MAKE THE
WORLD SEE

Milestone Systems

Servidor do XProtect® Mobile 2024 R2

Manual do administrador

milestone

Conteúdo

Copyright, marcas comerciais e limitação de responsabilidade

Marcas comerciais

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

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

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

Limitação de responsabilidade

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

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

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

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

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

Visão Geral

O que há de novo?

No servidor do XProtect Mobile 2023 R3

Informações de conexão:

- Verifique se o servidor móvel está acessível diretamente da Internet. Consulte Informações de conexão na página 14.

Alarmes:

- Adicione alarmes de Alerta de emergência para permitir que os usuários recebam notificações de alarme do mais alto nível de gravidade no cliente do XProtect Mobile. Consulte Adicionar alarmes de Alerta de emergência na página 51.

No servidor do XProtect Mobile 2023 R2

Compartilhamento de marcadores e vídeos ao vivo:

- Para compartilhar marcadores e vídeos ao vivo no cliente do XProtect Mobile, você tem que ativar a criptografia no servidor de gerenciamento. Consulte Requisitos para usar o Compartilhamento na página 10.

Notificações:

- Você pode remover dados de registro do dispositivo do banco de dados do VMS. Consulte Remova um ou todos os dispositivos registrados da lista de dispositivos registrados na página 40.

No servidor do XProtect Mobile 2022 R3

IDP externo:

- Faça login no XProtect Web Client e no cliente XProtect Mobile com um IDP externo. Veja IDP externo e XProtect Mobile na página 51

Gerenciamento de dispositivo móvel (MDM):

- O cliente XProtect Mobile agora é compatível com o gerenciamento de dispositivo móvel (MDM). Com o MDM, é possível gerenciar e proteger dispositivos, aplicativos e dados a partir de um console unificado. Para obter mais informações, consulte Gerenciamento de dispositivo móvel (Mobile device management, MDM) na página 48

Notificações por push:

- Quando você ativa esse recurso, um aviso informa que o sistema talvez não seja compatível com o GDPR

No XProtect Mobile 2022 R2

Notificações:

- Notificações são desativadas por padrão

Instalação:

- Ao instalar Mobile Server, é possível conectar-se ao sistema de monitoramento com um usuário básico

XProtect Mobile

O XProtect Mobile consiste em cinco componentes:

Cliente do 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.

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.

Servidor do XProtect Mobile

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.

Plug-in do XProtect Mobile

O plug-in do XProtect Mobile faz parte do componente XProtect Mobile Server. O plug-in do XProtect Mobile permite visualizar e gerenciar os servidores móveis em seu sistema VMS diretamente do nó **Servidores** no XProtect Management Client.

Você instala o plug-in do XProtect Mobile em qualquer computador com o XProtect Management Client no qual deseje gerenciar os servidores móveis.

Mobile Server Manager

Use o Mobile Server Manager para obter informações sobre o serviço, verificar o estado do serviço Mobile Server, visualizar registros ou mensagens de status e iniciar e interromper o serviço.

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

Requisitos e considerações

Antes de instalar o servidor do XProtect Mobile

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

Milestone recomenda que você instale o servidor XProtect Mobile em um computador separado. Antes de instalar e começar a usar o componente XProtect Mobile Server, verifique se:

- Você configurou câmeras e visualizações no XProtect Management Client.
- O computador do servidor móvel resolve os nomes de host dos computadores que executam os outros componentes do servidor de VMS.
- O computador do servidor de gerenciamento resolve o nome do host do computador do servidor móvel.
- Você tem um VMS em execução instalado.
- Você configurou ao menos um usuário do VMS. Para se conectar ao sistema de monitoramento, a função à qual esse usuário é adicionado requer permissões para o servidor de gerenciamento:
  - **Conectar**
  - **Ler**
  - **Editar**
- Se você estiver atualizando seu sistema, verifique se a versão do plug-in do XProtect Mobile corresponde à versão do servidor móvel. Seu sistema poderá não funcionar corretamente se as versões do plug-in e dos servidores móveis não forem idênticas.

Requisitos para a configuração das notificações

Para notificar usuários quando um evento ocorrer:

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

Para obter mais informações, consulte:

Configure notificações por push no servidor XProtect Mobile na página 38

Guia Notificações na página 27

Requisitos para configuração da Conexão inteligente

Para usar a conexão inteligente e verificar se você configurou o XProtect Mobile corretamente, você precisa ter:

- Um endereço IP público para o seu servidor do XProtect Mobile. O endereço pode ser estático ou dinâmico, mas geralmente é uma boa ideia usar endereços IP estáticos
- Uma licença válida para a conexão inteligente
- Um contrato de Milestone Care™ atualizado com a Milestone Systems

Requisitos para configuração da verificação em duas etapas do usuário

Para configurar usuários para a verificação em duas etapas por e-mail:

- Você instalou um servidor SMTP.
- Você adicionou os usuários e grupos ao seu sistema XProtect no Management Client nó **Funções** no painel **Navegação do Site**. Na função relevante, selecione a guia **Usuários e grupos**.
- Se você tiver atualizado o seu sistema vindo de uma versão anterior do XProtect, será necessário reiniciar o Mobile Server para ativar o recurso de verificação em duas etapas.

Para obter mais informações, consulte:

Configurar usuários para a verificação em duas etapas por e-mail na página 46

Guia Verificação em duas etapas na página 28

Requisitos para configuração de vídeo push

Para transmitir vídeo da câmera de um dispositivo móvel para o sistema de monitoramento XProtect, você precisa ter:

- Uma licença do dispositivo para cada canal que utilizar.

Requisitos para o streaming direto

XProtect Mobile é compatível com transmissão direta no modo ao vivo. Para usar o streaming direto no XProtect Web Client e cliente do XProtect Mobile, você deve ter as seguintes configurações na câmera:

- As câmeras precisam ser compatíveis com o codec H.264 ou o codec H.265.

  O XProtect Web Client é compatível somente com H.264.

- Recomenda-se definir o valor do **tamanho do GOP** para **1 segundo** e a definição de **FPS** precisa ter um valor superior a **10** quadros por segundo.

Requisitos para usar o Compartilhamento

Os usuários podem compartilhar marcadores e vídeos ao vivo enquanto usam o aplicativo do cliente do XProtect Mobile. Essas funcionalidades ficam disponíveis após:

- Você ativar a criptografia no servidor de gerenciamento.

Instalação

Instalar o servidor do XProtect Mobile

Depois que tiver instalado o servidor do XProtect Mobile, você poderá usar o cliente do XProtect Mobile e o 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.

Baixar o instalador do servidor do XProtect Mobile

1. Digite o 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. Selecione **Todos os idiomas** para o instalador do servidor XProtect Mobile.

Instalar o servidor do XProtect Mobile

1. Execute o arquivo baixado. Em seguida, selecione **Sim** para todos os avisos.
2. Selecione o idioma para o instalador. Em seguida, selecione **Continuar**.
3. Leia e aceite o contrato de licença. Em seguida, selecione **Continuar**.
4. Selecione o tipo de instalação:
   - Selecione **Típica** para instalar o servidor XProtect Mobile e plug-in
   - Selecione **Personalizada** para instalar apenas o servidor ou apenas o plug-in. Por exemplo, instalar apenas o plug-in é útil se você quiser usar o Management Client para gerenciar os servidores XProtect Mobile, mas se não precisar do servidor XProtect Mobile nesse computador

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

5. Apenas para a instalação personalizada: Selecione os componentes que deseja instalar. Em seguida, selecione **Continuar**.
6. Selecione uma conta de serviço para o servidor móvel. Em seguida, selecione **Continuar**.

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

7. Apenas para a instalação personalizada: Faça login com uma conta de usuário VMS existente ao se conectar ao sistema de monitoramento:
   - A **conta de serviço** é a conta que você selecionou na etapa 8. Para se conectar usando essa conta, certifique-se de que a conta de serviço seja membro de um domínio ao qual o servidor de gerenciamento tenha acesso
   - **Usuário básico.** Utilize um usuário básico quando a conta de serviço não for membro de um domínio ao qual o servidor de gerenciamento tem acesso

   > Para alterar ou editar a conta do serviço ou as credenciais do usuário básico posteriormente, você terá que reinstalar o servidor móvel.

   Selecione **Continuar**.
8. No campo **URL do servidor**, preencha o endereço do servidor de gerenciamento primário.

   Apenas para a instalação personalizada: Especifique as portas de conexão da comunicação com o servidor móvel. Em seguida, selecione **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).
9. Na página **Atribuir uma senha de proteção de dados do servidor móvel** e insira uma senha para criptografar suas investigações. Como administrador do sistema você terá que inserir essa senha para acessar os dados do servidor móvel em caso de uma recuperação do sistema ou ao expandir seu sistema com servidores móveis adicionais.

   > Você deve salvar esta senha e mantê-la segura. Não fazer isso pode comprometer a sua capacidade de recuperar dados do servidor móvel.

   Se não desejar que suas investigações sejam protegidas por senha, selecione **Eu opto por não usar uma senha de proteção de dados do servidor móvel e compreendo que as investigações não serão criptografadas**.

   Clique em **Continuar**.
10. Especificar a criptografia do servidor móvel. Em seguida, selecione **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.

Para obter mais informações sobre como estabelecer comunicação segura em seu sistema, consulte:

- Criptografia de dados do servidor móvel (explicado)
- O guia Milestone sobre certificados

Você também pode ativar a criptografia após a instalação ser concluída a partir do ícone de bandeja Mobile Server Manager na barra de tarefas do seu sistema operacional. (consulte Ativar criptografia no servidor móvel na página 34).

11. Selecione a localização do arquivo e o idioma do produto e então selecione **Instalar**.

    Quando a instalação estiver concluída, uma lista de componentes instalados com sucesso será exibida.

Configuração

Configurações do servidor móvel

No Management Client, você pode configurar e editar uma lista de configurações do servidor XProtect Mobile. Você pode acessar essas configurações 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 do servidor (consulte Guia Conectividade na página 17)
- Configurar o recurso Conexão inteligente (consulte Guia Conectividade na página 17)
- Veja o status atual do servidor e da lista de usuários ativos (consulte Guia Status do servidor na página 20)
- Configure parâmetros de desempenho para ativar o streaming direito ou o fluxo adaptável ou para definir as limitações do fluxo de vídeo (consulte Guia Desempenho na página 21)
- Configure as configurações de investigação (consulte Guia de investigações na página 24)
- Configure os recursos de vídeo push (consulte Guia Video Push na página 26)
- Configurar, ligar e desligar sistema e notificações push (consulte Guia Notificações na página 27)
- Ative e configure uma etapa de login adicional para usuários (consulte Guia Verificação em duas etapas na página 28)

Informações de conexão

As tabelas a seguir descrevem os status e as mensagens do servidor móvel que estão visíveis em todas as guias.

O servidor está acessível pela Internet

Cor	Status	Descrição
Laranja	N/A	O servidor móvel não foi configurado para ser acessível fora da rede local.
Vermelho	Não	Os usuários do cliente XProtect Web Client e XProtect Mobile não podem se conectar ao servidor móvel diretamente da Internet.
Verde	Sim	Os usuários do cliente XProtect Web Client e XProtect Mobile podem se conectar ao servidor móvel diretamente da Internet.

Conexão com o servidor

Cor	Mensagem	Descrição
Laranja	**Certificado HTTPS inválido**	O plug-in do XProtect Mobile não reconhece o certificado do servidor móvel.
Laranja	**HTTP/HTTPS fora de alcance**	O XProtect Management Client não conseguiu contatar o servidor móvel.
Vermelho	**HTTP/HTTPS não conectado**	O XProtect Management Client detectou o servidor móvel, mas não consegue estabelecer conexão com ele.
Verde	**HTTP/HTTPS**	O XProtect Management Client estabeleceu uma conexão com o servidor móvel.

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.

Características

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

Nome	Descrição
Ativar XProtect Web Client	Ativar acesso a XProtect Web Client. Este recurso é ativado por padrão.
Ativar a visualização Todas as câmeras para o cliente XProtect Mobile	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 favoritos	Ative o recurso de favoritos para localizar rapidamente sequências de vídeo no cliente XProtect Mobile e no XProtect Web Client. Este recurso é ativado por padrão.
Habilitar ações (saídas e eventos)	Ativar acesso a ações no cliente XProtect Mobile e XProtect Web Client. Este recurso é ativado por padrão. Se você desativar esse recurso, os usuários do cliente não poderão ver saídas e eventos, mesmo se estiverem configurados corretamente.
Ativar áudio de entrada	Ativar o recurso de áudio de entrada no XProtect Web Client cliente XProtect Mobile. Este recurso é ativado por padrão.
Ativar pressione-para-falar	Habilite o recurso push-to-talk (PTT) no XProtect Web Client e no 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
Local de arquivo de log	Veja onde o sistema salva os arquivos de registro.
Manter 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 37
- Enviar uma mensagem de e-mail para usuários na página 37
- Ativar conexões em uma rede complexa na página 36
- Ative a detectabilidade do Universal Plug and Play em seu roteador na página 36

Para obter mais informações, consulte Smart Connect na página 35.

> 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 34.

Geral

Nome	Descrição
Tempo limite do cliente	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. A Milestone recomenda que você não aumente o intervalo de tempo.
Ativar visibilidade UPnP	Isso faz com que o servidor do XProtect Mobile possa ser descoberto na rede por meio dos protocolos UPnP. O cliente XProtect Mobile possui a funcionalidade de varredura para localizar servidores XProtect Mobile com base em UPnP.
Habilitar o mapeamento automático de portas	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. 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.
Habilitar o Smart Connect	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.

Acesso à Internet

Nome	Descrição
Configure o acesso personalizado à Internet	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

Nome	Descrição
	compatível com UPnP ou se você tiver uma cadeia de roteadores.
• **HTTP** • **HTTPS**	Selecione o tipo de conexão.
Selecione para recuperar o endereço de IP de forma dinâmica	Marque a caixa de seleção se seus endereços IP mudam com frequência.
Use apenas o endereço URL configurado	Marque a caixa de seleção para se conectar ao servidor móvel apenas com um endereço IP ou nome de host com especificação personalizada.
Endereços do servidor	Lista todos os endereços URL conectados ao servidor móvel.

Notificação de Smart Connect

Nome	Descrição
Enviar e-mail de convite para	Insira o endereço de e-mail para o destinatário da notificação Smart Connect.
Idioma do e-mail	Especifique o idioma usado no e-mail.
Token do o Smart Connect	Um identificador exclusivo que os usuários de dispositivos móveis podem usar para conectar-se ao servidor XProtect Mobile.
Link para o Smart Connect	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: • **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.

Nome	Descrição
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 transcodificados	Mostra o número total de fluxos de vídeo transcodificados que estão atualmente abertos, para cada cliente do XProtect Mobile ou usuário do XProtect Web Client.
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	Após você ativar o recurso de fluxo adaptável, poderá selecionar o tipo de modo de fluxo da lista:

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

Nome	Descrição
Resolução máxima da imagem	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 vídeo gravado
- Investigar incidentes
- Preparar e baixar evidência de vídeo

Nome	Descrição
Habilitar 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.
Ver investigações feitas por outros usuários	Selecione essa caixa para permitir que usuários acessem investigações que não tenham sido criadas por eles.
Habilitar a limitação de	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

Nome	Descrição
tamanho da pasta de investigações	pode conter. O tamanho padrão é 2000 MB.
Ativar o tempo de retenção da investigação	Selecione esta caixa de seleção para definir um tempo de retenção para investigações. Por padrão, o tempo de retenção é de sete dias.
Formatos de exportação	Selecione esta caixa de seleção do formato de exportação que deseja usar. Os formatos de exportação disponíveis são: • **Formato do AVI** • **XProtect formato** • **Formato do MKV** Por padrão, as caixas de verificação estão limpas.
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.
Bits de áudio usados 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.

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, vocês desejar 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 **XProtect**, **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.
Porta	Número de porta para o canal de vídeo push em questão.
Endereço MAC	O endereço MAC para o canal de Video 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 42), 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.

Por padrão, as notificações estão desativadas.

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 39

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

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 46.

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.
Use 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.
Use Autenticação de Senha Segura (SPA)	Selecione esta caixa de seleção se o servidor SMTP suporta a SPA.

Nome	Descrição
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	Digite a mensagem que deseja enviar. Exemplo: O seu código é {0}.  Se você se esquecer de incluir a variável {0}, o código é adicionado ao final do texto por padrão.

Configurações do código de verificação

Nome	Descrição
Tempo limite da reconexão (0 a 30 minutos)	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. Essa configuração não se aplica ao XProtect Web Client.
O código expira após (1 a 10 minutos)	Especifique o prazo dentro do qual o usuário pode usar o código de verificação recebido. Após esse período, o código é invalidado e o usuário precisa solicitar um novo código. O período padrão é de cinco minutos.
Tentativas de inserção de código (1 a 10 tentativas)	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.
Comprimento do código (4 a 6 caracteres)	Especifique o número de caracteres para o código. O tamanho padrão é seis.
Composição do	Especifique a complexidade do código que você deseja que o sistema gere. Você

Nome	Descrição
código	pode selecionar entre: • **Maiúscula latina (A-Z)** • **Minúscula latina (a-z)** • **Dígitos (0-9)** • **Caracteres especiais (!@#...)**

Configurações do usuário

Nome	Descrição
Usuários e grupos	Lista os usuários e os grupos adicionados ao sistema XProtect. Se um grupo estiver configurado no Active Directory, o servidor móvel usa detalhes, como endereços de e-mail, do Active Directory.  Os grupos do Windows não dão suporte para a verificação em duas etapas.
Método de verificação	Selecione uma configuração de verificação para cada usuário ou grupo. Você pode selecionar entre: • **Nenhum login**: o usuário não consegue efetuar o login • **Nenhuma verificação em duas etapas**: o usuário deve digitar o nome de usuário e senha • **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

XProtect Mobile é compatível com transmissão direta no modo ao vivo.

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 cliente XProtect® Mobile também é compatível com o uso do codec H.265. O Streaming direto não requer nenhuma transcodificação e, portanto, elimina um pouco do estresse do sistema XProtect.

A tecnologia de streaming direito, 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 em 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 14).

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

- 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 9)
- 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

Fluxo adaptável

XProtect Mobile é compatível com fluxo adaptável no modo ao vivo.

Fluxo adaptável é útil quando você visualização 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 o 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 14).

Criptografia de dados do servidor móvel (explicado)

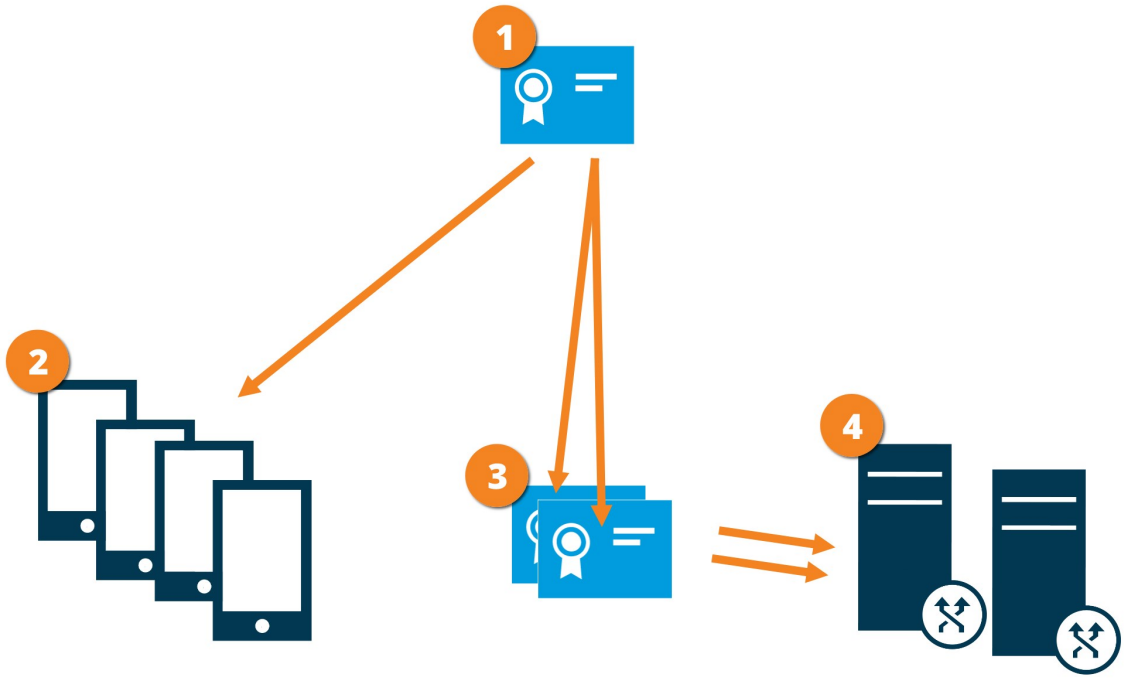
Por razões de segurança, Milestone recomenda que você use a comunicação segura entre o servidor móvel e os clientes ao gerenciar configurações de contas de usuários.

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

No VMS XProtect, a criptografia é ativada ou desativada para cada 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 acontece o processo de assinatura, atestado de confiabilidade e distribuição dos certificados no VMS XProtect para proteger a comunicação com o servidor móvel.



❶ Uma AC age como um terceiro confiável, confiável tanto pelo assunto/proprietário (servidor móvel) quanto pela parte que verifica o certificado (todos os clientes).

❷ O certificado da AC deve ser confiável em todos os clientes. Dessa maneira, os clientes podem verificar a validade dos certificados emitidos pela AC

❸ O certificado da AC é usado para estabelecer a conexão segura entre o servidor móvel e clientes e serviços

❹ O certificado da AC 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.

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

Ativar criptografia no servidor móvel

Para usar um protocolo HTTPS seguro para estabelecer conexão entre o servidor móvel e clientes e serviços, você deve aplicar um certificado válido ao servidor. O certificado confirma que o titular do certificado está autorizado a estabelecer conexões seguras.

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

Quando configurar a criptografia para um grupo de servidores, ela deve ser habilitada com um certificado pertencente ao mesmo certificado CA ou, se desabilitada, deve ser desabilitada em todos os computadores do grupo de servidores.

Certificados emitidos pela AC (Autoridade de Certificação) têm uma cadeia de certificados e na raiz de tal cadeia há o certificado raiz da AC. Quando um dispositivo ou navegador encontra esse certificado, ele compara seu certificado raiz com os certificados pré-instalados no SO (Android, iOS, Windows, etc.). Se o certificado raiz estiver listado na lista de certificados pré-instalados, o SO garante ao usuário que a conexão com o servidor é suficientemente segura. Esses certificados são emitidos para um nome de domínio e não são gratuitos.

Etapas:

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

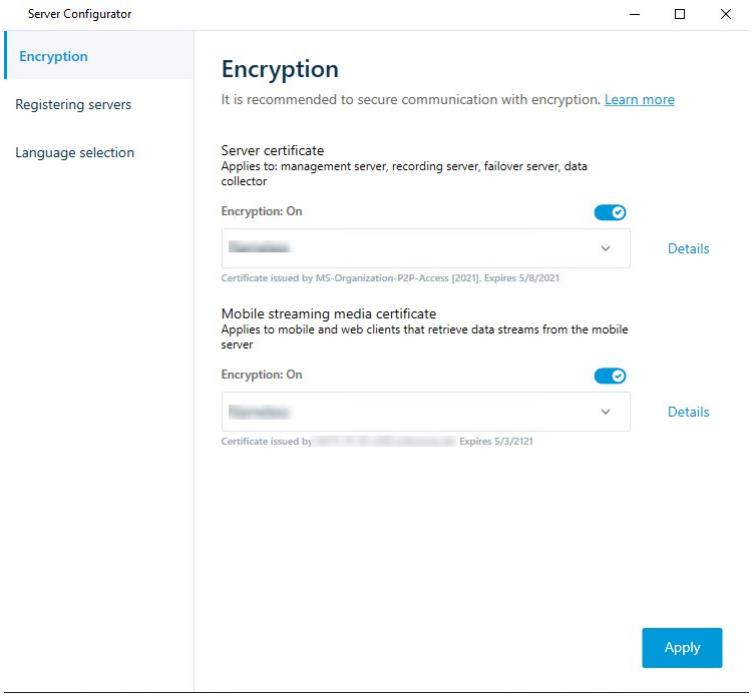
   ou

   - O Mobile Server Manager clicando com o botão direito no ícone Mobile Server Manager na barra de tarefas do computador
2. No **Server Configurator**, em **Certificado de mídia de streaming móvel**, ative a **Criptografia**.
3. Clique em **Selecionar certificado** para abrir uma lista com nomes de entidade únicos que têm uma chave privada e estão instalados no Repositório de certificados do Windows no computador local.
4. Selecione um certificado para criptografar a comunicação do cliente XProtect Mobile e com o servidor móvel XProtect Web Client.

   Selecione **Detalhes** para visualizar as informações do Repositório de certificados do Windows sobre o certificado selecionado.

   O usuário do serviço Mobile Server recebeu acesso à chave privada. É necessário que esse certificado

seja confiável em todos os clientes.



5. Clique em **Aplicar**.

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

Sites do Milestone Federated Architecture e principais/secundários

O Milestone Federated Architecture interconecta vários sistemas individuais padrão em uma hierarquia de sites federados de sites pai/filho.

Para obter acesso a todos os sites com seu XProtect Mobile ou XProtect Web Client, instale o servidor XProtect Mobile apenas no site pai.

Os usuários dos cliente XProtect Mobile ou XProtect Web Client devem se conectar ao servidor de gerenciamento no site pai.

Smart Connect

A Conexão Inteligente permite que você verifique se configurou o 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.

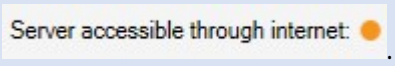
Configurar Smart Connect

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 XProtect Mobile Server 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 8

Guia Conectividade na página 17

Notificações

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.

Por padrão, as notificações estão desativadas.

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 8 e Guia Notificações na página 27.

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**. Leia o aviso sobre seus dados pessoais e selecione **Sim** se deseja prosseguir.
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**. Leia o aviso sobre seus dados pessoais e selecione **Sim** se deseja prosseguir

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.

Remova um ou todos os dispositivos registrados da lista de dispositivos registrados

Quando você desinstalar o aplicativo do XProtect Mobileainda podem ser mantidos no banco de dados do VMS.

O VMS remove os dados de registro do dispositivo quando:

- Você remove um usuário do sistema.
- O Milestone Care Plus não tiver sido renovado por mais de 180 dias.

No entanto, há situações em que os dados de registro do dispositivo não são removidos automaticamente.

Você tem que remover um ou mais dispositivos registrados quando:

- Um usuário tiver perdido seu telefone.
- Você quiser desinstalar o servidor móvel completamente e remover seus dados.
- Um usuário tiver parado de usar o aplicativo do cliente ou as notificações do XProtect Mobile.
- Você tiver adicionado um grupo de Active Directory (AD) a uma função do VMS e as permissões para um usuário tiverem mudado. Quando você adiciona um grupo de AD, o VMS não vê os usuários nessa função. Se você remover um usuário de um grupo de AD ou restringi-lo de usar o servidor móvel, é necessário remover o dispositivo desse usuário manualmente da lista.

Para remover um dispositivo registrado:

1. Em Management Client, selecione o servidor móvel e depois clique na guia **Notificações**.
2. Faça um dos seguintes:
    - Para dispositivos individuais, selecione o dispositivo e selecione **Remover**.
    - Para todos os dispositivos, selecione **Remover todos**.

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. 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.

5. 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.
6. Selecione a caixa de seleção **Ativar tempo de retenção de investigação** para definir um tempo de retenção para investigações. Por padrão, o tempo de retenção é de sete dias.
7. Em **Formatos de exportação**, selecione a caixa de seleção do formato de exportação que deseja usar. Os formatos de exportação disponíveis são:
   - **Formato do AVI**
   - **XProtect formato**
   - **Formato do MKV**

   Por padrão, as caixas de verificação estão limpas.

8. (Opcional) Para incluir a data e o horário em que um vídeo foi baixado, selecione a caixa de seleção **Incluir carimbos de data/hora para exportações AVI**.
9. 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.

10. 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.

    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 **XProtect**, **AVI** ou **MKV** para exportação

Uso de vídeo push para transmitir vídeo por streaming

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 Guia Video Push na página 26 e Requisitos para configuração de vídeo push na página 9.

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 Video 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 Video 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 Video 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 Video 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 para 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 para 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 Vídeo 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 Vídeo Push Driver como um dispositivo de hardware ao servidor de gravação

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 o driver de vídeo push:
   - Nome de usuário: Deixe o campo em branco para usar o nome de usuário padrão.
   - Senha: Digite **Milestone**, a senha gerada pelo sistema. Se você a alterou ao adicionar o canal de Vídeo Push no servidor móvel, insira a senha de sua preferência. Em seguida, 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 Video 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 Video 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 **Video 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 **Video 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 Video Push ao canal para Video 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 9), no 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 aba **Cliente**.
   Para obter mais informações, consulte a guia Cliente (dispositivos).
6. Na lado direito do campo **Microfone relacionado**, clique em . A caixa de diálogo **Dispositivo selecionado** é aberta.
7. Na guia **Servidores de gravação**, expanda a pasta do servidor de gravação e selecione o microfone relacionado ao vídeo push.
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. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/xprotect-comparison/).

Para impor uma etapa adicional de login aos usuários do cliente ou XProtect MobileXProtect 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 47.
2. Especifique o código de verificação que será enviado aos usuários na página 47.
3. Atribua o método de verificação para os usuários e grupos do Active Directory na página 47.

Consulte também Requisitos para configuração da verificação em duas etapas do usuário na página 9 e Guia Verificação em duas etapas na página 28.

Insira as informações sobre seu servidor SMTP

O provedor usa as informações sobre o servidor SMTP:

1. No painel de navegação, selecione **Servidores Mobile** 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 mais informações, consulte Guia Verificação em duas etapas na página 28.

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 fica inválido e o usuário deve solicitar 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 28.

Atribua o método de verificação 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 verificação**, selecione um método de verificação para cada usuário ou grupo.
2. No campo **Detalhes do usuário**, 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 dão suporte para a 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 28.

Ações

Você pode gerenciar a disponibilidade da guia **Ações** no cliente do 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 Guia Geral na página 15.

Gerenciamento de dispositivo móvel (Mobile device management, MDM)

Gerenciamento de dispositivo móvel (MDM) é um software que protege, monitora, gerencia e dá suporte a dispositivos móveis implantados em operadores móveis, provedores de serviço e empresas.

Geralmente, as soluções de gerenciamento de dispositivo móvel incluem um componente de servidor, que envia os comandos de gerenciamento aos dispositivos móveis, e um componente de cliente, que executa no dispositivo gerenciado e recebe e implementa os comandos de gerenciamento.

É possível distribuir o cliente XProtect Mobile e adicionar políticas personalizadas aos dispositivos na sua organização.

> Para usar a funcionalidade do gerenciamento de dispositivo móvel em um dispositivo móvel, é preciso configurar os detalhes do servidor móvel na plataforma de software MDM. Entre os detalhes do servidor móvel estão o nome, o endereço e a porta do servidor e o protocolo do tipo de conexão.

> Se você atualizou os detalhes de um servidor móvel já adicionado, o operador precisa excluir manualmente esse servidor da lista de **Servidores** e reiniciar o aplicativo XProtect Mobile.

Configure detalhes do servidor móvel na plataforma de gerenciamento de dispositivo móvel (administradores)

Para distribuir e gerenciar o cliente XProtect Mobile para dispositivos móveis a partir de uma plataforma de gerenciamento de dispositivo móvel, é necessário adicionar os detalhes do servidor. Para mais informações sobre a configuração, consulte a documentação sobre o seu software de gerenciamento de dispositivo móvel.

> Se você não digitou nenhum dos detalhes obrigatórios do servidor ou se forneceu detalhes incorretos, o servidor móvel não será adicionado ao aplicativo XProtect Mobile.

Para usuários Android

É possível especificar os detalhes do servidor na interface do usuário da sua plataforma de gerenciamento de dispositivo móvel. Você tem a opção de fazer o upload de um arquivo de configuração gerenciado com os detalhes do servidor.

Detalhes de servidor:

- **Nome do servidor** - (Obrigatório) Digite o nome do servidor
- **Endereço do servidor** - (Obrigatório) Digite o endereço do servidor
- **Porta do servidor** - (Obrigatório) Digite o número da porta do servidor
- **Tipo de protocolo de conexão** - Ative ao usar uma conexão HTTPS. Desative ao usar uma conexão HTTP. Por padrão, a conexão HTTPS está ativada

Para fazer o upload do arquivo na sua plataforma de gerenciamento de dispositivo móvel:

1. No fim deste manual, no Anexo A, encontre o modelo de configuração gerenciada para dispositivos Android. Copie o conteúdo.
2. Abra um editor de texto de sua escolha e cole o conteúdo.
3. Especifique os detalhes do servidor nos campos **android:description**.
4. Salve o arquivo como .XML.
5. Abra sua plataforma de gerenciamento de dispositivo móvel e faça o upload do arquivo de configuração gerenciada.

Para usuários iOS

Para gerenciar dispositivos iOS a partir de uma plataforma de gerenciamento de dispositivo móvel, é necessário especificar os detalhes da conexão no arquivo de configuração gerenciada.

1. No fim deste manual, no Anexo B, encontre o modelo de configuração gerenciada para dispositivos iOS. Copie o conteúdo.
2. Abra um editor de texto de sua escolha e cole o conteúdo.
3. Especifique os detalhes do servidor:
   - **versionConfig** - (Obrigatório) Digite a versão padrão da configuração do aplicativo **1.0.0**
   - **serverNameConfig** - (Obrigatório) Digite o nome do servidor
   - **serverAddressConfig** - (Obrigatório) Digite o endereço do servidor
   - **serverPortConfig** - (Obrigatório) Digite o número da porta do servidor
   - **serverConnectionProtocolTypeConfig** - O tipo de conexão padrão é **HTTPS**, para usar uma conexão não segura, digite **HTTP**
4. Salve o arquivo como .XML.
5. Abra sua plataforma de gerenciamento de dispositivo móvel e faça o upload do arquivo de configuração gerenciada.

Nomeando uma saída para uso no cliente XProtect Mobile e no XProtect Web Client

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 - 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 - 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 obter mais informações, consulte Saídas.

IDP externo e XProtect Mobile

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

Faça login no XProtect Web Client ou no cliente XProtect Mobile por meio de um IDP externo com XProtect 2022 R3 e posterior.

Para fazer login com um IDP externo em XProtect Web Client ou no cliente XProtect Mobile, é preciso usar uma conexão HTTPS.

Antes de configurar um login com IDP externo para XProtect Web Client e o cliente XProtect Mobile, verifique se você:

- Configurou um IDP externo
- Alegações registradas
- Mapeou alegações para funções

Para obter mais informações, consulte o manual do administrador do VMS XProtect.

Para fazer login no XProtect Web Client por meio de um IDP externo, é necessário configuração adicional. Consulte Configure o login do IDP externo para XProtect Web Client na página 51.

Configure o login do IDP externo para XProtect Web Client

A opção de fazer login através de um IDP externo para XProtect Web Client está disponível apenas para conexões HTTPS.

1. Em Management Client, selecione **Ferramentas** > **Opções** e abra a guia **IDP externo**.
2. Na seção **Redirecionar URIs para clientes da web**, selecione **Adicionar**.
3. Insira os endereços para XProtect Web Client no formato **https://[address]:[port number]/index.html**:
    - Para os endereços, insira o nome do host ou o endereço IP do computador no qual o servidor móvel é executado
    - Para o número da porta, insira a porta que o XProtect Web Client usa para comunicar-se com o servidor móvel. Para conexões HTTPS, o número da porta padrão é 8082

Adicionar alarmes de Alerta de emergência

Após a detecção de uma possível ameaça, o Alerta de emergência permite que os usuários do cliente do XProtect Mobile recebam notificações do alarme do mais alto nível de gravidade, visualizem os detalhes do alarme e ajam imediatamente. O Alerta de emergência é um tipo de alarme que você define no XProtect Management Client.

O funcionamento dessa funcionalidade requer notificações push. As notificações push só estarão disponíveis se você tiver adquirido uma licença Milestone Care Plus.

O recurso está disponível apenas em certos produtos do VMS XProtect. Veja a lista completa de recursos, que está disponível na página de visão geral do produto no Milestone site (https://www.milestonesys.com/products/software/xprotect-comparison/).

Para adicionar esse tipo de alarme, você precisa:

1. Adicionar uma nova categoria de alarme com nível 99 em **Alarmes** > **Configurações de dados de alarme**. Você pode criar quantas categorias de nível 99 precisar.
2. Adicione uma definição de alarme com essa categoria.

Manutenção

Mobile Server Manager

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 as funcionalidades do servidor móvel.

É possível:

- Acesso XProtect Web Client na página 53
- Iniciar, parar e reiniciar serviço Mobile Server na página 54
- Alterar a senha de proteção de dados na página 54
- Exibir/editar números de porta na página 55
- Ativar criptografia no servidor móvel na página 34 usando o **Server Configurator**
- Abrir o arquivo de registro de hoje (consulte Acessando registros e investigações na página 55)
- Abra a pasta Registro (consulte Acessando registros e investigações na página 55)
- Abra a pasta investigações (consulte Acessando registros e investigações na página 55)
- Alterar a pasta de investigações na página 56
- Veja o status do XProtect Mobile Server (consulte Exibir status na página 56)

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 (Microsoft Edge, 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

Alterar a senha de proteção de dados

A senha de proteção de dados do servidor móvel é usada para criptografar investigações. Como administrador do sistema você terá que inserir essa senha para acessar os dados do servidor móvel em caso de uma recuperação do sistema ou ao expandir seu sistema com servidores móveis adicionais.

Para alterar a senha de proteção de dados do servidor móvel:

1. Clique com o botão direito no ícone Mobile Server Manager e selecione **Alterar configurações da senha de proteção de dados.**. Uma nova caixa de diálogo é exibida.
2. No campo **Nova senha**, insira a sua nova senha.
3. Insira novamente a nova senha no campo **Confirmar nova senha**.

4. (Opcional) Se não desejar que suas investigações sejam protegidas por senha, selecione **Eu opto por não usar uma senha de proteção de dados do servidor móvel e compreendo que as investigações não serão criptografadas**.
5. Clique em **OK**.

Você deve salvar esta senha e mantê-la segura. Não fazer isso pode comprometer a sua capacidade de recuperar dados do servidor móvel.

Exibir/editar números de porta

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**.

Acessando registros e investigações

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 Investigação**

Registros de auditoria são criados para cada ação que ainda não está registrada pelo Management Server ou Recording Server.

As seguintes ações são sempre registradas (mesmo quando o registro de auditoria avançado não está ativado):

- Toda a administração (essas mensagens do registro de auditoria contêm o valor antigo e o valor novo)
- Todas as ações relacionadas à criação, edição ou exclusão de investigações, assim como a preparação e download de material exportado, e alteração de partes relevantes da configuração. O registro de auditoria contém detalhes sobre o que foi feito.

O streaming de vídeo push é registrado somente quando o registro de auditoria está ativado.

Se você desinstalar o servidor XProtect Mobile do seu sistema, seus arquivos de registro não serão excluídos. Administradores com permissões de usuário adequadas 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 **ProgramData**. Se você alterar o local padrão dos arquivos de registros, os registros existentes não são copiados para o novo local nem são excluídos.

Alterar a pasta de investigações

O local padrão das investigações está na pasta **ProgramData**. Se você alterar a localização 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 a 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

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 em funcionamento 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 em ação no servidor do 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.

Use um balanceador de carga para o servidor móvel

Como uma etapa de segurança adicional, o XProtect Mobile usa IDs na comunicação entre o servidor e o aplicativo para dispositivo móvel. Quando um usuário se conecta a um servidor móvel pelo aplicativo XProtect Mobile pela primeira vez, o ID de servidor do servidor móvel é copiado para o dispositivo do usuário. A cada tentativa de conexão a um servidor móvel, os IDs de servidor são comparados com aqueles obtidos inicialmente.

Por padrão, cada servidor tem um ID de servidor exclusivo. Para adicionar um servidor móvel a um grupo de balanceamento de carga, você deve se certificar de que o ID do servidor móvel corresponda ao ID usado pelos outros servidores móveis no grupo.

Em um host no grupo de balanceamento de carga

Para copiar os IDs de servidor de um host:

1. Acesse `C:\ProgramFiles\Milestone\Milestone Mobile Server` e copie o arquivo **VideoOS.MobileServer.Service.exe.config**.
2. Cole o arquivo na sua área de trabalho e use um editor de texto de sua preferência para abri-lo.

3. Pesquise a tag `ServerSettings` no arquivo. Ela deve ter essa aparência:

```
<ServerSetings>
 <Identification>
  <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
  <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
  <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
 </Identification>
---
</ServerSettings>
```

4. Copie os valores **ServiceID** e **ReportedServiceID**.

Nos outros hosts que são parte do grupo

Em um host que é parte do grupo de balanceamento de carga:

1. Vá para `C:\ProgramFiles\Milestone\Milestone Mobile Server` e abra o arquivo **VideoOS.MobileServer.Service.exe.config** com o editor de texto da sua preferência.
2. Pesquise a tag `ServerSettings` no arquivo e substitua os valores **ServiceID** e **ReportedServiceID** pelos valores do arquivo de configuração original.
3. Para aplicar as alterações, reinicie o serviço Mobile Server.
4. Solicite aos usuários cliente XProtect Mobile para adicionarem o servidor móvel novamente.

Repita os passos para todos os hosts que fazem parte do grupo de balanceamento de carga.

Migre um servidor móvel para outro host

Como uma etapa de segurança adicional, o XProtect Mobile usa IDs na comunicação entre o servidor e o aplicativo para dispositivo móvel. Quando um usuário se conecta a um servidor móvel pelo aplicativo XProtect Mobile pela primeira vez, o ID de servidor do servidor móvel é copiado para o dispositivo do usuário. Sempre que o aplicativo tenta se conectar a um servidor móvel, ele compara os IDs do servidor com os que obteve inicialmente. Se os IDs do servidor não corresponderem, a conexão falhará.

Ao migrar o servidor móvel para outro host mantendo o endereço original dele, você deve manter o ID de servidor do servidor antigo.

No host antigo

Antes de migrar o seu servidor móvel, você deve:

1. Ir para `C:\ProgramFiles\Milestone\Milestone Mobile Server`, copiar o arquivo **VideoOS.MobileServer.Service.exe.config** e abri-lo usando o editor de texto da sua preferência.
2. Pesquise a tag `ServerSettings` no arquivo. Ela deve ter essa aparência:

```
<ServerSetings>
 <Identification>
  <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
  <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
  <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
 </Identification>
---
</ServerSettings>
```

3. Copie os valores **ServiceID** e **ReportedServiceID**.

Agora, você está pronto par migrar o seu servidor móvel.

No host novo

Depois de instalar e configurar o servidor móvel no host novo:

1. Vá para `C:\ProgramFiles\Milestone\Milestone Mobile Server` e abra o arquivo **VideoOS.MobileServer.Service.exe.config** com o editor de texto da sua preferência.
2. Pesquise a tag `ServerSettings` no arquivo e substitua os valores **ServiceID** e **ReportedServiceID** pelos valores do arquivo de configuração original.
3. Para aplicar as alterações, reinicie o serviço Mobile Server.
4. Solicite aos usuários cliente XProtect Mobile para adicionarem o servidor móvel novamente.

Solução de problemas

Solução de problemas XProtect Mobile

Conexões

Por que eu não consigo conectar diretamente do meu cliente do XProtect Mobile às minhas gravações/servidor do XProtect Mobile?

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. Eles são instalados 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 14).

O campo de endereço do servidor deve conter um nome de host válido quando aplicado no dispositivo iOS. Os nomes de host válidos podem conter as letras ASCII 'a' a 'z' (sem distinção entre maiúsculas e minúsculas), os dígitos '0' a '9', ponto e o hífen ('-').

Acabei 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.

Como evitar o aviso de segurança quando eu executar o XProtect Web Client usando 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. Isso significa que as instruções fornecidas para a geração dos arquivos de solicitação de assinatura de certificado (CSR) pela autoridade de certificação usando o IIS não se aplicam ao servidor XProtect Mobile. Você deve criar um arquivo 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.

Eu não alterei o endereço do servidor móvel, mas os usuários do cliente XProtect Mobile não conseguem mais se conectar a ele. Por que?

Os clientes XProtect Mobile se conectam ao servidor móvel usando um ID de serviço exclusivo. Mesmo que o nome do host e o endereço IP do computador do servidor móvel permaneçam os mesmos, o ID do serviço pode não corresponder ao ID armazenado nos clientes, como por exemplo, quando:

- Você redefiniu seu computador e reinstalou o servidor móvel.
- Você moveu o servidor móvel para outro computador, mas manteve a configuração original dele.

Para reestabelecer a conexão, você pode:

- Atualizar o ID de serviço no novo servidor móvel para que o ID de serviço da configuração anterior fique igual. Consulte https://developer.milestonesys.com/s/article/unable-to-establish-connection-to-XProtect-Mobile-Server-using-Android-iOS-client.
- Solicitar aos usuários do cliente XProtect Mobile que se reconectem ao servidor móvel.

Qualidade da imagem

Por que a qualidade da imagem é ocasionalmente ruim quando eu visualizo vídeo no cliente do 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 do 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.

Por que a qualidade da imagem é ruim quando eu estabeleço conexão com o meu sistema de gerenciamento de vídeo XProtect em casa usando 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 precisaram 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 por hardware

O meu processador é compatível com decodificação acelerada por hardware?

Somente processadores Intel mais recentes suportam a decodificação acelerada por hardware. Consulte o site da Intel (https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&0_QuickSyncVideo=True) 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 na página 56).

O meu sistema operacional é compatível com decodificação acelerada por hardware?

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

Certifique-se de instalar os drivers gráficos mais recentes em seu sistema. Esses drivers não estão disponíveis na Atualização do Windows.

Como 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 VideoOS.MobileServer.Service.exe.config. 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.

Notificações

Não fiz nenhuma alteração na configuração de notificação, mas os dispositivos cadastrados pararam de receber notificações. Por que?

Se você tiver atualizado sua licença ou renovado sua assinatura do Milestone Care, será necessário reiniciar o serviço Mobile Server.

Anexos

Anexo A

Modelo de configuração gerenciada para Android

```
<?xml version="1.0" encoding="utf-8"?>

<restrictions xmlns:android="http://schemas.android.com/apk/res/android">

    <restriction
        android:defaultValue="1.0.0"
        android:description="The current version of the app configuration"
        android:key="version_config"
        android:restrictionType="hidden"
        android:title="Version" />

    <restriction
```

```
        android:description="(Mandatory) Enter the server name."
        android:key="server_name_config"
        android:restrictionType="string"
        android:title="Server name" />

    <restriction
        android:description="(Mandatory) Enter the server address."
        android:key="server_address_config"
        android:restrictionType="string"
        android:title="Server address" />

    <restriction
        android:description="(Mandatory) Enter the server port."
```

```
        android:key="server_port_config"

        android:restrictionType="integer"

        android:title="Server port" />


    <restriction

        android:description="Enable when you use an HTTPS connection. Disable
when you use an HTTP connection."

        android:key="server_secure_connection_config"

        android:restrictionType="bool"

        android:title="Connection protocol type"

        android:defaultValue="true"/>


</restrictions>
```

Anexo B

Modelo de configuração gerenciada para iOS

```
<managedAppConfiguration>
    <version>1</version>
    <bundleId>com.milestonesys.XProtect</bundleId>
    <dict>
        <string keyName="versionConfig">
            <defaultValue>
                <value>1.0.0</value>
            </defaultValue>
        </string>
        <string keyName="serverNameConfig">
        </string>
        <string keyName="serverAddressConfig">
        </string>
```

```
        <string keyName="serverPortConfig">
        </string>
        <string keyName="serverConnectionProtocolTypeConfig">
            <defaultValue>
                <value>HTTPS</value>
            </defaultValue>
        </string>
    </dict>
    <presentation defaultLocale="en-US">
        <field keyName="versionConfig" type="input">
            <label>
                <language value="en-US">Version</language>
            </label>
            <description>
```

```
                <language value="en-US">The current version of the app
configuration</language>

            </description>

        </field>

    <fieldGroup>

        <name>

            <language value="en-US">Mobile server</language>

        </name>

        <field keyName="serverNameConfig" type="input">

            <label>

                <language value="en-US">Server name</language>

            </label>

            <description>

                <language value="en-US">(Mandatory) Enter the server
name.</language>
```

```
            </description>
        </field>
        <field keyName="serverAddressConfig" type="input">
            <label>
                <language value="en-US">Server address</language>
            </label>
            <description>
                <language value="en-US">(Mandatory) Enter the server
address.</language>
            </description>
        </field>
        <field keyName="serverPortConfig" type="input">
            <label>
                <language value="en-US">Server port</language>
```

```
            </label>

            <description>

                <language value="en-US">(Mandatory) Enter the server
port.</language>

            </description>

        </field>

        <field keyName="serverConnectionProtocolTypeConfig" type="input">

            <label>

                <language value="en-US">Connection protocol type</language>

            </label>

            <description>

                <language value="en-US">To specify the connection protocol
type, enter HTTPS or HTTP.</language>

            </description>

        </field>
```

```
    </fieldGroup>

    </presentation>

</managedAppConfiguration>
```

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/.