

MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile Server 2020 R3

Manual do administrador



Índice

Copyright, marcas comerciais e limitação de responsabilidade	5
Visão Geral	6
XProtect Mobile (explicado)	6
XProtect Mobile servidor (explicado)	6
Gráfico de comparação de produtos	7
Requisitos e considerações	11
Pré-requisitos para a utilização do XProtect Mobile	11
Requisitos do sistema XProtect Mobile	11
Requisitos para a configuração das notificações	11
Requisitos para configuração da Conexão inteligente	12
Requisitos para configuração da verificação em duas etapas do usuário	12
Requisitos para configuração de vídeo push	12
Requisitos para o streaming direto	12
Instalação	13
Instalar o servidor XProtect Mobile	13
Configuração	15
Configurações do servidor móvel	15
Guia Geral	15
Guia Conectividade	17
Guia Status do servidor	19
Guia Desempenho	21
Guia de investigações	24
Guia Vídeo Push	25
Guia Notificações	26
Guia Verificação em duas etapas	27
Streaming direto (explicado)	30
Streaming adaptável (explicado)	30
Comunicação segura (explicado)	31

Criptografia de servidor de gerenciamento (explicado)	32
Criptografia do servidor de gerenciamento para o servidor de gravação (explicado)	34
Criptografia entre o servidor de gerenciamento e o Data Collector Server (explicado)	35
Criptografia para todos os clientes e servidores que recuperam dados do servidor de gravação (explicado)	36
Criptografia de dados do servidor móvel (explicado)	39
Requisitos de criptografia de servidor móvel para clientes	40
Ativar criptografia	40
Ativar criptografia para e do servidor de gerenciamento	40
Habilitar a criptografia do servidor para servidores de gravação ou servidores remotos	42
Ative a criptografia para cliente e serviços	43
Ativar criptografia no servidor móvel	45
Milestone Federated Architecture e servidores mestre/secundários (explicado)	47
Conexão inteligente (explicado)	48
Configurar Smart Connect	48
Ative a detectabilidade do Universal Plug and Play em seu roteador	48
Ativar conexões em uma rede complexa	49
Definir configurações de conexão	49
Enviar uma mensagem de e-mail para usuários	49
Enviando notificações (explicado)	50
Configure notificações por push no servidor XProtect Mobile	51
Ative o envio de notificações por push para dispositivos móveis específicos ou para todos os dispositivos móveis	51
Parar de enviar notificações por push a dispositivos móveis específicos ou para todos	51
Configurar investigações	52
Uso de Vídeo Push para transmitir vídeo por streaming (explicado)	53
Configurar vídeo push para transmitir vídeo por streaming	54
Adicionar um canal de Vídeo push para fluxo de vídeo	54
Editar um canal de vídeo push	55
Remover um canal de vídeo push	55
Alterar senha	55
Adicione o driver do Vídeo Push como um dispositivo de hardware no Recording Server	56

Adicionar o dispositivo do driver do Vídeo Push ao canal para vídeo push	57
Ativar áudio para canal de vídeo push existente	57
Configurar usuários para a verificação em duas etapas por e-mail	58
Insira as informações sobre seu servidor SMTP	58
Especifique o código de verificação que será enviado aos usuários	58
Atribua o método de login para os usuários e grupos do Active Directory	59
Ações (explicado)	59
Nomeando uma saída para uso em cliente XProtect Mobile e XProtect Web Client (explicado)	60
Manutenção	61
Mobile Server Manager (explicado)	61
Acesso XProtect Web Client	61
Iniciar, parar e reiniciar serviço Mobile Server	62
Preencha/edite o endereço do servidor de gerenciamento	62
Mostrar/editar números de portas	62
Ativar criptografia no servidor móvel	63
Acessando registros e investigações (explicado)	64
Alterar pasta de investigações	65
Exibir status (explicado)	65
Solução de problemas	67
Solução de problemas XProtect Mobile	67

Copyright, marcas comerciais e limitação de responsabilidade

Copyright © 2020 Milestone Systems A/S

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

XProtect Mobile (explicado)

O XProtect Mobile consiste em cinco componentes:

- Cliente XProtect Mobile

O cliente XProtect Mobile é um aplicativo de monitoramento móvel que você instala e usa em seu dispositivo Android ou Apple. Você pode usar tantas instalações do cliente XProtect Mobile quanto precisar.

Para obter mais informações, baixe o Manual do usuário do cliente XProtect Mobile no Milestone Systems site (<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>).

- XProtect Web Client

XProtect Web Client permite a visualização de vídeos ao vivo em seu navegador e o download de gravações. XProtect Web Client é instalado automaticamente junto com a instalação do servidor XProtect Mobile.

Para obter mais informações, baixe o Manual do usuário do XProtect Web Client no site Milestone Systems (<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>).

- Servidor XProtect Mobile
- Plug-in XProtect Mobile
- Mobile Server Manager

O servidor XProtect Mobile, o plug-in XProtect Mobile e Mobile Server Manager estão cobertos neste manual.

XProtect Mobile servidor (explicado)

O servidor do XProtect Mobile processa logins para o sistema do cliente do XProtect Mobile ou XProtect Web Client.

Um servidor do XProtect Mobile distribui fluxos de vídeo de servidores de gravação para o cliente do XProtect Mobile ou XProtect Web Client. Isso oferece uma configuração segura na qual os servidores de gravação nunca estão conectados à internet. Quando um servidor XProtect Mobile recebe fluxos de vídeo de servidores de gravação, ele também lida com a conversão complexa de codecs e formatos, permitindo o streaming de vídeo no dispositivo móvel.

Você deve instalar o servidor do XProtect Mobile em qualquer computador a partir do qual você queira acessar servidores de gravação. Ao instalar o servidor do XProtect Mobile, faça o login usando uma conta que tenha direitos de administrador. Caso contrário, a instalação não será concluída com sucesso (consulte Instalar o servidor XProtect Mobile na página 13).

O servidor do XProtect Mobile suporta o streaming direito a fluxo adaptável no modo ao vivo (somente para XProtect Expert e XProtect Corporate).

Gráfico de comparação de produtos

O VMS XProtect inclui os seguintes produtos:

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

A lista completa de recursos está disponível na página de visão geral do produto no Milestone site (<https://www.milestone.com/solutions/platform/product-index/>).

Abaixo se encontra uma lista das principais diferenças entre os produtos:

Nome	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Sites por SLC	1	1	Vários locais	Vários locais	Vários locais
Servidores de gravação por SLC	1	1	Ilimitado	Ilimitado	Ilimitado
Dispositivos de hardware por servidor de gravação	8	48	Ilimitado	Ilimitado	Ilimitado
Milestone Interconnect™	-	Site remoto	Site remoto	Site remoto	Site central/remoto
Milestone Federated Architecture™	-	-	-	Site remoto	Site central/remoto
Servidor do sistema de gravação ininterrupta (failover)	-	-	-	Cold e hot standby	Cold e hot standby
Serviços de conexão	-	-	-	-	✓

Nome	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
remota					
Suporte de armazenagem no dispositivo	-	-	✓	✓	✓
Armazenamento de vídeo multiestágio	Bancos de dados ao vivo + 1 arquivo	Bancos de dados ao vivo + 1 arquivo	Bancos de dados ao vivo + 1 arquivo	Bancos de dados ao vivo + arquivos ilimitados	Bancos de dados ao vivo + arquivos ilimitados
SNMP (notificação)	-	-	-	✓	✓
Permissões de acesso do usuário controladas pelo tempo	-	-	-	-	✓
Reduzir a taxa de quadros (grooming)	-	-	-	✓	✓
Criptografia de dados de vídeo (servidor de gravação)	-	-	-	✓	✓
Assinatura de banco de dados (servidor de gravação)	-	-	-	✓	✓
Níveis de prioridade PTZ	1	1	3	32000	32000
PTZ estendido (Reservar sessão PTZ e patrulha de XProtect Smart Client)	-	-	-	✓	✓

Nome	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Proteção de evidências	-	-	-	-	✓
Função de marcador	-	-	Somente manual	Manual e baseado em regras	Manual e baseado em regras
Multi-fluxo ao vivo ou multicasting/fluxo adaptável	-	-	-	✓	✓
Streaming direto	-	-	-	✓	✓
Segurança geral	Permissões de usuário cliente	Permissões de usuário cliente/ permissões de usuário administrador			
Perfis do XProtect Management Client	-	-	-	-	✓
Perfis do XProtect Smart Client	-	-	3	3	Ilimitado
XProtect Smart Wall	-	-	-	opcional	✓
Monitor do sistema	-	-	-	✓	✓
Mapa inteligente	-	-	-	✓	✓
Verificação em duas etapas	-	-	-	-	✓
Compatibilidade com	-	✓	✓	✓	✓

Nome	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
DLNA					
Máscara de privacidade	-	✓	✓	✓	✓
Gerenciamento de senha de dispositivo			✓	✓	✓

Requisitos e considerações

Pré-requisitos para a utilização do XProtect Mobile

Antes de poder começar a usar o XProtect Mobile, você precisa se certificar de que possui o seguinte:

- Um VMS em execução instalado e configurado com pelo menos um usuário
- Câmeras e visualizações configuradas no XProtect Smart Client
- Um dispositivo móvel executando Android ou iOS com acesso ao Google Play ou App StoreSM, onde você pode baixar o aplicativo do cliente do XProtect Mobile
- Um web browser para executar XProtect Web Client

Para ler mais sobre os requisitos, consulte Requisitos do sistema XProtect Mobile na página 11.

Requisitos do sistema XProtect Mobile

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

- Para encontrar requisitos para cliente XProtect Mobile, selecione o ícone do produto **XProtect Mobile**
- Para encontrar requisitos para XProtect Web Client, selecione o ícone do produto **XProtect Web Client**
- Para encontrar os requisitos para o servidor XProtect Mobile, selecione o ícone do produto XProtect que você tem instalado
- Os requisitos para o plug-in XProtect Mobile são:
 - Um Management Client em execução
 - O plug-in da Milestone é instalado para se integrar a seu VMS

Requisitos para a configuração das notificações

- Você precisa associar um ou mais alarmes a um ou mais eventos e regras. Isso não é necessário para notificações do sistema
- Certifique-se de que seu contrato Milestone CareTM com a Milestone Systems esteja atualizado
- O seu sistema deve ter acesso à internet

Para obter mais informações, consulte:

Configure notificações por push no servidor XProtect Mobile na página 51

Guia Notificações na página 26

Requisitos para configuração da Conexão inteligente

- Seu servidor XProtect Mobile deve usar um endereço IP público. O endereço pode ser estático ou dinâmico, mas geralmente é uma boa ideia usar endereços IP estáticos
- Você precisa ter uma licença válida para o Smart Connect

Requisitos para configuração da verificação em duas etapas do usuário

- Você instalou um servidor SMTP
- Você adicionou os usuários e grupos ao seu sistema XProtect no Management Client no **Funções** no painel **Navegação do Site**. Na função relevante, selecione a aba **Usuários e Grupos**
- Se você tiver atualizado o seu sistema a partir de uma versão anterior do XProtect, você deve reiniciar o servidor móvel para ativar o recurso de verificação de duas etapas

Para obter mais informações, consulte:

Configurar usuários para a verificação em duas etapas por e-mail na página 58

Guia Verificação em duas etapas na página 27

Requisitos para configuração de vídeo push

- Cada canal exige uma licença do dispositivo de hardware
- Para ativar áudio com Vídeo Push:
 1. Faça o download e instale o Milestone XProtect Device Pack 10.3a versão ou superior.
 2. Faça o download e instale o XProtect Mobile Server Installer.exe 13.2a ou superior.
 3. Reinicializar o serviço Recording Server.

Requisitos para o streaming direto

O XProtect Mobile suporta streaming direto no modo ao vivo (somente para XProtect Expert e XProtect Corporate).

Requisitos de configuração da câmera para o streaming direto

Para usar o streaming direto no XProtect Web Client e cliente do XProtect Mobile, você deve ter as seguintes configurações na câmera:

- As câmeras devem suportar o codec H.264 (para todos os clientes) ou codec H.265 (somente para o cliente do XProtect Mobile)
- Recomendamos definir o **valor do tamanho do GOP** para **1 segundo** e a definição de **FPS** deve ter um valor superior a **10 FPS**

Instalação

Instalar o servidor XProtect Mobile

Depois que tiver instalado o servidor XProtect Mobile, você pode usar o cliente XProtect Mobile e XProtect Web Client com o seu sistema. Para reduzir a utilização global dos recursos do sistema no computador que está executando o servidor de gerenciamento, instale o servidor XProtect Mobile em um computador separado.

O servidor de gerenciamento possui uma página pública de instalação integrada. A partir desta página da web, os administradores e os usuários finais podem fazer o download e instalar os componentes necessários do sistema XProtect a partir do servidor de gerenciamento ou de qualquer outro computador no sistema.



O servidor XProtect Mobile é instalado automaticamente quando você instala a opção de computador único.

Para instalar o servidor de XProtect Mobile:

1. Insira a seguinte URL no seu navegador: *http://[endereço do servidor de gerenciamento]/installation/admin* onde [endereço do servidor de gerenciamento] é o endereço IP ou nome do host do servidor de gerenciamento.
2. Clique em **Todos os idiomas** para o instalador do servidor XProtect Mobile.
3. Execute o arquivo baixado. Clique em **Sim** para todos os avisos. A descompactação começa.
4. Selecione o idioma para o instalador. Em seguida, clique em **Continuar**.
5. Leia e aceite o contrato de licença. Em seguida, clique em **Continuar**.
6. Selecione o tipo de instalação:
 - Clique em **Típico** para instalar o servidor XProtect Mobile e plug-in
 - Clique em **Personalizado** para instalar apenas o servidor ou apenas o plug-in. Por exemplo, instalar apenas o plug-in é útil se você quiser usar o XProtect Mobile para gerenciar os servidores Management Client, mas se não precisar do servidor XProtect Mobile nesse computador



O plug-in Management Client é necessário no computador que está executando o XProtect Mobile para gerenciar os servidores Management Client no XProtect Mobile.

7. Apenas para a instalação personalizada: Selecione os componentes que deseja instalar. Em seguida, clique em **Continuar**.

8. Selecione a conta de serviço para o servidor móvel: Em seguida, clique em **Continuar**.



Para alterar ou editar as credenciais da conta do serviço posteriormente, você terá que reinstalar o servidor móvel.

9. No campo **URL do servidor**, preencha o endereço do servidor de gerenciamento primário.
10. Apenas para a instalação personalizada: Especifique as portas de conexão para comunicação com o servidor móvel. Em seguida, clique em **Continuar**.



Em uma instalação típica, as portas de conexão recebem os números de porta padrão (8081 para a porta HTTP e 8082 para a porta HTTPS).

11. Especificar a criptografia do servidor móvel. Em seguida, clique em **Continuar**.

Na página **Selecionar criptografia**, você pode proteger os fluxos de comunicação:

- Entre os servidores móveis e os de gravação, coletores de dados e o servidor de gerenciamento. Para habilitar a criptografia para fluxos de comunicação interna, na seção **Certificado do servidor**, selecione um certificado
- Entre os servidor móveis e os clientes. Para habilitar a criptografia entre o servidor móvel e os clientes que recuperam fluxos de dados do servidor móvel, na seção **Certificado de mídia de streaming**, selecione um certificado



Se você não ativar a criptografia, alguns recursos em alguns clientes não estarão disponíveis. Para mais informações, consulte Requisitos de criptografia de servidor móvel para clientes na página 40.

Para obter mais informações sobre preparar o seu sistema para comunicações seguras, consulte Criptografia de dados do servidor móvel (explicado) na página 39 ou o [Guia de certificados Milestone](#) (somente em inglês).

Você também pode ativar a criptografia após a conclusão da instalação, a partir do ícone de bandeja do Mobile Server Manager na barra de tarefas do seu sistema operacional (consulte Ativar criptografia no servidor móvel na página 45).

12. Selecione a localização do arquivo e o idioma do produto e então clique em **Instalar**.
13. Quando a instalação estiver concluída, uma lista de componentes instalados com sucesso será exibida. Em seguida, clique em **Fechar**.

Você está pronto para configurar o XProtect Mobile (consulte Configurações do servidor móvel na página 15).

Configuração

Configurações do servidor móvel

Em Management Client você pode configurar e editar uma lista de configurações de servidor XProtect Mobile acessível através de guias na barra de ferramentas inferior da seção **Propriedades** do servidor móvel. De lá, você pode:

- Ativar ou desativar configuração geral dos recursos do servidor (consulte Guia Geral na página 15)
- Configurar configurações de conectividade de servidor e configurar o recurso Conexão inteligente (consulte a guia Guia Conectividade na página 17)
- Veja status atual do servidor e usuários ativos listados (consulte a Guia Status do servidor na página 19)
- Configure parâmetros de desempenho para ativar o streaming direito ou o fluxo adaptável ou para definir as limitações do fluxo de vídeo (consulte a guia Guia Desempenho na página 21)
- Configure as configurações de investigação (consulte a Guia de investigações na página 24)
- Configure os recursos de vídeo push (consulte a Guia Vídeo Push na página 25)
- Configurar, ligar e desligar sistema e notificações push (consulte a Guia Notificações na página 26)
- Ative e configure uma etapa de login adicional para usuários (consulte a Guia Verificação em duas etapas na página 27)

Guia Geral

A tabela a seguir descreve as configurações nesta aba.

Geral

Nome	Descrição
Nome do servidor	Insira um nome do servidor XProtect Mobile.
Descrição	Insira uma descrição opcional do servidor XProtect Mobile.
Servidor Mobile	Veja o nome do servidor XProtect Mobile selecionado no momento.
Método de	Selecione o método de autenticação a ser usado quando os usuários efetuarem o login no

Nome	Descrição
login	<p>servidor. Você pode escolher entre:</p> <ul style="list-style-type: none"> • Automático • Autenticação do Windows • Autenticação básica

Características

A tabela a seguir descreve como controlar a disponibilidade dos recursos do XProtect Mobile.

Nome	Descrição
Ativar o XProtect Web Client	Ativar acesso a XProtect Web Client. Este recurso é ativado por padrão.
Habilitar a visualização Todas as câmeras	Incluir a visualização Todas as câmeras . Esta visualização exibe todas as câmeras que um usuário tem permissão para visualizar em um servidor de gravação. Este recurso é ativado por padrão.
Habilitar ações (saídas e eventos)	<p>Ativar acesso a ações no cliente XProtect Mobile e XProtect Web Client. Este recurso é ativado por padrão.</p> <p>Se você desativar esse recurso, os usuários do cliente não poderão ver saídas e eventos, mesmo se estiverem configurados corretamente.</p>
Ativar áudio de entrada	Ativar o recurso de áudio de entrada no XProtect Web Client e cliente XProtect Mobile. Este recurso é ativado por padrão.
Ativar pressionar-para-falar	Ativar o recurso pressionar-para-falar (PTT) no XProtect Web Client e cliente XProtect Mobile. Este recurso é ativado por padrão.
Negar o acesso à função incorporada Administrador ao servidor XProtect Mobile	Ativar isto para prevenir que os usuários atribuídos à função incorporada Administrador acessem vídeos no cliente XProtect Mobile ou XProtect Web Client.

Configurações de registros

Você pode ver as informações de configurações de registros.

Nome	Descrição
Localização do arquivo de registro	Veja onde o sistema salva os arquivos de registro.
Manter os registros para	Veja o número de dias para manter os registros. O padrão é três dias.

Backup de configuração

Se seu sistema tiver vários servidores do XProtect Mobile, você poderá usar a função de backup para exportar as configurações atuais e importá-las em outros servidores do XProtect Mobile.

Nome	Descrição
Importar	Importar um arquivo XML com uma nova configuração do servidor XProtect Mobile.
Exportar	Exportar a sua configuração do servidor XProtect Mobile. O seu sistema armazena a configuração em um arquivo XML.

Guia Conectividade

As configurações na aba **Conectividade** são usadas nas seguintes tarefas:

- Definir configurações de conexão na página 49
- Enviar uma mensagem de e-mail para usuários na página 49
- Ativar conexões em uma rede complexa na página 49
- Ative a detectabilidade do Universal Plug and Play em seu roteador na página 48

Para obter mais informações, consulte Conexão inteligente (explicado) na página 48.



Você pode configurar como o cliente XProtect Mobile e os usuários XProtect Web Client devem se conectar ao servidor XProtect Mobile ao abrir o **Server Configurator** durante a instalação ou clicando com o botão direito no ícone Mobile Server Manager da bandeja após a instalação. O tipo de conexão pode ser HTTPS ou HTTP. Para obter mais informações, consulte Ativar criptografia no servidor móvel na página 63.

Geral

Nome	Descrição
Tempo limite do cliente (HTTP)	<p>Defina a frequência com a qual o cliente XProtect Mobile e XProtect Web Client devem indicar ao servidor XProtect Mobile que estão em execução. O valor padrão é 30 segundos.</p> <p>A Milestone recomenda que você não aumente o intervalo de tempo.</p>
Ativar visibilidade UPnP	<p>Isso faz com que o servidor do XProtect Mobile possa ser descoberto na rede por meio dos protocolos UPnP.</p> <p>O cliente XProtect Mobile possui a funcionalidade de varredura para localizar servidores XProtect Mobile com base em UPnP.</p>
Habilitar o mapeamento automático de portas	<p>Quando o servidor do XProtect Mobile está instalado atrás do firewall, um mapeamento de porta é necessário no roteador, para que todos os clientes ainda possam acessar o servidor da internet.</p> <p>A opção Ativar o mapeamento automático de portas habilita o servidor XProtect Mobile para fazer esse mapeamento de portas sozinho, desde que o roteador esteja configurado para isso.</p>
Habilitar o Smart Connect	<p>A Conexão Inteligente permite que você verifique se configurou o servidor XProtect Mobile corretamente sem efetuar login com um dispositivo móvel ou um tablet para fazer a validação. Ela também simplifica o processo de conexão para os usuários do cliente.</p>

Acesso à Internet

Nome	Descrição
Configurar acesso personalizado à internet	<p>Se você usar mapeamento de porta UPnP para direcionar conexões para uma conexão específica, selecione a caixa de seleção Configurar acesso personalizado à internet.</p> <p>Em seguida, forneça o endereço IP ou nome do host e a porta a ser usada para a conexão. Por exemplo, você pode fazer isso se seu roteador não for compatível com UPnP ou se você tiver uma cadeia de roteadores.</p>

Nome	Descrição
Desativar endereço padrão	Desative os endereços IP padrão para se conectar ao servidor móvel apenas com um endereço IP ou nome do host personalizados.
Selecione para recuperar o endereço IP de forma dinâmica	Se seu endereço IP mudar frequentemente, assinale a caixa de seleção Selecionar para recuperar endereço IP dinamicamente .
Porta HTTP	Insira o número da porta para a conexão HTTP. O número padrão é 8081.
Porta HTTPS	Insira o número da porta para a conexão HTTPS. O número padrão é 8082.
Endereços do servidor	Lista todos os endereços IP conectados ao servidor móvel.

Notificação de Smart Connect

Nome	Descrição
Convite por e-mail para	Insira o endereço de e-mail para o destinatário da notificação Conexão Inteligente.
Idioma do e-mail	Especifique o idioma usado no e-mail.
Token Conexão Inteligente	Um identificador exclusivo que os usuários de dispositivos móveis podem usar para conectar-se ao servidor XProtect Mobile.
Link para Conexão Inteligente	Um link que os usuários de dispositivos móveis podem usar para conectar-se ao servidor XProtect Mobile.

Guia Status do servidor

Veja os detalhes do status para o servidor XProtect Mobile. Os detalhes estão em formato de somente leitura:

Nome	Descrição
Servidor ativo desde	Mostra a data e hora do momento em que o servidor XProtect Mobile foi iniciado pela última vez.
Uso de CPU	Mostra a utilização atual da CPU no servidor móvel.
Largura de banda externa	Mostra a largura de banda atual em uso entre o cliente XProtect Mobile ou o XProtect Web Client e o servidor móvel.

Usuários ativos

Veja os detalhes do status do cliente XProtect Mobile ou do XProtect Web Client conectado ao servidor XProtect Mobile no momento.

Nome	Descrição
Nome de usuário	Mostra o nome de usuário para cada usuário do cliente XProtect Mobile ou usuário XProtect Web Client conectado ao servidor móvel.
Estado	Exibe a relação atual entre o servidor XProtect Mobile e o cliente XProtect Mobile ou o usuário do XProtect Web Client em questão. Status possíveis são: <ul style="list-style-type: none"> • Conectado: Um estado inicial quando os clientes e o servidor trocam chaves e criptografam credenciais • Logado: O cliente XProtect Mobile ou usuário XProtect Web Client efetuou login no sistema XProtect
Uso de largura de banda de vídeo (kB/s)	Mostra a largura de banda total dos fluxos de vídeo que estão atualmente abertos, para cada cliente do XProtect Mobile ou usuário do XProtect Web Client.
Uso de largura de banda de áudio (kB/s)	Mostra a largura de banda total dos fluxos de áudio que estão atualmente abertos, para cada usuário do XProtect Web Client.
Fluxos de vídeos transcódificados	Mostra o número total de fluxos de vídeo transcódificados que estão atualmente abertos, para cada cliente do XProtect Mobile ou usuário do XProtect Web Client.

Nome	Descrição
Fluxos de vídeo diretos	Mostra o número total de fluxos de vídeo diretos que estão atualmente abertos, para cada cliente do XProtect Mobile ou usuário do XProtect Web Client (somente para XProtect Expert e XProtect Corporate).
Fluxos de áudio transcodificados	Mostra o número total de fluxos de áudio transcodificados que estão atualmente abertos, para cada usuário do XProtect Web Client.

Guia Desempenho

Na guia **Desempenho**, você pode definir as seguintes configurações e limitações para o desempenho do servidor do XProtect Mobile:

Configurações do fluxo de vídeo (somente para XProtect Expert e XProtect Corporate)

Nome	Descrição
Ativar streaming direto	Ativar streaming direto no XProtect Web Client e cliente XProtect Mobile (para XProtect Expert e XProtect Corporate somente). Este recurso é ativado por padrão.
Ativar o streaming adaptável	Ativar o streaming adaptável no XProtect Web Client e no cliente XProtect Mobile (apenas para XProtect Expert e XProtect Corporate). Este recurso é ativado por padrão.
Modos de streaming	<p>Após você ativar o recurso de fluxo adaptável, poderá selecionar o tipo de modo de fluxo da lista:</p> <ul style="list-style-type: none"> • Otimizar qualidade do vídeo (padrão) - seleciona o fluxo com a menor resolução disponível igual ou superior à da resolução solicitada • Otimizar desempenho do servidor - reduz a resolução solicitada e depois seleciona o fluxo com a menor resolução disponível, igual ou superior à solicitação reduzida • Otimizar resolução para baixa largura de banda - seleciona o fluxo com a menor resolução possível (recomendado se você usa 3G ou uma rede instável)

Limitações do fluxo de vídeo transcodificado

Nível 1

Nível 1 é o padrão de limitação instalado no servidor XProtect Mobile. Qualquer limitação definida aqui, é sempre aplicada aos fluxos de vídeo transcodificados do XProtect Mobile.

Nome	Descrição
Nível 1	Selecione a caixa de seleção para ativar o primeiro nível de limitações ao desempenho do servidor XProtect Mobile.
FPS máx	Defina um limite para o número máximo de quadros por segundo (FPS) a ser enviado aos clientes pelo servidor XProtect Mobile.
Resolução de imagem máx	Defina um limite para a resolução de imagem a ser enviada aos clientes pelo servidor XProtect Mobile.

Nível 2

Se desejar aplicar um nível diferente de limitações do padrão do **Nível 1**, você selecione a caixa de seleção **Nível 2**. Não é possível definir configurações mais altas do que as que você definiu no primeiro nível. Se, por exemplo, você definir FPS máx para 45 no **Nível 1**, você pode definir FPS máx no **Nível 2** apenas para 44 ou menos.

Nome	Descrição
Nível 2	Selecione a caixa de seleção para ativar o segundo nível de limitações ao desempenho do servidor XProtect Mobile.
Limite de CPU	Defina um limite para a carga da CPU no servidor XProtect Mobile antes que o sistema implemente as limitações ao fluxo de vídeo.
Limite de largura de banda	Defina um limite para a carga da largura de banda no servidor XProtect Mobile antes que o sistema implemente as limitações ao fluxo de vídeo.

Nome	Descrição
FPS máx	Defina um limite para o número máximo de quadros por segundo (FPS) a ser enviado aos clientes pelo servidor XProtect Mobile.
Resolução de imagem máx	Defina um limite para a resolução de imagem a ser enviada aos clientes pelo servidor XProtect Mobile.

Nível 3

Você também pode selecionar uma caixa de seleção **Nível 3** para criar um terceiro nível de limitações. Você não pode definir nenhuma configuração maior do que você tiver definido para o **Nível 1** e o **Nível 2**. Se, por exemplo, você definir **FPS máx** para 45 no **Nível 1** e para o nível 32 no **Nível 2**, você pode definir **FPS máx** no **Nível 3** apenas para 31 ou menos.

Nome	Descrição
Nível 3	Selecione a caixa de seleção para ativar o terceiro nível de limitações para o desempenho do servidor XProtect Mobile.
Limite de CPU	Defina um limite para a carga da CPU no servidor XProtect Mobile antes que o sistema implemente as limitações ao fluxo de vídeo.
Limite de largura de banda	Defina um limite para a carga da largura de banda no servidor XProtect Mobile antes que o sistema implemente as limitações ao fluxo de vídeo.
FPS máx	Defina um limite para os quadros por segundo (FPS) a serem enviados aos clientes pelo servidor XProtect Mobile.
Resolução de imagem máx	Defina um limite para a resolução de imagem a ser enviada aos clientes pelo servidor XProtect Mobile.



O sistema não muda instantaneamente de um nível para outro. Se o seu limiar da CPU ou da largura de banda vai menos de 5% acima ou abaixo dos níveis indicados, o nível atual permanece em uso.

Guia de investigações

Configurações de investigações

Você pode ativar investigações para que as pessoas possam usar o cliente XProtect Mobile ou XProtect Web Client para acessar vídeos gravados e investigar incidentes, assim como para preparar e baixar evidência de vídeo.

Nome	Descrição
Ativar investigações	Marque esta caixa de seleção para permitir que usuários criem investigações.
Pasta de investigações	Exibe onde as exportações de vídeo estão salvas no seu disco rígido.
Ativa o limite de tamanho da pasta de investigações	Marque esta caixa de seleção para definir um tamanho limite para a pasta de investigações e insira o número máximo de megabytes que a pasta de investigações pode conter. O tamanho padrão é 2000 MB.
Ver investigações feitas por outros usuários	Selecione essa caixa para permitir que usuários acessem investigações que não tenham sido criadas por eles.
Incluir carimbos de data/hora para exportações AVI	Selecione esta caixa para incluir a data e o horário em que o arquivo AVI foi baixado.
Codec usado para exportações AVI	Selecione o formato de compressão a ser usado durante a preparação de pacotes AVI para download. Os codecs dentre os quais você pode escolher podem diferir, dependendo de seu sistema operacional. Se você não vir o codec que quer utilizar, você pode adicioná-lo à lista instalando-o no computador em que o servidor XProtect Mobile está sendo executado.
Bit de áudio usado para exportações de AVI	Selecione da lista a taxa de bits de áudio apropriada quando houver áudio incluído na exportação de vídeo. O padrão é 160000 Hz.

Nome	Descrição
Manter ou excluir os dados quando a exportação falhar (MKV e AVI)	Selecione se deseja manter ou excluir os dados que não foram preparados com sucesso para download em uma investigação.

Investigações

Nome	Descrição
Investigações	Lista as investigações que foram configuradas até agora no sistema. Utilize a tecla Excluir ou Excluir todos se você não deseja mais manter uma investigação. Isso pode ser útil se, por exemplo, você deseja disponibilizar mais espaço em disco no servidor.
Detalhes	Para excluir arquivos individuais de vídeo que foram exportados para uma investigação, porém mantendo a investigação, selecione a investigação na lista. No grupo Detalhes da investigação , selecione o ícone excluir à direita dos campos Banco de dados, AVI , ou MKV para exportações.

Guia Video Push

Você pode especificar as seguintes configurações se ativar o Video Push:

Nome	Descrição
Pré-carregamento de vídeo	Ativar o Vídeo Push no servidor móvel.
Número de canais:	Mostra o número de canais ativados do Vídeo push no seu sistema XProtect.
Canal	Exibe o número do canal para o canal em questão. Não editável.

Nome	Descrição
Porta	Número de porta para o canal de vídeo push em questão.
Endereço MAC	O endereço MAC para o canal de Vídeo Push em questão.
Nome de usuário	Insira o nome de usuário associado ao canal de vídeo push relevante.
Nome da Câmera	Mostra o nome da câmera se a câmera foi identificada.

Após ter concluído todas as etapas necessárias (consulte Configurar vídeo push para transmitir vídeo por streaming na página 54), selecione **Encontrar câmeras** para procurar pela câmera relevante.

Guia Notificações

Utilize a aba **Notificações** para ativar ou desativar o sistema de notificações e notificações por push.

Se você ativar as notificações e tiver configurado um ou mais alarmes e eventos, o XProtect Mobile notifica os usuários quando um evento ocorre. Quando o aplicativo está aberto, as notificações são entregues no XProtect Mobile no dispositivo móvel. Notificações por push são usadas para notificar usuários que não estão com o XProtect Mobile aberto. Essas notificações são enviadas ao dispositivo móvel.

Para obter mais informações, consulte: Ative o envio de notificações por push para dispositivos móveis específicos ou para todos os dispositivos móveis na página 51

A tabela a seguir descreve as configurações nesta aba.

Nome	Descrição
Notificações	Selecione esta caixa para ativar notificações.
Manter registros de dispositivos	Selecione esta caixa para armazenar informações sobre os dispositivos e usuários que se conectam a esse servidor. O sistema envia notificações a esses dispositivos. Se você desmarcar esta caixa de seleção, você também pode desmarcar a lista de dispositivos. Para que os usuários voltem a receber notificações, você precisa selecionar novamente a caixa e os usuários precisam reconectar seus dispositivos ao servidor.

Dispositivos registrados

Nome	Descrição
Ativado	Selecione esta caixa de seleção para iniciar o envio de notificações para o dispositivo.
Nome do Dispositivo	Uma lista dos dispositivos móveis que se conectaram a este servidor. Você pode iniciar ou interromper o envio de notificações para dispositivos específicos selecionando ou desmarcando a caixa de seleção Ativado .
Usuário	Nome do usuário que vai receber notificações.

Guia Verificação em duas etapas



As funcionalidades disponíveis dependem do sistema que você estiver usando. Consulte <https://www.milestonesys.com/solutions/platform/product-index/> para mais informações.

Use a guia **Verificação em duas etapas** para ativar e especificar uma etapa de login adicional para usuários de:

- App XProtect Mobile em seu dispositivo móvel iOS ou Android
- XProtect Web Client

O primeiro tipo de verificação é uma senha. O segundo tipo é um código de verificação, que você pode configurar para ser enviado por e-mail para o usuário.

Para obter mais informações, consulte Configurar usuários para a verificação em duas etapas por e-mail na página 58.

As tabelas a seguir descrevem as configurações desta guia.

Configurações do provedor > E-mail

Nome	Descrição
Servidor SMTP	Insira o endereço IP ou o nome do host do servidor SMTP (simple mail transfer protocol) para os e-mails de verificação em duas etapas.
Porta do servidor SMTP	Especifique a porta do servidor SMTP para enviar e-mails. O número de porta padrão é 25 sem SSL e 465 com SSL.

Nome	Descrição
Usar o SSL	Selecione esta caixa de seleção se o servidor SMTP suporta a criptografia SSL.
Nome de usuário	Especifique o nome de usuário para efetuar login no servidor SMTP.
Senha	Especifique a senha para efetuar login no servidor SMTP.
Usar Autenticação de Senha de Segurança (SPA)	Selecione esta caixa de seleção se o servidor SMTP suporta a SPA.
Endereço de e-mail do remetente	Especifique o endereço de e-mail para enviar os códigos de verificação.
Assunto do e-mail	Especifique o título do assunto para o e-mail. Exemplo: Seu código de verificação em duas etapas.
Texto do e-mail	<p>Digite a mensagem que deseja enviar. Exemplo: O seu código é {0}.</p> <div style="border: 1px solid #0070C0; padding: 5px; background-color: #D9E1F2;">  <p>Se você se esquecer de incluir a variável {0}, o código é adicionado ao final do texto por padrão.</p> </div>

Configurações do código de verificação

Nome	Descrição
Limite da nova conexão (0-30 minutos)	<p>Especifique o prazo dentro do qual os usuários do cliente XProtect Mobile não precisam fazer uma nova verificação de seu login no caso de, por exemplo, uma rede desconectada. O período padrão é de três minutos.</p> <p>Essa configuração não se aplica ao XProtect Web Client.</p>
O código expira após (1-10 minutos)	Especifique o prazo dentro do qual o usuário pode usar o código de verificação recebido. Após este período, o código é inválido e o usuário precisa pedir um novo código. O período padrão é de cinco minutos.
Tentativas de	Especifique o número máximo de tentativas de entrada de código, antes que o código

Nome	Descrição
introdução do código (1-10 tentativas)	fornecido se torne inválido. O número de porta padrão é três.
Tamanho do código (4 a 6 caracteres)	Especifique o número de caracteres para o código. O tamanho padrão é seis.
Composição do código	<p>Especifique a complexidade do código que você deseja que o sistema gere. Você pode selecionar entre:</p> <ul style="list-style-type: none"> • Maiúscula latina (A-Z) • Letras minúsculas latinas (a-z) • Dígitos (0-9) • Caracteres especiais (!@#...)

Configurações do usuário

Nome	Descrição
Usuários e grupos	<p>Lista os usuários e os grupos adicionados ao sistema XProtect.</p> <p>Se um grupo estiver configurado no Active Directory, o servidor móvel usa detalhes, como endereços de e-mail, do Active Directory.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  Os grupos do Windows não suportam uma verificação em duas etapas. </div>
Método de verificação	<p>Selecione uma configuração de verificação para cada usuário ou grupo. Você pode selecionar entre:</p> <ul style="list-style-type: none"> • Nenhum login: o usuário não consegue efetuar o login • Nenhuma verificação em duas etapas: o usuário deve digitar o nome de usuário e senha

Nome	Descrição
	<ul style="list-style-type: none"> • E-mail: o usuário deve digitar um código de verificação além do nome de usuário e senha
Detalhes de usuário	Digite o endereço de e-mail que cada usuário receberá os códigos.

Streaming direto (explicado)

O XProtect Mobile suporta streaming direto no modo ao vivo (somente para XProtect Expert e XProtect Corporate).

Streaming direto é uma tecnologia de fluxo de vídeo que transfere vídeo de um sistema do XProtect diretamente para os clientes em codec H.264, suportado pela maioria das câmeras IP modernas. O Streaming direto não requer nenhuma transcodificação e, portanto, elimina um pouco do estresse do sistema XProtect system.

A tecnologia de streaming direto, é em contraste com as configurações de transcodificação no XProtect, nas quais um sistema XProtect decodifica o vídeo do codec usado na câmera em arquivos JPEG. A ativação do recurso, resulta no uso reduzido da CPU para a mesma configuração de câmeras e fluxos de vídeo. O Streaming direto também aumenta o desempenho para o mesmo hardware - até cinco vezes o número de fluxos de vídeo concorrentes, em comparação com a transcodificação.

Você também pode usar o recurso de streaming direto para transferir vídeo de câmeras que suportem o codec H.265 diretamente para o cliente do XProtect Mobile.

No Management Client, você pode ativar ou desativar o streaming direto para clientes (consulte Configurações do servidor móvel na página 15).

O fluxo de vídeo retorna do streaming direto para a transcodificação se:

- O recurso de streaming direto tiver sido desativado no Management Client ou os requisitos não tiverem sido atendidos (consulte Requisitos para o streaming direto na página 12)
- O codec da câmera de streaming é diferente de H.264 (para todos os clientes) ou H.265 (somente para o cliente do XProtect Mobile)
- O vídeo não pode começar a reproduzir por mais de dez segundos
- A taxa de quadros da câmera de streaming é definida para **um** quadro por segundo (1 FPS)
- A conexão com o servidor ou com a câmera foi perdida
- Você usa o recurso de máscara de privacidade durante o vídeo ao vivo

Streaming adaptável (explicado)

O XProtect Mobile suporta o fluxo adaptável no modo ao vivo (somente para XProtect Expert e XProtect Corporate).

Fluxo adaptável é útil quando você visualiza diversos fluxos de vídeo ao vivo na mesma visualização de câmeras. O recurso otimiza o desempenho do servidor do XProtect Mobile e melhora a capacidade de decodificação e desempenho dos dispositivos executando o cliente XProtect Mobile e o XProtect Web Client.

Para aproveitar o streaming adaptável, suas câmeras devem ter diversos fluxos definidos com diferentes resoluções. Neste caso, o recurso permite que você:

- Otimizar qualidade do vídeo - seleciona o fluxo com a menor resolução disponível igual ou superior à da resolução solicitada
- Otimizar desempenho do servidor - reduz a resolução solicitada e depois seleciona o fluxo com a menor resolução disponível, igual ou superior à solicitação reduzida
- Otimizar resolução para baixa largura de banda - seleciona o fluxo com a menor resolução disponível (recomendado se você usa 3G ou uma rede instável)



Ao aplicar zoom, o fluxo de vídeo ao vivo solicitado é sempre aquele com a resolução mais alta disponível.



O uso da largura de banda é frequentemente reduzido quando a resolução dos fluxos solicitados é reduzida. O uso da largura de banda depende também de outras definições nas configurações dos fluxos definidos.

Você pode ativar e desativar o fluxo adaptável e definir o modo de fluxo preferencial do recurso na guia **Desempenho** das configurações do servidor móvel no Management Client (consulte Configurações do servidor móvel na página 15).

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 VMS XProtect, a comunicação segura é obtida usando SSL/TLS com criptografia assimétrica (RSA).

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

Uma autoridade de certificado (AC) pode emitir certificados para serviços da web em servidores usando um certificado da CA. 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 podem agora usar o certificado do servidor público e o privado, para trocar uma chave secreta e, assim, estabelecer uma conexão SSL/TLS segura.

Para obter mais informações sobre TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security



Os certificados têm uma data de vencimento. VMS XProtect 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 comunicados com ele
- Os servidores de gravação não mais confiarão no servidor de gerenciamento com o certificado expirado e, assim, não poderão ser comunicados com ele
- Os dispositivos móveis não mais confiarão no servidor móvel com o certificado expirado e, assim, não poderão ser comunicados com ele

Para renovar os certificados, siga as etapas neste guia, como você fez ao criar certificados.

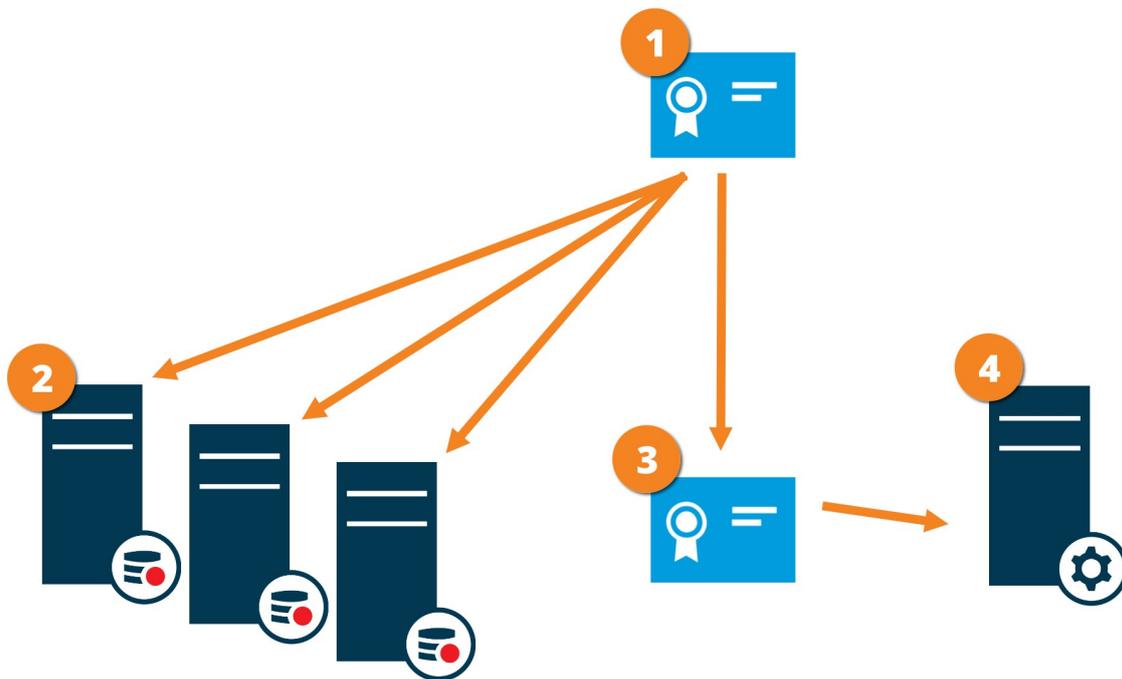
Quando você renova um certificado com o mesmo nome de assunto e o adiciona ao Repositório de certificados do Windows, os servidores escolherão automaticamente o novo certificado. Isso facilita a renovação de certificados para vários servidores sem ter que selecionar novamente o certificado para cada servidor e sem reiniciar os serviços.

Criptografia de servidor de gerenciamento (explicado)

Você pode criptografar a conexão de duas vias entre o servidor de gerenciamento e o servidor de gravação. Quando você ativa a criptografia no servidor de gerenciamento, isso se aplica a conexões de todos os servidores de gravação que se conectam ao servidor de gerenciamento. Se você ativar a criptografia no servidor de gerenciamento, também deverá ativar a criptografia em todos os servidores de gravação. Antes de você ativar a criptografia, você deve instalar certificados de segurança no servidor de gerenciamento e em todos os servidores de gravação.

Distribuição de certificado para servidores de gerenciamento

O gráfico ilustra o conceito básico de como os certificados são assinados, confiados e distribuídos no VMS XProtect para proteger a comunicação ao servidor de gerenciamento.



- ❶ Um certificado de AC age como um terceiro confiável, confiável tanto pelo assunto/proprietário (servidor de gerenciamento) quanto pela parte que verifica o certificado (servidores de gravação)
- ❷ O certificado da AC deve ser confiável em todos os servidores de gravação. Dessa maneira, os servidores de gravação podem verificar a validade dos certificados emitidos pela AC.
- ❸ O certificado da AC é usado para estabelecer a conexão segura entre o servidor de gerenciamento e os servidores de gravação
- ❹ O certificado da CA deve ser instalado no computador no qual o servidor de gerenciamento está sendo executado

Requisitos para o certificado de servidor de gerenciamento privado:

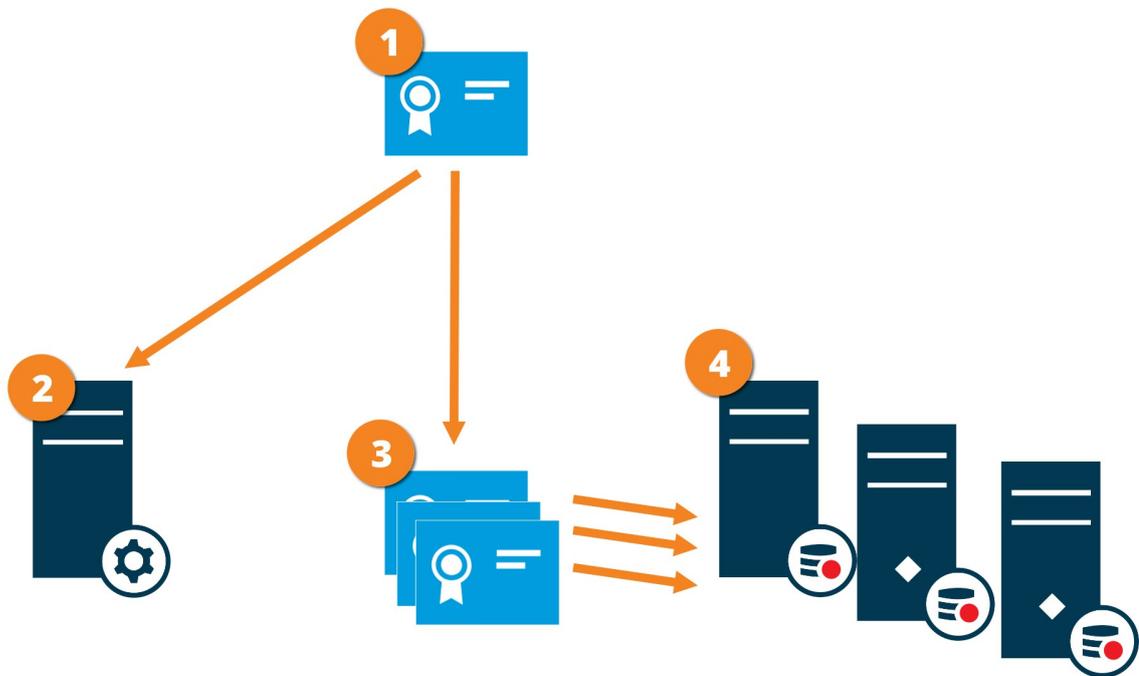
- Emitido para o servidor de gerenciamento, para que o nome do host do servidor de gerenciamento seja incluído no certificado, seja como assunto (proprietário) ou na lista de nomes DNS para a qual o certificado é emitido
- Confiável no próprio servidor de gerenciamento, confiando no certificado da AC usado para emitir o certificado do servidor de gerenciamento
- Confiável em todos os servidores de gravação conectados ao servidor de gerenciamento, confiando no certificado da AC usado para emitir o certificado do servidor de gerenciamento

Criptografia do servidor de gerenciamento para o servidor de gravação (explicado)

Você pode criptografar a conexão de duas vias entre o servidor de gerenciamento e o servidor de gravação. Quando você ativa a criptografia no servidor de gerenciamento, isso se aplica a conexões de todos os servidores de gravação que se conectam ao servidor de gerenciamento. A criptografia desta comunicação deve seguir a configuração de criptografia no servidor de gerenciamento. Assim, se a criptografia do servidor de gerenciamento estiver ativada, isso também deve ser ativado nos servidores de gravação e vice-versa. Antes de você ativar a criptografia, você deve instalar certificados de segurança no servidor de gerenciamento e em todos os servidores de gravação, incluindo os servidores do sistema de gravação ininterrupta.

Distribuição de certificado

O gráfico ilustra o conceito básico de como os certificados são assinados, confiados e distribuídos no VMS XProtect para proteger a comunicação do servidor de gerenciamento.



- 1 Um certificado de AC age como um terceiro confiável, confiável tanto pelo assunto/proprietário (servidor de gravação) quanto pela parte que verifica o certificado (servidor de gerenciamento)
- 2 O certificado CA deve ser confiável no servidor de gerenciamento. Dessa maneira, o servidor de gerenciamento pode verificar a validade dos certificados emitidos pela AC
- 3 O certificado da AC é usado para estabelecer a conexão segura entre os servidores de gravação e o servidor de gerenciamento

4 O certificado da CA deve ser instalado nos computadores nos quais os servidores de gravação estão sendo executados

Requisitos para o certificado de servidor de gravação privado:

- Emitido para o servidor de gravação para que o nome do host do servidor de gravação seja incluído no certificado, seja como assunto (proprietário) ou na lista de nomes DNS para a qual o certificado é emitido
- Confiável no servidor de gerenciamento, confiando no certificado da AC usado para emitir o certificado do servidor de gravação

Criptografia entre o servidor de gerenciamento e o Data Collector Server (explicado)

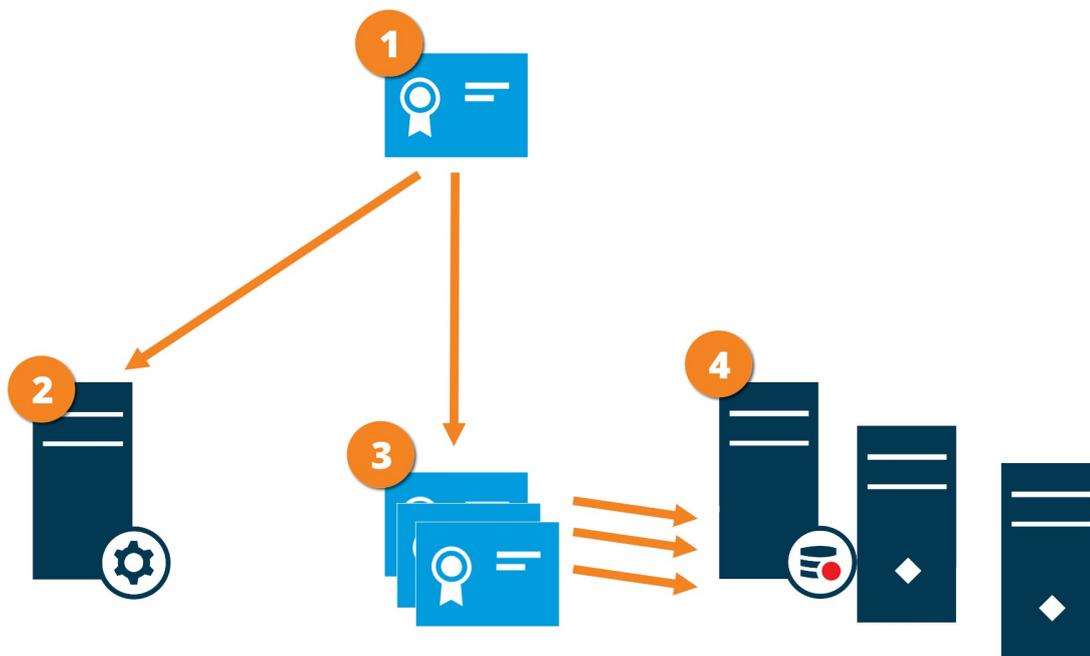
Você pode criptografar a conexão de duas vias entre o servidor de gerenciamento e o Data Collector afiliado, quando tiver um servidor remoto do seguinte tipo:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

Quando você ativa a criptografia no servidor de gerenciamento, isso se aplica a conexões de todos os servidores do Data Collector que se conectam ao servidor de gerenciamento. A criptografia desta comunicação deve seguir a configuração de criptografia no servidor de gerenciamento. Assim, se a criptografia do servidor de gerenciamento estiver ativada, isso também deve ser ativado nos servidores do Data Collector afiliados, com cada servidor remoto, e vice-versa. Antes de ativar a criptografia, você precisa instalar certificados de segurança no servidor de gerenciamento e em todos os servidores do Data Collector afiliados com servidores externos.

Distribuição de certificado

O gráfico ilustra o conceito básico de como os certificados são assinados, confiados e distribuídos no VMS XProtect para proteger a comunicação do servidor de gerenciamento.



- 1 Um certificado de AC age como um terceiro confiável, confiável tanto pelo assunto/proprietário (data collector server) quanto pela parte que verifica o certificado (servidor de gerenciamento)
- 2 O certificado CA deve ser confiável no servidor de gerenciamento. Dessa maneira, o servidor de gerenciamento pode verificar a validade dos certificados emitidos pela AC
- 3 O certificado da AC é usado para estabelecer a conexão segura entre os servidores coletores de dados e o servidor de gerenciamento
- 4 O certificado da CA deve ser instalado nos computadores nos quais os servidores coletores de dados estão sendo executados

Requisitos para o certificado do data collector server privado:

- Emitido para o data collector server para que o nome do host dele seja incluído no certificado, seja como assunto (proprietário) ou na lista de nomes DNS para a qual o certificado é emitido
- Confiável no servidor de gerenciamento, confiando no certificado da AC usado para emitir o certificado do data collector server

Criptografia para todos os clientes e servidores que recuperam dados do servidor de gravação (explicado)

Quando você ativa a criptografia em um servidor de gravação, a comunicação para todos os clientes, servidores e integrações que recuperam fluxos de dados do servidor de gravação é criptografada. Neste documento referidos como 'clientes':

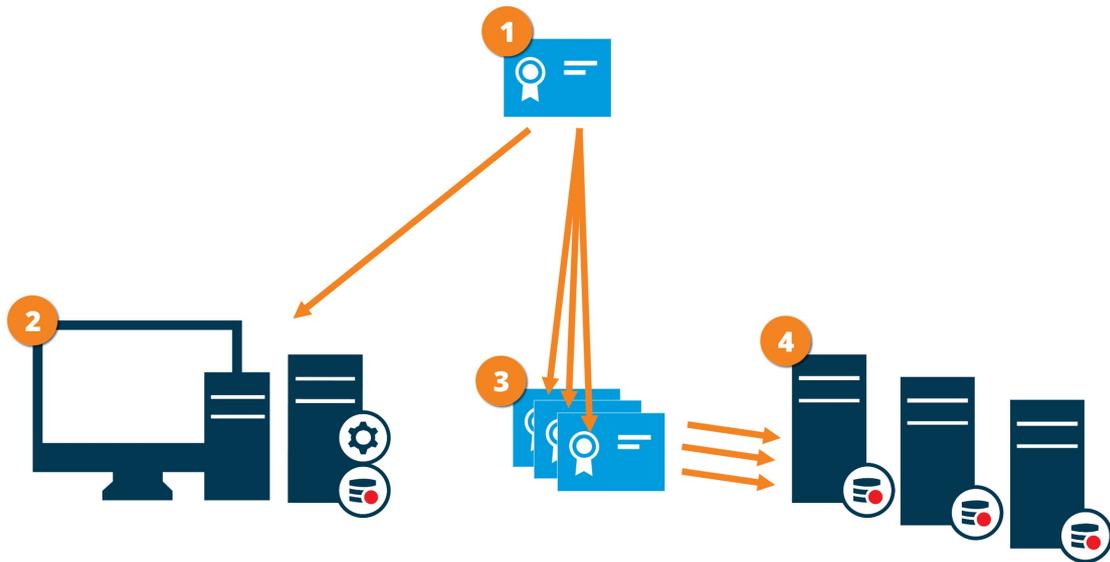
- XProtect Smart Client
- Management Client
- Management Server (para Monitor do Sistema e para imagens e clipes de vídeo AVI em notificações de e-mail)
- Servidor XProtect Mobile
- XProtect Event Server
- XProtect LPR
- Milestone Open Network Bridge
- XProtect DLNA Server
- Sites que recuperam os fluxos de dados do servidor de gravação por meio de Milestone Interconnect
- Algumas integrações de MIP SDK terceirizadas



Para soluções com MIP SDK 2018 R3 ou anteriores que acessam servidores de gravação: Se as integrações forem feitas usando bibliotecas MIP SDK elas precisam ser recompiladas com MIP SDK 2019 R1; se as integrações se comunicarem diretamente com as APIs do Recording Server sem usar as bibliotecas MIP SDK, os integradores devem adicionar eles mesmos o suporte de HTTPS.

Distribuição de certificado

O gráfico ilustra o conceito básico de como os certificados são assinados, confiados e distribuídos no VMS XProtect para proteger a comunicação ao servidor de gravação.



- 1 Um certificado de AC age como um terceiro confiável, confiável tanto pelo assunto/proprietário (servidor de gravação) quanto pela parte que verifica o certificado (todos os clientes)
- 2 O certificado da AC deve ser confiável em todos os clientes. Dessa maneira, os clientes podem verificar a validade dos certificados emitidos pela AC
- 3 O certificado da AC é usado para estabelecer a conexão segura entre os servidores de gravação e todos os clientes e serviços
- 4 O certificado da CA deve ser instalado nos computadores nos quais os servidores de gravação estão sendo executados

Requisitos para o certificado de servidor de gravação privado:

- Emitido para o servidor de gravação para que o nome do host do servidor de gravação seja incluído no certificado, seja como assunto (proprietário) ou na lista de nomes DNS para a qual o certificado é emitido
- Confiável em todos os computadores que executam serviços que recuperam fluxos de dados de servidores de gravação, confiando no certificado da AC que emitiu o certificado do servidor de gravação
- A conta de serviço que executa o servidor de gravação deve ter acesso à chave privada do certificado no servidor de gravação.



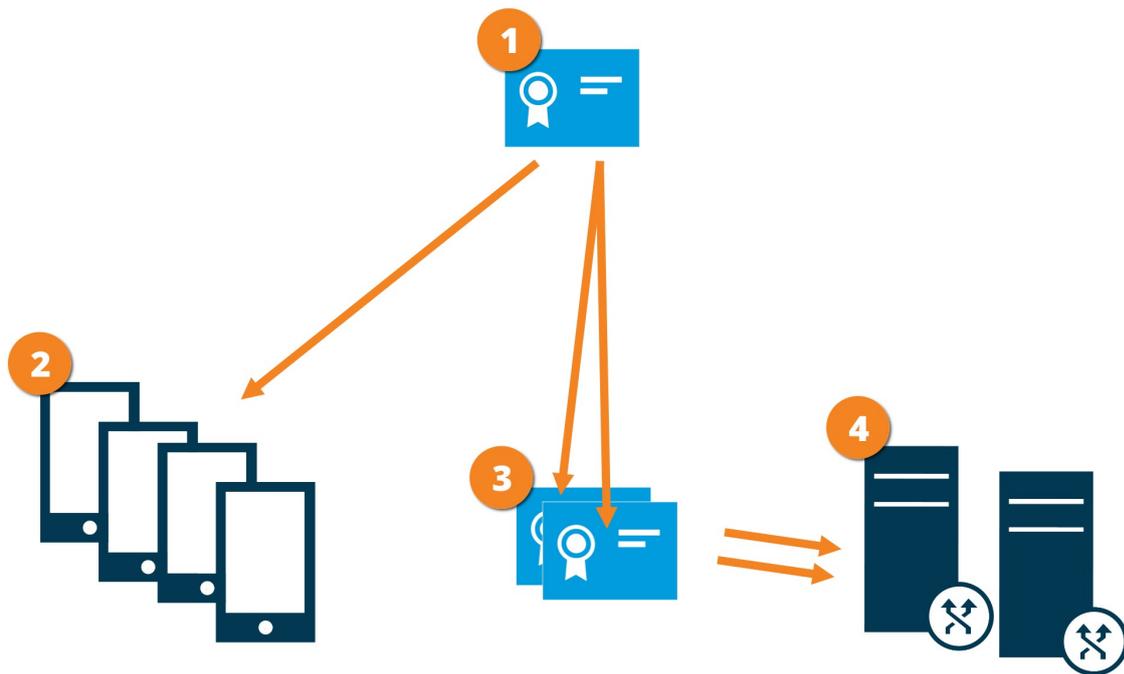
Se você ativar criptografia nos servidores de gravação e o seu sistema aplica servidores do sistema de gravação ininterrupta, o Milestone recomenda que você também prepare os servidores do sistema de gravação ininterrupta para criptografia.

Criptografia de dados do servidor móvel (explicado)

No VMS XProtect, a criptografia é ativada ou desativada por servidor móvel. Quando você ativa a criptografia em um servidor móvel, você terá a opção para usar a comunicação criptografada com todos os clientes, serviços e integrações que recuperam fluxos de dados.

Distribuição de certificado para servidores móveis

O gráfico ilustra o conceito básico de como os certificados são assinados, confiados e distribuídos no VMS XProtect para proteger a comunicação com o servidor móvel.



- 1** Uma AC age como um terceiro confiável, confiável tanto pelo assunto/proprietário (servidor móvel) quanto pela parte que verifica o certificado (todos os clientes).
- 2** O certificado da AC deve ser confiável em todos os clientes. Dessa maneira, os clientes podem verificar a validade dos certificados emitidos pela AC
- 3** O certificado da AC é usado para estabelecer a conexão segura entre o servidor móvel e clientes e serviços
- 4** O certificado da CA deve ser instalado no computador no qual o servidor móvel está sendo executado

Requisitos para o certificado de AC:

- O nome do host do servidor móvel deve ser incluído no nome do certificado, seja como assunto/proprietário ou na lista de nomes DNS para a qual o certificado é emitido
- Um certificado deve ser confiável em todos os dispositivos executando serviços que recuperam fluxos de dados do servidor móvel
- A conta de serviço que executa o servidor móvel deve ter acesso à chave privada do certificado no servidor de AC.

Requisitos de criptografia de servidor móvel para clientes

Se você não ativar a criptografia e usar uma conexão HTTP, o recurso push-to-talk XProtect Web Client não estará disponível.

Ativar criptografia

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.

Ativar criptografia para e do servidor de gerenciamento

Você pode criptografar a conexão de duas vias entre o servidor de gerenciamento e o servidor de gravação ou outros servidores remotos com o coletor de dados (Event Server, Log Server, LPR Server e Mobile Server).

Se o seu sistema contém diversos servidores de gravação ou servidores remotos, você deve ativar a criptografia em todos eles. Para obter mais informações, consulte Criptografia de servidor de gerenciamento (explicado) na página 32.

Pré-requisitos:

- Um certificado de autenticação do servidor é confiado no computador que abriga o servidor de gerenciamento

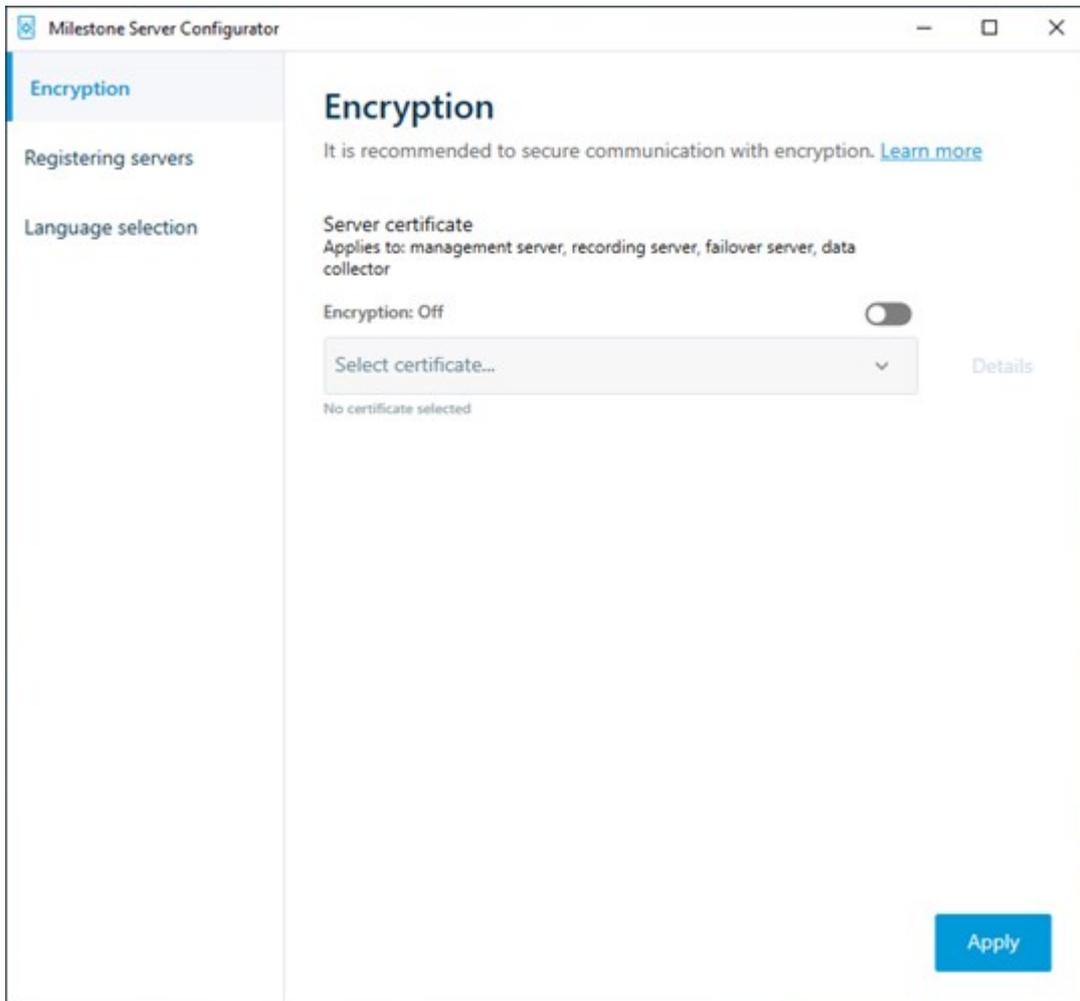
Primeiro, ative a criptografia no servidor de gerenciamento.

Etapas:

1. Em um computador com um servidor de gerenciamento instalado, abra o **Server Configurator** de:
 - Menu Iniciar do Windows Startou
 - 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 servidor coletor de dados.

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, a próxima etapa é atualizar as configurações de criptografia em cada servidor de gravação e em cada servidor com um coletor de dados (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 42.

Habilitar a criptografia do servidor para servidores de gravação ou servidores remotos

Você pode criptografar a conexão de duas vias entre o servidor de gerenciamento e o servidor de gravação ou outros servidores remotos com o coletor de dados (Event Server, Log Server, LPR Server e Mobile Server).

Se o seu sistema contém diversos servidores de gravação ou servidores remotos, você deve ativar a criptografia em todos eles. Para obter mais informações, consulte Criptografia do servidor de gerenciamento para o servidor de gravação (explicado) na página 34 e Criptografia entre o servidor de gerenciamento e o Data Collector Server (explicado) na página 35.

Pré-requisitos:

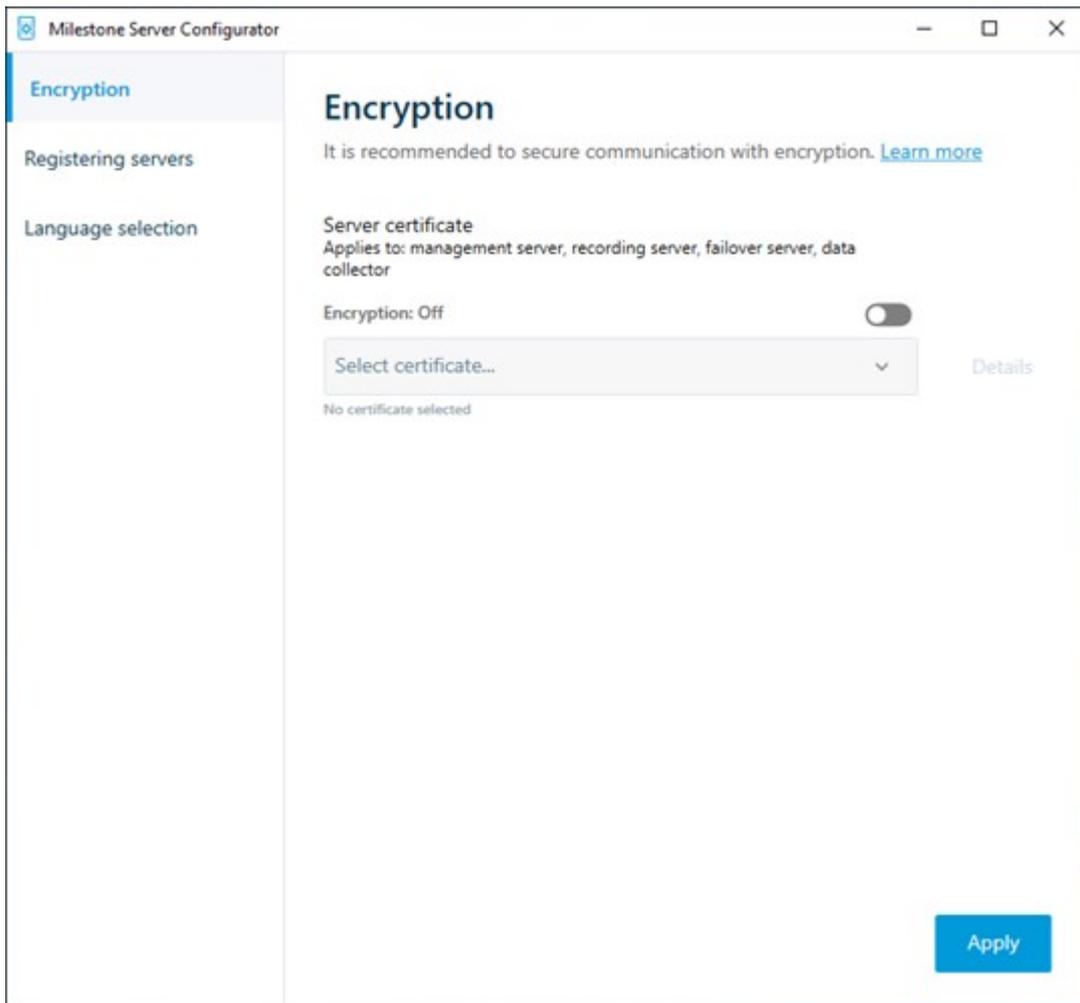
- Você ativou a criptografia no servidor de gerenciamento, consulte Ativar criptografia na página 40

Etapas:

1. Em um computador com um servidor de gravação instalado, abra o **Server Configurator** de:
 - Menu Iniciar do Windows Startou
 - 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 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.



2. 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.

Ative a criptografia para cliente e serviços

Você pode criptografar conexões do servidor de gravação para clientes e serviços que executam fluxo de dados a partir do servidor de gravação. Para mais informações, consulte Criptografia para todos os clientes e servidores que recuperam dados do servidor de gravação (explicado) na página 36.

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

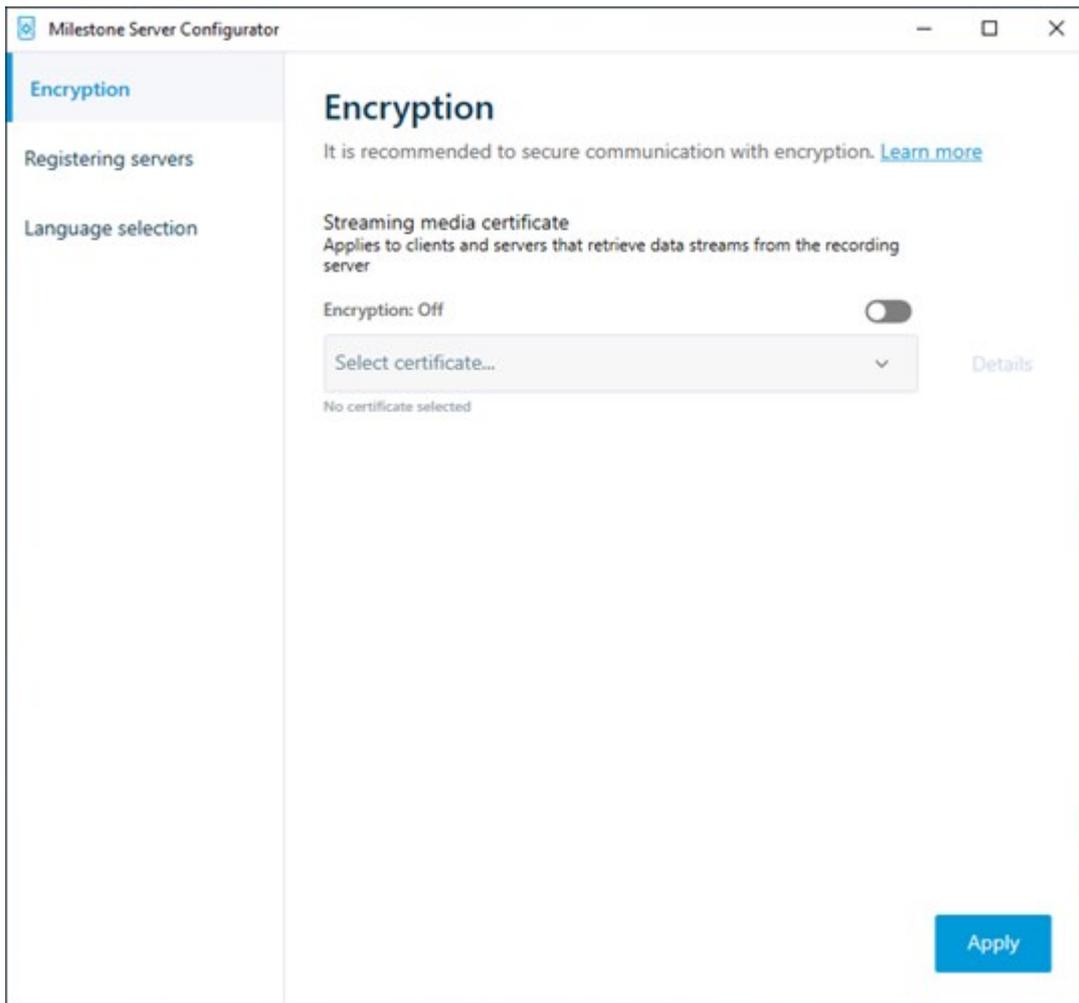
- XProtect Smart Client e todos os serviços que recuperam fluxos de dados do servidor de gravação devem ser da versão 2019 R1 ou superior
- Algumas soluções de terceiros criadas usando versões de MIP SDK anteriores à 2019 R1 podem precisar ser atualizadas.

Etapas:

1. Em um computador com um servidor de gravação instalado, abra o **Server Configurator** de:
 - Menu Iniciar do Windows Startou
 - 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.



2. 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

Se quiser 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 mais informações, consulte Criptografia de dados do servidor móvel (explicado) na página 39 e Requisitos de criptografia de servidor móvel para clientes na página 40.



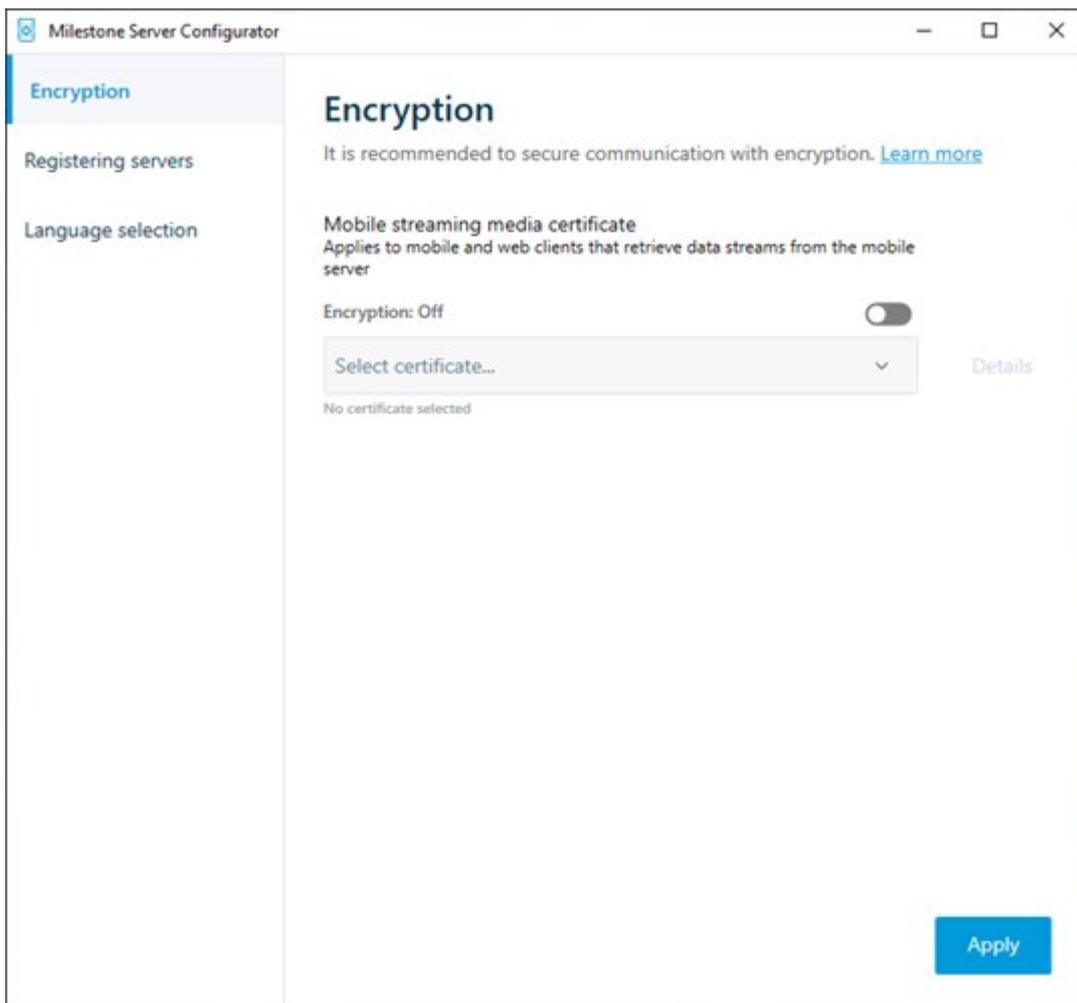
Certificados emitidos pela AC (Autoridade de Certificação) têm uma cadeia de certificados e na raiz de tal cadeia há o certificado raiz da AC. Quando um dispositivo ou navegador encontra esse certificado, ele compara seu certificado raiz com os certificados pré-instalados no SO (Android, iOS, Windows, 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 Startou
 - 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.



2. Clique em **Aplicar**.



Quando você aplica certificados, o serviço Mobile Server é reiniciado.

Milestone Federated Architecture e servidores mestre/secundários (explicado)

Se seu sistema for compatível com Milestone Federated Architecture ou servidores em configuração mestre/secundário, você pode acessar tais servidores com seu cliente XProtect Mobile ou XProtect Web Client. Utilize essa funcionalidade para obter acesso a todas as câmeras em todos os servidores secundários efetuando o login no servidor-mestre.

Se estiver usando uma configuração Milestone Federated Architecture, você obtém acesso a sites filho por meio do site central. Instale o servidor XProtect Mobile somente no site central.

Isso significa que quando os usuários do cliente XProtect Mobile ou XProtect Web Client efetuam login em um servidor para ver câmeras de todos os servidores em seu sistema, eles precisam se conectar ao endereço IP do servidor-mestre. Os usuários devem ter direitos de administrador em todos os servidores no sistema para que as câmeras apareçam no cliente XProtect Mobile ou XProtect Web Client.

Conexão inteligente (explicado)

A Conexão Inteligente permite que você verifique se configurou o servidor XProtect Mobile corretamente sem efetuar login com um dispositivo móvel ou um tablet para fazer a validação. Ela também simplifica o processo de conexão para clientes XProtect Mobile e usuários XProtect Web Client.

Esse recurso exige que seu servidor XProtect Mobile use um endereço de IP público e que seu sistema seja licenciado com um pacote de assinatura Milestone Care Plus.

O sistema dá a você um feedback instantâneo no Management Client se a configuração de conectividade remota foi configurada com êxito e confirma se o servidor XProtect Mobile está acessível na Internet.

A Conexão Inteligente permite que o servidor XProtect Mobile alterne facilmente entre os endereços IP internos e externos e se conecte ao XProtect Mobile a partir de qualquer localização.

Para facilitar a configuração dos clientes móveis dos consumidores, você pode enviar um e-mail diretamente de um Management Client para o usuário final. O e-mail inclui um link que adiciona o servidor diretamente ao XProtect Mobile. Isso completa a configuração sem qualquer necessidade de inserir os endereços de rede ou portas.

Configurar Smart Connect

Para configurar o recurso Conexão inteligente, faça o seguinte:

1. Em Management Client, no painel de navegação, expanda **Servidores** e selecione **Servidores móveis**.
2. Selecione o servidor móvel e clique na guia **Conectividade**.
3. Ative a detectabilidade do Universal Plug and Play em seu roteador.
4. Configurar as definições de conexão.
5. Enviar uma mensagem de e-mail para usuários.
6. Ativar conexões em uma rede complexa.

Ative a detectabilidade do Universal Plug and Play em seu roteador

Para facilitar a conexão de dispositivos móveis aos servidores XProtect Mobile, você pode ativar o Universal Plug and Play (UPnP) em seu roteador. O UPnP ativa o servidor XProtect Mobile para configurar o encaminhamento de porta automaticamente. Contudo, você também pode configurar o encaminhamento de porta manualmente em seu roteador, usando a interface da web dele. Dependendo do roteador, o processo para configurar o mapeamento de porta pode diferir. Se não tiver certeza de como configurar o encaminhamento de porta em seu roteador, consulte a documentação sobre esse dispositivo.



A cada cinco minutos, o serviço Servidor XProtect Mobile verifica se o servidor está disponível para os usuários na internet. O status é exibido no canto superior esquerdo do painel **Propriedades**: 

Ativar conexões em uma rede complexa

Se você tiver uma rede complexa, com configurações personalizadas, você pode fornecer as informações das quais os usuários precisam para se conectarem.

Na guia **Conectividade**, no grupo **Acesso à Internet**, especifique o seguinte:

- Se você usar mapeamento de porta UPnP para direcionar conexões para uma conexão específica, selecione a caixa de seleção **Configurar acesso personalizado à internet**. Em seguida, forneça o **endereço IP ou nome do host** e a porta a ser usada para a conexão. Por exemplo, você pode fazer isso se seu roteador não for compatível com UPnP ou se você tiver uma cadeia de roteadores
- Se seu endereço IP mudar frequentemente, selecione a caixa de seleção **Verificar para recuperar endereço IP dinamicamente**

Definir configurações de conexão

1. Em Management Client, no painel de navegação, expanda **Servidores** e selecione **Servidores móveis**.
2. Selecione o servidor e clique na guia **Conectividade**.
3. Utilize as opções no grupo **Geral** para especificar o seguinte:
 - Para fazer com que seja mais fácil para o cliente XProtect Mobile e os usuários XProtect Web Client conectarem aos servidores XProtect Mobile, selecione a caixa de seleção **Ativar conexão inteligente**
 - Defina a frequência com a qual o cliente XProtect Mobile e XProtect Web Client devem indicar ao servidor móvel que estão em execução
 - Para tornar o servidor XProtect Mobile detectável na rede por meio de protocolos UPnP, selecione a caixa de seleção **Ativar a capacidade de descoberta UPnP**
 - Para ativar o servidor XProtect Mobile, faça o mapeamento da porta isoladamente caso o roteador esteja configurado para isso, selecione a caixa de seleção **Ativar mapeamento automático da porta**

Enviar uma mensagem de e-mail para usuários

Para facilitar a configuração do cliente XProtect Mobile e XProtect Web Client, você pode enviar um e-mail diretamente de um Management Client para o usuário final. O e-mail inclui um link que adiciona o servidor diretamente ao XProtect Mobile. Isso completa a configuração sem qualquer necessidade de inserir os endereços de rede ou portas.

1. No campo **Enviar um convite por e-mail para**, insira o endereço de e-mail do destinatário da notificação Conexão inteligente, depois especifique um idioma.
2. Em seguida, faça um dos seguintes:
 - Para enviar a mensagem, clique em **Enviar**
 - Copie as informações no programa de mensagens que você utiliza

Para obter mais informações, consulte:

Requisitos para configuração da Conexão inteligente na página 12

Guia Conectividade na página 17

Enviando notificações (explicado)

Você pode ativar o XProtect Mobile para notificar usuários quando um evento ocorrer, como, por exemplo, quando um alarme disparar ou quando houver algo de errado com um dispositivo ou um servidor. As notificações sempre são entregues, independentemente se o aplicativo está sendo executado ou não. Quando o XProtect Mobile está aberto no dispositivo móvel, o aplicativo entrega a notificação. As notificações do sistema também são entregues mesmo quando o aplicativo não está sendo executado. Os usuários podem especificar os tipos de notificações que querem receber. Por exemplo, um usuário pode escolher receber notificações para o seguinte:

- Todos os alarmes
- Apenas os alarmes atribuídos a eles
- Apenas alarmes relacionados ao sistema

Estes podem ocorrer quando um servidor fica offline ou volta a ficar online.

Você também pode utilizar notificações por push para notificar usuários que não estejam com o XProtect Mobile aberto. Essas notificações são chamadas notificações por push. As notificações por push são entregues ao dispositivo móvel e são uma ótima maneira de manter os usuários informados quando eles estão em movimento.

Utilizar notificações por push



Para utilizar notificações por push, seu sistema precisa ter acesso à Internet.

Notificações por push utilizam serviços em nuvem da Apple, Microsoft, e Google:

- Serviço Apple Push Notification (APN)
- Microsoft Azure Notification Hub
- Serviço Google Cloud Messaging Push Notification

Há um limite para o número de notificações que seu sistema pode enviar durante um determinado período. Se seu sistema exceder o limite, ele só poderá enviar uma notificação a cada 15 minutos durante o período seguinte. Essa notificação contém um resumo dos eventos que ocorreram durante os 15 minutos. Após o período seguinte, a limitação é removida.

Consulte também Requisitos para a configuração das notificações na página 11 e a guia Guia Notificações na página 26.

Configure notificações por push no servidor XProtect Mobile

Para configurar notificações por push, siga os seguintes passos:

1. Em Management Client, selecione o servidor móvel e depois clique na guia **Notificações**.
2. Para enviar notificações a todos os dispositivos móveis que se conectam ao servidor, selecione a caixa **Notificações**.
3. Para armazenar informações sobre os usuários e dispositivos móveis que se conectam ao servidor, selecione a caixa **Manter registro de dispositivos**.



O servidor envia notificações apenas aos dispositivos móveis nessa lista. Se você desmarcar a caixa **Manter registro de dispositivos** e salvar a mudança, o sistema limpa a lista. Para voltar a receber notificações por push, os usuários precisam reconectar seus dispositivos.

Ative o envio de notificações por push para dispositivos móveis específicos ou para todos os dispositivos móveis

Para ativar XProtect Mobile, notifique usuários quando um evento ocorre enviando notificações push para dispositivos móveis específicos ou para todos os dispositivos móveis:

1. Em Management Client, selecione o servidor móvel e depois clique na guia **Notificações**.
2. Faça um dos seguintes:
 - Para dispositivos individuais, selecione a caixa de seleção **Ativado** para cada dispositivo móvel listado na tabela **Dispositivos registrados**
 - Para todos os dispositivos móveis, selecione a caixa **Notificações**

Parar de enviar notificações por push a dispositivos móveis específicos ou para todos

Há várias maneiras de parar de enviar notificações por push a dispositivos móveis específicos ou para todos.

1. Em Management Client, selecione o servidor móvel e depois clique na guia **Notificações**.
2. Faça um dos seguintes:
 - Para dispositivos individuais, desmarque a caixa **Ativado** para cada dispositivo móvel. O usuário pode utilizar outro dispositivo para se conectar ao servidor XProtect Mobile
 - Para todos os dispositivos, desmarque a caixa **Notificações**

Para interromper temporariamente o envio de notificações por push para todos os dispositivos, desmarque a caixa **Manter registro de dispositivos**, depois salve sua mudança. O sistema volta a enviar notificações depois que os usuários se reconectam.

Configurar investigações

Configure investigações para que as pessoas possam utilizar o XProtect Web Client e XProtect Mobile para acessar vídeos gravados e investigar incidentes, assim como preparar e baixar evidência de vídeo.

Para configurar investigações, siga os seguintes passos:

1. No Management Client, clique no servidor móvel, depois na guia **Investigações**.
2. Marque a caixa de seleção **Habilitar investigações**. Por padrão, a caixa está selecionada.
3. No campo **Pasta de investigações**, especifique onde deseja armazenar vídeos para investigação.
4. Marque a caixa de seleção **Habilitar tamanho limite da pasta de investigações** para definir um tamanho limite para a pasta de investigações e insira o número máximo de megabytes que a pasta de investigações pode conter.
5. Opcional: Para permitir que os usuários acessem investigações criadas por outros usuários, selecione a caixa **Visualizar investigações feitas por outros usuários**. Se você não selecionar essa caixa, os usuários só poderão ver suas próprias investigações.
6. Opcional: Para incluir a data e o horário em que um vídeo foi baixado, selecione a caixa **Incluir carimbos de data/hora para exportações AVI**.

7. No campo **Codec usado para exportações AVI**, selecione o formato de compressão a ser usado durante a preparação de pacotes AVI para download.



Os codecs na lista podem diferir, dependendo de seu sistema operacional. Se você não vir o codec que deseja utilizar, pode instalá-lo no computador em que o Management Client estiver sendo executado e ele será exibido na lista.



Além disso, os codecs podem utilizar diferentes taxas de compressão, que podem afetar a qualidade do vídeo. Taxas de compressão mais altas reduzem os requisitos de armazenamento, mas podem também reduzir a qualidade. Taxas de compressão mais baixas requerem maior capacidade de armazenamento e de rede, mas podem aumentar a qualidade. É uma boa ideia pesquisar os codecs antes de selecionar um.

8. Da lista **Taxa de bits de áudio usada para exportações de AVI**, selecione a taxa de bits de áudio apropriada quando houver áudio incluído na exportação de vídeo. O padrão é 160000 Hz.
9. No campo **Manter ou excluir dados com falha na exportação (MKV e AVI)**, especifique se deseja manter os dados que foram baixados com sucesso, embora possam estar incompletos, ou se prefere excluí-los.



Para permitir que os usuários salvem investigações, você precisa conceder a permissão **Exportar** para a função de segurança atribuída aos usuários.

Limpar investigações

Se você tiver investigações ou exportações de vídeo que não precisa mais guardar, você pode excluí-las. Por exemplo, isso pode ser útil se você quiser disponibilizar mais espaço de disco no servidor.

- Para excluir uma investigação e todas as exportações de vídeo criadas para ela, selecione a investigação na lista e clique em **Excluir**
- Para excluir arquivos individuais de vídeo que foram exportados para uma investigação, porém mantendo a investigação, selecione a investigação na lista. No grupo **Detalhes da investigação**, clique no ícone **Excluir** à direita dos campos **Banco de dados**, **AVI** ou **MKV** para exportação

Uso de Video Push para transmitir vídeo por streaming (explicado)

Você pode configurar o Video Push para que os usuários possam manter os outros informados a respeito de uma situação ou gravar um vídeo para investigá-lo mais tarde, transmitindo o vídeo por streaming diretamente da câmera de seus dispositivos móveis para o seu sistema de monitoramento XProtect. O fluxo de vídeo também pode ter áudio.

Consulte também a guia Guia Video Push na página 25 e Requisitos para configuração de vídeo push na página 12.

Configurar vídeo push para transmitir vídeo por streaming

Para permitir que os usuários transmitam vídeos a partir de seus dispositivos móveis para o sistema XProtect, configure o Video Push no servidor XProtect Mobile.

No Management Client, siga os passos abaixo na seguinte ordem:

1. Na guia **vídeo push**, selecione a caixa de seleção **vídeo push** para ativar o recurso.
2. Adicione um canal vídeo push para fluxo de vídeo.
3. Adicione o driver do vídeo push como dispositivo de hardware no Recording Server. O driver simula um dispositivo de câmera para que você possa transmitir o vídeo por streaming para o Recording Server.
4. Adicione o dispositivo do driver do vídeo push ao canal para vídeo push.

Adicionar um canal de Vídeo push para fluxo de vídeo

Para adicionar um canal, siga estes passos:

1. No painel de navegação, selecione **Servidor móvel** e então selecione o servidor móvel.
2. Na aba **Vídeo Push**, selecione a caixa **Vídeo Push**.
3. Em **Mapeamento de canais**, no canto inferior esquerdo, clique em **Adicionar** para adicionar um canal de Vídeo Push.
4. Na caixa de diálogo exibida, insira o nome da conta de usuário (adicionado em **Funções**) que utilizará o canal. Essa conta de usuário deve ter permissão para acessar o servidor XProtect Mobile e o servidor de gravação (na guia **Segurança Geral**).



Para utilizar o Vídeo Push, os usuários precisam efetuar o login no XProtect Mobile em seu dispositivo móvel, utilizando o nome de usuário e a senha para essa conta.



Quando você adiciona um novo canal de Vídeo Push no servidor móvel, o sistema gera o número da porta e o endereço MAC do canal que são usados quando o canal é adicionado como um dispositivo de hardware no servidor de gravação. O sistema também gera a senha que é usada para conectar o Recording Server com o Mobile Server. A senha padrão é **Milestone**.

5. Anote o número da porta. Você precisará dele quando adicionar o Vídeo Push Driver como um dispositivo de hardware ao servidor de gravação.
6. Clique em **OK** para fechar a caixa de diálogo do canal de vídeo push.
7. Para salvar o canal, clique em **Salvar** no canto superior esquerdo do painel de navegação.

Editar um canal de vídeo push

Você pode editar os detalhes de configuração de um canal de Video Push que tenha adicionado:

1. Em **Em Mapeamento de canais**, selecione o canal a ser editado e clique em **Editar**.
2. Quando terminar de editar, clique em **OK** para fechar a caixa de diálogo do canal de Video Push.
3. Para salvar as edições, clique em **Salvar** no canto superior esquerdo do painel de navegação.



Ao editar o número da porta e o endereço MAC de um canal de Video Push, certifique-se de substituir também os detalhes de configuração do canal de Video Push que você tenha adicionado anteriormente no servidor de gravação com as novas informações. Caso contrário, a conexão entre o Recording Server e o Mobile Server será interrompida.

Remover um canal de vídeo push

Você pode remover canais que não utiliza mais:

1. Em **Em Mapeamento de canais**, selecione o canal a ser removido e clique em **Remover**.
2. Para salvar a alteração, clique em **Salvar** no canto superior esquerdo do painel de navegação.

Alterar senha

Você pode alterar a senha gerada automaticamente que é usada para conectar o Recording Server com o Mobile Server:

1. Em **Mapeamento de canais**, no canto inferior direito, clique em **Alterar senha**.
2. Na caixa de diálogo **Alterar senha do Video Push**, digite a nova senha no primeiro campo, repita a nova senha no segundo campo e clique em **OK**.
3. Para salvar a alteração, clique em **Salvar** no canto superior esquerdo do painel de navegação.



Quando alterar a senha do canal Video Push, a alteração será aplicada a todos os canais de Video Push que já existem na lista ou serão adicionados no futuro. Mesmo se você remover todos os canais de Video Push existentes da lista, a nova senha permanecerá ativa e será aplicada aos canais futuros.



Depois que a alteração é salva, todos os canais de Vídeo Push existentes param de funcionar porque a conexão entre o Recording Server e o Mobile Server foi interrompida. Para restaurar esta conexão, no painel de navegação, clicando com o botão direito do mouse na guia **Servidores de gravação**, você deve executar o assistente **Substituir Hardware** e inserir a nova senha para o Driver de envio de vídeo que você adicionou como um dispositivo de hardware no Recording Server.

Adicione o driver do Vídeo Push como um dispositivo de hardware no Recording Server

1. No painel de navegação, clique em **Servidores de gravação**.
2. Clique com o botão direito no servidor para o qual você deseja transmitir vídeo por streaming, depois clique em **Adicionar hardware** para abrir o assistente de **Adicionar hardware**.
3. Selecione o método de detecção de hardware **Manual** e clique em **Avançar**.
4. Insira as credenciais de login para a câmera:
 - Nome de usuário: Insira os padrões de fábrica ou o nome de usuário especificado na câmera
 - Senha: Digite **Milestone** – a senha que é gerada pelo sistema ou, se você a alterou ao adicionar o canal de Vídeo Push no servidor móvel, insira a senha de sua preferência e clique em **Avançar**



Essas credenciais são para o hardware, não para o usuário. As credenciais não estão relacionadas à conta de usuário usada para acessar o canal de Vídeo Push.

5. Na lista de drivers, expanda **Milestone**, selecione a caixa **Vídeo Push Driver**, depois clique em **Avançar**.
6. No campo **Endereço**, insira o endereço IP do computador no qual o servidor XProtect Mobile está instalado.



É recomendável que você use o endereço MAC gerado pelo sistema. Modifique-o apenas se tiver problemas com o dispositivo Vídeo Push Driver ou, por exemplo, se editou o número da porta e o endereço MAC do canal de vídeo push no servidor móvel.

7. No campo **Porta**, insira o número da porta para o canal que você criou para a transmissão de vídeo por streaming. O número da porta foi atribuído quando você criou o canal.
8. Na coluna **Modelo de hardware**, selecione **Vídeo Push Driver**, depois clique em **Avançar**.
9. Quando o sistema detectar o novo hardware, clique em **Avançar**.

10. No campo **Modelo de nomenclatura de hardware**, especifique se deseja exibir o modelo do hardware e o endereço IP ou apenas o modelo.
11. Especifique se deseja ativar dispositivos relacionados selecionando a caixa **Ativado**. Você pode adicionar dispositivos relacionados à lista do **Vídeo Push Driver** mesmo que eles não estejam ativados. Você pode ativá-los mais tarde.



Se quiser usar informações de localização ao transmitir vídeo por streaming, você precisa ativar a porta de **Metadados**.



Se desejar reproduzir áudio durante o fluxo de vídeo, você deve ativar o microfone relacionado à câmera usada para o fluxo de vídeo.

12. Selecione os grupos padrão para os dispositivos relacionados à esquerda ou selecione um grupo específico no campo **Adicionar ao grupo**. Adicionar dispositivos a um grupo pode facilitar a aplicação de configurações a todos os dispositivos ao mesmo tempo ou a substituição de dispositivos.

Adicionar o dispositivo do driver do Vídeo Push ao canal para vídeo push

Para adicionar o dispositivo do driver do Vídeo Push ao canal para Vídeo Push, siga essas etapas:

1. No painel **Navegação do Site**, clique em **Servidores Móveis**, depois clique na aba **Vídeo Push**.
2. Clique em **Encontrar câmeras**. Se obtiver êxito, o nome da câmera do Driver do Vídeo Push é exibido no campo **Nome da Câmera**.
3. Salve sua configuração.

Ativar áudio para canal de vídeo push existente

Após você ter atendido os requisitos para ativar áudio em vídeo push (consulte Requisitos para configuração de vídeo push na página 12), em Management Client:

1. No painel **Navegação do Site**, expanda o nó **Servidores** e clique em **Servidores de gravação**.
2. No painel de visão geral, selecione a pasta relevante do servidor de gravação, em seguida, expanda a pasta **Driver de vídeo push** e clique com o botão direito no microfone relacionado ao vídeo push.
3. Selecione **Ativado** para ativar o microfone.
4. Na mesma pasta, selecione a câmera relacionada ao vídeo push.
5. No painel **Propriedades**, clique na guia **Cliente** (consulte [Guia cliente \(dispositivos\)](#)).

6. Na lado direito do campo **Microfone relacionado**, clique em . A caixa de diálogo **Dispositivo selecionado** é aberta.
7. On the **Recording Servers** tab, expand the recording server folder and select the vídeo push related microphone.
8. Clique em **OK**.

Configurar usuários para a verificação em duas etapas por e-mail



As funcionalidades disponíveis dependem do sistema que você estiver usando. Consulte <https://www.milestonesys.com/solutions/platform/product-index/> para mais informações.

Para impor uma etapa adicional de login aos usuários do cliente XProtect Mobile ou XProtect Web Client, configure a verificação em duas etapas no servidor XProtect Mobile. Além do nome de usuário e senha padrão, o usuário deve digitar um código de verificação recebido por e-mail.

A verificação em duas etapas aumenta o nível de proteção do seu sistema de monitoramento.

Em Management Client, execute estas etapas:

1. Insira as informações sobre seu servidor SMTP na página 58.
2. Especifique o código de verificação que será enviado aos usuários na página 58.
3. Atribua o método de login para os usuários e grupos do Active Directory na página 59.

Consulte também Requisitos para configuração da verificação em duas etapas do usuário na página 12 e a guia Guia Verificação em duas etapas na página 27.

Insira as informações sobre seu servidor SMTP

O provedor usa as informações sobre o servidor SMTP:

1. No painel de navegação, selecione **Servidores Móveis** e selecione o servidor móvel relevante.
2. Na aba **Verificação em duas etapas**, selecione a caixa de seleção **Ativar a verificação em duas etapas**.
3. Abaixo das **Configurações do provedor**, na aba **E-mail**, insira as informações sobre o servidor SMTP e especifique o e-mail que o sistema enviará aos usuários do cliente quando eles fizerem login e forem configurados para um login secundário. Para obter detalhes sobre cada parâmetro, consulte a guia Guia Verificação em duas etapas na página 27.

Para obter mais informações, consulte Guia Verificação em duas etapas na página 27.

Especifique o código de verificação que será enviado aos usuários

Para especificar a complexidade do código de verificação:

1. Na guia **Verificação em duas etapas**, na seção **Configurações do código de verificação**, especifique o período no qual os usuários do cliente XProtect Mobile não precisam fazer uma nova verificação de seu login no caso de, por exemplo, uma rede desconectada. O período padrão é de três minutos.
2. Especifique o prazo dentro do qual o usuário pode usar o código de verificação recebido. Após este período, o código é invalidado e o usuário precisa pedir um novo código. O período padrão é de cinco minutos.
3. Especifique o número máximo de tentativas de entrada de código, antes que o código fornecido se torne inválido. O número de porta padrão é três.
4. Especifique o número de caracteres para o código. O tamanho padrão é seis.
5. Especifique a complexidade do código que você deseja que o sistema gere.

Para obter mais informações, consulte Guia Verificação em duas etapas na página 27.

Atribua o método de login para os usuários e grupos do Active Directory

Na guia **Verificação em duas etapas**, na seção **Configurações do usuário**, a lista de usuários e grupos adicionados ao seu sistema XProtect aparece.

1. Na coluna **Método de login**, selecione um método de verificação para cada usuário ou grupo.
2. No campo **Detalhes**, adicione os detalhes da entrega, como endereços de e-mail dos usuários individuais. Na próxima vez que o usuário fizer login em XProtect Web Client ou no aplicativo XProtect Mobile, ele será solicitado a fazer um login secundário.
3. Se um grupo estiver configurado no Active Directory, o servidor XProtect Mobile usa detalhes, como endereços de e-mail, do Active Directory.



Os grupos do Windows não suportam uma verificação em duas etapas.

4. Salve sua configuração.

Você concluiu as etapas para a configuração de seus usuários para a verificação em duas etapas por e-mail.

Para obter mais informações, consulte Guia Verificação em duas etapas na página 27.

Ações (explicado)

Você pode gerenciar a disponibilidade da guia **Ações** no cliente XProtect Mobile ou no XProtect Web Client ativando ou desativando **Ações** na guia **Geral**. **As ações** são ativadas por padrão, e todas as ações disponíveis para os dispositivos conectados são mostradas aqui.

Para obter mais informações, consulte a Guia Geral na página 15.

Nomeando uma saída para uso em cliente XProtect Mobile e XProtect Web Client (explicado)

Para que as ações sejam exibidas corretamente junto com a câmera atual, você deve criar um grupo de saída com o mesmo nome da câmera.

Exemplo:

Quando você cria um grupo de saída com saídas conectadas a uma câmera chamada "AXIS P3301,P3304 - 10.100.50.110 - Câmera 1", você deve inserir o mesmo nome no campo **Nome** (sob **Informações do grupo de dispositivos**).

No campo **Descrição**, você pode acrescentar uma descrição adicional, por exemplo, "AXIS P3301,P3304 - 10.100.50.110 - Câmera 1 - Interruptor de luz".



Se você não seguir essas convenções de nomenclatura, as ações não estarão disponíveis na lista de ações para a visualização da câmera associada. Em vez disso, as ações aparecerão na lista de outras ações na guia **Ações**.

Para mais informações, consulte [Dispositivos de saída \(explicado\)](#).

Manutenção

Mobile Server Manager (explicado)

O Mobile Server Manager é um recurso controlado por bandeja e conectado ao servidor móvel. Clique com o botão direito do mouse no ícone Mobile Server Manager no sistema para abrir um menu, onde você pode acessar a funcionalidade do servidor móvel.

É possível:

- Acesso XProtect Web Client na página 61
- Iniciar, parar e reiniciar serviço Mobile Server na página 62
- Preencha/edite o endereço do servidor de gerenciamento na página 62
- Mostrar/editar números de portas na página 62
- Ativar criptografia no servidor móvel na página 63 usando o **Server Configurator**
- Abra o arquivo de registro de hoje (consulte Acessando registros e investigações (explicado) na página 64)
- Abra a pasta de registro (consulte Acessando registros e investigações (explicado) na página 64)
- Abra a pasta de investigação (consulte Acessando registros e investigações (explicado) na página 64)
- Alterar pasta de investigações na página 65
- Veja Servidor XProtect Mobile status (consulte Exibir status (explicado) na página 65)

Acesso XProtect Web Client

Se você tem um servidor XProtect Mobile instalado no seu computador, pode usar o XProtect Web Client para acessar suas câmeras e visualizações. Como não é necessário instalar o XProtect Web Client, é possível acessá-lo do computador no qual foi instalado o servidor XProtect Mobile, ou de qualquer outro computador que você queira usar para esta finalidade.

1. Configurar o servidor XProtect Mobile no Management Client.
2. Se estiver usando o computador onde o servidor XProtect Mobile está instalado, você pode clicar com o botão direito no ícone Mobile Server Manager na bandeja do sistema e selecionar **Abrir XProtect Web Client**.
3. Se não estiver usando o computador onde o servidor XProtect Mobile está instalado, você pode acessá-lo de um navegador. Continue com a etapa 4 deste processo.
4. Abra um navegador da internet (Internet Explorer, Mozilla Firefox, Google Chrome ou Safari).

5. Digite o endereço IP externo, ou seja, o endereço externo e a porta do servidor nos quais o servidor XProtect Mobile estiver sendo executado.

Exemplo: O servidor XProtect Mobile está instalado em um servidor com o endereço IP 127.2.3.4 e está configurado para aceitar conexões HTTP na porta 8081 e conexões HTTPS na porta 8082 (configurações padrão do instalador).

Na barra de endereços do navegador, digite: **http://127.2.3.4:8081** se quiser usar uma conexão HTTP padrão ou **https://127.2.3.4:8082** para usar uma conexão HTTPS segura. Agora você pode começar a usar o XProtect Web Client.

6. Adicione o endereço como um marcador no seu navegador para fácil acesso ao XProtect Web Client no futuro. Se você usa XProtect Web Client no computador local no qual instalou o servidor XProtect Mobile, também pode usar o atalho da área de trabalho criado pelo instalador. Clique no atalho para abrir seu navegador padrão e abra XProtect Web Client.



Você deve limpar o cache dos navegadores que executam o XProtect Web Client antes de usar uma nova versão do XProtect Web Client. Os administradores do sistema devem pedir que seus usuários do XProtect Web Client limpem o cache do navegador após atualizar, ou forcem esta ação remotamente (você pode fazer isso apenas no Internet Explorer em um domínio).

Iniciar, parar e reiniciar serviço Mobile Server

Se necessário, você pode iniciar, parar e reiniciar o serviço Mobile Server a partir do Mobile Server Manager.

- Para executar qualquer uma destas tarefas, clique com o botão direito do mouse no ícone Mobile Server Manager e selecione **Iniciar Mobile Server serviço**, **Parar serviço Mobile Server** ou **Reiniciar Mobile Server serviço**, respectivamente

Preencha/edite o endereço do servidor de gerenciamento

1. Clique com o botão direito no ícone do Mobile Server Manager e selecione **Endereço do servidor de gerenciamento**.
2. No campo **URL do servidor**, insira o endereço URL do servidor.
3. Clique em **OK**.

Mostrar/editar números de portas

1. Clique com o botão direito do mouse no ícone Mobile Server Manager e selecione **Mostrar/Editar números de portas**.
2. Para editar os números de porta, digite o número da porta correspondente. Você pode indicar um número

padrão de porta para conexões HTTP ou um número de porta segura para conexões HTTPS, ou ambos.

3. Clique em **OK**.

Ativar criptografia no servidor móvel

Se quiser 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 mais informações, consulte Criptografia de dados do servidor móvel (explicado) na página 39 e Requisitos de criptografia de servidor móvel para clientes na página 40.



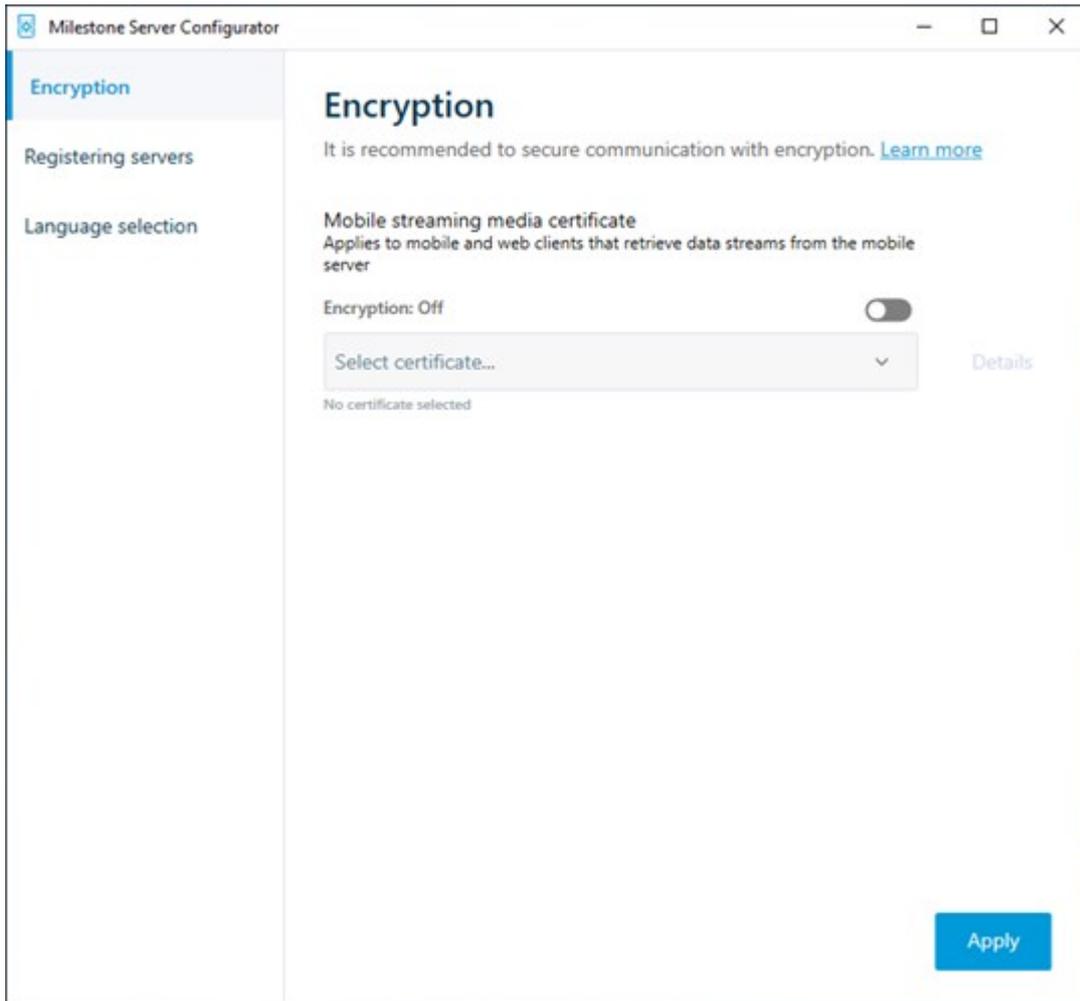
Certificados emitidos pela AC (Autoridade de Certificação) têm uma cadeia de certificados e na raiz de tal cadeia há o certificado raiz da AC. Quando um dispositivo ou navegador encontra esse certificado, ele compara seu certificado raiz com os certificados pré-instalados no SO (Android, iOS, Windows, 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 Startou
 - 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.



2. Clique em **Aplicar**.



Quando você aplica certificados, o serviço Mobile Server é reiniciado.

Acessando registros e investigações (explicado)

O Mobile Server Manager permite que você acesse rapidamente o arquivo de registro do dia, abra a pasta onde os arquivos de registros são salvos, e abra a pasta onde as investigações estão salvas.

Para abrir qualquer um deles, clique com o botão direito do mouse no ícone Mobile Server Manager e selecione:

- **Abrir o arquivo de registro de hoje**
- **Abrir Servidor de Registros**
- **Abrir pasta de investigações**



Se você desinstalar o servidor XProtect Mobile do seu sistema, seus arquivos de registro não serão excluídos. Administradores com direitos de usuário adequados podem acessar esses arquivos de registro posteriormente ou decidir excluí-los se não forem mais necessários. O local padrão dos arquivos de registro está na pasta **Dados do Programa**. Se você alterar o local padrão dos arquivos de registros, os registros existentes não são copiados para o novo local nem são excluídos.

Alterar pasta de investigações

O local padrão das investigações está na pasta **Dados do Programa**. Se você alterar o local padrão da pasta de investigações, as investigações existentes não serão automaticamente copiadas para o novo local nem serão excluídas. Para alterar o local onde você salva as exportações de investigações em seu disco rígido:

1. Clique com o botão direito no ícone Mobile Server Manager e selecione **Alterar pasta de investigações**.
A janela **Local das investigações** é exibida.
2. Próximo ao campo **Pasta**, que mostra a localização atual, clique no ícone da pasta para procurar uma pasta existente ou criar uma nova pasta > Clique em **OK**.
3. Da lista **Investigações antigas**, selecione a ação que você deseja aplicar às investigações existentes que estão armazenadas no local atual. As opções são:

- **Mover**: Move as investigações existentes para a nova pasta



Se você não mover as investigações existentes para a nova pasta, não poderá mais visualizá-las.

- **Excluir**: Exclui as investigações existentes
 - **Não fazer nada**: As investigações existentes permanecem na localização atual da pasta. Você não conseguirá mais vê-las após alterar o local padrão das pastas de investigações
4. Clique em **Aplicar** > clique em **OK**.

Exibir status (explicado)

Clique com o botão direito do mouse no ícone Mobile Server Manager e selecione **Exibir status** ou clique duas vezes no ícone Mobile Server Manager para abrir uma janela que mostra o status do servidor XProtect Mobile. Você pode ver a seguinte informação:

Nome	Descrição
Servidor funcionando desde	Data e hora do momento em que o servidor XProtect Mobile foi iniciado pela última vez.
Usuários conectados	Número de usuários atualmente conectados ao servidor XProtect Mobile.
Decodificação de hardware	Indica se a decodificação acelerada por hardware está ocorrendo no servidor XProtect Mobile.
Uso de CPU	O % da CPU que está sendo usado atualmente pelo servidor XProtect Mobile.
Histórico de uso de CPU	Um gráfico que detalha o histórico do uso de CPU pelo servidor XProtect Mobile.

Solução de problemas

Solução de problemas XProtect Mobile

Conexões

1. **Por que eu não consigo conectar a partir do meu cliente XProtect Mobile às minhas gravações/XProtect Mobile servidor?**

Para conectar às suas gravações, o servidor XProtect Mobile deve ser instalado no servidor que executa o seu sistema XProtect, ou alternativamente, em um servidor dedicado. As configurações relevantes do XProtect Mobile também são necessárias na sua configuração de gerenciamento de vídeo do XProtect. Elas são instaladas como plug-in ou parte de uma instalação ou atualização do produto. Para obter detalhes sobre como obter o servidor do XProtect Mobile e sobre como integrar as configurações relacionadas ao cliente XProtect Mobile em seu sistema XProtect, veja a seção de configuração (consulte Configurações do servidor móvel na página 15).

2. **Eu acabo de ativar meu firewall e agora não consigo conectar um dispositivo móvel ao meu servidor. Por que não?**

Se o seu firewall foi desativado enquanto você instalava o servidor XProtect Mobile você deve ativar as comunicações TCP e UDP manualmente.

3. **Como evitar o aviso de segurança quando eu executo o XProtect Web Client através de uma conexão HTTPS?**

O aviso aparece pois as informações do endereço do servidor no certificado estão incorretas. A conexão ainda será criptografada.

O certificado auto-assinado no servidor XProtect Mobile precisa ser substituído pelo seu próprio certificado correspondendo ao endereço do servidor usado para conectar ao servidor do XProtect Mobile. Esses certificados são obtidos através de autoridades de assinatura de certificado, como a Verisign. Consulte a autoridade de assinatura escolhida para obter mais detalhes.

O servidor XProtect Mobile não usa Microsoft IIS. Isto significa que as instruções fornecidas para gerar arquivos de solicitação de assinatura de certificado (CSR) pela autoridade assinando usando o IIS não se aplicam ao servidor do XProtect Mobile. Você deve criar o arquivo de CSR manualmente, usando ferramentas de certificado de linha de comando ou outro aplicativo de terceiros semelhante. Esse processo deve ser realizado somente por administradores do sistema e usuários avançados.

Qualidade da imagem

1. Por que a qualidade da imagem é ruim algumas vezes quando eu visualizo vídeo no cliente XProtect Mobile?

O servidor do XProtect Mobile ajusta a qualidade da imagem automaticamente, de acordo com a largura de banda disponível entre o servidor e o cliente. Se você vivenciar uma imagem de qualidade mais baixa do que no XProtect® Smart Client, pode ser que você tenha muito pouca largura de banda para obter imagens de resolução completa através do cliente XProtect Mobile. A razão para isso pode ser muito pouca largura de banda de upstream do servidor ou muito pouca largura de banda downstream no cliente. Para obter mais informações, consulte o [manual de usuário do XProtect Smart Client](#).

Se você estiver em uma área com largura de banda sem fio, poderá notar que a qualidade da imagem melhora ao entrar em uma área com largura de banda melhor.

2. Por que a qualidade da imagem é ruim quando eu conecto ao meu sistema de gerenciamento de vídeo XProtect em casa, através de um Wi-Fi em meu escritório?

Verifique a largura da banda da sua internet residencial. Muitas conexões privadas à internet têm diferentes larguras de banda para download e upload, frequentemente descritas como, por exemplo, 20 Mbit/2 Mbit. Isso é devido a usuários de residências raramente precisarem fazer o upload de grandes quantidades de dados para a internet, mas ao invés disso, consomem grandes quantidades de dados. O sistema de gerenciamento de vídeo do XProtect precisa enviar vídeo para o cliente do XProtect Mobile e é limitado pela velocidade de upload da sua conexão. Se a qualidade da imagem for baixa consistentemente em diversos locais onde a velocidade do download da rede do cliente XProtect Mobile for boa, o problema pode ser resolvido pela atualização da velocidade de upload da sua conexão de Internet de casa.

Decodificação acelerada de hardware

1. O meu processador suporta a decodificação acelerada por hardware?

Somente processadores Intel mais recentes suportam a decodificação acelerada por hardware. Consulte o site da Intel (<https://ark.intel.com/Search/FeatureFilter?productType=processors/>) para ver se o seu processador é suportado.

No menu, assegure-se de que **Tecnologias > Intel Quick Sync Video** está definido para **Sim**.

Se o seu processador for suportado, a decodificação acelerada por hardware estará ativada, por padrão. Você pode ver o status atual em **Mostrar status** no Mobile Server Manager (consulte Exibir status (explicado) na página 65).

2. O meu sistema operacional suporta a decodificação acelerada por hardware?

Todos os sistemas operacionais que o XProtect suporta, também suportam aceleração de hardware.

Não deixe de instalar os drivers gráficos mais recentes a partir do site da Intel no seu sistema. Esses drivers não estão disponíveis na Atualização do Windows.

A decodificação acelerada por hardware não é suportada se o servidor móvel estiver instalado em um ambiente virtual.

3. Como eu desativo a decodificação acelerada por hardware no servidor móvel? (Avançado)

Se o processador no servidor móvel suportar decodificação acelerada por hardware, ela estará ativada, por padrão. Para desativar a decodificação acelerada por hardware, faça o seguinte:

1. Localize o arquivo de configuração VideoOS.MobileServer.Service.exe. O caminho padrão é:
C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config.
2. Abra o arquivo no Notepad ou um editor de texto similar. Se necessário, associe o tipo de arquivo .config com o Notepad.
3. Localize o campo `<add key="HardwareDecodingMode" value="Auto" />`.
4. Substitua o valor "Auto" por "Des".
5. Salvar e fechar o arquivo.



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/>.

