo de expressão	Indica quão específico o sistema deve ser ao analisar pacotes de dados recebidos. As opções são as seguintes:

Componente	Exigência
	• **Busca**: Para que o evento ocorra, o pacote de dados recebidos deve conter o texto especificado no campo **Expressão**, mas também pode haver mais conteúdo **Exemplo**: Se você especificou que o pacote recebido deveria conter os termos `Usuário001` e `Porta053`, o evento será acionado se o pacote recebido contiver os termos `Usuário001` e `Porta053` e `Domingo`, já que os seus dois termos necessários estão contidos no pacote recebido • **Correspondência**: Para que o evento ocorra, o pacote de dados recebidos deve conter o texto exato especificado no campo **Expressão** e nada mais • **Expressão regular**: Para que o evento ocorra, o texto especificado no campo **Expressão:** precisa identificar padrões específicos nos pacotes de dados recebidos Se você mudar de **Pesquisar:** ou **Corresponder:** para **Expressão regular**, o texto no campo **Expressão** será automaticamente traduzido para uma expressão regular.
Prioridade	A prioridade precisa ser especificada como um número entre 0 (maior prioridade) e 999999 (menor prioridade). O mesmo pacote de dados pode ser analisado por eventos diferentes. A habilidade de atribuir uma prioridade a cada evento permite que você administre que evento deve ser ativado se um pacote recebido corresponder aos critérios de alguns eventos. Quando o sistema recebe um pacote TCP e/ou UDP, a análise do pacote começará com a análise do evento com a prioridade mais alta. Desta forma, quando um pacote corresponder aos critérios por alguns eventos, somente o evento com a prioridade mais alta será ativado. Se um pacote corresponder aos critérios por vários eventos com uma prioridade idêntica, p. ex., dois eventos com prioridade 999, todos os eventos com esta prioridade serão ativados.
Verifique se a expressão corresponde a sequência de eventos	Uma sequência de eventos a ser testada contra uma expressão inserida no campo **Expressão**.

Webhooks (nó de regras e eventos)

No nó **Webhooks**, você pode criar, editar e excluir pontos de extremidade de webhook.

Os seguintes campos estão disponíveis ao criar e editar webhooks:

Campo	Descrição
Nome	Insira um nome exclusivo do ponto de extremidade de webhook. O nome de webhook não pode estar vazio.
Endereço	O URL do servidor da web ou aplicativo para o qual você deseja enviar dados de eventos. Se o URL do servidor da web for atualizado, você deverá atualizar o webhook URL no nó webhook. O uso de HTTP através de redes não seguras (como internet aberta) expõe todos os eventos em texto simples.
Token	Insira um token que seja usado para ajudar a proteger a comunicação com outros aplicativos validando a origem do HTTP POST. Usar um token para proteger a comunicação é opcional, mas recomendado.
Versão da API	A versão do plug-in webhook e API utilizada para a funcionalidade webhook.

Nó de segurança

Funões (nó Segurança)

Aba Informações (funções)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Na aba **Informações** de uma função, você pode definir o seguinte:

Nome	Descrição
Nome	Digite um nome para a função.
Descrição	Digite uma descrição para a função.
Perfil do Management Client	Selecione um perfil Management Client para associar com a função. Não é possível aplicar isto à função **Administradores** padrão.  Requer permissões para gerenciar a segurança do servidor de gerenciamento.
Perfil do Smart Client	Selecione um perfil Smart Client para associar com a função.  Requer permissões para gerenciar a segurança do servidor de gerenciamento.
Perfil de tempo padrão	Selecione um perfil de tempo padrão para associar à função. Não é possível aplicar isto à função **Administradores** padrão.
Perfil de proteção de evidências	Selecione um perfil de proteção de evidências para associar à função.
Login no Smart Client dentro do perfil de tempo	Selecione um perfil de tempo para o qual o usuário XProtect Smart Client associado a essa função tenha permissão para entrar. Se o usuário XProtect Smart Client estiver conectado quando o prazo expirar, será automaticamente desconectado. Não é possível aplicar isto à função **Administradores** padrão.
Permitir o login em Smart Client	Selecione a caixa de seleção para permitir que os usuários associados a essa função efetuem login em XProtect Smart Client. O acesso ao Smart Client não é permitido por padrão. Desmarque a caixa de seleção para negar acesso ao XProtect Smart Client.
Permitir o login no	Selecione a caixa de seleção para permitir que os usuários associados a essa

Nome	Descrição
cliente XProtect Mobile	função efetuem login no cliente XProtect Mobile. O acesso ao cliente XProtect Mobile não é permitido por padrão. Desmarque a caixa de seleção para negar acesso ao cliente XProtect Mobile.
Permitir o login em XProtect Web Client	Selecione a caixa de seleção para permitir que os usuários associados a essa função efetuem login em XProtect Web Client. O acesso ao XProtect Web Client não é permitido por padrão. Desmarque a caixa de seleção para negar acesso ao XProtect Web Client.
Autorização de login necessária	Selecione a caixa de seleção para ativar as autorizações de login à função. Isso quer dizer que o XProtect Smart Client ou o Management Client solicita uma segunda autorização, normalmente por um super usuário ou administrador, quando o usuário fizer login. Para permitir que os administradores autorizem usuários, configure a permissão **Autorizar usuários** do servidor de gerenciamento na guia **Segurança geral**. Não é possível aplicar isto à função **Administradores** padrão.
Tornar os usuários anônimos durante sessões de PTZ	Marque a caixa de seleção para ocultar os nomes de usuários associados a esse papel quando controlam sessões PTZ.

Guia Usuários e grupos (funções)

Na guia **Usuários e grupos**, você atribui usuários e grupos a funções (consulte Atribuir/remover usuários e grupos para/de funções na página 297). Você pode atribuir usuários Windows e grupos ou usuários básicos (consulte Usuários (explicado) na página 66).

IDP externo (funções)

Na guia **IDP externo**, é possível visualizar alegações existentes e adicionar novas alegações a funções.

Nome	Descrição
IDP externo	O nome do IDP externo.
Nome da reivindicação	Uma variável que é definida no IDP externo.
Valor da reivindicação	O valor da reivindicação, como um nome de grupo, que pode ser usado para atribuir a função apropriada ao usuário.

Guia Segurança Geral (funções)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Na guia **Segurança geral**, você configura permissões gerais para funções. Para cada componente disponível em seu sistema, defina as permissões de acesso para as funções definindo **Permitir** ou **Negar**. Quando uma função tem o acesso negado a um componente, esse componente não é visível na guia **Segurança geral** para um usuário nessa função.

A guia **Segurança Geral** não está disponível no XProtect Essential+ gratuito.

Você pode definir mais permissões de acesso para o XProtect Corporate do que para outros produtos VMS XProtect. Isso ocorre porque só é possível configurar permissões de administrador diferenciadas no XProtect Corporate, ainda que seja possível configurar permissões gerais para uma função que usa XProtect Smart Client, XProtect Web Client ou cliente XProtect Mobile em todos os produtos.

As configurações gerais de segurança aplicam-se somente ao site atual.

Se você associar um usuário a mais de uma função e selecionar **Negar** em uma configuração de segurança para uma função e **Permitir** para outra, a permissão **Negar** anulará a permissão **Permitir**.

A seguir, as descrições mostram o que acontece em cada permissão individual para os diferentes componentes do sistema se você selecionar **Permitir** para a função em questão. Se utilizar XProtect Corporate, é possível ver as configurações que estão disponíveis **apenas** para seu sistema em cada componente do sistema.

Para cada componente ou funcionalidade do sistema, o administrador do sistema completo pode usar as caixas de seleção **Permitir** ou **Negar** para configurar as permissões de segurança da função. Todas as permissões de segurança que você configura aqui são configuradas para todas as funcionalidades ou componentes. Assim, por exemplo, se você marcar a caixa de seleção **Negar** em **Câmeras**, todas as câmeras adicionadas ao sistema ficarão indisponíveis para a função. Por outro lado, se marcar a caixa de seleção **Allow** (Permitir), a função poderá visualizar todas as câmeras adicionadas ao sistema. O resultado da seleção de **Permitir** ou **Negar** nas câmeras é que as configurações da câmera na guia **Dispositivos** herdarão as seleções na guia **Segurança Geral**, de modo que todas as câmeras ficarão disponíveis ou indisponíveis para a função específica.

Se quiser configurar as permissões de segurança para câmeras **individuais** ou similares, isso terá que ser feito na guia do componente ou da funcionalidade relevante do sistema se você **não tiver configurado nenhuma permissão geral** para o componente ou para a funcionalidade do sistema na guia **Overall Security** (Segurança geral).

As descrições abaixo também se aplicam às permissões que você pode configurar por meio do MIP SDK.

> Se você quiser mudar sua licença básica do XProtect Corporate para um dos outros produtos, certifique-se de remover todas as permissões de segurança disponíveis apenas para XProtect Corporate. Se você não remover essas permissões, não poderá concluir a troca.

Servidor de gerenciamento

> As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Conectar	Permite que usuários se conectem no Management Server. Esta permissão é ativada por padrão. Você pode negar a permissão de conexão em funções para fins de manutenção e, depois aplicar novamente o acesso ao sistema.

Permissão de segurança	Descrição
	Esta permissão deve ser selecionada para permitir acesso ao sistema.
Ler	Essa permissão é uma permissão administrativa altamente privilegiada que oferece direitos de acesso significativos ao XProtect VMS, incluindo acesso a dados sensíveis como por exemplo, credenciais configuradas no sistema. Permite acessar uma ampla gama de funcionalidades, incluindo: • Login com o Management Client • Lista de tarefas atuais • Registros de servidor Também ativa o acesso a: • Serviços de Conexão Remota • Perfis do Smart Client • Perfis do Management Client • Matrix • Perfis de tempo • Servidores Registrados e Serviço de Registro API: Essa permissão também revela algumas informações sensíveis ao cliente: • Credenciais para qualquer IDP externo configurado • Credenciais, IP-endereços e outras informações para todas as câmeras no XProtect VMS • Credenciais para servidor de e-mail configurado • Credenciais para qualquer matrix configurado

Permissão de segurança	Descrição
	• Credenciais configuradas para recurso interconectado • Credenciais configuradas para ativação de licença Essa permissão não revela credenciais para usuários do XProtect VMS. Isso inclui usuários básicos, usuários do Windows e usuários de IDPs externos.
Editar	Permite modificar dados em uma ampla gama de funcionalidades, incluindo: • Opções • Gerenciamento de Licenças Também permite aos usuários criar, excluir e editar o seguinte: • Serviços de Conexão Remota • Grupos de dispositivos • Matrix • Perfis de tempo • Perfis de Notificação • Servidores Registrados  Dá permissão para configurar intervalos de IP locais ao configurar a rede no servidor de gravação.
Monitor do sistema	Dá permissão para visualizar os dados do monitor do sistema.
Status API:	Dá permissão para realizar consultas na API de Status localizada no servidor de gravação. Isso significa que a função com essa permissão habilitada tem acesso para ler o status dos itens localizados no servidor de gravação.
Gerenciamento da Hierarquia de site Federado	Dá permissão para adicionar e desanexar o site atual de outros sites em uma hierarquia de sites federados.

Permissão de segurança	Descrição
	Se essa permissão for definida como permitido apenas no site filho, o usuário ainda pode desconectar o site a partir do site pai.
Backup da configuração:	Dá permissão para criar backups da configuração do sistema usando a funcionalidade de backup e restauração do sistema.
Autorizar usuários	Habilita a permissão para autorizar usuários quando eles são solicitados a fazer um segundo login no XProtect Smart Client ou no Management Client. Na guia **Informações**, você define se uma função requer autorização de login.
Gerenciar segurança	Dá permissão para gerenciar permissões para o Management Server. Também permite aos usuários criar, excluir e editar as seguintes características: • Funções • Usuários básicos • Perfis do Smart Client • Perfis do Management Client

Servidores de gravação

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Editar	Dá permissão para editar propriedades nos servidores de gravação, exceto para definições de configuração de rede que exigem permissão de edição no servidor de gerenciamento.
Excluir	Dá permissão para excluir servidores de gravação. Para isso, você também deve dar ao usuário permissões de exclusão em: • Grupo de segurança de hardware, se tiver adicionado hardware ao servidor de gravação Se qualquer um dos dispositivos no servidor de gravação contiver proteção de evidências, você só pode excluir o servidor de gravação se ele estiver off-line.
Gerenciar hardware	Dá permissão para adicionar hardware em servidores de gravação.
Gerenciar armazenamento	Dá permissão para administrar contêineres de armazenamento no servidor de gravação, ou seja, para criar, excluir, mover e esvaziar contêineres de armazenamento.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança para servidores de gravação.

Servidores de failover

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para ver e acessar servidores de failover no Management Client.
Editar	Dá permissão para criar, atualizar, excluir, mover e habilitar ou desabilitar servidores de failover no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança para servidores de failover.

Servidores Mobile

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para ver e acessar servidores móveis no Management Client.
Editar	Dá permissão para editar e excluir servidores móveis no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança para os servidores móveis.
Criar	Dá permissão para adicionar servidores móveis ao sistema.

Hardware

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Editar	Dá permissão para editar propriedades no hardware.
Excluir	Dá permissão para excluir hardware. Se qualquer um dos dispositivos de hardware contiver proteção de evidências, você só pode excluir o hardware quando o servidor de gravação estiver off-line.
Comandos do driver	Dá permissão para enviar comandos especiais aos drivers e, assim, controlar recursos e configuração no próprio dispositivo. A permissão **Comandos do driver** é apenas para plug-ins MIP desenvolvidos especialmente nos clientes. Ele não controla tarefas padrão de configuração.
Visualizar senhas	Dá permissão para visualizar senhas em dispositivos de hardware na caixa de diálogo **Editar hardware**.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança para o hardware.

Câmeras

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar dispositivos de câmera nos clientes e no Management Client.
Editar	Dá permissão para editar propriedades para câmeras no Management Client. Também permite ao usuário ativar ou desativar uma câmera.
Visualizar em Tempo Real	Dá permissão para visualizar vídeo ao vivo de câmeras nos clientes e no Management Client.
Visualização restrita ao vivo	Ativa a permissão para visualizar vídeos restritos ao vivo de câmeras nos clientes e no Management Client.
Reprodução	Dá permissão para reproduzir vídeo gravado de câmeras em todos os clientes.
Reprodução restrita de gravações	Ativa a permissão para reproduzir vídeos restritos gravados de câmeras em todos os clientes.
Recuperar gravações remotas	Dá permissão para recuperar gravações nos clientes de câmeras em locais remotos ou de armazenamentos no dispositivo em câmeras.
Ler sequências	Dá permissão para ler as informações de sequência relacionadas com, por exemplo, a reprodução de vídeo nos clientes.
Pesquisa inteligente	Dá permissão para usar a função Pesquisa inteligente nos clientes.
Exportar	Dá permissão para exportar gravações dos clientes.
Criar marcadores	Dá permissão para criar marcadores em vídeos gravados e ao vivo nos clientes.
Ler marcadores	Dá permissão para pesquisa e leitura dos detalhes de marcadores nos clientes.

Permissão de segurança	Descrição
Editar marcadores	Dá permissão para editar marcadores nos clientes.
Excluir marcadores	Dá permissão para excluir marcadores nos clientes.
Criar e estender proteções de evidências	Dá permissão para criar e ampliar proteções de evidências nos clientes.
Ler proteções de evidências	Dá permissão para pesquisar e ler proteções de evidências nos clientes.
Excluir e reduzir proteções de evidências	Dá permissão para excluir ou reduzir proteções de evidências nos clientes.
Criar e estender restrições de reprodução e ao vivo	Ativa a permissão para criar e ampliar restrições nos clientes.
Ler restrições de reprodução e ao vivo	Ativa a permissão para visualizar uma lista de restrições existentes nos clientes.
Excluir e reduzir restrições de reprodução e ao vivo	Ativa a permissão para excluir e reduzir restrições nos clientes.
Iniciar gravação manual	Dá permissão para iniciar gravação manual de vídeo nos clientes.
Parar gravação manual	Dá permissão para interromper gravação manual de vídeo nos clientes.
Comandos AUX	Dá permissão para usar comandos auxiliares (AUX) na câmera dos clientes.

Permissão de segurança	Descrição
	Os **comandos AUX** dão ao usuário controle de, por exemplo, limpadores em uma câmera conectada por meio de um codificador de vídeo. Dispositivos associados a câmeras interligados por conexões auxiliares são controlados desde o cliente.
PTZ Manual	Dá permissão para usar funções PTZ em câmeras PTZ nos clientes e no Management Client.
Ativar predefinições PTZ ou perfis de patrulha	Dá permissão para mover câmeras PTZ para posições predefinidas, iniciar e parar perfis de patrulha e pausar uma patrulha nos clientes e no Management Client. Para permitir que esta função use outras funções PTZ na câmera, habilite a permissão **PTZ manual**.
Gerenciar predefinições PTZ ou perfis de patrulha	Dá permissão para adicionar, editar e excluir predefinições de PTZ e perfis de patrulha em câmeras PTZ nos clientes no Management Client. Para permitir que esta função use outras funções PTZ na câmera, habilite a permissão **PTZ manual**.
Travar/destravar predefinições PTZ	Dá permissão para bloquear e desbloquear predefinições de PTZ no Management Client. Isso impede ou permite que outros usuários modifiquem posições predefinidas nos clientes e no Management Client.
Reservar sessões PTZ	Dá permissão para definir câmeras PTZ no modo de sessão PTZ reservado nos clientes e no Management Client. Em uma sessão PTZ reservada, outros usuários com maior prioridade PTZ não podem assumir o controle. Para permitir que esta função use outras funções PTZ na câmera, habilite a permissão **PTZ manual**.
Liberar sessões PTZ	Habilita a permissão para liberar as sessões PTZ de outros usuários do Management Client. As suas próprias sessões de PTZ sempre podem ser liberadas por

Permissão de segurança	Descrição
	você (independentemente dessa permissão).
Excluir gravações	Dá permissão para excluir gravações de vídeo armazenadas do sistema por meio do Management Client.
Remover máscaras de privacidade	Dá permissão para remover temporariamente máscaras de privacidade no XProtect Smart Client. Ele também dá a permissão para autorizar outros usuários do XProtect Smart Client a retirar as máscaras de privacidade. A remoção de máscaras de privacidade aplica-se apenas a máscaras de privacidade configuradas como máscaras de privacidade removíveis no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para a câmera.

Microfones

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar dispositivos de microfone nos clientes e no Management Client.

Permissão de segurança	Descrição
Editar	Dá permissão para editar propriedades de microfone no Management Client. Também permite ao usuário ativar ou desativar microfones.
Escutar em tempo real	Habilita a permissão para ouvir áudio ao vivo de alto-falantes nos clientes e no Management Client.
Ouvir áudios restritos ao vivo	Ativa a permissão para ouvir áudios restritos ao vivo de alto-falantes nos clientes e no Management Client.
Reprodução	Dá permissão para reproduzir áudio gravado de microfones nos clientes.
Reprodução restrita de gravações	Ativa a permissão para reproduzir áudios restritos gravados de microfones nos clientes.
Recuperar gravações remotas	Dá permissão para recuperar gravações nos clientes de microfones em locais remotos ou de armazenamentos no dispositivo em câmeras.
Ler sequências	Dá permissão para ler as informações de sequência relacionadas com, por exemplo, a guia **Reprodução** nos clientes.
Exportar	Dá permissão para exportar gravações dos clientes.
Criar marcadores	Dá permissão para criar marcadores nos clientes.
Ler marcadores	Dá permissão para pesquisa e leitura dos detalhes de marcadores nos clientes.
Editar marcadores	Dá permissão para editar marcadores nos clientes.
Excluir marcadores	Dá permissão para excluir marcadores nos clientes.
Criar e estender proteções de evidências	Dá permissão para criar ou ampliar bloqueios de evidência nos clientes.

Permissão de segurança	Descrição
Ler proteções de evidências	Dá permissão para pesquisar e ler detalhes de proteções de evidências nos clientes.
Excluir e reduzir proteções de evidências	Dá permissão para excluir ou reduzir proteções de evidências nos clientes.
Criar e estender restrições de reprodução e ao vivo	Ativa a permissão para criar e ampliar restrições em microfones nos clientes.
Ler restrições de reprodução e ao vivo	Ativa a permissão para visualizar uma lista de restrições existentes em microfones nos clientes.
Excluir e reduzir restrições de reprodução e ao vivo	Ativa a permissão para excluir e reduzir restrições em microfones nos clientes.
Iniciar gravação manual	Dá permissão para iniciar gravação manual de áudio nos clientes.
Parar gravação manual	Dá permissão para interromper gravação manual de áudio nos clientes.
Excluir gravações	Dá permissão para excluir gravações armazenadas do sistema.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para microfones.

Alto-falantes

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar dispositivos de alto-falante nos clientes e no Management Client.
Editar	Dá permissão para editar propriedades para alto-falantes no Management Client. Também permite ao usuário ativar ou desativar alto-falantes.
Escutar em tempo real	Habilita a permissão para ouvir áudio ao vivo de alto-falantes nos clientes e no Management Client.
Ouvir áudios restritos ao vivo	Ativa a permissão para ouvir áudios restritos ao vivo de alto-falantes nos clientes e no Management Client.
Falar	Dá permissão para falar pelos alto-falantes nos clientes.
Reprodução	Dá permissão para reproduzir áudio gravado de alto-falantes nos clientes.
Reprodução restrita de gravações	Dá permissão para reproduzir áudio gravado de alto-falantes nos clientes.
Recuperar gravações remotas	Dá permissão para recuperar gravações nos clientes de alto-falantes em locais remotos ou de armazenamentos no dispositivo em câmeras.
Ler sequências	Dá permissão para usar a função Sequências enquanto se navega pelo áudio de alto-falantes nos clientes.
Exportar	Dá permissão para exportar áudio gravado de dispositivos de alto-falantes nos clientes.
Criar marcadores	Dá permissão para criar marcadores nos clientes.
Ler marcadores	Dá permissão para pesquisa e leitura dos detalhes de marcadores nos clientes.

Permissão de segurança	Descrição
Editar marcadores	Dá permissão para editar marcadores nos clientes.
Excluir marcadores	Dá permissão para excluir marcadores nos clientes.
Criar e estender proteções de evidências	Dá permissão para criar ou ampliar bloqueios de evidência para proteger áudios gravados nos clientes.
Ler proteções de evidências	Dá permissão para visualizar áudio gravado protegido por proteções de evidências nos clientes.
Excluir e reduzir proteções de evidências	Dá permissão para excluir ou reduzir proteções de evidências em áudio protegido nos clientes.
Criar e estender restrições de reprodução e ao vivo	Ativa a permissão para criar e ampliar restrições em alto-falantes nos clientes.
Ler restrições de reprodução e ao vivo	Ativa a permissão para visualizar uma lista de restrições existentes em alto-falantes nos clientes.
Excluir e reduzir restrições de reprodução e ao vivo	Ativa a permissão para excluir e reduzir restrições em alto-falantes nos clientes.
Iniciar gravação manual	Dá permissão para iniciar gravação manual de áudio nos clientes.
Parar gravação manual	Dá permissão para interromper gravação manual de áudio nos clientes.
Excluir gravações	Dá permissão para excluir gravações armazenadas do sistema.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para alto-falantes.

Metadados

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para receber metadados nos clientes.
Editar	Dá permissão para editar propriedades de metadados no Management Client. Também permite ao usuário ativar ou desativar dispositivos de metadados.
Ao vivo	Dá permissão para receber metadados ao vivo de câmeras nos clientes.
Visualização restrita ao vivo	Ativa a permissão para receber metadados restritos ao vivo de dispositivos de metadados nos clientes.
Reprodução	Dá permissão para reproduzir dados gravados de dispositivos de metadados nos clientes.
Reprodução restrita de gravações	Ativa a permissão para reproduzir dados restritos gravados de dispositivos de metadados nos clientes.
Recuperar gravações remotas	Dá permissão para recuperar gravações nos clientes de dispositivos de metadados em locais remotos ou de armazenamentos no dispositivo em câmeras.
Ler sequências	Dá permissão para ler as informações de sequência relacionadas com, por exemplo, a guia **Reprodução** nos clientes.
Exportar	Dá permissão para exportar gravações nos clientes.
Criar e estender	Dá permissão para criar proteções de evidências nos clientes.

Permissão de segurança	Descrição
proteções de evidências	
Ler proteções de evidências	Dá permissão para visualizar proteções de evidências nos clientes.
Excluir e reduzir proteções de evidências	Dá permissão para excluir ou reduzir proteções de evidências nos clientes.
Criar e estender restrições de reprodução e ao vivo	Ativa a permissão para criar e ampliar restrições em metadados nos clientes.
Ler restrições de reprodução e ao vivo	Ativa a permissão para visualizar uma lista de restrições existentes em metadados nos clientes.
Excluir e reduzir restrições de reprodução e ao vivo	Ativa a permissão para apagar e excluir restrições em metadados nos clientes.
Iniciar gravação manual	Dá permissão para iniciar gravação manual de metadados nos clientes.
Parar gravação manual	Dá permissão para interromper gravação manual de metadados nos clientes.
Excluir gravações	Dá permissão para excluir gravações armazenadas do sistema.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para metadados.

Entrada

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar dispositivos de entrada nos clientes e no Management Client.
Editar	Dá permissão para editar propriedades para dispositivos de entrada no Management Client. Também permite ao usuário ativar ou desativar um dispositivo de entrada.
Gerenciar segurança	Ativa a permissão para gerenciar permissões de segurança no Management Client para dispositivos de entrada.

Saída

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar dispositivos de saída nos clientes.
Editar	Dá permissão para editar propriedades para dispositivos de saída no Management Client. Também permite ao usuário ativar ou desativar um dispositivo de saída.

Permissão de segurança	Descrição
Ativar	Dá permissão para ativar saídas nos clientes.
Gerenciar segurança	Ativa a permissão para gerenciar permissões de segurança no Management Client para dispositivos de saída.

Smart Wall

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Habilita a permissão para gerenciar todas as permissões de segurança em XProtect Management Client.
Ler	Habilita a permissão para visualizar um videowall no XProtect Smart Client.
Editar	Habilita a permissão para editar propriedades para a definição do Smart Wall no XProtect Management Client.
Excluir	Habilita a permissão para excluir definições do Smart Wall existentes no XProtect Management Client.
Operar	Habilita a permissão para ativar e modificar definições do Smart Wall, por exemplo, para alterar e ativar predefinições ou aplicar câmeras em visualizações no XProtect Smart Client e no XProtect Management Client. Você pode associar **Operar** a perfis de tempo que definem quando a permissão do usuário se aplica.
Criar Smart Wall	Habilita a permissão para criar novas definições do Smart Wall no XProtect

Permissão de segurança	Descrição
	Management Client.
Gerenciar segurança	Habilita a permissão para gerenciar todas permissões de segurança no XProtect Management Client para a definição do Smart Wall.
Reprodução	Habilita a permissão para reproduzir dados gravados de um videowall em XProtect Smart Client. Você pode associar **Reproduzir** a perfis de tempo que definem quando a permissão do usuário se aplica.

Grupos de Visualização

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar grupos de visualização nos clientes e no Management Client. Grupos de visualização são criados no Management Client.
Editar	Dá permissão para editar propriedades nos grupos de visualização no Management Client.
Excluir	Dá permissão para excluir grupos de visualização no Management Client.
Operar	Dá permissão para usar Visualização de grupos no XProtect Smart Client, ou seja, para criar e excluir subgrupos e exibições.

Permissão de segurança	Descrição
Criar grupo de visualização	Dá permissão para criar grupos de visualização no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para grupos de visualização.

Eventos definidos pelo usuário:

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar eventos definidos por usuário nos clientes.
Editar	Dá permissão para editar propriedades em eventos definidos por usuário no Management Client.
Excluir	Dá permissão para excluir eventos definidos por usuário no Management Client.
Disparar	Dá permissão para ativar eventos definidos por usuário nos clientes.
Gerenciar segurança	Ativa a permissão para gerenciar permissões de segurança no Management Client para eventos definidos por usuário.
Criar evento definido pelo usuário	Dá permissão para criar novos eventos definidos por usuário no Management Client.

Eventos analíticos

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar eventos analíticos no Management Client.
Editar	Dá permissão para editar propriedades em eventos analíticos no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para todos os eventos analíticos.

Eventos genéricos

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar eventos genéricos nos clientes e no Management Client.
Editar	Dá permissão para editar propriedades em eventos genéricos no Management Client.
Gerenciar segurança	Ativa a permissão para gerenciar permissões de segurança no Management Client para eventos genéricos.

Matrix

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para selecionar e enviar vídeo para o destinatário Matrix dos clientes.
Editar	Dá permissão para editar propriedades para um Matrix no Management Client.
Excluir	Dá permissão para excluir um Matrix no Management Client.
Criar Matrix	Permite criar um novo Matrix no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para todos os Matrix.

Regras

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar regras existentes no Management Client.
Editar	Dá permissão para editar propriedades para regras e definir comportamento de regra no Management Client.

Permissão de segurança	Descrição
	Também requer que o usuário tenha permissões de leitura em todos os dispositivos afetados pela regra.
Excluir	Dá permissão para excluir regras do Management Client. Também requer que o usuário tenha permissões de leitura em todos os dispositivos afetados pela regra.
Criar regra	Dá permissão para criar novas regras no Management Client. Também requer que o usuário tenha permissões de leitura em todos os dispositivos afetados pela regra.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para todas as regras.

Sites

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar outros locais no Management Client. Sites conectados são ligados pelo Milestone Federated Architecture. Para editar propriedades, você precisa Editar permissões no servidor de gerenciamento em cada site.
Gerenciar segurança	Habilita a permissão para gerenciar todas as permissões de segurança em todos os locais.

Monitor do sistema

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar monitores do sistema no XProtect Smart Client.
Editar	Dá permissão para editar propriedades para monitores do sistema no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para todos monitores do sistema.

Pesquisa de metadados

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar a funcionalidade **Uso de metadados** no Management Client e suas configurações relacionadas, mas não dá permissão para alterar as configurações.
Editar a configuração	Dá permissão para habilitar ou desabilitar categorias de pesquisa de metadados,

Permissão de segurança	Descrição
de pesquisa de metadados	como, por exemplo, metadados para pessoas ou veículos, no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança para pesquisas de metadados.

Pesquisar

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Ler pesquisas públicas	Dá permissão para visualizar e abrir pesquisas públicas salvas no XProtect Smart Client.
Criar pesquisas públicas	Dá permissão para salvar pesquisas recém-configuradas como pesquisas públicas no XProtect Smart Client.
Editar pesquisas públicas	Dá permissão para editar os detalhes ou a configuração de pesquisas públicas salvas no XProtect Smart Client, como, por exemplo, nome, descrição, câmeras e categorias de pesquisa.
Excluir pesquisas públicas	Dá permissão para excluir pesquisas públicas salvas.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para pesquisa.

Alarmes

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Gerenciamento	Dá permissão para gerenciar alarmes no Smart Client. Por exemplo, alterar prioridades de alarmes, reatribuir alarmes a outros usuários, reconhecer alarmes, alterar o estado de alarme de vários alarmes (por exemplo, de **Novo** para **Atribuído**). Para editar as configurações de alarme, você também precisa da permissão **Editar configurações de alarme**. Somente quando você isso é definido como permitido, a guia **Alarmes e Eventos** é exibida no diálogo **Opções**.
Visualização	Ativa a permissão para visualizar a guia **Gerenciador de alarmes** no XProtect Smart Client e recuperar alarmes e configurações de alarme por meio da API. Para visualizar alarmes no XProtect Smart Client, é necessário ativar a permissão de **Visualização** de ao menos uma definição de alarme. Por padrão, você visualiza alarmes de soluções de terceiros.
Desativar alarmes	Dá permissão para desativar alarmes.
Receber notificações	Dá permissão para receber notificações sobre alarmes em clientes XProtect Mobile e XProtect Web Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança dos alarmes.
Editar configurações de alarme	Ativa a permissão para editar definições de alarme, estados de alarme, categorias de alarme, sons de alarme, retenção de alarme e retenção de eventos. Para editar as configurações de alarme, você também precisa da permissão **Gerenciar**.

Definições de alarme

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Visualização	Ativa a permissão para visualizar definições de alarme, estados de alarme, categorias de alarme, sons de alarme, retenção de alarme e retenção de eventos.
Gravar	Ativa a permissão **Visualizar**.
Gerenciar segurança	Ativa a permissão para gerenciar permissões de segurança para definições de alarmes.

Registros de servidor

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler as entradas do registro do sistema	Dá permissão para ver entradas de registro do sistema.
Ler entradas do registro de auditoria	Dá permissão para ver as entradas do registro de auditoria.
Ler entradas do registro disparado por regra	Dá permissão para ver as entradas de registro ativadas por regras.
Ler configuração do registro	Dá permissão para ler configurações de registro em **Ferramentas** > **Opções** > **Registros do servidor**.
Atualiza configuração do	Dá permissão para alterar as configurações de registro em **Ferramentas** >

Permissão de segurança	Descrição
registro	**Opções** > **Registros do servidor**.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança dos alarmes.

Controle de acesso

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Editar	Dá permissão para editar propriedades para sistemas de controle de acesso no Management Client.
Usar o controle de acesso	Permite que o usuário use qualquer recurso relacionado a controle de acesso nos clientes.
Visualizar lista de portadores de cartão	Permite ao usuário visualizar a lista de titulares na guia **Controle de acesso** nos clientes.
Receber notificações	Permite que o usuário receba notificações sobre solicitações de acesso nos clientes.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança para todos os sistemas de controle de acesso.

LPR

Se o seu sistema for executado com XProtect LPR, especifique as seguintes permissões para o usuário:

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Usar LPR	Dá permissão para usar quaisquer recursos relacionados a LPR nos clientes.
Gerenciar listas de correspondências	Ativa a permissão para adicionar, importar, modificar, exportar e excluir listas de correspondências no Management Client.
Ler listas de correspondências	Ativa a permissão para visualizar listas de correspondências.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para definições de todas as transações.

Fontes de transações

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar propriedades para fontes de Transação no Management Client.
Editar	Dá permissão para editar propriedades para fontes de Transação no Management Client.
Excluir	Dá permissão para excluir novas fontes de Transação no Management Client.
Criar	Dá permissão para criar novas fontes de Transação no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para todas as fontes de Transação.

Definições da transação

Permissão de segurança	Descrição
Controle total	Dá permissão para gerir todas as entradas de segurança nesta parte do sistema.
Ler	Dá permissão para visualizar propriedades para definições de Transação no Management Client.
Editar	Dá permissão para editar propriedades para definições de Transação no Management Client.
Excluir	Dá permissão para criar excluir definições de Transação no Management Client.
Criar	Dá permissão para criar novas definições de Transação no Management Client.
Gerenciar segurança	Dá permissão para gerenciar permissões de segurança no Management Client para definições de todas as transações.

Plug-ins do MIP

Por meio do MIP SDK, um fornecedor terceirizado pode desenvolver plug-ins personalizados para seu sistema, como por exemplo, integração a sistemas de controle de acesso externo ou funcionalidade semelhante.

Guia Dispositivos (funções)

As funcionalidades disponíveis dependem do sistema que você estiver usando. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/product-index/).

A guia **Dispositivo** permite que você especifique quais usuários/grupos de recursos com as funções selecionadas poderão usar para cada dispositivo (p. ex., uma câmera) ou grupo de dispositivos no XProtect Smart Client.

Lembre-se de repetir para cada dispositivo. Você também pode selecionar um grupo de dispositivos e especificar permissões de função para todos os dispositivos do grupo de uma só vez.

Você ainda pode marcar ou desmarcar tais caixas de seleção, mas observe que sua escolha neste caso se aplicará a **todos** os dispositivos do grupo de dispositivos. Como alternativa, selecione os dispositivos individuais no grupo de dispositivos para verificar exatamente a quais dispositivos a permissão em questão se aplica.

Permissões relacionadas a câmeras

Especifique as seguintes permissões para dispositivos de câmera:

Nome	Descrição
Ler	A(s) câmera(s) selecionada(s) estará(ão) visível(eis) nos clientes.
Visualizar em tempo real	Permite visualização ao vivo do vídeo da(s) câmera(s) selecionada(s) nos clientes. Para o XProtect Smart Client, é necessário que a função tenha recebido permissão para visualizar a guia **Ao vivo** dos clientes. Essa permissão é concedida como parte das permissões do aplicativo. Especifique o perfil de tempo ou deixe o valor padrão.
Visualização restrita ao vivo	Permite a visualização ao vivo de vídeos restritos da(s) câmera(s) selecionada(s) nos clientes. Para o XProtect Smart Client, é necessário que a função tenha recebido permissão para visualizar a guia **Ao vivo** dos clientes. Essa permissão é concedida como parte das permissões do aplicativo. Especifique o perfil de tempo ou deixe o valor padrão.
Reprodução > dentro do perfil de tempo	Permite visualização do vídeo gravado da(s) câmera(s) selecionada(s) nos clientes. Especifique o perfil de tempo ou deixe o valor padrão.
Reprodução > Limite a reprodução a	Permite visualização do vídeo gravado da(s) câmera(s) selecionada(s) nos clientes. Especifique um limite de reprodução ou não aplique restrições.
Reprodução restrita de gravações	Permite a reprodução de vídeos restritos gravados da(s) câmera(s) selecionada(s) nos clientes. Especifique o perfil de tempo ou deixe o valor padrão.
Ler sequências	Dá permissão para ler as informações de sequência relacionadas a, p. ex., o explorador de sequências nos clientes.
Pesquisa inteligente	Dá permissão para usar a função Pesquisa inteligente nos clientes.
Exportar	Dá permissão para exportar gravações dos clientes.
Iniciar gravação	Permite iniciar a gravação manual do vídeo da(s) câmera(s) selecionada(s) nos

Nome	Descrição
manual	clientes.
Parar gravação manual	Permite interromper a gravação manual do vídeo da(s) câmera(s) selecionada(s) nos clientes.
Ler marcadores	Dá permissão para pesquisa e leitura dos detalhes de marcadores nos clientes.
Editar marcadores	Dá permissão para editar marcadores nos clientes.
Criar marcadores	Dá permissão para criar marcadores nos clientes.
Excluir marcadores	Dá permissão para excluir marcadores nos clientes.
Comandos AUX	Permite o uso de comandos auxiliares nos clientes.
Criar e estender proteções de evidências	Dá permissão ao usuário cliente para: • Adicionar a câmera a proteções de evidências novas ou existentes • Estende o tempo de expiração de proteções de evidências existentes • Estende o intervalo de proteção de proteções de evidências existentes Exige permissões de usuário para todos os dispositivos incluídos na proteção de evidências.
Excluir e reduzir proteções de evidências	Dá permissão ao usuário cliente para: • Excluir a câmera de proteções de evidências existentes • Exclui proteções de evidências existentes • Reduz o tempo de expiração de proteções de evidências existentes • Reduz o intervalo de proteção de proteções de evidências existentes Exige permissões de usuário para todos os dispositivos incluídos na proteção de evidências.

Nome	Descrição
Ler proteções de evidências	Dá permissão para buscar e ler detalhes das proteções de evidências.
Criar e estender restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Criar uma restrição ao vivo na câmera • Criar uma restrição de reprodução nas gravações da câmera • Adicionar uma nova câmera a uma restrição ao vivo ou de reprodução • Ampliar o período de restrição das gravações da câmera Exige permissões de usuário para todos os dispositivos incluídos na restrição.
Ler restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Visualizar uma lista de restrições ao vivo e de reprodução na câmera • Filtrar e buscar a lista de restrições ao vivo e de reprodução na câmera
Excluir e reduzir restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Remover uma restrição ao vivo na câmera • Remover uma restrição de reprodução nas gravações da câmera • Reduzir o período de restrição das gravações da câmera • Alterar as configurações da restrição ao vivo ou de reprodução Exige permissões de usuário para todos os dispositivos incluídos na restrição.

Permissões relacionadas a microfone

Especifique as seguintes permissões para dispositivos de microfones:

Nome	Descrição
Ler	O(s) microfones(s) selecionado(s) estará(ão) visível(eis) nos clientes.
Escutar em tempo real	Dá permissão para ouvir áudio ao vivo nos microfones selecionados nos clientes. Para o XProtect Smart Client, é necessário que a função tenha recebido permissão para visualizar a guia **Ao vivo** dos clientes. Essa permissão é concedida como parte das permissões do aplicativo. Especifique o perfil de tempo ou deixe o valor padrão.
Ouvir áudios restritos ao vivo	Permite ouvir vídeos restritos ao vivo no(s) microfone(s) selecionado(s) nos clientes. Para o XProtect Smart Client, é necessário que a função tenha recebido permissão para visualizar a guia **Ao vivo** dos clientes. Essa permissão é concedida como parte das permissões do aplicativo. Especifique o perfil de tempo ou deixe o valor padrão.
Reprodução > dentro do perfil de tempo	Permite ouvir o áudio gravado do(s) microfone(s) selecionado(s) nos clientes. Especifique o perfil de tempo ou deixe o valor padrão.
Reprodução > Limite a reprodução a	Permite ouvir o áudio gravado do(s) microfone(s) selecionado(s) nos clientes. Especifique um limite de reprodução ou não aplique restrições.
Reprodução restrita de gravações	Permite reproduzir áudios restritos gravados do(s) microfone(s) selecionado(s) nos clientes. Especifique o perfil de tempo ou deixe o valor padrão.
Ler sequências	Dá permissão para ler as informações de sequência relacionadas a, p. ex., o explorador de sequências nos clientes.
Exportar	Dá permissão para exportar gravações dos clientes.
Iniciar gravação manual	Permite iniciar a gravação manual do áudio do(s) microfone(s) selecionado(s) nos clientes.
Parar gravação manual	Permite interromper a gravação manual do áudio do(s) microfone(s) selecionado(s) nos clientes.
Ler marcadores	Dá permissão para pesquisa e leitura dos detalhes de marcadores nos clientes.

Nome	Descrição
Editar marcadores	Dá permissão para editar marcadores nos clientes.
Criar marcadores	Dá permissão para criar marcadores nos clientes.
Excluir marcadores	Dá permissão para excluir marcadores nos clientes.
Criar e estender proteções de evidências	Dá permissão ao usuário cliente para: • Adicionar o microfone a proteções de evidências novas ou existentes • Estende o tempo de expiração de proteções de evidências existentes • Estende o intervalo de proteção de proteções de evidências existentes Exige permissões de usuário para todos os dispositivos incluídos na proteção de evidências.
Excluir e reduzir proteções de evidências	Dá permissão ao usuário cliente para: • Excluir o microfone de proteções de evidências existentes • Exclui proteções de evidências existentes • Reduz o tempo de expiração de proteções de evidências existentes • Reduz o intervalo de proteção de proteções de evidências existentes Exige permissões de usuário para todos os dispositivos incluídos na proteção de evidências.
Ler proteções de evidências	Dá permissão para buscar e ler detalhes das proteções de evidências.
Criar e estender restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Criar uma restrição ao vivo no microfone • Criar uma restrição de reprodução nas gravações de áudio • Adicionar um novo microfone a uma restrição ao vivo ou de reprodução

Nome	Descrição
	• Ampliar o período de restrição das gravações de áudio  Exige permissões de usuário para todos os dispositivos incluídos na restrição.
Ler restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Visualizar uma lista de restrições ao vivo e de reprodução no microfone • Filtrar e buscar a lista de restrições ao vivo e de reprodução no microfone
Excluir e reduzir restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Remover uma restrição ao vivo no microfone • Remover uma restrição de reprodução nas gravações de áudio • Reduzir o período de restrição das gravações de áudio • Alterar as configurações da restrição ao vivo ou de reprodução  Exige permissões de usuário para todos os dispositivos incluídos na restrição.

Permissões relacionadas a alto-falantes

Especifique as seguintes permissões para dispositivos de alto-falantes:

Nome	Descrição
Ler	O(s) alto-falante(s) selecionado(s) estará(ão) visível(eis) nos clientes.
Escutar em tempo real	Dá permissão para ouvir áudio ao vivo do(s) alto-falante(s) selecionado(s) nos clientes. Para o XProtect Smart Client, é necessário que a função tenha recebido permissão para visualizar a guia **Ao vivo** dos clientes. Essa permissão é concedida como parte das permissões do aplicativo. Especifique o perfil de tempo ou deixe o valor padrão.

Nome	Descrição
Ouvir áudios restritos ao vivo	Permite ouvir vídeos restritos ao vivo no(s) alto-falante(s) selecionado(s) nos clientes. Para o XProtect Smart Client, é necessário que a função tenha recebido permissão para visualizar a guia **Ao vivo** dos clientes. Essa permissão é concedida como parte das permissões do aplicativo. Especifique o perfil de tempo ou deixe o valor padrão.
Reprodução > dentro do perfil de tempo	Permite ouvir o áudio gravado do(s) alto-falante(s) selecionado(s) nos clientes. Especifique o perfil de tempo ou deixe o valor padrão.
Reprodução > Limite a reprodução a	Permite ouvir o áudio gravado do(s) alto-falante(s) selecionado(s) nos clientes. Especifique um limite de reprodução ou não aplique restrições.
Reprodução restrita de gravações	Permite reproduzir áudios restritos gravados do(s) alto-falante(s) selecionado(s) nos clientes. Especifique o perfil de tempo ou deixe o valor padrão.
Ler sequências	Dá permissão para ler as informações de sequência relacionadas a, p. ex., o explorador de sequências nos clientes.
Exportar	Dá permissão para exportar gravações dos clientes.
Iniciar gravação manual	Permite iniciar a gravação manual do áudio do(s) alto-falante(s) selecionado(s) nos clientes.
Parar gravação manual	Permite interromper a gravação manual do áudio do(s) alto-falante(s) selecionado(s) nos clientes.
Ler marcadores	Dá permissão para pesquisa e leitura dos detalhes de marcadores nos clientes.
Editar marcadores	Dá permissão para editar marcadores nos clientes.
Criar marcadores	Dá permissão para criar marcadores nos clientes.
Excluir marcadores	Dá permissão para excluir marcadores nos clientes.

Nome	Descrição
Criar e estender proteções de evidências	Dá permissão ao usuário cliente para: • Adicionar o alto-falante a proteções de evidências novos ou existentes • Estende o tempo de expiração de proteções de evidências existentes • Estende o intervalo de proteção de proteções de evidências existentes Exige permissões de usuário para todos os dispositivos incluídos na proteção de evidências.
Excluir e reduzir proteções de evidências	Dá permissão ao usuário cliente para: • Excluir o alto-falante de proteções de evidências existentes • Exclui proteções de evidências existentes • Reduz o tempo de expiração de proteções de evidências existentes • Reduz o intervalo de proteção de proteções de evidências existentes Exige permissões de usuário para todos os dispositivos incluídos na proteção de evidências.
Ler proteções de evidências	Dá permissão para buscar e ler detalhes das proteções de evidências.
Criar e estender restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Criar uma restrição ao vivo nos alto-falantes • Criar uma restrição de reprodução nas gravações de áudio • Adicionar um novo microfone a uma restrição ao vivo ou de reprodução • Ampliar o período de restrição das gravações de áudio Exige permissões de usuário para todos os dispositivos incluídos na restrição.

Nome	Descrição
Ler restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Visualizar uma lista de restrições ao vivo e de reprodução nos alto-falantes • Filtrar e buscar a lista de restrições ao vivo e de reprodução nos alto-falantes
Excluir e reduzir restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Remover uma restrição ao vivo nos alto-falantes • Remover uma restrição de reprodução nas gravações de áudio • Reduzir o período de restrição das gravações de áudio • Alterar as configurações da restrição ao vivo ou de reprodução Exige permissões de usuário para todos os dispositivos incluídos na restrição.

Permissões relacionadas a metadados

Especifique as seguintes permissões para dispositivos de metadados:

Nome	Descrição
Ler	Dá permissão para ver dispositivos de metadados e recuperar dados deles nos clientes.
Editar	Dá permissão para editar propriedades de metadados. Também permite usuários a ativar ou desativar dispositivos de metadados em Management Client e pelo MIP SDK.
Visualizar em Tempo Real	Dá permissão para visualizar metadados ao vivo de câmeras nos clientes. Para o XProtect Smart Client, é necessário que a função tenha recebido permissão para visualizar a guia **Ao vivo** dos clientes. Essa permissão é concedida como parte das permissões do aplicativo.
Visualizar	Ativa a permissão para visualizar metadados restritos ao vivo de câmeras nos

Nome	Descrição
restrição ao vivo	clientes. Para o XProtect Smart Client, é necessário que a função tenha recebido permissão para visualizar a guia **Ao vivo** dos clientes. Essa permissão é concedida como parte das permissões do aplicativo.
Reprodução	Dá permissão para reproduzir dados gravados de dispositivos de metadados nos clientes.
Reprodução restrita de gravações	Ativa a permissão para reproduzir dados restritos gravados de dispositivos de metadados restritos nos clientes.
Ler sequências	Dá permissão para usar a função Sequências enquanto se navega pelos dados gravados de dispositivos de metadados nos clientes.
Exportar	Dá permissão para exportar áudio gravado de dispositivos de metadados nos clientes.
Criar e estender proteções de evidências	Dá permissão para criar e ampliar as proteções de evidências em metadados nos clientes.
Ler proteções de evidências	Dá permissão para visualizar proteções de evidências em metadados nos clientes.
Excluir e reduzir proteções de evidências	Dá permissão para excluir ou reduzir proteções de evidências em metadados nos clientes.
Iniciar gravação manual	Dá permissão para iniciar gravação manual de metadados nos clientes.
Parar gravação manual	Dá permissão para interromper gravação manual de metadados nos clientes.
Criar e estender restrições de	Dá permissão ao usuário cliente para:

Nome	Descrição
reprodução e ao vivo	• Criar uma restrição ao vivo no dispositivo de metadados • Criar uma restrição de reprodução no dispositivo de metadados • Adicionar um novo metadado a uma restrição ao vivo ou de reprodução • Ampliar o período de restrição do dispositivo de metadados Exige permissões de usuário para todos os dispositivos incluídos na restrição.
Ler restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Visualizar uma lista de restrições ao vivo e de reprodução no dispositivo de metadados • Filtrar e buscar a lista de restrições ao vivo e de reprodução no dispositivo de metadados
Excluir e reduzir restrições de reprodução e ao vivo	Dá permissão ao usuário cliente para: • Remover uma restrição ao vivo no dispositivo de metadados • Remover uma restrição de reprodução no dispositivo de metadados • Reduzir o período de restrição do dispositivo de metadados • Alterar as configurações da restrição ao vivo ou de reprodução Exige permissões de usuário para todos os dispositivos incluídos na restrição.

Permissões relacionadas a entrada

Especifique as seguintes permissões para dispositivos de entrada:

Nome	Descrição
Ler	A(s) entrada(s) selecionada(s) estará(ão) visível(eis) nos clientes.

Permissões relacionadas a saída

Especifique as seguintes permissões para dispositivos de saída:

Nome	Descrição
Ler	A(s) saídas selecionada(s) estará(ão) visível(eis) nos clientes. Se visível, a saída estará selecionável numa lista nos clientes.
Ativar	A(s) saída(s) selecionada(s) poderão ser ativada(s) no Management Client e nos clientes. Especifique o perfil de tempo ou deixe o valor padrão.

Guia PTZ (funções)

Você configura permissões para câmeras pan-tilt-zoom (PTZ) na guia **PTZ**. É possível especificar que características os usuários/grupos podem utilizar nos clientes. É possível selecionar câmeras PTZ individuais ou grupos de dispositivos contendo câmeras PTZ.

Especifique as seguintes permissões para PTZ:

Nome	Descrição
PTZ Manual	Determina se a função selecionada pode usar recursos de PTZ e pausar uma patrulha na câmera selecionada. Especifique um perfil de tempo, selecione **Sempre**, ou deixe o valor padrão que acompanha o perfil de tempo padrão definido na guia **Informações** para essa função.
Ativar predefinições PTZ ou perfis de patrulha	Determina se a função selecionada é capaz de mover a câmera PTZ selecionada para posições predefinidas, iniciar e finalizar perfis de patrulha e interromper uma patrulha. Especifique um perfil de tempo, selecione **Sempre**, ou deixe o valor padrão que acompanha o perfil de tempo padrão definido na guia **Informações** para essa função. Para permitir que esta função use outras funções PTZ na câmera, habilite a permissão **PTZ manual**.
Prioridade de PTZ	Determina a prioridade de câmeras PTZ. Quando muitos usuários em

Nome	Descrição
	um sistema de monitoramento desejam controlar a mesma câmera PTZ ao mesmo tempo, podem ocorrer conflitos. Esta situação pode ser evitada especificando-se uma prioridade de uso da(s) câmera(s) PTZ selecionada(s) pelos usuários/grupos com a função selecionada. Especifique uma prioridade de 1 a 32.000, onde 1 é a mais baixa. A prioridade padrão é 3.000. A função com prioridade mais alta é a única que pode controlar a(s) câmera (s) PTZ.
Gerenciar predefinições PTZ ou perfis de patrulha	Determina a permissão para adicionar, editar e excluir predefinições de PTZ e perfis de patrulha na câmera selecionada em Management Client e XProtect Smart Client. Para permitir que esta função use outras funções PTZ na câmera, habilite a permissão **PTZ manual**.
Travar/destravar predefinições PTZ	Determina se o papel pode bloquear e desbloquear posições predefinidas para a câmera selecionada.
Reservar sessões PTZ	Determina a permissão para definir a câmera selecionada no modo de sessão PTZ reservado. Em uma sessão PTZ reservada, outros usuários ou sessões de patrulha com maior prioridade PTZ não podem assumir o controle. Para permitir que esta função use outras funções PTZ na câmera, habilite a permissão **PTZ manual**.
Liberar sessões PTZ	Determina se a função selecionada pode liberar sessões PTZ de outros usuários do Management Client. As suas próprias sessões de PTZ sempre podem ser liberadas por você (independentemente dessa permissão).

Guia Fala (funções)

Relevante apenas se há alto-falantes no seu sistema. Especifique as seguintes permissões para alto-falantes:

Nome	Descrição
Falar	Determine se os usuários com a função selecionada poderão falar pelo(s) alto-falante(s) selecionado(s). Especifique o perfil de tempo ou deixe o valor padrão.
Prioridade de fala	Quando muitos usuários de clientes desejam falar pelo mesmo alto-falante ao mesmo tempo, podem ocorrer conflitos. Resolva o problema especificando uma prioridade de uso do(s) alto-falante(s) selecionado(s) pelos usuários/grupos com a função selecionada. Especifique uma prioridade desde **Muito baixa** a **Muito alta**. A função com a maior prioridade tem permissão para usar o alto-falante antes de outras funções. Se dois usuários com a mesma função quiserem falar ao mesmo tempo, o princípio de quem chegar primeiro se aplica.

Guia Gravações remotas (papéis)

Especifique as seguintes permissões para gravações remotas:

Nome	Descrição
Recuperar gravações remotas	Dá permissão para recuperar gravações nos clientes de câmeras, microfones, alto-falantes e dispositivos de metadados em locais remotos ou de armazenamentos no dispositivo em câmeras.

Guia Smart Wall (funções)

Por meio de funções, você pode conceder permissões de usuário relacionadas ao Smart Wall aos usuários do cliente:

Nome	Descrição
Ler	Permite que os usuários visualizem o Smart Wall selecionado no XProtect Smart Client.
Editar	Permite que os usuários visualizem o Smart Wall selecionado no Management Client.

Nome	Descrição
Excluir	Permite que os usuários excluam o Smart Wall selecionado no Management Client.
Operar	Permite que os usuários apliquem layouts ao Smart Wall selecionado no XProtect Smart Client e ativem as predefinições.
Reprodução	Permite que os usuários reproduzam dados gravados do Smart Wall selecionado no XProtect Smart Client.

Guia Evento externo (funções)

Especifique as seguintes permissões para eventos externos:

Nome	Descrição
Ler	Permite que os usuários pesquisem e visualizem o evento do sistema externo selecionado nos clientes e no Management Client.
Editar	Permite que os usuários editem o evento do sistema externo selecionado no Management Client.
Excluir	Permite que os usuários excluam o evento do sistema externo selecionado no Management Client.
Disparar	Permite que os usuários ativem o evento do sistema externo selecionado no nos clientes.

Guia Grupo de Visualização (funções)

Na guia **Grupo de visualização**, você especifica quais grupos de visualização os usuários e os grupos de usuários com a função selecionada podem usar nos clientes.

Especifique as seguintes permissões para grupos de visualização:

Nome	Descrição
Ler	Dá permissão para visualizar os grupos de visualização nos clientes e no Management Client. Grupos de visualização são criados no Management Client.
Editar	Dá permissão para editar propriedades em grupos de visualização no Management Client.
Excluir	Dá permissão para excluir grupos de visualização no Management Client.
Operar	Dá permissão para usar grupos de visualização no XProtect Smart Client, ou seja, para criar e excluir subgrupos e visualizações.

Aba Servidores (funções)

A especificação de permissões de função na guia **Servidores** só é relevante se seu sistema funcionar em uma configuração Milestone Federated Architecture.

Nome	Descrição
Sites	Dá permissão para visualizar o local selecionado no Management Client. Sites conectados são ligados pelo Milestone Federated Architecture. Para editar propriedades, você precisa Editar permissões no servidor de gerenciamento em cada site.

Consulte Configurando Milestone Federated Architecture na página 97 para mais informações.

Guia Matrix (funções)

Se você configurou destinatários do Matrix em seu sistema, pode configurar permissões de função do Matrix. A partir de um cliente é possível enviar vídeos para destinatários selecionados Matrix. Selecione os usuários que podem receber este na guia Matrix.

As seguintes permissões estão disponíveis:

Nome	Descrição
Ler	Determine se usuários e grupos com uma função têm permissão para selecionar e enviar vídeos para o destinatário Matrix a partir dos clientes.

Guia Alarmes (funções)

Se você usar alarmes na configuração do seu sistema para fornecer visão geral e controle central de sua instalação (incluindo quaisquer outros servidores XProtect), você pode usar a guia **Alarmes** para especificar as permissões de alarme para usuários e grupos com a função selecionada que eles devem ter, por exemplo, como lidar com alarmes nos clientes.

Em **Alarmes**, você especifica as permissões dos alarmes:

Permissão de segurança	Descrição
Gerenciamento	Dá permissão para gerenciar alarmes no Smart Client. Por exemplo, alterar prioridades de alarmes, reatribuir alarmes a outros usuários, reconhecer alarmes, alterar o estado de alarme de vários alarmes (por exemplo, de **Novo** para **Atribuído**). Para editar as configurações de alarme, você também precisa da permissão **Editar configurações de alarme**. Somente quando você isso é definido como permitido, a guia **Alarmes e Eventos** é exibida no diálogo **Opções**.
Visualização	Ativa a permissão para visualizar a guia **Gerenciador de alarmes** no XProtect Smart Client e recuperar alarmes e configurações de alarme por meio da API. Para visualizar alarmes no XProtect Smart Client, é necessário ativar a permissão de **Visualização** de ao menos uma definição de alarme. Por padrão, você visualiza alarmes de soluções de terceiros.
Desativar alarmes	Dá permissão para desativar alarmes.
Receber notificações	Dá permissão para receber notificações sobre alarmes em clientes XProtect Mobile e XProtect Web Client.
Editar configurações de alarme	Ativa a permissão para editar definições de alarme, estados de alarme, categorias de alarme, sons de alarme, retenção de alarme e retenção de eventos. Para editar as configurações de alarme, você também precisa da permissão **Gerenciar**.

Em **Definições de alarme**, você especifica as permissões de uma definição de alarme específica:

Nome	Descrição
Visualização	Ativa a permissão para visualizar definições de alarme, estados de alarme, categorias de alarme, sons de alarme, retenção de alarme e retenção de eventos.
Gravar	Ativa a permissão **Visualizar**.

Guia controle de acesso (funções)

Ao adicionar ou editar usuários básicos, usuários do Windows ou grupos, você pode especificar configurações de controle de acesso:

Nome	Descrição
Usar o controle de acesso	Permite que o usuário use qualquer recurso relacionado a controle de acesso nos clientes.
Visualizar lista de portadores de cartão	Permite ao usuário visualizar a lista de titulares na guia **Controle de acesso** nos clientes.
Receber notificações	Permite que o usuário receba notificações sobre solicitações de acesso nos clientes.

Guia LPR (funções)

Se o seu sistema for executado com XProtect LPR, especifique as seguintes permissões para os usuários:

Nome	Descrição
Usar LPR	Dá permissão para usar quaisquer recursos relacionados a LPR nos clientes.
Gerenciar listas de correspondências	Ativa a permissão para adicionar, importar, modificar, exportar e excluir listas de correspondências no Management Client.
Ler listas de correspondências	Ativa a permissão para visualizar listas de correspondências.

Guia Incidentes (funções)

Se você tiver XProtect Incident Manager, é possível especificar as seguintes permissões para suas funções.

Para dar a uma função de administrador do Management Client as permissões para gerenciar ou visualizar as propriedades do incidente, selecione o nó **Propriedades do incidente**.

Para dar a um operador do XProtect Smart Client permissão para visualizar as propriedades definidas do incidente, selecione **Propriedades do incidente** e dê permissão de **Visualização**. Para dar permissões gerais para gerenciar ou visualizar os projetos de incidente, selecione o nó **Projeto de incidente**. Expanda o nó **projeto de incidente** e selecione um ou mais nós secundários para dar permissões para esses recursos ou funcionalidades específicos adicionais.

Nome	Descrição
Gerenciamento	Permissão para gerenciar (visualizar, criar, editar e excluir) as configurações e as propriedades relacionadas a um recurso ou visualizar um elemento da interface do usuário representado pelo nó selecionado em Management Client ou XProtect Smart Client.
Visualização	Permissão para visualizar (mas não para criar, editar e excluir) as configurações e as propriedades relacionadas a um recurso, visualizar propriedades do incidente definidas ou visualizar um elemento da interface do usuário representado pelo nó selecionado em Management Client ou XProtect Smart Client.

Guia MIP (funções)

Por meio do MIP SDK, um fornecedor terceirizado pode desenvolver plug-ins personalizados para seu sistema, como por exemplo, integração a sistemas de controle de acesso externo ou funcionalidade semelhante. Os plug-ins de terceiros terão suas próprias configurações em guias individuais.

As configurações que você altera dependem do plug-in. As configurações padrão de plug-ins podem ser encontradas na guia **MIP**.

Usuário básico (nó de segurança)

Há dois tipos de conta de usuário no Milestone XProtect VMS: Usuários básicos e usuários Windows.

Usuários básicos são contas de usuário criadas no Milestone XProtect VMS. Trata-se de uma conta de usuário dedicada do sistema com um nome de usuário básico e autenticação de senha para o usuário individual.

Usuários Windows são contas de usuário adicionadas através de Microsoft de Active Directory.

Há algumas diferenças entre usuários básicos e usuários Windows:

- Usuários básicos são autenticados por uma combinação de nome de usuário e senha e específicos de um sistema/site. Observe que, mesmo quando um usuário básico criado em um site federado tem o mesmo nome e a mesma senha que um usuário básico em outro site federado, o usuário básico tem acesso somente ao site em que ele foi criado.
- Os usuários do Windows são autenticados com base em seu login do Windows e são específicos de uma máquina.

Nó do painel do sistema

Nó do painel do sistema

No nó **Painel do sistema**, você encontra diferentes funcionalidades para monitorar o seu sistema e seus diversos componentes do sistema.

Nome	Descrição
Tarefa atual	Obtenha uma visão geral das tarefas em andamento num servidor de gravação selecionado.
Monitor do sistema	Monitorar o status de seus servidores e câmeras com parâmetros que você define.
Limites do monitor do sistema	Define valores limite para os parâmetros do monitor no servidor e monitora os quadros usados no Monitor Do Sistema.
Proteção de Evidências	Tenha uma visão geral de todos os dados protegidos do sistema.
Relatórios de configuração	Imprimir um relatório com a sua configuração do sistema. Você pode decidir o que incluir no relatório.

Tarefas atuais (nó do Painel do sistema)

A janela **Tarefas atuais** mostra uma visão geral das tarefas em andamento em um servidor de gravação selecionado. Se você iniciou uma tarefa que leva muito tempo e é executada em segundo plano, pode abrir a janela **Tarefas atuais** para ver o andamento da tarefa. Alguns exemplos de tarefas demoradas iniciadas pelo usuário são atualizações de firmware e movimentação de hardware. Você pode ver informações sobre hora de início, hora de término estimada e progresso da tarefa.

As informações exibidas na janela **Tarefas atuais** não são atualizadas dinamicamente, mas um instantâneo das tarefas atuais a partir do momento em que você abriu a janela. Se a janela está aberta há algum tempo, atualize as informações clicando no botão **Atualizar** no canto inferior direito da janela.

Monitor do sistema (nó Painel de controle do sistema)

A funcionalidade do **Monitor do sistema** fornece uma visão geral rápida e visual do bem-estar atual dos servidores e câmeras do seu sistema.

Janela do painel de controle do monitor do sistema

Quadros

A parte superior da janela do **Painel de controle do monitor do sistema** mostra quadros coloridos que representam o estado do hardware do servidor do seu sistema e do hardware da câmera.

O quadros mudam de estado e, assim, de cor conforme os valores-limite estabelecidos no nó **Limites do Monitor do sistema**. Para obter mais informações, consulte Limites do monitor do sistema (nó Painel de controle do) na página 582. Defina os limites, para que as cores dos blocos signifiquem o seguinte:

Cor dos quadros:	Descrição
Verde	Estado **Normal**. Tudo está correndo normalmente.
Amarelo	Estado **Atenção**. Um ou mais parâmetros de monitoramento está acima do valor limite para o estado **Normal**.
Vermelho	Estado **Crítico**. Um ou mais parâmetros de monitoramento está acima do valor limite para os estados **Normal** e **Atenção**.

Lista de hardware com parâmetros de monitoramento

Se você clicar em um quadro, poderá ver o estado de cada parâmetro de monitoramento selecionado para cada hardware representado pelo quadro na parte inferior da janela do **painel do monitor do sistema**.

Exemplo: Os parâmetros de monitoramento ao vivo de uma câmera FPS atingiram o estado de Atenção.

Personalizar janela do painel de controle

Selecione **Personalizar** no canto superior direito da janela para abrir a janela **Personalizar painel de controle**.

Na janela **Personalizar painel de controle**, você pode selecionar qual quadro criar, editar ou excluir. Ao criar ou editar quadros, você pode selecionar qual hardware e quais parâmetros de monitoramento deseja monitorar no bloco.

Janela de detalhes

Se selecionar um quadro e, em seguida, na lista de hardware com parâmetros de monitoramento, selecionar o botão **Detalhes** à direita de uma câmera ou servidor, você pode – dependendo do hardware selecionado – visualizar informações do sistema e criar relatórios sobre:

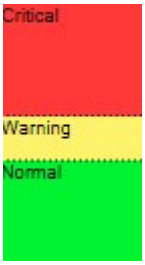
Hardware	Informações
Servidor de gerenciamento	Exibir dados sobre: • Uso de CPU • Memória disponível Selecione **Histórico** para ver os estados históricos de seu hardware e criar um relatório sobre os dados acima.
Servidor(es) de gravação	Exibir dados sobre: • Uso de CPU • Memória disponível • Discos • Armazenamento • Rede • Câmeras Selecione **Histórico** para ver os estados históricos de seu hardware e criar um relatório sobre os dados acima.
Servidores de gravação de failover	Exibir dados sobre: • Uso de CPU • Memória disponível • Servidores de gravação monitorados Selecione **Histórico** para ver os estados históricos de seu hardware e criar um relatório sobre os dados acima.
Servidores de log, servidores de eventos e mais	Exibe dados a respeito • Uso de CPU • Memória disponível

Hardware	Informações
	Selecione **Histórico** para ver os estados históricos de seu hardware e criar um relatório sobre os dados acima.
Câmeras	Exibir dados sobre: • Armazenamento • Espaço usado • FPS ao vivo (Padrão) • FPS de gravação • Formato de vídeo ao vivo • Formato de gravação de vídeo • Dados de mídia recebidos (Kbit/s) • Memória disponível Selecione o nome da câmera para ver seus estados históricos e criar um relatório sobre: • Dados recebidos da câmera • Uso do disco da câmera

Se você acessar os detalhes do monitor a partir de um sistema operacional de um servidor, poderá ver uma mensagem sobre **Configuração de segurança melhorada do Internet Explorer**. Siga as instruções para adicionar a página **Monitor do sistema** à **Zona de sites confiáveis** antes de prosseguir.

Limites do monitor do sistema (nó Painel de controle do)

Os limites do monitor do sistema permitem definir e ajustar os limites quando os quadros no **Painel de controle do monitor do sistem** a devem indicar visualmente que o hardware do sistema muda de estado. Por exemplo, quando o uso da CPU de um servidor muda de um estado normal (verde) para um estado de alerta (amarelo) ou de um estado de alerta (amarelo) para um estado crítico (vermelho).



Exemplo de limites entre os três estados

Você pode alterar os limites de servidores, câmeras, discos e armazenamento, e todos os limites têm alguns botões e configurações comuns.

Elementos comuns da interface do usuário

Botões e configurações	Descrição	Unidade
Intervalo de cálculo	Frequentemente, ocorrem pequenas interrupções na conexão com o hardware diferente. Se você especificar um intervalo de cálculo de 0 segundo, todas essas interrupções curtas irão disparar alertas sobre mudanças no estado do hardware. Portanto, defina um intervalo de cálculo de algum comprimento. Se você definir um cálculo interno de um (1) minuto, significa que você só receberá alertas se o valor médio de todo o minuto exceder o limite. Com a configuração correta do intervalo de cálculo, você não receberá alertas de falso positivo, mas apenas alertas sobre problemas constantes com, por exemplo, uso de CPU ou consumo de memória. Para alterar os valores dos intervalos de cálculo, consulte Editar limites para quando os estados do hardware devem mudar na página 306.	seg
Avançado	Se você selecionar o botão **Avançado**, poderá definir limites e intervalos de cálculo para servidores, câmeras, discos e armazenamento individuais. Para obter mais informações, veja abaixo.	-
Criar regra	Você pode combinar eventos do **Monitor do sistema** e regras para acionar ações, por exemplo, quando o uso da CPU de um servidor estiver crítico ou quando o espaço livre em disco estiver acabando. Para obter mais informações, consulte Regras e eventos (explicados) na página 81 e Adicionar regras na página 282.	-

Limites do servidor

Limite	Descrição	Unidade
Uso de CPU	Limites para o uso de CPU nos servidores que você monitora.	%
Memória disponível	Limites para a RAM em uso nos servidores que você monitora.	MB
Decodificação NVIDIA	Limites para o uso da descodificação NVIDIA nos servidores que você monitora.	%
Memória NVIDIA	Limites para a NVIDIA RAM em uso nos servidores que você monitora.	%
Renderização NVIDIA	Limites para o uso da renderização NVIDIA nos servidores que você monitora.	%

Limites da câmera

Limite	Descrição	Unidade
FPS ao vivo	Limites para os FPSs da câmera em uso quando vídeo ao vivo for mostrado nas câmeras que você monitora.	%
FPS de gravação	Limites para os FPSs das câmeras em uso quando o sistema estiver gravando vídeo nas câmeras que você monitora.	%
Espaço usado	Limites para o espaço usado pelas câmeras que você monitora.	GB

Limites de disco

Limite	Descrição	Unidade
Espaço livre	Limites para o espaço disponível nos discos que você monitora.	GB

Limites de armazenamento

Limite	Descrição	Unidade
Tempo de retenção	Limite que mostra uma previsão para quando o espaço termina no seu armazenamento. O estado é mostrado com base na configuração do seu sistema e atualizado duas vezes ao dia.	Dias

Proteção de evidências (nó Painel do sistema)

No **Painel do Sistema**, **Proteção de evidências** exibe uma visão geral de todos os dados protegidos do sistema de monitoramento atual.

Os metadados a seguir estão disponíveis para todos os bloqueios de evidência:

- Data de início e fim para os dados protegidos
- O usuário que protegeu a evidência
- Quando a evidência não estiver mais protegida
- Onde os dados foram armazenados
- O tamanho de cada proteção de evidências

Todas as informações mostradas na janela **Proteção de evidências** são instantâneos. Pressione F5 para recarregar.

Relatórios de configuração (nó do Painel do sistema)

Você faz muitas escolhas ao instalar e configurar seu sistema VMS e pode ser necessário documentá-las. Com o tempo, também é difícil lembrar de todas as configurações que você alterou desde a instalação e a configuração inicial – ou apenas durante os últimos meses. Por isso é possível imprimir um relatório com todas as suas opções de configuração.

As seguintes configurações estão disponíveis ao criar e imprimir relatórios de configuração:

Nome	Descrição
Relatórios	Lista de elementos que podem ser incluídos em um relatório de configuração.
Selecionar tudo	Adiciona todos os elementos na lista **Relatórios** ao relatório de configuração.

Nome	Descrição
Limpar Tudo	Remove todos os elementos da lista **Relatórios** do relatório de configuração.
Página inicial	Personalize a primeira página do relatório.
Formatação	Formate o relatório.
Excluir dados sensíveis	Remove dados pessoais como nomes de usuário, endereços de e-mail e outros tipos de dados sensíveis do relatório de configuração e o torna compatível com o GDPR. Informações sobre o proprietário da licença são sempre excluídas do relatório.
Exportar	Selecione um local para salvar o relatório e criá-lo como PDF.

Nó Registros de servidor

Nó Registros de servidor

Registros do sistema (guia)

Cada linha de um registro representa uma entrada de registro. Uma entrada de registro contém diversos campos de informação:

Nome	Descrição
Nível de registro	Informações, aviso ou erro.
Hora local	Carimbado com a hora local do servidor de seu sistema.
Texto da mensagem	O número de identificação do incidente registrado.
Categoria	O tipo do incidente registrado.
Tipo de fonte	O tipo de equipamento no qual o incidente registrado ocorreu, por

Nome	Descrição
	exemplo, servidor ou dispositivo.
Nome da fonte	O nome do equipamento em que ocorreu o incidente registrado.
Tipo de evento	O tipo de evento representado pelo incidente registrado.

Registros de auditoria (guia)

Cada linha de um registro representa uma entrada de registro. Uma entrada de registro contém diversos campos de informação:

Nome	Descrição
Hora local	Carimbado com a hora local do servidor de seu sistema.
Texto da mensagem	Mostra a descrição do incidente registrado.
Permissão	A informação sobre se a ação do usuário remoto foi permitida (concedida) ou não.
Categoria	O tipo do incidente registrado.
Tipo de fonte	O tipo de equipamento no qual o incidente registrado ocorreu, por exemplo, servidor ou dispositivo.
Nome da fonte	O nome do equipamento em que ocorreu o incidente registrado.
Usuário	O nome de usuário do usuário remoto causando incidente registrado.
Local do usuário	O endereço IP ou nome do host do computador de onde o usuário remoto causou o incidente registrado.

Registros acionados por regras (guia)

Cada linha de um registro representa uma entrada de registro. Uma entrada de registro contém diversos campos de informação:

Nome	Descrição
Hora local	Carimbado com a hora local do servidor de seu sistema.
Texto da mensagem	Mostra a descrição do incidente registrado.
Categoria	O tipo do incidente registrado.
Tipo de fonte	O tipo de equipamento no qual o incidente registrado ocorreu, por exemplo, servidor ou dispositivo.
Nome da fonte	O nome do equipamento em que ocorreu o incidente registrado.
Tipo de evento	O tipo de evento representado pelo incidente registrado.
Nome da regra	O nome da regra que ativa a entrada de registro.
Nome do serviço	O nome do serviço onde ocorreu o incidente registrado.

Nó de uso de metadados

Pesquisa de metadados e metadados

Para gerenciar e configurar dispositivos de metadados, consulte Mostrar ou ocultar as categorias de pesquisa de metadados e filtros de pesquisa na página 308.

O que são metadados?

Metadados são dados sobre dados, por exemplo, dados que descrevem a imagem do vídeo, o conteúdo ou objetos na imagem, ou a localização de origem da gravação da imagem.

Os metadados podem ser gerados por:

- O próprio dispositivo entregando os dados, por exemplo, uma câmera entregando vídeo
- Um sistema de terceiros ou integração através de um driver genérico de metadados

Pesquisa de metadados

A pesquisa de metadados é qualquer pesquisa por gravações de vídeo no XProtect Smart Client que usa categorias e filtros de pesquisa relacionados aos metadados.

As categorias de pesquisa de metadados padrão do Milestone são:

- Local:Os usuários podem definir coordenadas geográficas e pesquisar raios a partir de tais coordenadas.
- Pessoas: Os usuários podem pesquisar por gênero e altura e idade aproximadas, bem como selecionar a opção de mostrar resultados com rostos.
- Veículos:Os usuários podem pesquisar por cor, velocidade e tipo de veículo, bem como por placas específicas.

Requisitos da pesquisa de metadados

Para obter os resultados da pesquisa, você precisa de uma das condições a seguir:

- Pelo menos um dispositivo no seu sistema de vigilância por vídeo, que possa realizar análises de vídeo e esteja configurado corretamente.
- Um serviço de processamento de vídeo no seu sistema de vigilância por vídeo que gere metadados

Em qualquer um dos casos, metdados deverão estar no formato de metadados exigido.

Para mais informações, consulte a documentação para integração da pesquisa de metadados.

Nó de controle de acesso

Propriedades do controle de acesso

Guia Configurações Gerais (Controle de Acesso)

Nome	Descrição
Ativar	Os sistemas são habilitados por padrão, o que significa que são visíveis no XProtect Smart Client para usuários com permissões suficientes e que o sistema XProtect recebe eventos de controle de acesso. Você pode desativar um sistema, por exemplo, durante a manutenção, para evitar alarmes desnecessários.
Nome	O nome do sistema de controle de acesso integrado como aparece no aplicativo de gerenciamento e nos clientes. Você pode substituir o nome existente por um novo.
Descrição	Mostra uma descrição da integração do controle de acesso. Isto é opcional.

Nome	Descrição
Plug-in de integração	Mostra o tipo de sistema de controle de acesso selecionado durante a integração inicial.
Última atualização de configuração	Mostra a data e a hora da última vez que a configuração foi importada do sistema de controle de acesso.
Atualizar configuração	Clique no botão quando precisar refletir as alterações de configuração feitas no sistema de controle de acesso em XProtect, por exemplo, se você adicionou ou excluiu uma porta. É mostrado um resumo das mudanças na configuração do sistema de controle de acesso. Reveja a lista para certificar-se que seu sistema de controle de acesso está refletido corretamente antes de aplicar a nova configuração.
Autenticação do operador exigida	Ativa um login adicional para os usuários do cliente se o sistema de controle de acesso suporta permissões de usuário diferenciados. Se você ativar esta opção, o sistema de controle de acesso não ficará disponível no cliente do XProtect Mobile. Esta opção só é visível se o plug-in de integração suporta permissões de usuário diferenciados.

Os nomes e o conteúdo dos seguintes campos são importados a partir do plug-in de integração. Abaixo, exemplos de alguns campos típicos:

Nome	Descrição
Endereço	Digite o endereço do servidor que hospeda o sistema de controle de acesso integrado.
Porta	Especifique o número da porta no servidor para o qual o sistema de controle de acesso está conectado.
Nome de usuário	Digite o nome do usuário, conforme definido no sistema de controle de acesso, que deve ser o administrador do sistema integrado no XProtect.
Senha	Especifique a senha para o usuário.

Portas e guia Câmeras Associadas (Controle de Acesso)

Esta guia fornece mapeamentos entre pontos de acesso de portas e câmeras, microfones ou alto-falantes. Você associa câmeras como parte do assistente de integração, mas pode alterar a configuração a qualquer momento. Os mapeamentos a microfones e alto-falantes estão implícitos através do microfone ou alto-falante relacionado na câmera.

Nome	Descrição
Portas	Lista os pontos de acesso de porta disponíveis definidos no sistema de controle de acesso, agrupados por porta. Para uma navegação mais fácil para as portas importantes, você pode filtrar as portas no seu sistema de controle de acesso na caixa de lista suspensa no topo. **Ativado**: Por padrão, as portas licenciadas estão desativadas. Você pode desativar uma porta para liberar uma licença. **Licença**: Mostra se uma porta está licenciada ou se a licença expirou. Quando a porta está desativada, o campo permanece em branco. **Remover**: Clique em **Remover** para remover uma câmera de um ponto de acesso. Se remover todas as câmeras, a caixa de seleção das câmeras associadas é limpa automaticamente.
Câmeras	Lista as câmeras configuradas no sistema XProtect. Selecione uma câmera da lista e arraste e solte-a no ponto de acesso relevante para associar o ponto de acesso com a câmera.

Guia Eventos de Controle de acesso (Controle de Acesso)

As categorias de eventos permitem agrupar eventos. A configuração de categorias de eventos afeta o comportamento do controle de acesso no sistema XProtect e permite, por exemplo, definir um alarme para disparar um único alarme em vários tipos de evento.

Nome	Descrição
Evento de controle de acesso	Lista os eventos de controle de acesso importados do sistema de controle de acesso. O plug-in de integração controla ativação e desativação padrão de eventos. Você pode desativar ou ativar eventos a qualquer momento após a integração.

Nome	Descrição
	Quando um evento é ativado, ele é armazenado no banco de dados de eventos XProtect e fica, por exemplo, disponível para a filtragem em XProtect Smart Client.
Tipo de fonte	Mostra a unidade de controle de acesso que pode disparar o evento de controle de acesso.
Categoria de evento	Atribua nenhuma, uma ou mais categorias de eventos para os eventos de controle de acesso. O sistema mapeia automaticamente as categorias de eventos relevantes para os eventos durante a integração. Isso permite uma configuração padrão no sistema XProtect. Você pode alterar o mapeamento a qualquer instante. Categorias integradas de eventos são: • Acesso negado • Acesso concedido • Solicitação de acesso • Alarme • Erro • Aviso Eventos e categorias de eventos definidos pelo plug-in de integração também são mostrados, mas também é possível definir suas próprias categorias de eventos. Consulte **Categorias definidas pelo usuário**. ⚠ Se você alterar as categorias de eventos em XProtect Corporate, certifique-se de que as regras de controle de acesso existentes ainda funcionam.
Categorias definidas pelo usuário	Permite criar, modificar ou excluir categorias de eventos definidas pelo usuário. Você pode criar categorias de eventos quando as categorias integradas não atendem às suas necessidades, por exemplo, em conexão com a definição de eventos disparadores para ações de controle de acesso. As categorias são globais para todos os sistemas de integração adicionados ao sistema XProtect. Elas permitem configurar o gerenciamento de sistemas cruzados, por exemplo, sobre definições de alarme.

Nome	Descrição
	Se você excluir uma categoria de evento definida pelo usuário, receberá um aviso caso ela esteja sendo utilizada por qualquer integração. Se você excluí-la mesmo assim, todas as configurações feitas com esta categoria, por exemplo, as ações de controle de acesso, não funcionarão mais.

Guia Notificação de Solicitação de Acesso (Controle de Acesso)

Selecione as notificações de solicitação de acesso que aparecem na tela XProtect Smart Client quando um determinado evento ocorrer.

Nome	Descrição
Nome	Dar um nome à notificação de solicitação de acesso.
Adicionar notificação de solicitação de acesso	Clique para adicionar e definir notificações de solicitação de acesso. Para excluir uma notificação, clique no **X** no lado direito. Se um usuário de XProtect Smart Client faz login em um site pai em uma hierarquia Milestone Federated Architecture, notificações de solicitação de acesso dos sites filhos também são mostradas no XProtect Smart Client.
Detalhes da notificação de solicitação de acesso	Especifique quais câmeras, microfones ou alto-falantes mostrados nas notificações de solicitação de acesso quando ocorrer um determinado evento. Também especifique o som para alertar o usuário quando a notificação aparece.
Adicionar comando	Selecione os comandos que devem estar disponíveis como botões nos diálogos de notificações de solicitação de acesso no XProtect Smart Client. Comandos relacionados de solicitação de acesso: • Ativa todos os comandos relacionados com as operações de solicitação de acesso disponíveis na unidade da fonte. Por exemplo, **Abrir porta** Todos os comandos relacionados:

Nome	Descrição
	• Ativa todos os comandos na unidade da fonte Comando de controle de acesso: • Ativa um comando de controle de acesso selecionado Comando do sistema: • Ativa um comando predefinido no sistema XProtect Para excluir um comando, clique no **X** no lado direito.

Guia Titulares de Cartão (Controle de Acesso)

Use a aba **Titular do cartão** para analisar as informações dos titulares obtidas no sistema de controle de acesso.

Nome	Descrição
Pesquisar titular do cartão	Digite os primeiros caracteres do nome de um titular do cartão e ele aparece na lista, se existir.
Nome	Lista os nomes dos titulares do cartão recuperados do sistema de controle de acesso.
Tipo	Lista o tipo do titular do cartão, por exemplo: • Funcionário • Guarda • Convidado

Se o seu sistema de controle de acesso suporta inclusão/exclusão de fotos no sistema XProtect, você pode inserir fotos dos titulares. Isso é útil se o sistema de controle de acesso não inclui fotos dos titulares de cartões.

Nome	Descrição
Selecionar imagem	Especifique o caminho a um arquivo com uma foto do titular do cartão. Este botão não estará visível se o sistema de controle de acesso gerencia as imagens. Os formatos de arquivo permitidos são .bmp, .png e .jpg. As imagens são redimensionadas para maximizar a visualização. Milestone recomenda que se use uma imagem quadrática.
Excluir imagem	Clique para excluir a imagem. Se o sistema de controle de acesso tinha uma imagem, esta imagem é mostrada após a eliminação.

Nó de incidentes

Propriedades do incidente (nó Incidentes)

As informações a seguir descrevem as configurações relacionadas ao XProtect Incident Manager.

Você define todas as propriedades do incidente para os operadores do XProtect Smart Client nestas guias:

- Tipos
- Estados
- Categorias
- Categoria 1-5

Todas as propriedades do incidente têm as configurações abaixo:

Nome	Descrição
Nome	Nomes de propriedades do incidente não têm de ser únicos, mas nomes únicos e descritivos é vantajoso em várias situações.
Descrição	Uma explicação mais detalhada da propriedade do incidente definida. Por exemplo, se você criou uma categoria denominada *Localização*, a descrição poderia ser *Onde o incidente aconteceu?*

Nó de transação

Fontes de transação (nó Transação)

A tabela a seguir descreve as propriedades para as fontes de transação.

Para obter mais informações sobre como adicionar uma fonte, consulte Adicionar fonte de transação (assistente).

Fontes de transação (propriedades)

Nome	Descrição
Ativar	Se você deseja desativar a fonte de transação, desmarque esta caixa de seleção. O fluxo de dados da transação para, mas os dados já importados permanecem no servidor de eventos. Você pode ainda visualizar as transações de uma fonte de transação desativada em XProtect Smart Client durante o seu período de retenção. Mesmo uma fonte de transação com deficiência exige uma licença de fonte de transação.
Nome	Se você desejar alterar o nome, digite um novo nome aqui.
Conector	Você não pode alterar o conector que você selecionou quando criou a fonte de transação. Para selecionar um conector diferente, você precisa criar uma nova fonte de transação e, durante o assistente, selecionar o conector que deseja.
Definições da transação	Você pode selecionar uma definição de transação diferente que define como transformar os dados de transação recebidos em transações e linhas de transação. Isso inclui definir: • Quando a transação inicia e termina • Como as transações são exibidas em XProtect Smart Client
Período de Retenção	Especificar, em dias, por quanto tempo os dados de transação são mantidos no servidor de eventos. O padrão de período de retenção é de 30 dias. Quando o período de retenção expira, os dados são eliminados automaticamente. Isso é para evitar a situação em que a capacidade de armazenamento do banco de dados for excedida. O valor mínimo é de 1 dia, sendo que o valor máximo é de 1.000 dias.

Nome	Descrição
Conector de cliente TCP	Se você selecionou **Conector de cliente TCP**, especifique estas configurações: • **Nome do host**: digite o nome do host do servidor TCP associado à fonte de transação • **Porta**: digite o nome da porta no servidor TCP associado com a fonte de transação
Conector em porta serial	Se você tiver selecionado **conector de porta Serial**, especifique as configurações e certifique-se de que elas correspondem às configurações na fonte de transação: • **Porta Serial**: selecione a porta COM • **Baud taxa**: especifique o número de bits transmitidos por segundo • **Paridade**: especifique o método de detecção de erros nas transmissões. Por padrão, **Nenhum** é selecionado • **Bits de dados**: especifique o número de bits usados para representar um caractere de dados • **Bits de parada**: especifique o número de bits para indicar quando um byte foi transmitido. A maioria dos dispositivos precisam de 1 bit • **Aperto de mãos**: especifique o método aperto de mãos que determina o protocolo de comunicação entre a fonte de transação e o servidor de eventos

Definições de transação (nó Transação)

A tabela a seguir descreve as propriedades das definições a serem usadas para as fontes de transação.

Para obter mais informações sobre como criar e adicionar definições de transação, consulte Criar e adicionar definições de transações.

Definições de transação (propriedades)

Nome	Descrição
Nome	Digite um nome.
Codificando	Selecione o conjunto de caracteres usado pela fonte de transação, por exemplo, a caixa registradora. Isso ajuda XProtect Transact a converter os dados transacionais

Nome	Descrição
	para textos compreensíveis com os quais você pode trabalhar quando configurar a definição. Se você selecionar a codificação errada, os dados podem ser exibidos como um texto sem sentido.
Iniciar captação de dados	Coletar dados de transação de fontes de transação conectadas. Você pode usar os dados para configurar uma definição de transação. Espere por pelo menos uma, mas, de preferência, mais transações para completar.
Parar coleta de dados	Quando você tiver coletado dados suficientes para configurar a definição, clique neste botão.
Carregar a partir do arquivo	Se você deseja importar os dados de um arquivo já existente, clique neste botão. Normalmente, este é um arquivo que você criou anteriormente no formato de arquivo .capture. Ele pode ter outros formatos de arquivo. O importante aqui é que a codificação do arquivo importado corresponda à codificação selecionada para a definição atual.
Salvar em arquivo	Se você deseja salvar os dados não processados coletados em um arquivo, clique neste botão. Você pode reutilizá-lo mais tarde.
Tipo de correspondência	Selecione o tipo de correspondência para pesquisar pelo padrão de início e de interrupção nos dados não processados coletados: • Use correspondência exata: A pesquisa identifica sequências de caracteres que contêm exatamente o que você digitou nos campos **Padrão de início** e **Padrão de interrupção**

Nome	Descrição
	• Usar caracteres curinga: A pesquisa identifica sequências de caracteres que contêm tudo aquilo que você inseriu nos campos **Padrão de início** e **Padrão de interrupção** em combinação com um símbolo curinga (*, #, ?) * compatível com qualquer número de caracteres. Por exemplo, se você entrou "Iniciar tra*ção", a pesquisa identifica as sequências que contêm "Iniciar transação". # coincide exatamente com 1 dígito. Por exemplo, se você entrou "# melancia", a pesquisa identifica as sequências que contêm, por exemplo, "1 melancia". ? coincide exatamente com 1 caractere. Por exemplo, você pode usar a expressão de pesquisa "Iniciar trans?ção" para identificar as sequências que contêm "Iniciar transação" • Usar expressão regular: Use esse tipo de correspondência para identificar as sequências que contêm métodos específicos de notação ou convenções, por exemplo, um formato de data ou de número de cartão de crédito. Para maiores informações, consulte o website da Microsoft (https://docs.microsoft.com/dotnet/standard/base-types/regular-expression-language-quick-reference/)
Dados não processados	Sequências de dados de transação de fontes de transação conectadas são apresentadas nesta seção.
Padrão de início	Especifique um padrão de início para indicar onde uma transação é iniciada. As linhas horizontais estão inseridas no campo **Pré-visualização** para visualizar o local onde a transação começa e termina, e ajudarão a manter transações individuais separadas.
Padrão de interrupção	Especifique um padrão de interrupção para indicar o local onde uma transação termina. Um padrão de interrupção não é obrigatório, mas é útil se os dados recebidos contiverem informações irrelevantes, tais como informações sobre o horário de abertura ou ofertas especiais entre as transações propriamente ditas. Se você não especificar um padrão de interrupção, o fim do recibo é definido a partir de onde o recibo seguinte começar. O início é determinado pelo que está escrito no campo **Padrão de início**.
Adicionar filtro	Use o botão **Adicionar filtros** para mostrar os caracteres que você deseja que sejam omitidos em XProtect Smart Client ou substituídos por outros caracteres ou uma

Nome	Descrição
	quebra de linha. Substituir os caracteres é útil quando a sequência de fontes de transação contiver caracteres de controle para fins de não impressão. Adicionar quebras de linha é necessário para fazer com que recibos em XProtect Smart Client se assemelhem aos recibos originais.
Filtrar texto	Exibe os caracteres selecionados no momento, na seção **Dados não processados**. Se você souber quais caracteres deseja que sejam omitidos ou substituídos, mas que não ocorrem na sequência de dados não processados coletados, você pode digitar os caracteres manualmente no campo **Caracteres**. Se o caractere é um caractere de controle, você precisa digitar o seu valor byte hexadecimal. Use este formato para o valor do byte: {XX} e {XX, XX,...} se os caracteres consistirem em mais bytes.
Ação	Para cada um dos filtros que você adicionar, você deve especificar o modo como os caracteres que você selecionou são tratados: • Omitir: os caracteres que você selecionar serão filtrados • Substituir: os caracteres que você selecionar serão substituídos pelos caracteres que você especificar • Adicionar quebra de linha: os caracteres que você selecionar serão substituídos por uma quebra de linha
Substituição	Digite o texto para substituir os caracteres selecionados. Só é relevante se você tiver selecionado a ação **Substituir**.
Remova caracteres de controle não definidos como texto de filtro	Remova caracteres não imprimíveis que ainda não foram removidos após adicionar filtros. No painel **Dados brutos** e na seção **Pré-visualização**, veja como as sequências de dados transacionais mudam quando você ativa ou desativa essa configuração.
Visualizar	Use a seção **Pré-visualização** para verificar que você identificou e filtrou os caracteres indesejados. A saída que você vê aqui se assemelha a um recibo da vida real como em XProtect Smart Client.

Nó de alarmes

Definições de alarme (nó de Alarmes)

Quando o sistema registra um evento no seu sistema, você pode configurar o sistema para gerar um alarme no XProtect Smart Client. Você deve definir alarmes antes que possa usá-los, e os alarmes são definidos com base em eventos registrados nos servidores do sistema. Você também pode usar os eventos definidos pelo usuário para acionar alarmes e usar o mesmo evento para acionar vários alarmes diferentes.

Configurações da definição de alarme:

Nome	Descrição
Ativar	Por padrão, a definição do alarme está habilitada. Desmarque a caixa para desativar.
Nome	Nomes de alarmes não têm de ser únicos, mas usar nomes únicos e descritivos é vantajoso em várias situações.
Instruções	Digite um texto descritivo sobre o alarme e como resolver o problema que causou o alarme. O texto aparece em XProtect Smart Client quando o usuário manipula o alarme.
Evento disparador	Selecione a mensagem de evento para usar quando o alarme for acionado. Escolha a partir de dois menus suspensos: • O primeiro menu suspenso: Selecione o tipo de evento, por exemplo, evento de análise e evento de sistema • O segundo menu suspenso: Selecione a mensagem de evento específico a usar. As mensagens disponíveis são determinadas pelo tipo de evento selecionado no primeiro menu suspenso
Fontes	Especifique as fontes que dão origem aos eventos. Além de câmeras ou outros dispositivos, fontes também podem ser definidas por plug-ins, por exemplo, VCA e MIP. As opções dependem do tipo de evento que você selecionou.

Disparar alarme:

Nome	Descrição
Perfil de tempo	Selecione o botão **Perfil de tempo** para especificar o intervalo de tempo no qual a definição de alarme estará ativa. Somente o perfil tempo definido de acordo com as **Regras e Eventos** é mostrado na lista. Se nenhum for definido, apenas a opção **Sempre** estará disponível.
Baseado em evento	Se quiser que o alarme seja baseado em um evento, selecione este botão. Uma vez selecionado, especifique os eventos de início e de parada. Você pode selecionar eventos de hardware definidos em câmeras, servidores de vídeo e entrada. Consulte também Visão geral de eventos. Também podem ser usadas definições de eventos globais/manuais. Consulte também Eventos definidos pelo usuário (explicado).

Ação do operador exigida:

Nome	Descrição
Limite de tempo	Selecionar um limite de tempo para quando a ação do operador é solicitada. O valor padrão é 1 minuto. O limite de tempo não é ativado antes de um evento ser anexado no menu suspenso **Evento de ativação**.
Eventos ativados	Selecione qual evento ativar quando o tempo limite for atingido.

Mapas:

Nome	Descrição
Visualização do gerenciador de alarmes	Atribua um mapa inteligente ou um mapa alarme, quando o alarme estiver listado em XProtect Smart Client > **Gerenciador de alarmes**. O mapa inteligente exibe alarmes se eles forem acionados por um dispositivo e se o dispositivo for adicionado ao mapa inteligente.

Outros:

Nome	Descrição
Câmeras relacionadas	Selecione até 15 câmeras para incluir na definição de alarme, mesmo que elas próprias não acionem o alarme. Isso pode ser relevante, por exemplo, se você tiver selecionado uma mensagem de evento externo (como uma porta sendo aberta) como a fonte de seu alarme. Ao definir uma ou mais câmeras perto da porta, você pode anexar gravações do incidente das câmeras ao alarme.
Proprietário inicial do alarme	Selecione um usuário padrão responsável pelo alarme.
Prioridade inicial do alarme	Selecione uma prioridade para o alarme. Use essas prioridades no XProtect Smart Client para determinar a importância de um alarme.
Categoria do alarme	Selecione uma categoria de alarme para o alarme, por exemplo, **Falso alarme** ou **Precisa de investigação**.
Eventos acionados por alarme	Defina um evento que o alarme pode disparar no XProtect Smart Client.
Fechamento automático de alarme	Se você quer que um evento específico pare o alarme automaticamente, marque esta caixa de seleção. Nem todos os eventos podem disparar alarmes. Desmarque a caixa de seleção para desativar o alarme novo desde o início.
Alarme atribuível a administradores	Marque a caixa de seleção para incluir usuários com uma função de administrador na lista **Atribuído a**. A lista **Atribuído a** está nos detalhes de alarme, na guia **Gerenciador de Alarmes**, no XProtect Smart Client. Desmarque a caixa de seleção para filtrar usuários com uma função de administrador na lista **Atribuído a**, com o objeto de reduzi-la.

Definições de dados de alarme (nó de Alarmes)

Ao configurar definições de dados de alarme, especifique o seguinte:

Guia Níveis de dados de alarme

Prioridades

Nome	Descrição
Nível	Adicione novas prioridades, com números de nível de sua escolha, ou use/edite os níveis de prioridade padrão (números 1, 2 ou 3). Esses níveis de prioridade são utilizados para configurar a definição **Prioridade inicial do alarme**.
Nome	Digite um nome para a entidade. Você pode criar a quantidade que quiser.
Som	Selecione o som a ser associado com o alarme. Use um desses se desejar os sons padrão ou adicione mais nas **Configurações de som**.
Repetir som	Decida se o som deve ser reproduzido uma vez ou repetidamente até que no XProtect Smart Client, o operador clique no alarme na lista de alarmes.
Ativar notificações na área de trabalho	Para cada prioridade de alarme, você pode ativar ou desativar as notificações na área de trabalho. Se estiver usando um VMS XProtect que suporte perfis Smart Client você também deve ativar notificações nos perfis Smart Client necessários. Consulte Guia Gerenciador de Alarmes (perfis Smart Client) na página 486.

Estados

Nome	Descrição
Nível	Além dos níveis de estado padrão (números **1**, **4**, **9** e **11**, os quais não podem ser editados ou reutilizados), adicione novos estados com números de nível de sua escolha. Esses níveis de estado só são visíveis na *Lista de alarmes* do XProtect Smart Client.

Categorias

Nome	Descrição
Nível	Adicione novas categorias com números de níveis à sua escolha. Esses níveis de categoria são utilizados para definir a configuração da **Categoria inicial do alarme**. O nível 99 é reservado para o alarme de Alerta de Emergência no cliente do XProtect Mobile.
Nome	Digite um nome para a entidade. Você pode criar a quantidade que quiser.

Aba Configuração de lista de alarmes

Nome	Descrição
Colunas disponíveis	Use > para selecionar quais colunas devem estar disponíveis na *Lista de alarmes* do XProtect Smart Client. Use < para limpar a seleção. Quando terminar, **Colunas selecionadas** devem conter os itens a ser incluídos.

Guia Motivos para encerramento

Nome	Descrição
Ativar	Selecione para ativar que todos os alarmes devem ter uma razão para serem encerrados antes que sejam finalizados.
Motivo	Adicione razões para encerramento entre as quais o usuário pode escolher quando encerrar os alarmes. Os exemplos poderiam ser *Resolvidos - Violador* ou *Alarme falso*. Você pode criar a quantidade que quiser.

Configurações de som (nó Alarmes)

Ao configurar as definições de dados de alarme, especifique o seguinte:

Nome	Descrição
Sons	Selecione o som a ser associado com o alarme. A lista de sons contém um número de sons padrão do Windows. Você também pode adicionar novos sons (.wav ou .mp3).
Adicionar	Adicionar sons. Procure pelo arquivo para fazer o upload de um ou vários arquivos .wav ou .mp3.
Remover	Remova um som selecionado da lista de sons adicionados manualmente. Sons padrão não podem ser removidos.
Teste	Teste o som. Selecione o som na lista. O som é reproduzido uma vez.

Hierarquia de sites federados

Propriedades de sites federados

Esta seção descreve a guia **Geral** e a guia **Site primário**.

Guia Geral

É possível mudar algumas informações relacionadas ao site ao qual você está conectado no momento.

Nome	Descrição
Nome	Digite o nome do site.
Descrição	Digite uma descrição para o site.
URLs	Use a lista para adicionar e remover URL(s) deste site e indique se são externos ou não. Endereços externos podem ser alcançados de fora da rede local.
Versão	Número da versão do servidor de gerenciamento dos site.
Conta de Serviço	A conta de serviço sob a qual o servidor de gerenciamento está sendo executado.
Tempo da última	Hora e data da última sincronização da hierarquia.

Nome	Descrição
sincronização	
Status da última sincronização	Status da última sincronização da hierarquia. Pode ser **Bem sucedido** ou **Falhou**.

Guia Site Pai

Esta guia mostra informações relacionadas ao site pai do site ao qual você está conectado no momento. A guia não fica visível se seu site não tiver site pai.

Nome	Descrição
Nome	Mostra o nome do site primário.
Descrição	Mostra uma descrição do site primário (opcional).
URLs	Lista URL(s) para o site pai e indica se eles são externos ou não. Endereços externos podem ser alcançados de fora da rede local.
Versão	Número da versão do servidor de gerenciamento dos site.
Conta de Serviço	A conta de serviço sob a qual o servidor de gerenciamento está sendo executado.
Tempo da última sincronização	Hora e data da última sincronização da hierarquia.
Status da última sincronização	Status da última sincronização da hierarquia. Pode ser **Bem sucedido** ou **Falhou**.

helpfeedback@milestone.dk

Sobre a Milestone

A Milestone Systems é uma fornecedora líder de sistema de gerenciamento de vídeo em plataforma aberta; uma tecnologia que ajuda a garantir a segurança, proteger ativos e aumentar a eficiência dos negócios no mundo todo. A Milestone Systems possibilita a existência de uma comunidade em plataforma aberta que impulsiona colaboração e inovação no desenvolvimento e no uso da tecnologia de vídeo em rede, com soluções consistentes e expansíveis comprovadas em mais de 150 mil locais no mundo todo. Fundada em 1998, a Milestone Systems é uma empresa autônoma do Canon Group. Para obter mais informações, visite https://www.milestonesys.com/.