Bosch IP video products

pt-BR Guia de segurança cibernética

Sumário

1 Finalidade do documento e público-alvo

A tecnologia está evoluindo com grande – e às vezes impressionante – velocidade. Por causa dos rápidos avanços na inteligência artificial (IA) e Internet das Coisas (IoT), bem como sua utilização massiva (AIoT), alteram o perfil de risco de produtos e serviços. Quanto mais conectividade, maiores são as chances de ataques maliciosos serem realizados. Tendo esse cenário em vista, o objetivo da Bosch é fornecer aos clientes produtos seguros e confiáveis.

Este guia de segurança deve auxiliar integradores na proteção de produtos de vídeo IP da Bosch para que haja uma melhor adesão a políticas e procedimentos de segurança nas redes existentes dos clientes.

Este guia abordará:
- Informações críticas sobre os recursos e os fundamentos dos dispositivos de vídeo IP da Bosch
- Recursos específicos que podem ser modificados ou desativados
- Recursos específicos que podem ser ativados e utilizados
- Práticas recomendadas, uma vez que estejam relacionadas a sistemas de vídeo e segurança

Este guia terá como foco principal a utilização do Configuration Manager para executar as configurações discutidas. Na maioria dos casos, todas as configurações podem ser executadas utilizando o BVMS Configuration Client, o Configuration Manager e a interface da Web integrada de um dispositivo de vídeo.

2 Considerações e conceito de segurança

Os produtos de vídeo IP estão se tornando comuns no ambiente de rede atualmente e, assim como ocorre com qualquer dispositivo IP inserido em uma rede, administradores de TI e gerentes de segurança têm o direito de saber a verdadeira extensão do conjunto de recursos e das capacidades de um dispositivo.

Ao lidar com dispositivos de vídeo IP da Bosch, a primeira linha de proteção do usuário são os próprios dispositivos. Os codificadores e as câmeras da Bosch são fabricados em um ambiente seguro e controlado, continuamente fiscalizado. Os dispositivos podem ser gravados somente por meio de um carregamento válido de firmware, o qual é específico para uma série de hardware e chipset.

A maioria dos dispositivos de vídeo IP da Bosch é fornecida com um chip de segurança interno que fornece funcionalidade semelhante aos SmartCards criptográficos e com o chamado Trusted Platform Module ou TPM para abreviar. Esse chip funciona como uma segurança para dados críticos, protegendo certificados, chaves, licenças contra o acesso não autorizado mesmo quando a câmera está fisicamente aberta para obter acesso.

Os dispositivos de vídeo IP da Bosch foram submetidos a mais de 30.000 (trinta mil) testes de vulnerabilidade e penetração executados por fornecedores de segurança independentes. Até o momento, não houve ataque cibernético bem-sucedido em um dispositivo adequadamente protegido.

3 Instalação segura

3.1 Servidores e dispositivos de armazenamento

Todos os componentes do servidor (por exemplo, servidor BVMS Management Server e Video Recording Manager) e dispositivos de armazenamento devem ser instalados em uma área segura. O acesso à área segura deve ser garantido com um sistema de controle de acesso e precisa ser monitorado. O grupo de usuários, que tem acesso à sala do servidor central, deve ser limitado a um grupo pequeno de pessoas.
Embora os servidores e dispositivos de armazenamento estejam instalados em uma área segura, eles devem ser protegidos contra acesso não autorizado.

Consulte

- *Proteção de servidores, página 33*
- *Proteção de armazenamento, página 32*

3.2 Câmeras e dispositivos de borda

Para a instalação de câmeras e dispositivos de borda, é preciso escolher um local de instalação e uma orientação de montagem seguros. Idealmente, deve ser um local onde o dispositivo não possa sofrer interferências, sejam elas intencionais ou acidentais.

4 Configuração segura

4.1 Atribuição de endereços IP

Todos os dispositivos de vídeo IP da Bosch são atualmente fornecidos em um estado padrão de fábrica prontos para aceitar um endereço IP DHCP.
Se nenhum servidor DHCP estiver disponível na rede ativa em que um dispositivo é implantado, o dispositivo aplicará automaticamente, se estiver executando o firmware 6.32 ou superior, um link/endereço local fora da faixa de 169.254.1.0 a 169.254.254.255 ou 169.254.0.0/16.
Com firmware anterior, o dispositivo atribuirá o endereço IP padrão 192.168.0.1 a ele mesmo.
Existem várias ferramentas que podem ser usadas para executar a atribuição de Endereço IP aos dispositivos de vídeo IP da Bosch, incluindo:

- Bosch Configuration Manager
- BVMS Configuration Client
- BVMS Configuration Wizard

Todas as ferramentas de software fornecem a opção de atribuir um endereço IPv4 estático único, bem como uma faixa de endereços IPv4 para vários dispositivos simultaneamente. Isso inclui máscara de sub-rede e endereçamento padrão de gateway.
Todos os endereços IPv4 e valores de máscara de sub-rede precisam ser inseridos na assim-chamada "notação de ponto decimal".

Aviso!
Uma das primeiras etapas na limitação das possibilidades de ataques cibernéticos internos em uma rede, executados por dispositivos de rede não autorizados conectados localmente, é restringir os endereços IP disponíveis não utilizados. Isso é feito usando o IPAM (**IP A**ddress **M**anagement) ou Gerenciamento de Endereços IP, juntamente com a sub-rede da faixa de endereços IP que será usada.

Divisão em sub-redes é o ato de emprestar bits da parte principal (host) de um endereço IP para dividir uma rede grande em várias redes menores. Quanto mais bits você emprestar, mais redes poderá criar, mas cada rede será compatível com menos endereços do host.

Sufixo	Hosts	CIDR	Emprestado	Binário
.255	1	/32	0	.11111111
.254	2	/31	1	.1111111**0**
.252	4	/30	2	.111111**00**
.248	8	/29	3	.11111**000**
.240	16	/28	4	.1111**0000**
.224	32	/27	5	.111**00000**
.192	64	/26	6	.11**000000**
.128	128	/25	7	.1**0000000**

Desde 1993, a Internet Engineering Task Force (IETF) introduziu um novo conceito de alocação de blocos de endereço IPv4 de uma maneira mais flexível do que era usada na antiga arquitetura de endereçamento de "rede classful". O novo método é denominado “Classless Inter-Domain Routing” (CIDR) e também é usado com endereços IPv6.

As redes classful IPv4 são designadas como Classes A, B e C, com bits de número de rede 8, 16 e 24, respectivamente, e a Classe D que é usada para endereçamento multicast.

Exemplo:
Para que seja um exemplo de fácil compreensão, usaremos um cenário de endereço de Classe C. A máscara padrão de sub-rede de um endereço de Classe C é 255.255.255.0. Tecnicamente, nenhuma divisão de sub-rede foi feita para essa máscara, portanto o último octeto inteiro está disponível para o endereçamento de host válido. À medida que emprestamos bits do endereço de host, temos as seguintes opções possíveis de máscara no último octeto:
.128, .192, .224, .240, .248 e .252.

Se utilizar a máscara de sub-rede 255.255.255.240 (4 bits), estaremos criando 16 redes menores que oferecem suporte a 14 endereços de hosts por sub-rede.
- ID da sub-rede 0:
  faixa de endereços de host 192.168.1.1 a 192.168.1.14. Endereço de broadcast 192.168.1.15
- ID da sub-rede 16:
  faixa de endereços de host 192.168.1.17 a 192.168.1.30. Endereço de broadcast 192.168.1.31
- IDs de sub-rede: 32, 64, 96, etc.

Para redes maiores, poderá ser necessária a próxima rede Classe B maior ou um bloco CIDR apropriado poderá ser definido.

Exemplo:
Antes de implantar sua rede de segurança por vídeo, execute um cálculo simples de quantos dispositivos IP serão necessários na rede, a fim de incluir espaço para crescimento futuro:
- 20 estações de trabalho de vídeo
- 1 servidor central
- 1 servidor VRM
- 15 matrizes de armazenamento iSCSI
- 305 câmeras IP

Total = 342 endereços IP necessários

Levando em consideração o número calculado de 342 endereços IP, precisamos, no mínimo, de um esquema de endereço IP de Classe B para acomodar esses vários endereços IP. O uso da máscara de sub-rede Classe B padrão de 255.255.0.0 permite que 65.534 endereços IP disponíveis sejam usados na rede.

Como alternativa, a rede pode ser planejada usando um bloco CIDR com 23 bits usados como prefixo, fornecendo um espaço de 512 endereços, respectivamente, 510 hosts.

Ao dividir uma rede grande em partes menores, simplesmente dividindo a rede ou especificando um bloco CIDR, você pode reduzir este risco.

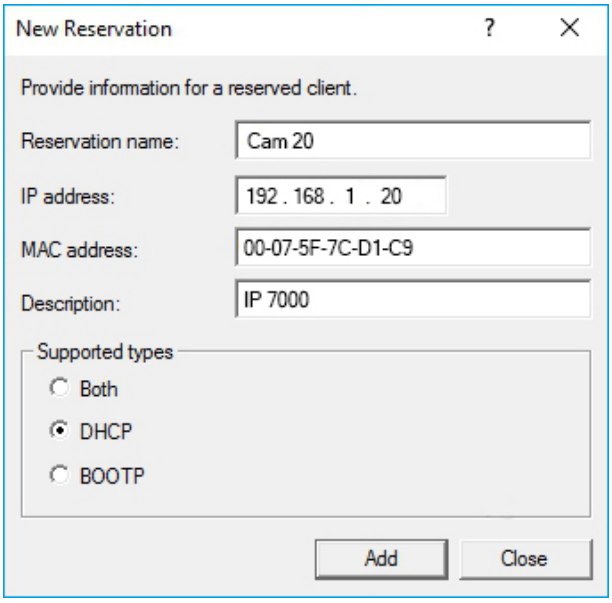
Exemplo:

	Padrão	**Dividido em redes**
Faixa de endereços IP	172.16.0.0 - 172.16.255.255	172.16.8.0 - 172.16.9.255
Máscara de sub-rede	255.255.0.0	255.255.254.0
Notação CIDR	172.16.0.0/16	172.16.8.0/23
Número de sub-redes	1	128
Número de hosts	65.534	510
Endereços excedentes	65.192	168

4.1.1 Gerenciamento do DHCP

O IPAM pode utilizar o DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuração de Host Dinâmico) como uma poderosa ferramenta no controle e no uso de endereços IP em seu ambiente. O DHCP pode ser configurado para utilizar um escopo específico de endereços IP. Ele também pode ser configurado para excluir uma faixa de endereços.

Se estiver utilizando o DHCP, será melhor, ao implantar dispositivos de vídeo, configurar reservas de endereços que não expiram com base no endereço MAC de cada dispositivo.



Aviso!
Mesmo antes de usar o IP Address Management para rastrear o uso de endereços IP, uma prática recomendada de gerenciamento de rede é limitar o acesso à rede por meio da segurança de porta em switches de borda, por exemplo, somente um endereço MAC específico pode acessar por meio de uma porta específica.

4.2 Contas de usuário e senhas

Todas as câmeras de vídeo e codificadores IP da Bosch são fornecidos com três contas de usuário integradas:

– **live**
  Essa conta de usuário padrão permite acesso apenas a streaming de vídeo ao vivo.

– **user**
  Essa conta de usuário mais avançada permite acesso a vídeo ao vivo e gravado, bem como controles de câmera, como o controle PTZ.
  Essa conta não permite acesso a definições de configuração.
– **service**
  Essa conta de administrador fornece acesso a todos os menus e definições de configuração do dispositivo.

Uma senha deve ser atribuída para cada uma das contas de usuário.
A atribuição de senha é uma etapa crítica na proteção de qualquer dispositivo de rede. É veementemente recomendável que sejam atribuídas senhas a todos os dispositivos de vídeo em rede instalados.

Aviso!
Com a versão de firmware 6.30, o gerenciamento de usuário foi aprimorado para mais flexibilidade, a fim de permitir outros usuários e nomes de usuário com as próprias senhas. Os níveis de conta antigos agora representam os níveis de grupo de usuários.
Com a versão de firmware 6.32, foi introduzida uma política de senha mais restrita (para obter mais detalhes, consulte *Atribuição de senhas usando a página da Web do dispositivo, página 12*).

4.2.1 Atribuição de senhas

As senhas podem ser atribuídas de várias maneiras, dependendo do tamanho do sistema de segurança por vídeo e do software em uso. Em instalações menores que consistem em apenas algumas poucas câmeras, as senhas podem ser definidas utilizando a página da Web do dispositivo, uma vez que ela oferece suporte conveniente à configuração de vários dispositivos simultaneamente e a um assistente de configuração, ou um Bosch Configuration Manager.

Aviso!
Conforme informado anteriormente, a proteção por senha é crítica ao proteger dados de possíveis ataques cibernéticos. Isso se aplica a todos os dispositivos de rede em sua infraestrutura completa de segurança. A maioria das organizações já tem políticas de senha forte definidas, mas se você estiver trabalhando com uma nova instalação sem políticas definidas, a seguir estão descritas algumas práticas recomendadas ao implementar a proteção por senha:
- As senhas devem ter entre 8 e 12 caracteres.
- As senhas devem conter letras maiúsculas e minúsculas.
- As senhas devem conter pelo menos um caractere especial.
- As senhas devem conter pelo menos um dígito.

Exemplo:
O uso da frase secreta "to be or not to be" e de nossas regras básicas para geração de senha adequada.
– 2be0rnOt!t0Be

Aviso!
Existem algumas restrições para o uso de caracteres especiais, como: ‘@’, '&', '<', '>', ‘:’, em senhas devido a seus significados dedicados em XML e outras linguagens de marcação. Embora a interface da Web aceitará esses caracteres, outros softwares de configuração e gerenciamento poderão recusar a aceitação.

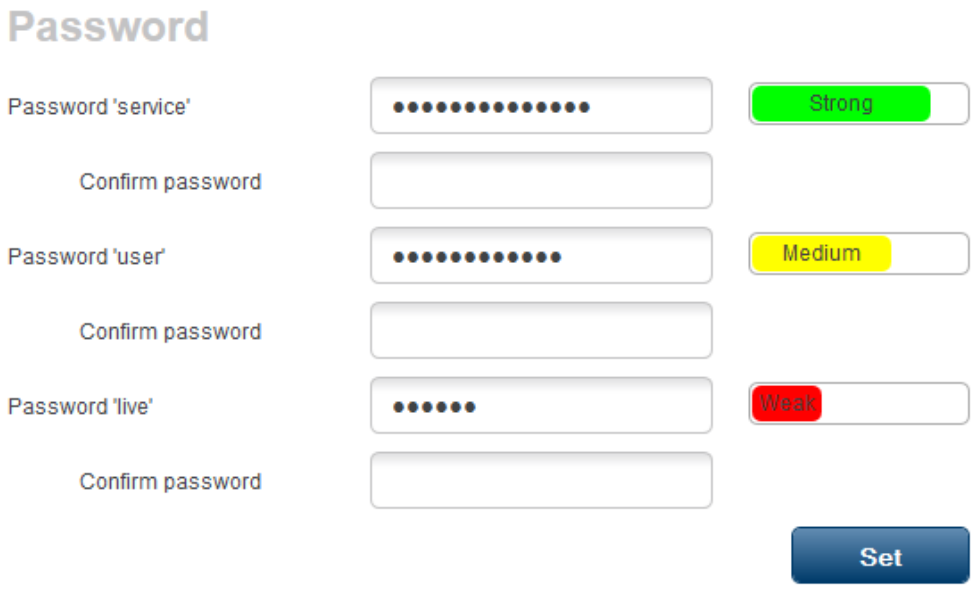
4.2.2 Atribuição de senhas usando a página da Web do dispositivo

1. Na página da Web do dispositivo, navegue para a página **Configuração** (Configuração).
2. Selecione o menu **Geral** (Geral) e o submenu **Gestão de utilizadores** (Gerenciamento de usuários) (Nota: Antes da versão de firmware 6.30, o submenu **Gestão de utilizadores** era chamado **Palavra-passe** [Senha]).

Ao entrar pela primeira vez na página da Web de uma câmera, é solicitado que o usuário atribua senhas para garantir proteção mínima.
Isso será persistentemente repetido em todos os novos carregamentos de páginas da Web da câmera enquanto nenhuma senha for definida. Clicar em **OK** leva ao menu **Gestão de utilizadores** (Gerenciamento de usuários) automaticamente.

O firmware 6.30 tinha a opção de ativar uma caixa de seleção **Do not show...** (Não mostrar...). Essa opção foi removida no firmware 6.32 para evitar escapes de segurança.

1. Selecione o menu **Gestão de utilizadores** (Gerenciamento de usuários) e insira e confirme a senha desejada para cada uma das três contas.
   Observe:
   - As senhas precisam ser atribuídas no nível de acesso mais alto (**Palavra-passe "service"** [Serviço de senha]) primeiro.
   - Da versão de firmware 6.20 em diante, um novo indicador denominado "medidor de intensidade da senha" deve dar dicas sobre a possível intensidade das senhas. Essa é uma ferramenta de suporte e não garante que uma senha corresponda realmente à demanda de segurança de uma instalação.
2. Clique em **Definir** (Definir) para enviar e salvar as alterações.



O **Gestão de utilizadores** (Gerenciamento de usuários), introduzido com a versão de firmware 6.30, oferece mais flexibilidade para criar usuários livremente denominados com as próprias senhas. Os níveis de conta antigos agora representam os níveis de grupo de usuários.

Os usuários antigos ainda existem, utilizando ainda as senhas que foram atribuídas durante a execução do firmware anterior, os quais não podem ser excluídos nem o respectivo nível do grupo de usuários alterado.

As senhas podem ser atribuídas ou alteradas clicando em ou .
Uma mensagem de aviso é exibida, uma vez que nem todos os usuários têm proteção por senha.

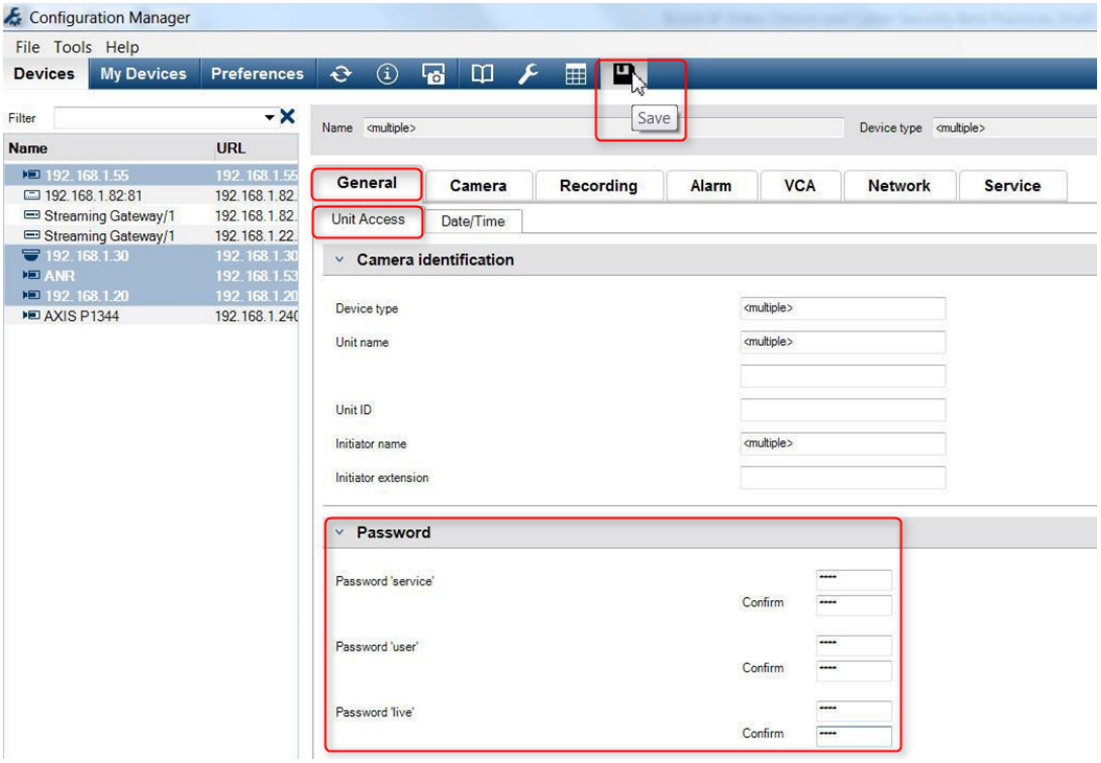
1. Para adicionar um novo usuário, clique em **Adicionar** (Adicionar).
   Uma janela pop-up é exibida.
2. Insira as novas credenciais e atribua o grupo de usuários.
3. Clique em **Definir** (Definir) para salvar as alterações.

Aviso!
Com a versão de firmware 6.32, também foi introduzida uma política de senha mais restrita. As senhas agora devem ter, no mínimo, 8 caracteres.

4.2.3 Atribuição de senhas usando o Configuration Manager

É possível aplicar senhas com facilidade a um ou vários dispositivos simultaneamente utilizando o Bosch Configuration Manager.

1. No Configuration Manager, selecione um ou mais dispositivos.
2. Selecione a guia **Geral** (Geral) e, em seguida, selecione **Acesso à Unidade** (Acesso à unidade).
3. No menu **Palavra-passe** (Senha), insira e confirme a senha desejada para cada uma das três contas (**Palavra-passe 'service '**, **Palavra-passe 'user'** e **Palavra-passe 'live'**).
4. Clique em para enviar e salvar as alterações.



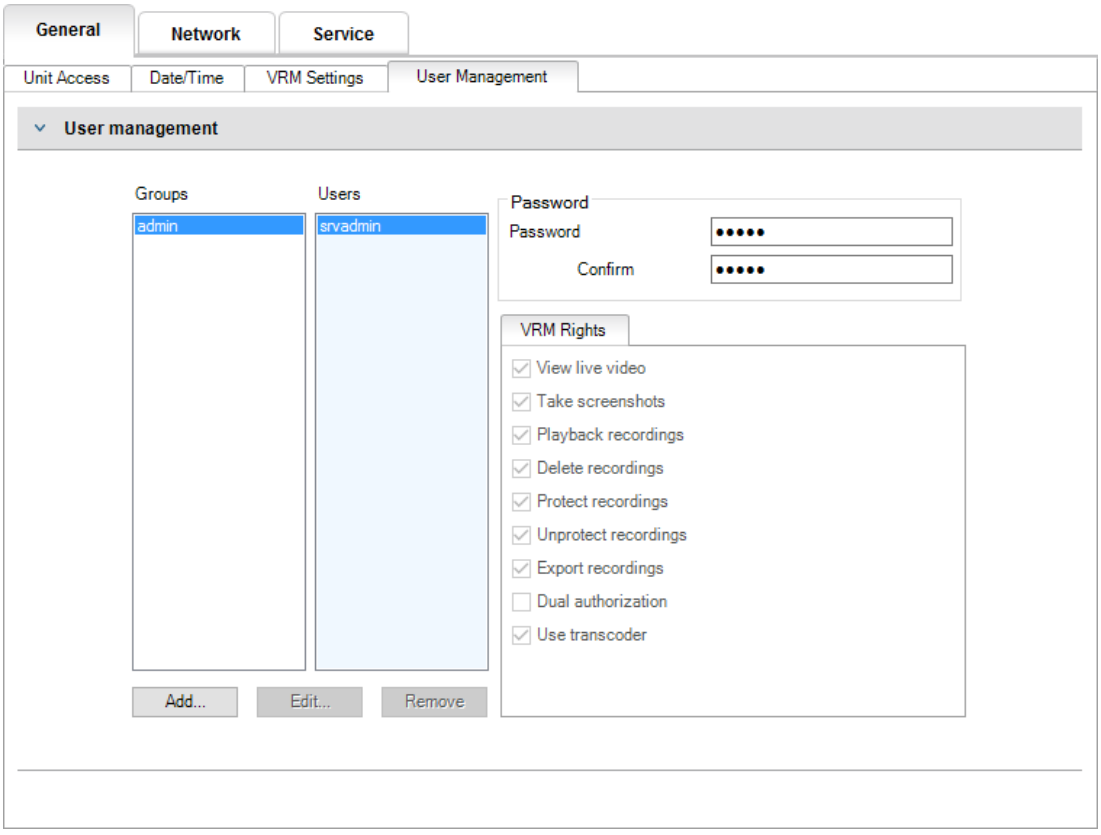
Em instalações maiores que são gerenciadas pelo BVMS ou pelo Video Recording Manager instalado em um aparelho de gravação, senhas globais podem ser aplicadas a todos os dispositivos de vídeo IP adicionados ao sistema. Isso permite o fácil gerenciamento e garante um nível padrão de segurança em todo o sistema de vídeo em rede.

4.2.4 Atribuição de senhas para instalação independente do VRM

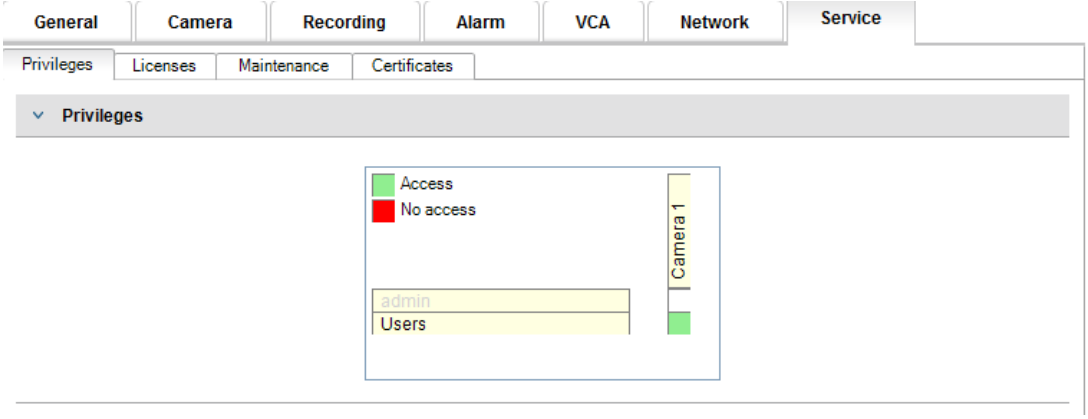
O Video Recording Manager fornece gerenciamento de usuário para aprimorar a flexibilidade e a segurança.

Por padrão, não há senhas atribuídas a nenhuma das contas de usuário. A atribuição de senha é uma etapa crítica na proteção de qualquer dispositivo de rede. É veementemente recomendável atribuir senhas a todos os dispositivos de vídeo em rede instalados.

O mesmo é válido para os usuários do Video Recording Manager.



Além disso, membros de um grupo de usuários podem ser atribuídos para ter acesso a certas câmeras e privilégios. Dessa forma, um gerenciamento correto detalhado baseado no usuário pode ser obtido.



4.2.5 Atribuição de senhas usando o BVMS (no DIVAR IP ou independente)

Proteção do dispositivo por senha

Câmeras e codificadores, gerenciados pelo BVMS, podem ser protegidos contra acesso não autorizado com uma proteção por senha.

As senhas para as contas de usuário integradas de codificadores/câmeras podem ser configuradas com o Configuration Client do BVMS.

Para definir uma senha para as contas de usuário integradas no BVMS Configuration Client:

1. Na Device tree (Árvore de dispositivos), selecione o codificador desejado.
2. Clique com o botão direito do mouse no codificador e clique em **Alterar a palavra-passe... (Alterar senha).**
3. Insira uma senha para as três contas de usuário integradas live, user e service.

Proteção por senha padrão

O BVMS versões 5.0 e posterior fornecem o recurso para implementar senhas globais em todos os dispositivos em um sistema de vídeo de até 2.000 câmeras IP. Esse recurso pode ser acessado pelo BVMS Configuration Wizard ao trabalhar com os aparelhos de gravação DIVAR IP 3000 ou DIVAR IP 7000 ou por meio do Configuration Client do BVMS em qualquer sistema.

Para acessar o menu de senhas globais no Configuration Client do BVMS:

1. No menu **Hardware**, clique em **Proteger Dispositivos com Palavra-passe Predefinida...** (Proteger dispositivos com senha padrão).
2. No campo **Palavra-passe predefinida global** (Senha padrão global), insira uma senha e selecione **Impor proteção por palavra-passe na ativação** (Aplicar proteção por senha na ativação).

Depois de salvar e ativar as alterações no sistema, a senha inserida será aplicada às contas live, user e service de todos os dispositivos, incluindo a conta de administrador do Video Recording Manager.

Aviso!

Se os dispositivos já tiverem senhas existentes definidas em qualquer uma das contas, elas não serão substituídas.

Por exemplo, se a senha estiver definida para service, mas não para live e user, a senha global será configurada apenas para as contas live e user.

Configurações do BVMS e VRM

Por padrão, o BVMS usa a conta de administração integrada **srvadmin** para se conectar ao Video Recording Manager com uma proteção por senha. Para evitar acesso não autorizado ao Video Recording Manager, a conta de administrador **srvadmin** deverá ser protegida com uma senha complexa.

Para alterar a senha da conta **srvadmin** no Configuration Client do BVMS:

1. Na Device tree (Árvore de dispositivos), selecione o dispositivo VRM.
2. Clique com o botão direito no dispositivo VRM e clique em **Alterar Palavra-passe VRM.** A caixa de diálogo **Alterar a palavra-passe...** é exibida.
3. Insira uma nova senha para a conta **srvadmin** e clique em **OK**.

Comunicação criptografada para câmeras
Desde o BVMS versão 7.0, a comunicação de controle e de dados de vídeo ao vivo entre a câmera e o Operator Client, Configuration Client, o Management Server e o Video Recording Manager do BVMS pode ser criptografada.
Depois de ativar a conexão segura na caixa de diálogo **Editar Codificador**, o BVMS Server, o Operator Client e o Video Recording Manager usarão uma conexão HTTPS segura para conectar a uma câmera ou um codificador.
A cadeia de conexão usada internamente do BVMS será alterada de rcpp://a.b.c.d (conexão RCP+ simples na porta 1756) para https://a.b.c.d (conexão HTTPS na porta 443).
Para dispositivos legados que não são compatíveis com HTTPS, a cadeia de conexão permanece inalterada (RCP+).

Se a comunicação HTTPS for selecionada, ela utilizará HTTPS (TLS) para criptografar toda a comunicação de controle e a carga de vídeo por meio do mecanismo de criptografia no dispositivo. Ao utilizar o TLS, toda a comunicação de controle HTTPS e carga de vídeo é criptografada com uma chave de criptografia AES com até 256 bits.
Para ativar a comunicação criptografada no Configuration Client do BVMS:
1. Na Device tree (Árvore de dispositivos), selecione o codificador ou a câmera desejado.
2. Clique com o botão direito do mouse no codificador/câmera e clique em **Editar Codificador** (Editar codificador).
3. Na caixa de diálogo **Editar Codificador** (Editar codificador), ative **Ligação segura (Conexão segura (criptografia)).**
4. Salve e ative a configuração.

Depois de ativar a conexão segura com o codificador, outros protocolos podem ser desativados (consulte *Uso geral da porta de rede e transmissão de vídeo, página 17*).

Aviso!
O BVMS é compatível apenas com a porta 443 padrão do HTTPS. O uso de portas diferentes não é permitido.

4.3 Proteção de acesso a dispositivo

Todos os dispositivos de vídeo IP da Bosch são fornecidos com páginas da Web multipropósito integradas. As páginas da Web de dispositivo específico oferecem suporte a funções de vídeo ao vivo e de reprodução de vídeo, bem como algumas definições de configuração específicas que podem não estar acessíveis por meio de um sistema de gerenciamento de vídeo. As contas de usuário integradas funcionam como o acesso às diferentes seções das páginas da Web dedicadas. Embora não seja possível desativar completamente o acesso à página da Web por meio da própria página, o Configuration Manager poderá ser usado, existem vários métodos para encobrir a presença do dispositivo, restringir o acesso e gerenciar o uso de porta de vídeo.

4.3.1 Uso geral da porta de rede e transmissão de vídeo

Todos os dispositivos de vídeo IP da Bosch utilizam o Remote Control Protocol Plus (RCP+) (Protocolo de Controle Remoto +) para detecção, controle e comunicação. O RCP+ é um protocolo de propriedade da Bosch que usa portas estáticas específicas para detectar e se comunicar com os dispositivos de vídeo IP da Bosch: 1756, 1757 e 1758. Ao trabalhar com o BVMS ou outro sistema de gerenciamento de vídeo de terceiro que tenha dispositivos de vídeo IP da Bosch integrados por meio do Bosch VideoSDK, as portas listadas devem estar acessíveis na rede para que os dispositivos de vídeo IP funcionem corretamente.

O vídeo pode ser transmitido dos dispositivos de várias maneiras: UDP (Dinâmico), HTTP (80) ou HTTPS (443).
O uso das portas HTTP e HTTPS pode ser modificado (consulte *Uso das portas HTTP, HTTPS e de vídeo, página 18*). Antes de fazer qualquer modificação de porta, a forma desejada de comunicação para um dispositivo deve ser configurada. O menu Communication (Comunicação) pode ser acessado usando o Configuration Manager (Gerenciador de configuração).

1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Geral** (Geral) e, em seguida, selecione **Acesso à Unidade** (Acesso à unidade).
3. Localize a parte **Acesso ao dispositivo** (Acesso ao dispositivo) da página.

4. Na lista **Protocolo** (Protocolo), selecione o protocolo desejado:

– RCP+
– HTTP (padrão)
– HTTPS

Se a comunicação HTTPS for selecionada, a comunicação entre o Configuration Manager e os dispositivos de vídeo utilizará o protocolo HTTPS (TLS) para criptografar a carga com uma chave de criptografia do AES de até 256 bits. Esse é um recurso básico gratuito. Ao utilizar o TLS, toda a comunicação de controle HTTPS e carga de vídeo é criptografada por meio do mecanismo de criptografia no dispositivo.

Aviso!
A criptografia é especificamente para o "caminho de transmissão". Depois que o vídeo é recebido por um decodificador de software ou hardware, o stream é permanentemente descriptografado.

4.3.2 Versão mínima do TLS (Transport Layer Security, Segurança da Camada de Transporte)

Talvez alguns clientes mais antigos precisem usar versões do TLS mais antigas e menos seguras. Contudo, se possível, defina uma versão mínima do TLS para evitar que os clientes exponham o dispositivo a um modo de acesso menos seguro.
Selecione a versão do TLS mais recente possível como uma versão mínima.

Aviso!
Ao definir o nível mínimo de segurança para acessar dispositivos de um software de cliente, verifique se todas as portas e protocolos que permitem um nível de acesso mais baixo estão desligadas ou desativadas nos dispositivos.

4.3.3 Uso das portas HTTP, HTTPS e de vídeo

É possível alterar ou desativar o uso das portas HTTP e HTTPS em todos os dispositivos. A comunicação criptografada pode ser imposta desativando as portas RCP+ e HTTP, forçando toda a comunicação a usar criptografia. Se o uso da porta HTTP estiver desativado, a porta HTTPS permanecerá ativada e todas as tentativas para desativá-la falharão.

1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Rede** (Rede) e, em seguida, selecione **Acesso à Rede** (Acesso À rede).
3. Localize a parte **Detalhes** (Detalhes) da página.

4. Na parte **Detalhes** (Detalhes), modifique as portas HTTP e HTTPS do navegador e a porta RCP+ usando o menu suspenso:
   - Modificação da porta HTTP do navegador: 80 ou portas 10000 a 10100
   - Modificação da porta HTTPS do navegador: 443 ou portas 10443 a 10543
   - RCP+ porta 1756: **On (Ativada)** ou **Off (Desativada)**

Aviso!
Na versão de firmware 6.1x, se a porta HTTP estiver desativada e for feita uma tentativa de acessar a página da Web do dispositivo, a solicitação será direcionada para a porta HTTPS que está definida atualmente.
O recurso de redirecionamento é omitido na versão de firmware 6.20 e superior. Se a porta HTTP estiver desativada e a porta HTTPS tiver sido modificada para utilizar uma porta diferente de 443, o acesso às páginas da Web poderá ser realizado apenas navegando para o endereço IP dos dispositivos mais a porta atribuída.

Exemplo:
https://192.168.1.21:10443. Qualquer tentativa de conexão com o endereço padrão falhará.

4.3.4 Software de vídeo e seleção de porta

O ajuste dessas configurações também afetará a porta que é utilizada para transmissão de vídeo ao usar o software de gerenciamento de vídeo na LAN.
Se todos os dispositivos de vídeo IP forem definidos como porta HTTP 10000, como um exemplo, e o Operator Client do BVMS estiver configurado para "TCP tunneling" (Túnel TCP), todas as transmissões de vídeo na rede serão feitas pela porta HTTP 10000.

Aviso!
As alterações nas configurações de porta nos dispositivos devem corresponder às configurações no sistema de gerenciamento e em seus componentes, bem como nos clientes.

Aviso!
Dependendo do cenário de implantação e das metas de segurança da instalação, as práticas recomendadas podem variar. A desativação e o redirecionamento do uso de porta de HTTP ou HTTPS têm seus benefícios. A alteração da porta em qualquer protocolo pode ajudar a evitar o fornecimento de informações para ferramentas de rede, como o NMAP (Network Mapper, scanner de segurança gratuito). Aplicativos como o NMAP geralmente são usados como ferramentas de reconhecimento para identificar os pontos fracos de qualquer dispositivo em uma rede. Esta técnica, combinada com a implementação de senha forte, é adicionada à segurança geral do sistema.

4.3.5 Tunelamento SSH

Para acesso remoto a um dispositivo com o BVMS Operator Client por meio de redes públicas, o BVMS fornece um tunelamento SSH (Secure Shell) para garantir comunicação segura (criptografada).
O tunelamento SSH cria um túnel criptografado estabelecido por uma conexão de protocolo/soquete SSH. Esse túnel criptografado pode fornecer transporte para tráfego criptografado e não criptografado. A implementação SSH da Bosch também utiliza o protocolo Omni-Path, que é um protocolo de comunicação de alta performance e baixa latência desenvolvido pela Intel.

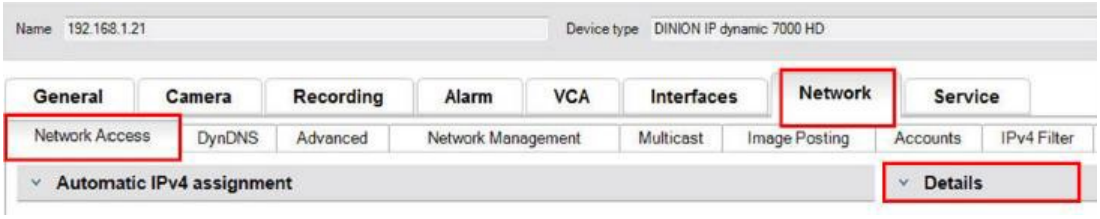
Para obter mais informações sobre como configurar o serviço SSH no BVMS, consulte a documentação do BVMS.
Para obter mais informações sobre como configurar sistemas DIVAR IP para um acesso remoto seguro com o BVMS Operator Client, consulte a documentação do DIVAR IP.

4.3.6 Acesso Telnet

Telnet é um protocolo de camada de aplicativo que proporciona a comunicação com dispositivos por meio de uma sessão de terminal virtual para fins de manutenção e solução de problemas. Todos os dispositivos de vídeo IP da Bosch são compatíveis com Telnet e, por padrão, o suporte de Telnet está ativado nas versões de firmware até 6.1x. Da versão de firmware 6.20 em diante, a porta Telnet é desativada por padrão.

Aviso!
Houve um aumento de ataques cibernéticos utilizando o protocolo desde 2011. No ambiente atual, as práticas recomendadas indicam se você deve desativar o suporte de Telnet em todos os dispositivos até que ele seja necessário para manutenção ou solução de problemas.

1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Rede** (Rede) e, em seguida, selecione **Acesso à Rede** (Acesso À rede).
3. Localize a parte **Detalhes** (Detalhes) da página.



4. Na parte **Detalhes** (Detalhes), ative ou desative **Suporte de Telnet On (Ativado)** ou **Off (Desativado)** usando o menu suspenso.

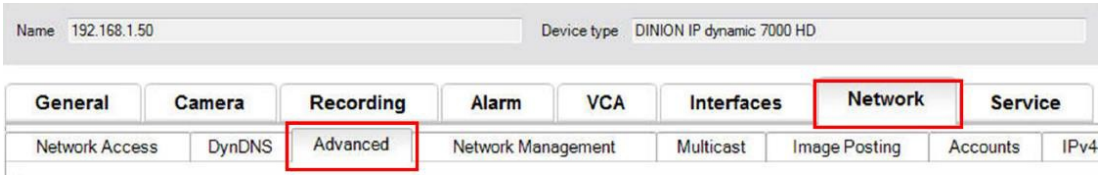
Aviso!
Desde a versão de firmware 6.20, o Telnet também é suportado por meio dos assim-chamados "soquetes da Web", os quais usam conexões HTTPS seguras. Os soquetes da Web não estão usando a porta Telnet padrão e oferecem uma maneira segura de acessar a interface de linha de comando do dispositivo IP, se necessário.

4.3.7 RTSP: Real Time Streaming Protocol

Real Time Streaming Protocol (RTSP) é o principal componente de vídeo utilizado pelo protocolo ONVIF para fornecer streaming de vídeo e controle de dispositivo para ONVIF em conformidade com sistemas de gerenciamento de vídeo. O RTSP também é utilizado por

vários aplicativos de vídeo de terceiros para funções básicas de streaming e, em alguns casos, pode ser usado para solução de problemas de dispositivo e de rede. Todos os dispositivos de vídeo IP da Bosch têm capacidade para fornecer streams usando o protocolo RTSP.
Os serviços de RTSP podem ser facilmente modificados usando o Configuration Manager (Gerenciador de configuração).

1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Rede** (Rede) e, em seguida, selecione **Avançado** (Avançado).



3. Localize a parte **RTSP** da página.
4. No menu suspenso **Porta RTSP** (Porta RTSP), desative ou modifique o serviço de RSTP:
   - Porta padrão de RTSP: 554
   - Modificação da porta de RTSP: 10554 a 10664

Aviso!
Existem relatórios recentes de ataques cibernéticos que utilizam um ataque de buffer de estouro de pilha do RTSP. Esses ataques foram gravados para atingir dispositivos de fornecedores específicos. As práticas recomendadas serão desativar o serviço se ainda não estiver sendo utilizado por um sistema de gerenciamento de vídeo em conformidade com ONVIF ou para streaming básico em tempo real.
Como alternativa e quando o cliente de recebimento permitir, a comunicação RTSP poderá ser colocada em túnel usando uma conexão HTTPS, que mais adiante será a única maneira de transmitir dados de RTSP criptografados.

Aviso!
Para obter mais detalhes sobre RTSP, consulte a nota de aplicação *RTSP usage with Bosch VIP Devices* (Uso de RTSP com dispositivos VIP da Bosch) no catálogo de produtos online da Bosch Security Systems no seguinte link:
https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf

4.3.8 UPnP: Universal Plug and Play

Os dispositivos de vídeo IP da Bosch têm capacidade para se comunicar com dispositivos de rede por meio do **UPnP**. Esse recurso é utilizado principalmente em sistemas menores, com apenas algumas câmeras, em que as câmeras aparecem automaticamente no diretório de rede do PC e, dessa forma, podem ser encontradas com facilidade. Porém, é assim que elas funcionam para qualquer dispositivo na rede.
O **UPnP** pode ser desativado usando o Configuration Manager (Gerenciador de configuração).

1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Rede** (Rede) e, em seguida, selecione **Gestão de Rede** (Gerenciamento de rede).

3. Localize a parte **UPnP** da página.
4. No menu suspenso **UPnP**, selecione **Off** (Desativar) para desativar o **UPnP**.

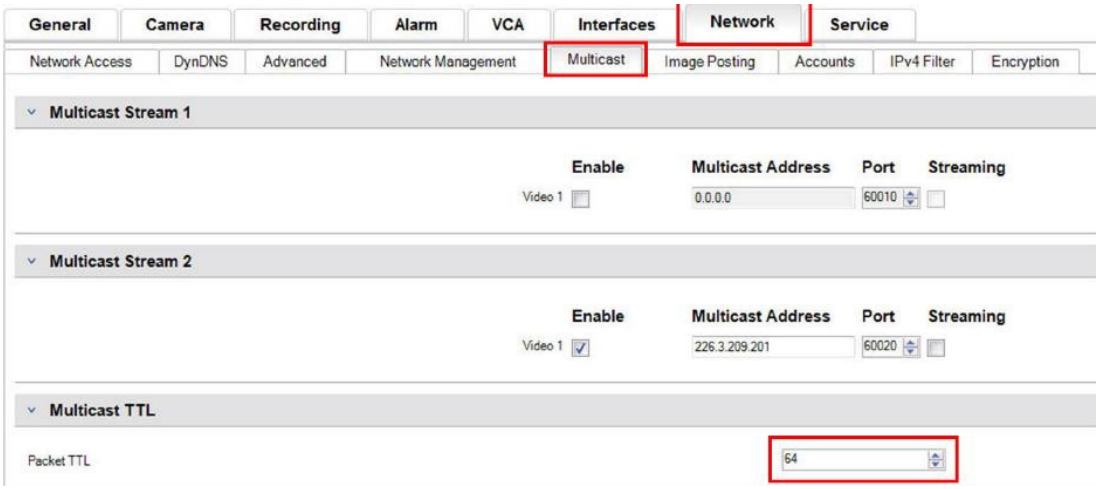
Aviso!
UPnP não deve ser usado em instalações grandes devido ao grande número de notificações de registro e ao possível risco de acesso ou ataque indesejado.

4.3.9 Multicasting

Todos os dispositivos de vídeo IP da Bosch têm capacidade para fornecer vídeo “Multicast on Demand” ou “Multicast Streaming”. Nos locais onde as transmissões de vídeo unicast são baseadas em destino, a multicast é baseada na origem, podendo apresentar problemas de segurança no nível da rede, incluindo, controle de acesso a grupos, confiança do centro de grupos e confiança do roteador. Embora a configuração do roteador vá além do escopo deste guia, há uma solução de segurança que pode ser implementada do próprio dispositivo de vídeo IP.

O escopo de TTL define onde e a que distância o tráfego multicast tem permissão para fluir em uma rede, com cada salto diminuindo o TTL em um. Ao configurar dispositivos de vídeo IP para uso de multicast, o pacote TTL do dispositivo pode ser modificado.

1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Rede** (Rede) e, em seguida, selecione **Multicast**.
3. Localize a parte **Multicast TTL** (TTL de multicast) da página.
4. Ajuste as configurações de **Pacote TTL** (Pacote TTL) usando os seguintes valores de TTL e Limites de escopo:
   - Valor 0 de TTL = Restrito para o host local
   - Valor 1 de TTL = Restrito para a mesma sub-rede
   - Valor 15 de TTL = Restrito para o mesmo site
   - Valor 64 de TTL (padrão) = Restrito para a mesma região
   - Valor 127 de TTL = Mundial
   - Valor 191 de TTL = Mundial com largura de banda limitada
   - Valor 255 de TTL = Dados irrestritos

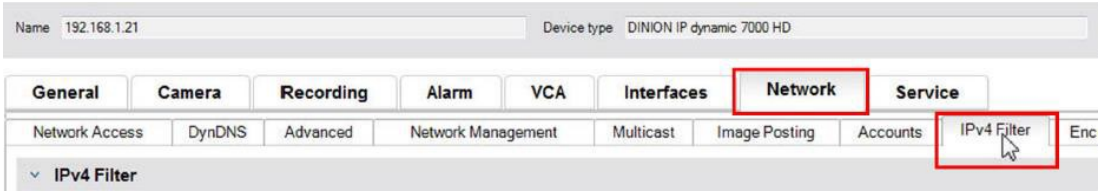


Aviso!
Ao lidar com dados de vigilância por vídeo, uma prática recomendada será definir as configurações de TTL como 15, restrito para o mesmo site. Ou melhor, se você souber o número máximo exato de saltos, use um valor de TTL para isso.

4.3.10 Filtragem de IPv4

É possível restringir o acesso a qualquer dispositivo de vídeo IP da Bosch por meio de um recurso denominado filtragem de IPv4. A filtragem de IPv4 utiliza os fundamentos básicos da "subdivisão de rede" para definir até duas faixas de endereço IP permissíveis. Depois de definida, ela nega acesso de qualquer endereço IP fora dessas faixas.

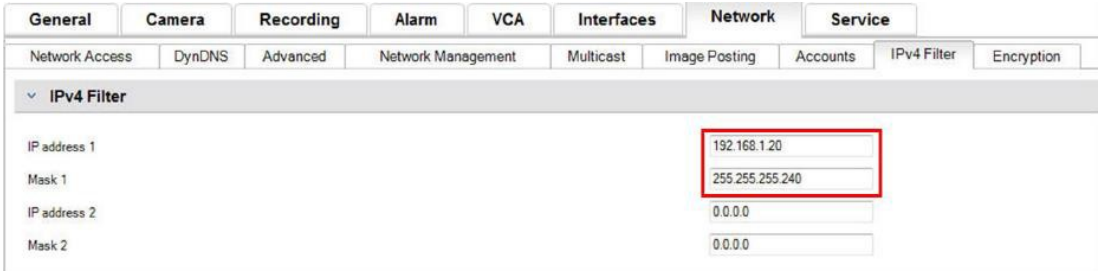
1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Rede** (Rede) e, em seguida, selecione **Filtro IPv4** (Filtro de IPv4).



Aviso!
Para configurar com êxito esse recurso, é necessário ter uma compreensão básica da subdivisão de rede ou ter acesso a uma calculadora de sub-rede. A inserção de valores incorretos nessa configuração pode restringir o acesso ao próprio dispositivo e uma reconfiguração padrão de fábrica precisa ser executada para recuperar o acesso.

3. Para adicionar uma regra de filtro, especifique duas entradas:
   - Insira um endereço IP base que esteja dentro da regra de sub-rede criada.
     O endereço IP base especifica qual sub-rede você está permitindo e ela deve estar dentro da faixa desejada.
   - Insira uma máscara de sub-rede que define os endereços IP com os quais o dispositivo de vídeo IP aceitarão comunicação.

No exemplo a seguir, o **Endereço IP 1** (Endereço IP 1) 192.168.1.20 e a **Máscara 1** (Máscara 1) 255.255.255.240 foram inseridos. Essa configuração restringirá o acesso de dispositivos que estão dentro da faixa de IP definida entre 192.168.1.16 e 192.168.1.31.



Ao utilizar o recurso **Filtro IPv4** (Filtro de IPv4), será possível verificar os dispositivos por meio do protocolo RCP+, mas o acesso a definições de configuração não será possível por meio de clientes que estão fora da faixa de endereços IP permitida. Isso inclui o acesso via navegador da Web.
O próprio dispositivo de vídeo IP não precisa ser localizado na faixa de endereços permitida.

Aviso!
Com base na configuração do sistema, o uso da opção **Filtro IPv4** (Filtro de IPv4) pode reduzir a visibilidade indesejada de dispositivos em uma rede. Se estiver ativada, essa função garantirá a documentação das configurações para referência futura.
Observe que o dispositivo ainda será acessível por meio do IPv6, portanto, a filtragem de IPv4 fará sentido somente em redes IPv4 puras.

4.3.11 SNMP

Simple Network Management Protocol (SNMP) é um protocolo comum para monitorar o status de integridade de um sistema. Esse sistema de monitoramento geralmente tem um servidor de gerenciamento central que coleta todos os dados dos componentes e dispositivos compatíveis do sistema.
O SNMP fornece dois métodos para obter o status de integridade do sistema:

- O servidor de gerenciamento da rede pode sondar o status de integridade de um dispositivo por meio de solicitações de SNMP.
- Os dispositivos podem notificar ativamente o servidor de gerenciamento da rede sobre o status de integridade do sistema no caso de condições de erro ou alarme por meio do envio de armadilhas de SNMP para o servidor SNMP. Essas armadilhas devem ser configuradas dentro do dispositivo.

O SNMP também permite a configuração de algumas variáveis dentro de dispositivos e componentes.
As informações, de quais mensagens um dispositivo tem suporte e de quais armadilhas ele pode enviar, são derivadas do arquivo MIB (Management Information Base), que é fornecido com um produto para fácil integração em um sistema de monitoramento de rede.

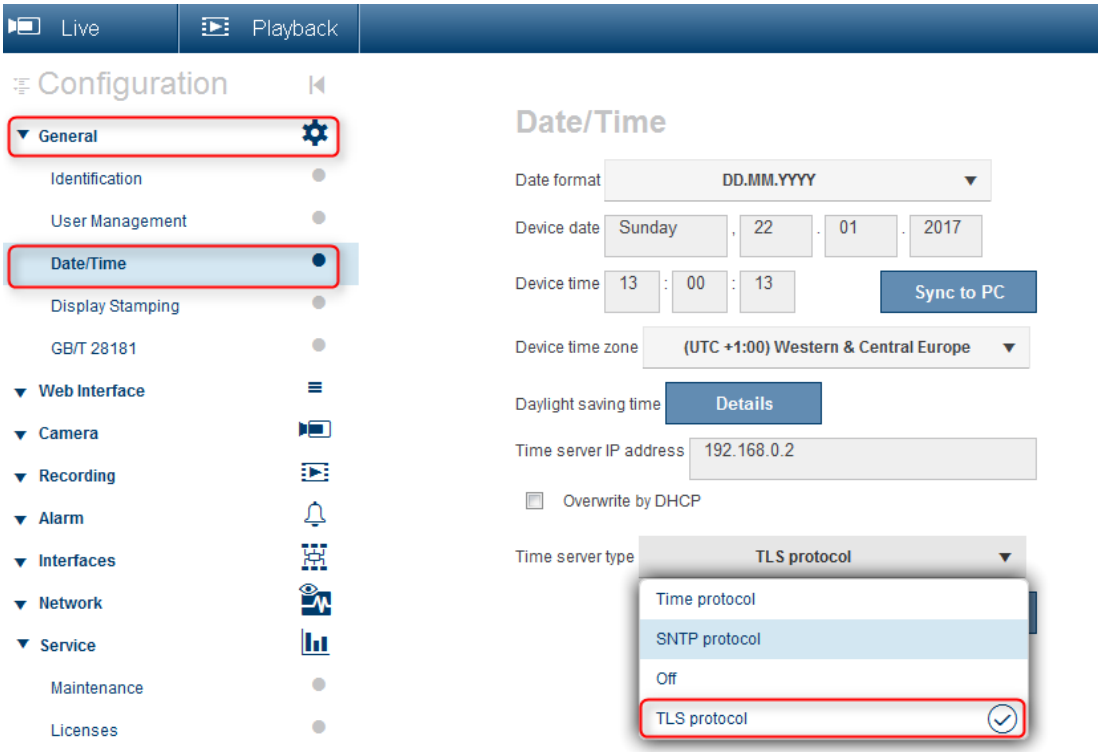
Existem três versões diferentes do protocolo SNMP:

- SNMP versão 1
  O SNMP versão 1 (SNMPv1) é a implementação inicial do protocolo SNMP. Essa versão é amplamente usada e se tornou o protocolo padrão real para gerenciamento e monitoramento de rede.
  Portanto, o SNMPv1 se tornou uma ameaça devido a sua falta de recursos de segurança. Ele usa apenas '*cadeias de comunidade*' como um tipo de senhas, que são transmitidas em texto não criptografado.
  Dessa forma, o SNMPv1 deve ser usado apenas quando é possível assegurar que a rede está fisicamente protegida contra acesso não autorizado.
- SNMP versão 2
  O SNMP versão 2 (SNMPv2) incluiu melhorias em segurança e confidencialidade, entre outras, e introduziu uma solicitação global para recuperar grandes quantidades de dados em uma única solicitação. No entanto, seu método de segurança foi considerado muito complexo, inibindo a sua aceitação.
  Dessa forma, ele foi substituído logo em seguida pela versão SNMPv2c, que é igual à SNMPv2, mas sem seu modelo de segurança controverso, revertendo para o método baseado em comunidade da versão SNMPv1, apresentando similarmente a falta de segurança.
- SNMP versão 3
  O SNMP versão 3 (SNMPv3) inclui principalmente aprimoramentos de segurança e de configuração remota. Eles incluem melhorias em confidencialidade por criptografia de pacotes, integridade de mensagem e autenticação.
  Essa versão também determina a implantação em grande escala do SNMP.

Aviso!
As versões SNMPv1 e SNMPv2c ficaram sob ameaça devido à falta de recursos de segurança. Elas usam apenas as ‘cadeias de comunidade’ como um tipo de senhas, que são transmitidas em texto não criptografado.
Dessa forma, SNMPv1 ou SNMPv2c deverá ser usado apenas quando for possível assegurar que a rede esteja fisicamente protegida contra acesso não autorizado.
No momento, as câmeras Bosch são compatíveis apenas com SNMPv1. Desative o protocolo SNMP caso não o utilize.

4.3.12 Base temporal segura

Além do protocolo Time e SNTP (Simple Network Time Protocol, Protocolo Simples de Tempo de Rede), que são protocolos não protegidos, um terceiro modo para o cliente Timeserver foi introduzido com o firmware 6.20, usando o protocolo TLS. Esse método também é comumente conhecido como *TLS-Date*.
Nesse modo, qualquer servidor HTTPS arbitrário pode ser usado como servidor de horário. O valor de horário é derivado como um efeito colateral do processo de handshake do HTTPS. A transmissão é protegida por TLS. Um certificado raiz opcional para o servidor HTTPS pode ser carregado para o repositório de certificados da câmera para autenticação do servidor.



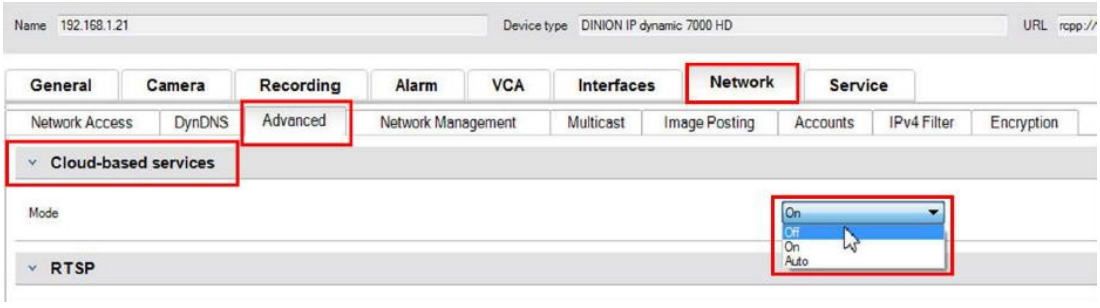
Aviso!
Verifique se o endereço IP do servidor de horário inserido tem uma própria base temporal estável e sem comprometimento.

4.3.13 Serviços baseados na nuvem

Todos os dispositivos de vídeo IP da Bosch podem se comunicar com os serviços baseados em nuvem da Bosch, como Remote Portal. Dependendo da região de implantação, isso permite que os dispositivos de vídeo IP usem serviços como Remote Device Management ou Cloud VMS para encaminhar alarmes e outros dados para uma estação central.
Para obter mais informações, consulte a base de conhecimento da Bosch Building Technologies:
https://community.boschsecurity.com.

Existem três modos de operação dos serviços baseados na nuvem:
- **On** (Ativado):
  o dispositivo de vídeo pesquisará constantemente o servidor de nuvem.
- **Auto** (Automático) (padrão):
  os dispositivos de vídeo tentarão sondar o servidor de nuvem algumas vezes e, se não obtiverem êxito, cessarão a tentativa de alcançar o servidor de nuvem.
- **Off** (Desativado):
  Nenhuma sondagem será executada.

Os serviços baseados em nuvem podem ser facilmente desativados usando Configuration Manager.
1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Rede** (Rede) e, em seguida, selecione a guia **Avançado** (Avançado).
3. Localize a seção **Serviços com base na nuvem** (Serviços baseados em nuvem) da página e selecione **Off** (Desativado) na lista.



Aviso!
Se você estiver utilizando os serviços baseados em nuvem da Bosch, mantenha a configuração padrão.
Em todos os outros casos, alterne o modo de serviços baseados em nuvem para **Off** (Desativado).

4.4 Proteção de câmeras IP

As câmeras IP da Bosch são fornecidas com uma configuração padrão que permite fácil integração em diferentes ambientes.
Dependendo do ambiente-alvo e do nível de segurança pretendido, talvez seja necessário alterar algumas configurações da câmera de modo a aumentar a segurança cibernética e de dados.
No entanto, pode haver limitações do ambiente operacional que obriguem o uso de determinado protocolo ou recurso menos seguro (por exemplo, SNMPv1).

4.4.1 Níveis de proteção

Existem dois níveis de proteção definidos: *elevado* e *rigoroso*.
O nível de proteção *rigoroso* apresenta o meio mais seguro de configurar um dispositivo, mas pode limitar seu uso, já que alguns recursos (por exemplo, a descoberta automática de um dispositivo) ficam desativados. Para cada recurso, é preciso avaliar se a configuração de *elevado* ou *rigoroso* pode ser aplicada.

4.4.2 Visão geral sobre proteção

Rede - Serviços de rede	**Padrão**	**Elevado**	**Rigoroso**
HTTP	Ativado	Desativado	Desativado
HTTPS	Ativado	Ativado	Ativado
RTSP	Ativado	Opcional	Desativado
RCP	Ativado	Desativado	Desativado
SNMPv1	Desativado	Desativado	Desativado
SNMPv3	Desativado	Ativado	Ativado
iSCSI	Ativado	Opcional	Desativado
UPnP	Desativado	Desativado	Desativado
Servidor do NTP	Desativado	Desativado	Desativado
Discovery	Ativado	Ativado	Desativado
ONVIF Discovery	Ativado	Ativado	Desativado
GBT/28181	Desativado	Desativado	Desativado
Mecanismo de redefinição de senha	Ativado	Desativado	Desativado
Resposta de ping	Ativado	Ativado	Desativado
RTSPS	Ativado	Ativado	Ativado
HTTP	Ativado	Desativado	Desativado

Rede - Acesso à rede	**Padrão**	**Elevado**	**Rigoroso**
Versão mínima do TLS	1.0	1.2	1.2
HSTS	Desativado	Ativado	Ativado

Rede - Avançadas	**Padrão**	**Elevado**	**Rigoroso**
802.1x	Desativado	Opcional	Ativado
Syslog	Desativado	TCP	TLS

Rede - Gestão de rede	Padrão	Elevado	Rigoroso
Modo SNMPv3	Desativado	SHA1 / AES	SHA1 / AES

Rede - Filtro IPv4	Padrão	Elevado	Rigoroso
Filtro IPv4	Desativado	Ativado	Ativado

Geral - Data/Hora	Padrão	Elevado	Rigoroso
Data/hora (cliente NTP)	Desativado	Data de SNTP / TLS	Date de TLS

Conectividade - Serviços de nuvem	Padrão	Elevado	Rigoroso
Remote Portal	Desativado	Ativado	Ativado

Assistência técnica - Registar	Padrão	Elevado	Rigoroso
Vedação de software	Desativado	Ativado	Ativado

4.4.3 Descrição do recurso e recomendações de proteção

HTTP

O HTTP é ativado por padrão, mas não criptografado; portanto, as credenciais ou configurações são transferidas sem criptografia, quando usadas.

Recomendação: o HTTP simples deve ser desabilitado em favor do HTTPS criptografado, especialmente se a rede não for confiável.

HTTPS

O HTTPS é criptografado e deve ser a opção padrão para acessar a interface da Web ou acessar a API (Application Programming Interface, Interface de Programação de Aplicativos) baseada na Web RCP. Recomenda-se o uso de PKI e certificados próprios.

Recomendação: o HTTPS é o protocolo seguro padrão usado para configuração e deve permanecer ativado.

RTSP

O RTSP é usado para fluxo de vídeo, mas costuma não ser criptografado. Se o software que recebe o fluxo de vídeo for capaz de usar RTSPS, é recomendável desabilitar o RTSP simples. Ao usar outros componentes da Bosch (por exemplo, decodificadores/BVMS/VRM/DIVAR IP), uma criptografia de propriedade da Bosch para RTSP pode ser ativada, tornando a transmissão segura.

Recomendação: abordagem baseada em risco se for possível transmitir o vídeo sem criptografia ou por meio da criptografia da Bosch. Se for viável, use RTSPS criptografado.

RCP
O Remote Control Protocol plus da Bosch é o protocolo de configuração para câmeras IP da Bosch. Como RCP simples não é criptografado, as configurações são transferidas sem criptografia. Todas as ferramentas da Bosch agora usam a comunicação RCP via HTTPS por algum tempo, mas talvez seja necessário para ferramentas de integração de terceiros ou ferramentas de script que ainda dependem desse protocolo.
Recomendação: desative RCP se não for usado por ferramentas de terceiros ou sistemas herdados.

SNMPv1
O SNMP é o protocolo de monitoramento de rede comum usado para consultar informações sobre a integridade de um dispositivo ou enviar interceptações para um receptor remoto, mas não criptografado.
Recomendação: mantenha desativado se não for necessário para monitoramento de integridade ou outros motivos de compatibilidade. Use SNMPv3 se possível.

SNMPv3
SNMPv3 é o sucessor de SNMPv1 e também pode ser usado com criptografia.
Recomendação: pode ser usado se o monitoramento de SNMP precisar ser implementado.

iSCSI
Desativa o servidor interno iSCSI que é usado para tornar as gravações internas na câmera acessíveis via iSCSI. O iSCSI é um protocolo não criptografado.
Recomendação: desative o servidor iSCSI se não for usado na câmera.

UPnP
A câmera torna-se detectável por meio do protocolo UPnP.
Recomendação: desative UPnP se não for necessário.

Servidor do NTP
Habilite um servidor NTP na câmera para permitir que outros dispositivos ou câmeras sincronizem a hora. Se possível, um dispositivo dedicado deve fornecer tempo para a rede de câmeras permitindo a separação de serviços. Se nenhum outro dispositivo estiver disponível, o tempo pode ser fornecido por uma câmera.
Recomendação: o servidor NTP deve ser desabilitado se não for necessário.

Discovery
Use um mecanismo de propriedade da Bosch para tornar as câmeras detectáveis por um software da Bosch, como Configuration Manager.
Recomendação: ao trabalhar com endereços IP dinâmicos, esse recurso deve permanecer ativado. Ao trabalhar em um ambiente com endereços IP fixos, esse recurso pode ser desativado.

ONVIF Discovery
Permita a descoberta de dispositivos de câmera por meio do protocolo ONVIF Discovery
Recomendação: ao trabalhar com endereços IP dinâmicos e ferramentas ONVIF compatíveis, esse recurso deve permanecer ativado. Ao trabalhar em um ambiente com endereço IP fixo, esse recurso pode ser desativado.

GBT/28181
GBT/28181 é um padrão chinês para interoperabilidade entre diferentes dispositivos.
Recomendação: mantenha desativado se não for necessário.

Mecanismo de redefinição de senha
As câmeras IP podem ser montadas em locais muito remotos, o que dificulta o trabalho de manutenção ou a redefinição de fábrica, caso o acesso à câmera tenha sido bloqueado. A Bosch oferece a possibilidade de redefinir a senha de uma câmera por meio do mecanismo de desafio-resposta baseado em um recurso seguro de chave pública/privada.
Recomendação: se esse recurso não for necessário, desative-o.

Resposta de ping
Configura se a câmera responde a solicitações de ping na rede. Pode ajudar na depuração. Em uma rede altamente segura, pode ser desabilitado para evitar a enumeração de dispositivos por meio de varredura de ping, embora existam vários outros meios de descoberta de dispositivos que podem ser usados por um invasor.
Recomendação: abordagem baseada em risco; pode ser desabilitado para redes com alta segurança.

RTSPS
RTSPS é a versão criptografada de RTSP, além de ser usado para fluxo de vídeo. Se o software receptor for compatível, RTSPS sempre deve ser a opção de preferência em vez de RTSP simples. Como muitos clientes RTSP não são compatíveis com a variante segura, RTSP ainda está habilitado para segurança de nível 1.
Recomendação: use RTSPS se possível.

Versão mínima do TLS
As câmeras IP só permitem SSLv3 seguro ou conexões mais recentes. TLS 1.0 e 1.1 tornaram-se obsoletos pelo IETF, além de haver possíveis problemas de segurança conhecidos (BEAST, FREAK).
As câmeras CPP4, CPP6, CPP7 e CPP7.3 são compatíveis com o TLS 1.2, que deve ser definido como a versão mínima necessária.
As câmeras CPP13 e CPP14 não permitem versões do TLS anteriores a 1.2. Elas também são compatíveis com a especificação do TLS 1.3 mais recente.
Recomendação: defina a versão mínima do TLS como 1.2.

HSTS
HTTP Strict Transport Security (HSTS) é uma política definida por um site para proteger contra ataques man-in-the-middle e ataques de downgrade de protocolo. Com ele, o site orienta o navegador a autorizar apenas conexões HTTPS dentro dessa conexão e não permitir nenhuma conexão HTTP não criptografada.
Recomendação: ative HSTS na câmera.

802.1x
802.1x é um padrão para Network Access Control (NAC). Ele permite que os dispositivos sejam autenticados na rede. Assim, apenas dispositivos autenticados recebem acesso à rede. As câmeras IP da Bosch são compatíveis com 802.1x por meio de senha ou autenticação baseada em certificado, sendo a última o método de preferência. Para usar 802.1x, o comutador de rede deve permitir esse padrão e um servidor de autenticação é necessário.
Recomendação: se a infraestrutura de rede permitir, use a autenticação de rede com 802.1x.

Syslog
Como a câmera fornece apenas um espaço limitado para mensagens de log, estas devem ser enviadas para um local central e analisadas para detectar quaisquer ataques ou configurações incorretas.
Recomendação: use TCP Syslog para evitar a perda de mensagens por causa da perda de pacotes. Use Syslog com TLS para criptografar e autenticar mensagens.

Modo SNMPv3
SNMPv3 é o sucessor de SNMPv1 e permite autenticação segura e transferência de informações.
Recomendação: ao utilizar SNMPv3, aplique SHA1 como protocolo de autenticação e AES como protocolo de privacidade (se compatível).

Filtro IP
No filtro IP, podem ser definidos vários endereços IP (hosts únicos ou sub-redes de rede), que têm permissão para acessar a câmera. Recomenda-se definir aqui os computadores ou redes que acessam a câmera.
Recomendação: use o filtro IP para definir hosts ou redes permitidos.

Data/hora
Para ter o carimbo de data/hora correto em logs e dados de vídeo, é recomendável sincronizar a hora com um servidor de horário central. A data de SNTP e TLS pode ser usada para realizar essa configuração. A vantagem de SNTP é uma sincronização de tempo mais precisa. A vantagem da data de TLS é a possibilidade de verificar se o certificado está correto, o que torna a solução mais segura.
Recomendação: use um meio seguro de sincronizar a hora, seja com a data de SNTP ou TLS.

Serviços baseados na nuvem
A Bosch oferece seus próprios serviços baseados em nuvem para gerenciar câmeras na nuvem da Bosch (Remote Portal). Os serviços de nuvem não se conectam automaticamente ao Remote Portal e ficam desabilitados por padrão. Cada câmera precisa ser conectada primeiro ao Remote Portal quando há necessidade de utilização. Todas as precauções foram tomadas para garantir a conexão entre o Remote Portal e a câmera; portanto, se necessário, o Remote Portal pode ser usado em qualquer ambiente.
Recomendação: o Remote Portal pode ser usado dependendo se a solução de nuvem está em uso.

Vedação de software
Uma vez feita a configuração completa de uma câmera IP, as definições do dispositivo não devem ser alteradas. Um selo de software pode ser ativado para notificar alterações na configuração do dispositivo.
Recomendação: ative a vedação de software se não houver alterações de configuração pendentes.

4.4.4 Defesa em profundidade

A defesa em profundidade é uma abordagem de segurança em camadas, na qual a segurança do produto não se limita a uma medida isolada; o invasor precisa violar várias camadas para explorar o produto. A cada versão de um produto, é avaliado se novos recursos são necessários para mitigar novos ataques ou aumentar sua segurança geral.
Aqui está uma visão geral das principais funções de segurança da câmera IP.

– **Assinatura de firmware**
  Cada arquivo de atualização de firmware é criptografado e assinado por um certificado da Bosch. Somente as atualizações publicadas pela Bosch podem ser instaladas nas câmeras, evitando a instalação de firmware malicioso.
– **Inicialização segura**
  As câmeras das plataformas CPP13, CPP14 ou mais recentes possuem um mecanismo de inicialização segura. A inicialização segura verifica a integridade de todo o sistema, do carregador de inicialização ao próprio firmware nas câmeras; cada etapa do processo de inicialização verifica a próxima, tendo como ponto de partida a raiz de confiança cujo hardware é imutável. Isso impede que um invasor modifique o carregador de inicialização ou o firmware do dispositivo.
– **Firewall de login**
  Para proteger a senha contra ataques de força bruta e de negação de serviço (DoS), mas ao mesmo tempo permitir que os administradores façam login normalmente, o firewall de login verifica as tentativas de login com base na análise comportamental e bloqueia ou permite dinamicamente o acesso com base em endereços IP.
– **Autenticação da câmera**
  Para identificar e autenticar exclusivamente uma câmera, um certificado de dispositivo da Bosch é criado em cada câmera durante a produção. Esse certificado pode ser usado para verificar se há comunicação com um dispositivo genuíno da Bosch. Além disso, certificados personalizados podem ser carregados ou criados na câmera para fornecer integração com um ambiente de PKI para proteção contra ataques man-in-the-middle.

4.5 Proteção de armazenamento

Uma vez que as câmeras IP ou codificadores da Bosch são capazes de estabelecer uma sessão iSCSI diretamente para uma unidade iSCSI e de gravar dados de vídeo em uma unidade iSCSI, as unidades iSCSI precisarão ser conectadas à mesma LAN ou WAN que os dispositivos periféricos da Bosch.
Por evitar o acesso não autorizado aos dados de vídeo gravados, as unidades iSCSI devem estar protegidas contra acesso não autorizado:

– Use a autenticação de senha por meio do CHAP para garantir que apenas dispositivos conhecidos tenham permissão para acessar o destino da iSCSI. Defina uma senha com o CHAP (Challenge Hardware Authentication Protocol, Protocolo de Autenticação de Hardware de Desafio) no destino da iSCSI e insira a senha definida na configuração do VRM. A senha do CHAP é válida para o VRM e é enviada para todos os dispositivos

automaticamente. Se uma senha com CHAP for usada em um ambiente VRM do BVMS, todos os sistemas de armazenamento deverão ser configurados para usar a mesma senha.
- Remova todos os nomes de usuário e senhas padrão do destino da iSCSI.
- Use uma senha forte para contas de usuário administrativo do destino da iSCSI.
- Desative o acesso administrativo via Telnet aos destinos da iSCSI. Em vez disso, use o acesso SSH.
- Proteja o acesso do console ao destino da iSCSI por meio da senha forte.
- Desative as placas de interface de rede não utilizadas.
- Monitore o status do sistema dos armazenamentos de iSCSI por meio de ferramentas de terceiros para identificar anomalias.

4.5.1 Definição de uma senha com CHAP em dispositivos iSCSI

Quando você define uma senha com CHAP global no BVMS Configuration Client, ela é automaticamente transferida para todos os codificadores, decodificadores e dispositivos VSGs (Geradores de Sinais Vetoriais).
Essa função não é compatível com alguns dispositivos iSCSI. É preciso definir manualmente a senha com CHAP em tais dispositivos.

Aviso!
Defina a senha com CHAP global nos dispositivos iSCSI antes de adicioná-los ao BVMS. Dispositivos iSCSI não podem ser adicionados a uma configuração do BVMS onde a senha com CHAP global já esteja ativada.

Para definir manualmente uma senha com CHAP em um dispositivo iSCSI (por exemplo, DIVAR IP), que é baseado em uma versão recente do sistema operacional Microsoft Windows Server:

1. Abra o **Server Manager** e navegue até **File and Storage Services > iSCSI** (Serviços de arquivo e armazenamento > iSCSI).
2. Na lista **ISCSI TARGETS** (DESTINOS DE ISCSI), clique com o botão direito do mouse no destino de iSCSI desejado e clique em **Properties** (Propriedades).
   A caixa de diálogo **Properties** (Propriedades) é exibida.
3. Na caixa de diálogo **Properties** (Propriedades), clique em **Security** (Segurança) e marque a caixa de seleção **Enable CHAP** (Habilitar CHAP).
4. Insira o seguinte:
   - **User name:** usuário
   - **Password:** insira a senha com CHAP global conforme fornecida no BVMS Configuration Client (no menu **Hardware > Protect iSCSI storages with CHAP password...** [Hardware > Proteger armazenamentos de iSCSI com senha com CHAP...]).
5. Clique em **OK**.
   A senha com CHAP será atribuída ao destino de iSCSI.

4.6 Proteção de servidores

4.6.1 Configurações recomendadas de hardware do servidor

- O BIOS do servidor oferece o recurso para definir senhas de nível mais baixo.
  Essas senhas permitem restringir que pessoas inicializem o computador e dispositivos removíveis, bem como que alterem as configurações do BIOS ou da UEFI (Unified Extensible Firmware Interface) sem permissão.

– Para impedir a transferência de dados para o servidor, as portas USB e a unidade de CD/DVD devem ser desativadas.
  Além disso, as portas NIC não utilizadas devem ser desativadas e as portas de gerenciamento, como as portas do console ou da interface HP ILO (HP Integrated Lights-Out), devem estar desativadas ou protegidas por senha.

4.6.2 Configurações de segurança recomendadas do sistema operacional Windows

Os servidores devem fazer parte de um Domínio do Windows.
Com a integração dos servidores a um domínio do Windows, as permissões de usuário são atribuídas a usuários da rede gerenciados por um servidor central. Como essas contas de usuário geralmente implementam as regras de intensidade e expiração de senha, essa integração pode melhorar a segurança sobre as contas locais que não têm essas restrições.

4.6.3 Atualizações do Windows

Os patches e as atualizações do software Windows devem ser instalados e permanecer atualizados. As atualizações do Windows geralmente incluem patches para vulnerabilidades de segurança recém-descobertas, como a vulnerabilidade Heartbleed SSL, que afetou milhões de computadores no mundo todo. Devem ser instalados os patches referentes a esses problemas significativos.

4.6.4 Instalação de software antivírus

Instale o software antivírus e anti-spyware e mantenha-o atualizado.

4.6.5 Configurações recomendadas do sistema operacional Windows

As seguintes configurações de política de grupo local são configurações de grupo recomendadas em um sistema operacional Windows Server. Para alterar as Políticas do Computador Local (LCP, Local Computer Policies) padrão, use o Editor de Política de Grupo Local.
É possível abrir o Editor de Política de Grupo Local usando a linha de comando ou o Console de Gerenciamento Microsoft (MMC).

Para abrir o Editor de Política de Grupo Local da linha de comando:

- Clique em **Iniciar** e, na caixa de pesquisa de **Iniciar**, digite **gpedit.msc** e pressione Enter.

Para abrir o Editor de Política de Grupo Local como um snap-in MMC:

1. Clique em **Iniciar** e, na caixa Pesquisar de **Iniciar**, digite **mmc** e pressione Enter.
2. Na caixa de diálogo **Adicionar ou Remover Snap-ins**, clique em **Editor de Política de Grupo Local** e em **Adicionar**.
3. Na caixa de diálogo **Selecionar Objeto de Política de Grupo**, clique em **Procurar**.
4. Clique em **Este computador** para editar o objeto de Política de Grupo Local ou clique em **Usuários** para editar os objetos de Política de Grupo Local Administrador, Não Administrador ou por usuário.
5. Clique em **Concluir**.

4.6.6 Ativar Controle de Conta de Usuário no servidor

Políticas do Computador Local -> Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas Locais -> Opções de Segurança

Controle de Conta de Usuário: Modo de Aprovação de Administrador para a conta de Administrador Interno	Ativado

Controle de Conta de Usuário: permitir que aplicativos UIAccess solicitem elevação sem usar a área de trabalho protegida	Desativado
Controle de Conta de Usuário: comportamento do prompt de elevação de administradores no Modo de Aprovação de Administrador	Pedir consentimento
Controle de Conta de Usuário: comportamento do prompt de elevação de usuários padrão	Solicitar credenciais na área de trabalho protegida
Controle de Conta de Usuário: detectar instalações de aplicativos e perguntar se deseja elevar	Ativado
Controle de Conta de Usuário: elevar somente executáveis assinados e validados	Desativado
Controle de Conta de Usuário: executar todos os administradores no Modo de Aprovação de Administrador	Ativado
Controle de Conta de Usuário: alternar para a área de trabalho segura ao pedir elevação	Ativado
Controle de Conta de Usuário: virtualizar falhas de gravação de arquivos e Registros para locais por usuário	Ativado

Políticas do Computador Local -> Configuração do Computador -> Modelos Administrativos -> Componentes do Windows -> Interface do Usuário de Credenciais

Enumerar contas de administrador na elevação	Desativado

4.6.7 Desativar Reprodução Automática

Políticas do Computador Local -> Configuração do Computador -> Modelos Administrativos -> Componentes do Windows -> Políticas de Reprodução Automática

Desativar Reprodução Automática	Ativada em todas as unidades
Comportamento padrão para AutoRun	Ativado, não execute comandos AutoRun
Desativar Reprodução Automática para dispositivos de não volume	Ativado

4.6.8 Dispositivos Externos

Políticas do Computador Local -> Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas Locais -> Opções de Segurança

Dispositivos: permitir desencaixe sem fazer logon	Desativado
Dispositivos: permite formatar e ejetar a mídia removível	Administradores
Dispositivos: evita que usuários instalem drivers de impressora	Ativado
Dispositivos: restringir acesso ao CD-ROM apenas aos usuários com logon local	Ativado
Dispositivos: restringir acesso ao disquete apenas aos usuários com logon local	Ativado

4.6.9 Configuração de atribuição de direitos do usuário

Políticas do Computador Local -> Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas Locais -> Atribuição de Direitos de Usuário

Acessar Gerenciador de Credenciais como chamador confiável	Ninguém
Acesso a este computador pela rede	Usuários autenticados
Atuar como parte do sistema operacional	Ninguém
Adicionar estações de trabalho ao domínio	Ninguém
Permitir logon pelos Serviços de Área de Trabalho Remota	Administradores, Usuários de Área de Trabalho Remota
Alterar a hora do sistema	Administradores
Alterar o fuso horário	Administradores, Serviço Local
Criar um arquivo de páginas	Administradores
Criar um objeto token	Ninguém
Criar objetos compartilhados permanentemente	Ninguém
Negar acesso a este computador pela rede	Logon Anônimo, Grupo Convidado
Negar logon como um trabalho em lotes	Logon Anônimo, Grupo Convidado
Negar logon como um serviço	Ninguém
Negar logon local	Logon Anônimo, Grupo Convidado
Negar logon pelos Serviços de Área de Trabalho Remota	Logon Anônimo, Convidado
Ativar computador e contas de usuário para serem confiáveis para delegação	Ninguém
Forçar o desligamento a partir de um sistema remoto	Administradores
Gerar auditoria de segurança	Serviço Local, Serviço de Rede
Aumentar a prioridade de planejamento	Administradores
Carregar e descarregar drivers de dispositivos	Administradores
Modificar rótulo de objeto	Ninguém
Alterar valores de ambiente de firmware	Administradores
Executar tarefas de manutenção de volume	Administradores
Traçar um perfil de um único processo	Administradores
Remover o computador da base de encaixe	Administradores
Restaurar arquivos e pastas	Administradores

Desligar o sistema	Administradores
Sincronizar dados do serviço de diretório	Ninguém
Apropriar-se de arquivos ou de outros objetos	Administradores

4.6.10 Protetor de tela

– Ative o protetor de tela protegido por senha e defina o tempo limite:
Políticas do Computador Local -> Configuração do Usuário -> Modelos Administrativos -> Painel de Controle -> Personalização

Habilitar a proteção de tela	Ativado
Proteger com senha a proteção de tela	Ativado
Tempo limite de Proteção de Tela	1.800 segundos

4.6.11 Ativar configurações de política de senha

– A ativação de configurações de política de senha assegura que as senhas dos usuários atendam aos requisitos mínimos de senha.

Políticas do Computador Local -> Configurações do Windows -> Configurações de Segurança -> Políticas de Conta -> Políticas de Senha

Impor histórico de senhas	10 senhas lembradas
Tempo de vida máximo da senha	90 dias
Tempo de vida mínimo da senha	1 dia
Comprimento mínimo da senha	10 caracteres
A senha deve satisfazer a requisitos de complexidade	Ativado
Armazenar senha usando criptografia reversível para todos os usuários no domínio	Desativado

4.6.12 Desativar serviços não essenciais do Windows

– A desativação de Serviços não essenciais do Windows permite um nível de segurança mais alto e minimiza os pontos de ataque.

Serviço Gateway de Camada de Aplicativo	Desativado
Gerenciamento de Aplicativos	Desativado
Pesquisador de Computadores	Desativado
Cliente de Rastreamento de Link Distribuído	Desativado
Host de Provedor da Descoberta de Função	Desativado
Publicação de Recursos de Descoberta de Função	Desativado
Acesso a Dispositivo de Interface Humana	Desativado
ICS (Compartilhamento de Conexão com a Internet)	Desativado
Mapeador da Descoberta de Topologia da Camada de Link	Desativado

Agendador de Classes de Multimídia	Desativado
Arquivos Offline	Desativado
Gerenciador de Conexão de Acesso Remoto Automático	Desativado
Gerenciador de Conexão de Acesso Remoto	Desativado
Roteamento e Acesso Remoto	Desativado
Detecção do hardware do shell	Desativado
Assistente de console de administração especial	Desativado
Descoberta SSDP	Desativado

4.6.13 Contas de usuário do sistema operacional Windows

As contas de usuário do Sistema operacional Windows precisam estar protegidas com senhas complexas.
Os servidores normalmente são gerenciados e mantidos com contas de administrador do Windows. Assegure que sejam usadas senhas fortes para as contas de administrador.

As senhas devem conter caracteres de três das seguintes categorias:
- Caracteres maiúsculos de idiomas europeus (A a Z, com marcas diacríticas, caracteres gregos e cirílicos)
- Caracteres minúsculos de idiomas europeus (a-Z, s nítido, com marcas diacríticas, caracteres gregos e cirílicos)
- Dígitos de Base 10 (0 a 9)
- Caracteres não alfanuméricos: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Qualquer caractere Unicode que seja categorizado com um caractere alfabético, mas que não seja uma letra maiúscula ou minúscula. Isso inclui os caracteres Unicode dos idiomas asiáticos.

Uso de Bloqueio de Conta do Windows para dificultar o sucesso dos ataques de violação de senhas.
A recomendação de Linhas de Base de Segurança do Windows 8.1 é de 10/5/15:
- 10 tentativas inválidas
- Duração de bloqueio de 15 minutos
- Reinício do contador após 15 minutos

Políticas do Computador Local -> Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas de Conta -> Política de Bloqueio de Conta

Duração do bloqueio de conta	Duração do bloqueio de conta
15 minutos Limite de bloqueio de conta 10 tentativas de logon inválidas	15 minutos Limite de bloqueio de conta 10 tentativas de logon inválidas
Zerar contador de bloqueios de conta após	Zerar contador de bloqueios de conta após

- Verifique se todas as senhas padrão do servidor e do sistema operacional Windows são substituídas pelas novas senhas fortes.

4.6.14 Ativar firewall no servidor

- Ative a comunicação da porta padrão do BVMS de acordo com as portas do BVMS.

Aviso!
Consulte a documentação do BVMS para obter configurações e uso de porta relevantes. Verifique novamente as configurações sobre atualizações de firmware ou software.

4.7 Proteção de clientes Windows

4.7.1 Estações de Trabalho do Windows

Os sistemas operacionais para desktop Windows, usados para aplicativos do BVMS, como o BVMS Operator Client ou o Configuration Client, são instalados fora da área segura. As estações de trabalho precisam ser protegidas para proteger os dados de vídeo, os documentos e outros aplicativos contra acesso não autorizado.
As configurações a seguir devem ser aplicadas ou verificadas.

4.7.2 Configurações recomendadas do hardware de Estação de Trabalho do Windows

- Defina uma senha de BIOS/UEFI para restringir pessoas de inicializar sistemas operacionais alternativos.
- Para evitar a transferência de dados para o cliente, as portas USB e a unidade de CD/DVD devem estar desativadas. Além disso, as portas NIC não usadas devem ser desativadas.

4.7.3 Configurações de segurança recomendadas do sistema operacional Windows

- A estação de trabalho deve fazer parte de um Domínio do Windows.
  Com a integração da estação de trabalho a um domínio do Windows, as configurações relevantes de segurança podem ser gerenciadas centralmente.
- Atualizações do Windows
  Fique atualizado com patches e atualizações do sistema operacional Windows.
- Instalação do software Antivírus
  Instale o software antivírus e anti-spyware e mantenha-o atualizado.

4.7.4 Configurações recomendadas do sistema operacional Windows

As seguintes configurações de política de grupo local são configurações de grupo recomendadas em um sistema operacional Windows Server. Para alterar as Políticas do Computador Local (LCP, Local Computer Policies) padrão, use o Editor de Política de Grupo Local.
É possível abrir o Editor de Política de Grupo Local usando a linha de comando ou o Console de Gerenciamento Microsoft (MMC).

Para abrir o Editor de Política de Grupo Local da linha de comando:

- Clique em **Iniciar** e, na caixa de pesquisa de **Iniciar**, digite **gpedit.msc** e pressione Enter.

Para abrir o Editor de Política de Grupo Local como um snap-in MMC:

1. Clique em **Iniciar** e, na caixa Pesquisar de **Iniciar**, digite **mmc** e pressione Enter.
2. Na caixa de diálogo **Adicionar ou Remover Snap-ins**, clique em **Editor de Política de Grupo Local** e em **Adicionar**.
3. Na caixa de diálogo **Selecionar Objeto de Política de Grupo**, clique em **Procurar**.

4. Clique em **Este computador** para editar o objeto de Política de Grupo Local ou clique em **Usuários** para editar os objetos de Política de Grupo Local Administrador, Não Administrador ou por usuário.
5. Clique em **Concluir**.

4.7.5 Ativar Controle de Conta de Usuário no servidor

Políticas do Computador Local -> Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas Locais -> Opções de Segurança

Controle de Conta de Usuário: Modo de Aprovação de Administrador para a conta de Administrador Interno	Ativado
Controle de Conta de Usuário: permitir que aplicativos UIAccess solicitem elevação sem usar a área de trabalho protegida	Desativado
Controle de Conta de Usuário: comportamento do prompt de elevação de administradores no Modo de Aprovação de Administrador	Pedir consentimento
Controle de Conta de Usuário: comportamento do prompt de elevação de usuários padrão	Solicitar credenciais na área de trabalho protegida
Controle de Conta de Usuário: detectar instalações de aplicativos e perguntar se deseja elevar	Ativado
Controle de Conta de Usuário: elevar somente executáveis assinados e validados	Desativado
Controle de Conta de Usuário: executar todos os administradores no Modo de Aprovação de Administrador	Ativado
Controle de Conta de Usuário: alternar para a área de trabalho segura ao pedir elevação	Ativado
Controle de Conta de Usuário: virtualizar falhas de gravação de arquivos e Registros para locais por usuário	Ativado

Políticas do Computador Local -> Configuração do Computador -> Modelos Administrativos -> Componentes do Windows -> Interface do Usuário de Credenciais

Enumerar contas de administrador na elevação	Desativado

4.7.6 Desativar Reprodução Automática

Políticas do Computador Local -> Configuração do Computador -> Modelos Administrativos -> Componentes do Windows -> Políticas de Reprodução Automática

Desativar Reprodução Automática	Ativada em todas as unidades
Comportamento padrão para AutoRun	Ativado, não execute comandos AutoRun
Desativar Reprodução Automática para dispositivos de não volume	Ativado

4.7.7 Dispositivos Externos

Políticas do Computador Local -> Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas Locais -> Opções de Segurança

Dispositivos: permitir desencaixe sem fazer logon	Desativado
Dispositivos: permite formatar e ejetar a mídia removível	Administradores
Dispositivos: evita que usuários instalem drivers de impressora	Ativado
Dispositivos: restringir acesso ao CD-ROM apenas aos usuários com logon local	Ativado
Dispositivos: restringir acesso ao disquete apenas aos usuários com logon local	Ativado

4.7.8 Configuração de atribuição de direitos do usuário

Políticas do Computador Local -> Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas Locais -> Atribuição de Direitos de Usuário

Acessar Gerenciador de Credenciais como chamador confiável	Ninguém
Acesso a este computador pela rede	Usuários autenticados
Atuar como parte do sistema operacional	Ninguém
Adicionar estações de trabalho ao domínio	Ninguém
Permitir logon pelos Serviços de Área de Trabalho Remota	Administradores, Usuários de Área de Trabalho Remota
Alterar a hora do sistema	Administradores
Alterar o fuso horário	Administradores, Serviço Local
Criar um arquivo de páginas	Administradores
Criar um objeto token	Ninguém
Criar objetos compartilhados permanentemente	Ninguém
Negar acesso a este computador pela rede	Logon Anônimo, Grupo Convidado
Negar logon como um trabalho em lotes	Logon Anônimo, Grupo Convidado
Negar logon como um serviço	Ninguém
Negar logon local	Logon Anônimo, Grupo Convidado
Negar logon pelos Serviços de Área de Trabalho Remota	Logon Anônimo, Convidado
Ativar computador e contas de usuário para serem confiáveis para delegação	Ninguém
Forçar o desligamento a partir de um sistema remoto	Administradores

Gerar auditoria de segurança	Serviço Local, Serviço de Rede
Aumentar a prioridade de planejamento	Administradores
Carregar e descarregar drivers de dispositivos	Administradores
Modificar rótulo de objeto	Ninguém
Alterar valores de ambiente de firmware	Administradores
Executar tarefas de manutenção de volume	Administradores
Traçar um perfil de um único processo	Administradores
Remover o computador da base de encaixe	Administradores
Restaurar arquivos e pastas	Administradores
Desligar o sistema	Administradores
Sincronizar dados do serviço de diretório	Ninguém
Apropriar-se de arquivos ou de outros objetos	Administradores

4.7.9 Protetor de tela

– Ative o protetor de tela protegido por senha e defina o tempo limite:
Políticas do Computador Local -> Configuração do Usuário -> Modelos Administrativos -> Painel de Controle -> Personalização

Habilitar a proteção de tela	Ativado
Proteger com senha a proteção de tela	Ativado
Tempo limite de Proteção de Tela	1.800 segundos

4.7.10 Ativar configurações de política de senha

– A ativação de configurações de política de senha assegura que as senhas dos usuários atendam aos requisitos mínimos de senha.

Políticas do Computador Local -> Configurações do Windows -> Configurações de Segurança -> Políticas de Conta -> Políticas de Senha

Impor histórico de senhas	10 senhas lembradas
Tempo de vida máximo da senha	90 dias
Tempo de vida mínimo da senha	1 dia
Comprimento mínimo da senha	10 caracteres
A senha deve satisfazer a requisitos de complexidade	Ativado
Armazenar senha usando criptografia reversível para todos os usuários no domínio	Desativado

4.7.11 Desativar serviços não essenciais do Windows

– A desativação de Serviços não essenciais do Windows permite um nível de segurança mais alto e minimiza os pontos de ataque.

Serviço Gateway de Camada de Aplicativo	Desativado
Gerenciamento de Aplicativos	Desativado
Pesquisador de Computadores	Desativado
Cliente de Rastreamento de Link Distribuído	Desativado
Host de Provedor da Descoberta de Função	Desativado
Publicação de Recursos de Descoberta de Função	Desativado
Acesso a Dispositivo de Interface Humana	Desativado
ICS (Compartilhamento de Conexão com a Internet)	Desativado
Mapeador da Descoberta de Topologia da Camada de Link	Desativado
Agendador de Classes de Multimídia	Desativado
Arquivos Offline	Desativado
Gerenciador de Conexão de Acesso Remoto Automático	Desativado
Gerenciador de Conexão de Acesso Remoto	Desativado
Roteamento e Acesso Remoto	Desativado
Detecção do hardware do shell	Desativado
Assistente de console de administração especial	Desativado
Descoberta SSDP	Desativado

4.7.12 Contas de usuário do sistema operacional Windows

As contas de usuário do Sistema operacional Windows precisam estar protegidas com senhas complexas.
Os servidores normalmente são gerenciados e mantidos com contas de administrador do Windows. Assegure que sejam usadas senhas fortes para as contas de administrador.

As senhas devem conter caracteres de três das seguintes categorias:
- Caracteres maiúsculos de idiomas europeus (A a Z, com marcas diacríticas, caracteres gregos e cirílicos)
- Caracteres minúsculos de idiomas europeus (a-Z, s nítido, com marcas diacríticas, caracteres gregos e cirílicos)
- Dígitos de Base 10 (0 a 9)
- Caracteres não alfanuméricos: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Qualquer caractere Unicode que seja categorizado com um caractere alfabético, mas que não seja uma letra maiúscula ou minúscula. Isso inclui os caracteres Unicode dos idiomas asiáticos.

Uso de Bloqueio de Conta do Windows para dificultar o sucesso dos ataques de violação de senhas.
A recomendação de Linhas de Base de Segurança do Windows 8.1 é de 10/5/15:
- 10 tentativas inválidas
- Duração de bloqueio de 15 minutos

– Reinício do contador após 15 minutos

Políticas do Computador Local -> Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas de Conta -> Política de Bloqueio de Conta

Duração do bloqueio de conta	Duração do bloqueio de conta
15 minutos Limite de bloqueio de conta 10 tentativas de logon inválidas	15 minutos Limite de bloqueio de conta 10 tentativas de logon inválidas
Zerar contador de bloqueios de conta após	Zerar contador de bloqueios de conta após

– Verifique se todas as senhas padrão do servidor e do sistema operacional Windows são substituídas pelas novas senhas fortes.
– Desative as contas não utilizadas do sistema operacional Windows.
– Desative o Acesso à Área de Trabalho Remota para a estação de trabalho cliente.
– Execute direitos não administrativos na estação de trabalho para evitar que o usuário padrão altere as configurações do sistema.

4.7.13 Ativar firewall na estação de trabalho

▸ Ative a comunicação da porta padrão do BVMS de acordo com as portas do BVMS.

Aviso!
Consulte a documentação do BVMS para obter configurações e uso de porta relevantes. Verifique novamente as configurações sobre atualizações de firmware ou software.

4.8 Proteção do acesso à rede

Atualmente, muitos sistemas de vigilância por vídeo IP de pequeno a médio porte são implantados na infraestrutura de rede existente do cliente, assim como "outro aplicativo de TI".
Embora isso tenha seus benefícios no que diz respeito a custo e manutenção, esse tipo de implantação também expõe o sistema de segurança a ameaças indesejadas, incluindo aquelas internas. Medidas apropriadas precisam ser aplicadas, e elas devem evitar situações como vídeo de evento sendo vazado na Internet ou na mídia social. Eventos como estes podem não apenas violar a privacidade, mas possivelmente prejudicar a empresa.

Existem duas tecnologias principais para criar uma rede em uma rede. Qual será escolhida pelos arquitetos de infraestrutura de TI depende altamente da infraestrutura da rede existente, do equipamento de rede implantado, dos recursos exigidos e da topologia da rede.

4.8.1 VLAN: Virtual LAN

Uma LAN virtual é criada subdividindo uma LAN em vários segmentos. A segmentação de rede é feita por uma configuração de roteador ou switch de rede. Uma VLAN tem a vantagem de que as necessidades de recursos precisam ser determinadas sem religar as conexões de rede do dispositivo.
Esquemas de qualidade de serviço, aplicados a segmentos específicos, como para vigilância por vídeo, podem ajudar não apenas a melhorar a segurança, mas o desempenho também.

As VLANs são implementadas na camada de link de dados (camada 2 de OSI) e fornecem analogia para a subdivisão de rede IP (consulte *Atribuição de endereços IP, página 8*) que é similar na camada de rede (camada 3 de OSI).

4.8.2 VPN: Virtual Private Network

Uma Rede Virtual Privada é uma rede separada (privada) que geralmente se estende por redes públicas ou pela Internet. Vários protocolos estão disponíveis para criar uma VPN; geralmente, um túnel que transmite o tráfego protegido. As redes virtuais privadas podem ser projetadas como túneis ponto a ponto, conexões de qualquer ponto a qualquer ponto ou conexões de vários pontos. As VPNs podem ser implantadas com comunicações criptografadas ou, simplesmente, contam com comunicação segura na própria VPN.

As VPNs podem ser usadas para conectar sites remotos por meio de conexões de rede remota (WAN), ao mesmo tempo que também protegem a privacidade e aumentam a segurança em uma rede local (LAN). Como uma VPN funciona como uma rede separada, todos os dispositivos adicionais à VPN funcionarão perfeitamente como se estivessem em uma rede típica. Uma VPN não apenas adiciona outra camada de proteção para um sistema de vigilância, mas também fornece o benefício adicional de segmentação do tráfego de negócios e de vídeo das redes de produção.

Aviso!
Se aplicável, a VLAN ou a VPN aumenta o nível de segurança do sistema de vigilância combinado à infraestrutura de TI existente.

Além de proteger o sistema de vigilância contra o acesso não autorizado na infraestrutura de TI compartilhada, é necessário ficar de olho em quem tem permissão para conectar à rede como um todo.

4.8.3 Desativar portas de switches não usadas

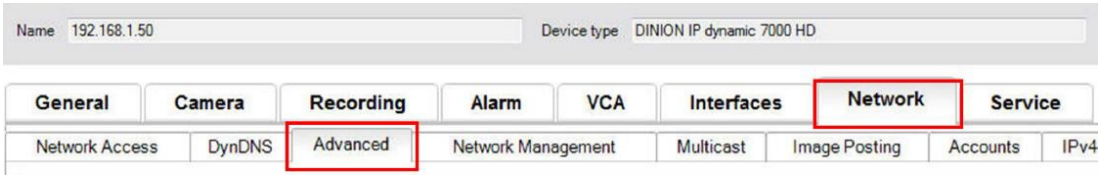
A desativação de portas de rede não usadas garante que os dispositivos não usados não tenham acesso à rede. Isso diminui o risco de alguém tentar acessar uma sub-rede de segurança conectando o dispositivo a um switch ou a um soquete de rede não usado. A opção para desativar portas específicas é uma opção comum em switches gerenciados, tanto de baixo custo quanto empresarial.

4.8.4 Redes protegidas 802.1x

Todos os dispositivos de vídeo IP da Bosch podem ser configurados como clientes 802.1x. Isso permite que eles sejam autenticados para um Servidor RADIUS e participem de uma rede protegida. Antes de colocar os dispositivos de vídeo na rede protegida, você precisará conectar diretamente do laptop de um técnico ao dispositivo de vídeo para inserir credenciais válidas, conforme detalhado nas etapas a seguir.

Os serviços 802.1x podem ser facilmente configurados por meio do Configuration Manager (Gerenciador de configuração).

1. No Configuration Manager (Gerenciador de configuração), selecione o dispositivo desejado.
2. Selecione a guia **Rede** (Rede) e, em seguida, selecione **Avançado** (Avançado).



3. Localize a parte **802.1x** da página.
4. No menu suspenso **802.1x** , selecione **On** (Ativado).

5. Insira uma **Identidade** (Identidade) e uma **Palavra-passe (Senha) válidas.**
6. Salve as alterações.
7. Desconecte e coloque os dispositivos na rede protegida.

Aviso!
A rede 802.1x em si não fornece uma comunicação segura entre o suplicante e o servidor de autenticação.
Como resultado, o nome de usuário e a senha poderão ser "farejados" da rede. A rede 802.1x pode usar EAP-TLS para garantir a comunicação segura.

Protocolo de Autenticação Extensível - Transport Layer Security (TLS)
O Protocolo de Autenticação Extensível (EAP) fornece suporte para vários métodos de autenticação. O protocolo TLS (Transport Layer Security) fornece autenticação mútua, negociação do pacote de codificações protegido por integridade e troca de chaves entre dois pontos de extremidade. O protocolo EAP-TLS inclui suporte para autenticação mútua baseada em certificados e derivação de chaves. Em outras palavras, o protocolo EAP-TLS encapsula o processo em que o servidor e o cliente enviar certificado um ao outro.

Aviso!
Consulte a Documentação técnica (White Paper) específica *Network Authentication - 802.1x - Secure the Edge of the Network*, disponível no catálogo de produtos online do Bosch Security Systems em:
http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

5 Operação segura

5.1 Separação de rede

Se possível, o dispositivo deve ser operado em uma rede separada (por exemplo, usando VLANs) com restrições de acesso para limitar o tráfego de transmissão e proteger o dispositivo contra ataques de rede.

5.2 Armazenamento seguro de chaves no cofre de hardware

As chaves privadas dos certificados são mais bem protegidas quando armazenadas com segurança em um componente de hardware ou cofre de hardware. Esses chips fornecem proteção contra acesso não autorizado a chaves privadas, mesmo quando o dispositivo está fisicamente aberto para obter acesso.
Nas câmeras da Bosch, essas chaves são armazenadas em um criptocoprocessador separado ou elemento seguro (secure element, SE). Ambos fornecem armazenamento seguro, bem como funções criptográficas que nunca expõem chaves privadas a locais ou memória onde poderiam ser recuperadas.
Em estações de trabalho e servidores, geralmente um chip de TPM (Trusted Platform Module, Módulo de Plataforma Confiável) está disponível. Bibliotecas e funções criptográficas devem ser configuradas para usar o armazenamento do TPM sempre que possível.

5.3 Certificados de dispositivo exclusivos

Embora geralmente haja um certificado padrão autoassinado em todos os dispositivos com capacidade para TLS ou HTTPS, esse certificado não deve ser considerado suficiente apenas para autenticação, já que não protege contra um ataque man-in-the-middle (MITM).

Se forem implantados dispositivos em um ambiente em que etapas adicionais são necessárias para validar a identidade de cada dispositivo de vídeo IP individual, novos certificados e chaves privadas poderão ser criados e carregados para os próprios dispositivos de vídeo. Novos certificados podem ser obtidos de uma autoridade de certificação (certificate authority, CA) ou eles podem ser criados com um OpenSSL Toolkit.

Se forem usados dispositivos em redes públicas, será recomendável obter certificados de uma autoridade de certificação pública ou ter certificados próprios assinados dessa forma, o qual também será capaz de verificar a origem e a validade - em outras palavras, a confiança - do certificado do dispositivo.

Há anos, todas as câmeras Bosch vêm com um certificado de dispositivo exclusivo pré-instalado e uma chave privada, derivada do certificado raiz da Bosch e instalada em um ambiente de produção seguro, provando que a câmera é um dispositivo "originalmente fabricado" pela Bosch. Este certificado é usado para conexões HTTPS automaticamente e pode ser usado para identificar e autenticar um dispositivo verificando a cadeia de certificados até o certificado raiz da Bosch.

Aviso!
Os certificados devem ser usados para autenticar um único dispositivo. É recomendável criar um certificado específico por dispositivo, derivado de um certificado raiz.

A variante mais segura de uma implantação de certificado consiste em gerar uma solicitação de assinatura de certificado (CSR) no dispositivo e solicitar um certificado de uma autoridade de certificação interna ou externa.
Com uma solicitação de assinatura de certificado, o dispositivo mantém a chave privada interna e apenas expõe o restante do certificado para ser assinado pela autoridade de certificação. A chave privada é armazenada com segurança no SE da câmera ou, por exemplo, no TPM do dispositivo.
Portanto, sempre que um dispositivo fornecer uma possibilidade de CSR, essa deve ser a maneira preferencial de criar um certificado.

Os certificados podem ser carregados em um dispositivo usando a página da Web do dispositivo de um dispositivo de vídeo ou usando o Configuration Manager.

Upload de certificados usando a página da Web do dispositivo
Os certificados podem ser carregados usando a página da Web de um dispositivo de vídeo. Na página da Web do dispositivo, em **Certificados** (Certificados), novos certificados podem ser adicionados e excluídos, e seu uso pode ser definido.

Upload de certificados usando o Configuration Manager
No Configuration Manager, os certificados podem ser facilmente carregados para um ou vários dispositivos simultaneamente.
Para carregar certificados:
1. No Configuration Manager, selecione um ou mais dispositivos.
2. Clique com o botão direito do mouse em **Upload de Ficheiro** (Carregamento de arquivo) e, em seguida, clique em **Certificado SSL...** (Certificado SSL).
   Uma janela do Windows Explorer é aberta para localizar o certificado para carregamento.

Em sistemas menores, o Configuration Manager fornece uma função de suporte chamada **MicroCA**, que permite criar ou usar uma CA raiz e derivar certificados de dispositivo dela, ou usá-la para assinar as solicitações de assinatura de certificado dos dispositivos, também para vários dispositivos simultaneamente. Para obter mais detalhes, consulte o Manual do Usuário do Configuration Manager.

Consulte
– *Criação de confiança com certificados, página 49*

5.4 Verificação de arquivos de log

Monitorar os arquivos de log é uma parte importante da análise de segurança ou da atividade de manutenção. A revisão regular dos arquivos de log pode revelar problemas de configuração ou violações de segurança, como logins falsos.
Para analisar os arquivos de log e armazená-los por um longo prazo, envie os arquivos de log do dispositivo para um servidor syslog ou um sistema SIEM; por exemplo, uma câmera reservará um espaço fixo para registrar internamente, mas substituirá os logs mais antigos se esse espaço estiver cheio.

5.5 Sistema SIEM

O sistema de gerenciamento de informações e eventos de segurança (Security Information and Event Management, SIEM) é usado para coletar e analisar informações de diferentes dispositivos e sistemas. Os dispositivos podem ser integrados a um sistema SIEM por meio do envio dos logs via protocolo syslog. A análise desses logs pode ajudar na manutenção e detectar erros de configuração ou ataques ao dispositivo (por exemplo, logins falsos).

5.6 PKI

Infraestrutura de Chave Pública (PKI, Public Key Infrastructure) refere-se aos sistemas necessários para gerar e gerenciar certificados digitais. Para HTTPS, autenticação de rede com 802.1x, autenticação de usuário com certificados e outras funções de criptografia, certificados personalizados podem ser instalados no dispositivo.

5.7 AD FS

O Active Directory Federation Services (AD FS) é um serviço oferecido pela Microsoft que permite a autenticação em um Active Directory local (usando um servidor AD FS) ou na nuvem da Azure. Além da autenticação de usuário local com senhas ou autenticação baseada em certificado, a integração de dispositivos em um domínio do Active Directory é possível com o AD FS para autenticar e gerenciar o acesso do usuário centralmente.

5.8 Operação segura de câmeras IP

5.8.1 Criação de confiança com certificados

Todas as câmeras IP da Boschque executam o FW 6.10 ou mais recente usam um repositório de certificados, que pode ser encontrado no menu **Assistência técnica** (Serviço) da configuração da câmera.

Certificados específicos de servidor, certificados de cliente e certificados confiáveis podem ser adicionados ao repositório.

Para adicionar um certificado ao repositório:

1. Na página da Web do dispositivo, navegue para a página **Configuração** (Configuração).
2. Selecione o menu **Assistência técnica** (Serviço) e o submenu **Certificados** (Certificados).
3. Na seção **Lista de ficheiros** (Lista de arquivos), clique em **Adicionar** (Adicionar).
4. Carregue os certificados desejados.
   Depois de concluir o carregamento, os certificados serão exibidos na seção **Lista de utilizações** (Lista de usos).
5. Na seção **Lista de utilizações** (Lista de usos), selecione o certificado desejado.
6. Para ativar o uso dos certificados, a câmera deve ser reinicializada. Para reinicializar a câmera, clique em **Definir**.

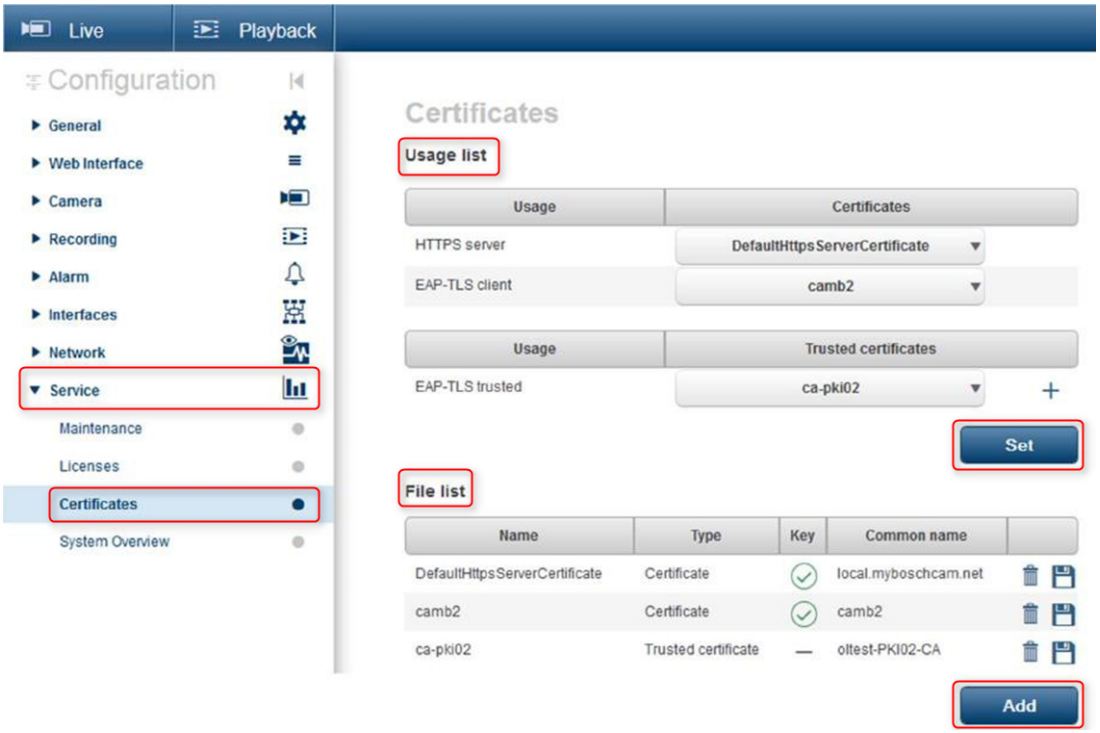


Figura 5.1: Exemplo: Certificados EAP/TLS armazenados em uma câmera Bosch (FW 6.11)

Os certificados são aceitos em formato *.pem, *.cer ou *.crt e devem ser codificados como base64. Eles podem ser carregados como um arquivo combinado ou divididos em partes de chaves e certificados e podem ser carregados como arquivos separados para serem novamente combinados de forma automática.

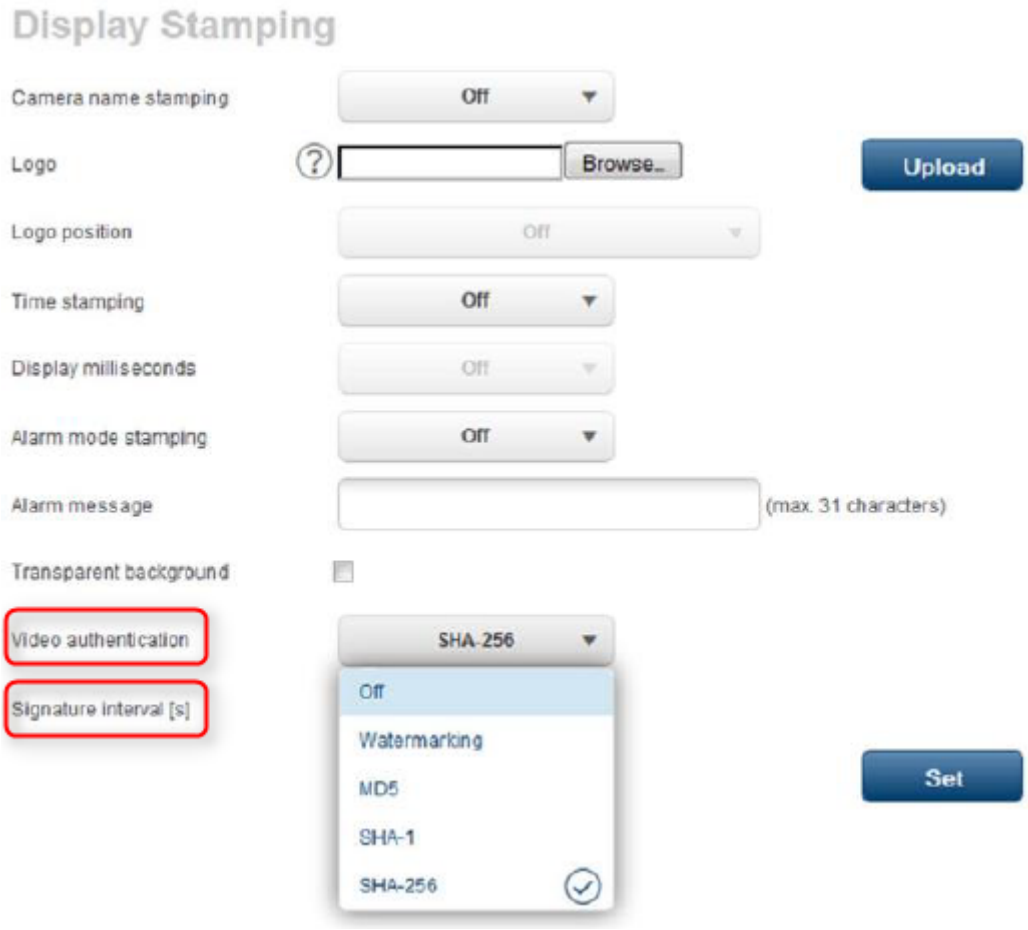
Desde a versão 6.20 do firmware, as chaves privadas PKCS 8 protegidas por senha (criptografadas pelo AES) são compatíveis e devem ser carregadas no formato *.pem com codificação base64.

5.8.2 Autenticação de vídeo

Depois que os dispositivos em um sistema estiverem protegidos e autenticados corretamente, também valerá a pena analisar os dados do vídeo fornecidos por eles. O método é denominado autenticação de vídeo.
A autenticação de vídeo lida exclusivamente com métodos de validação da autenticidade do vídeo. A autenticação de vídeo não lida com a transmissão de vídeo, ou com dados, de alguma maneira.
Antes da versão de firmware 5.9, a marca d' água foi executada por um algoritmo de soma de verificação simples durante o stream de vídeo. Ao usar a marca d' água básica, não há uso de certificados ou criptografia. A soma de verificação é uma avaliação da linha de base da "Invariabilidade de dados" de um arquivo e valida a integridade de um arquivo.
Para configurar a autenticação de vídeo, por exemplo, no navegador da Web:

1. Navegue para o menu **Geral** (Geral) e selecione **Ver marca** (Exibir carimbos).
2. No menu suspenso **Autenticação de vídeo** (Autenticação de vídeo), selecione a opção desejada:
   As versões de firmware 5.9 e posterior fornecem três opções em autenticação de vídeo, além da marca d' água clássica:
   – MD5: resumo da mensagem que produz um valor de hash de 128 bits.

- SHA-1: desenvolvida pela Agência Nacional de Segurança dos Estados Unidos e é uma certificação U.S. Federal Information Processing Standard publicada pela NIST dos Estados Unidos. A autenticação SHA-1 produz um valor de hash de 160 bits.
- SHA-256: o algoritmo SHA-256 gera um hash de 256 bits (32 bytes) de tamanho fixo e quase exclusivo.



Aviso!
Hash é uma função unidirecional, que não pode ser novamente descriptografada.

Ao utilizar a autenticação de vídeo, cada pacote de um stream de vídeo tem um valor de hash. Esses hashes são incorporados no stream de vídeo e misturados com os dados de vídeo. Isso garante a integridade do conteúdo do stream.

Os hashes são assinados em períodos regulares, definidos pelo intervalo de assinatura, usando a chave privada do certificado armazenado no TPM do dispositivo. As gravações de alarme e as alterações de bloco nas gravações de iSCSI estão todas fechadas com uma assinatura para garantir a autenticidade contínua do vídeo.

Aviso!
O cálculo da assinatura digital exige capacidade de computação que pode influenciar no desempenho geral de uma câmera se foi feito com muita frequência. Portanto, deve ser escolhido um intervalo razoável.

Como os hashes e as assinaturas digitais estão incorporados no stream de vídeo, também serão armazenados na gravação, permitindo a autenticação de vídeo também para reprodução e exportações.

6 Gerenciamento de atualizações de segurança

Antes de operar o dispositivo pela primeira vez, instale a versão mais recente do software aplicável. Para obter consistência de funcionalidade, compatibilidade, desempenho e segurança, atualize regularmente o software ao longo da vida útil do dispositivo. Siga as instruções na documentação do produto sobre as atualizações de software.
Os links a seguir contêm mais informações:

- Informações gerais: https://www.boschsecurity.com/xc/en/support/product-security/
- Conselhos de segurança, com uma lista de vulnerabilidades identificadas e soluções propostas: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

A Bosch não assume nenhuma responsabilidade por quaisquer danos causados pela operação de seus produtos com componentes de software desatualizados.

É possível encontrar as versões mais recentes de firmware e software na loja de downloads da Bosch Security and Safety Systems:
https://downloadstore.boschsecurity.com/
Para dispositivos conectados ao Remote Portal, os usuários podem receber uma notificação por e-mail sobre as atualizações de firmware disponíveis por meio do serviço Remote Alert.
Pacotes de download mais abrangentes são distribuídos por meio do catálogo de produtos da Bosch Security and Safety Systems:
https://www.boschsecurity.com

7 Monitoramento de segurança

Como os requisitos mudam constantemente, 100% de segurança nunca é garantido. Portanto, um processo estruturado de gerenciamento de vulnerabilidades e incidentes é estabelecido na Bosch para gerenciar profissionalmente possíveis vulnerabilidades e incidentes de segurança do produto.

O tratamento sistemático profissional das vulnerabilidades de segurança relatadas, bem como a transparência para com o cliente, é muito importante para nós. É por isso que investigamos todos os relatórios de vulnerabilidade. Realizamos uma avaliação das vulnerabilidades de segurança do produto de acordo com o Common Vulnerability Scoring System (CVSS) ou Sistema de Pontuação de Vulnerabilidades Comuns. O CVSS é um padrão da indústria gratuito e aberto para avaliar a gravidade das vulnerabilidades de segurança do sistema de computador. As pontuações são calculadas com base em uma fórmula que depende de várias métricas que aproximam a facilidade de exploração e o impacto da exploração. As pontuações variam de 0 a 10, sendo 10 a mais grave.

Se uma vulnerabilidade de segurança for identificada no produto ou na solução, ela será informada aos clientes, juntamente com a publicação de um aviso de segurança. Todos os avisos de segurança contêm:

- Descrição da vulnerabilidade com referência a Common Vulnerabilities and Exposures (CVE) e pontuação do CVSS.
- Identidade de produtos afetados conhecidos e versões de software/hardware.
- Informações sobre fatores atenuantes e soluções alternativas.
- Linha do tempo e localização das correções disponíveis ou outras medidas corretivas.

Você pode encontrar a lista de avisos de segurança publicados em nosso site https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html.
Sempre que você achar que identificou uma vulnerabilidade ou qualquer outro problema de segurança relacionado a um produto ou serviço da Bosch, entre em contato com a Equipe de Resposta a Incidentes de Segurança de Produtos Bosch (PSIRT): https://psirt.bosch.com.

8 Descarte e descomissionamento seguros

Em determinado ponto no ciclo de vida do produto ou sistema, talvez seja necessário substituir ou descartar o dispositivo ou componente. Como eles podem conter dados confidenciais, como credenciais ou certificados, exclua esses dados de forma completa e segura.

É possível redefinir a maioria dos dispositivos para o padrão de fábrica.
Na maioria das câmeras e codificadores IP, você pode usar o botão de redefinição (reset). Nos casos em que não há botão de redefinição, utilize a função padrão de fábrica por meio da interface da Web antes de retirá-los da rede.
Todos os usuários e suas respectivas senhas serão excluídos e as configurações, redefinidas para os padrões de fábrica. Todos os certificados e as respectivas chaves que estavam armazenados no TPM ou elemento seguro também serão excluídos.

Outros dispositivos podem ter opções diferentes para serem redefinidos para o padrão de fábrica. Consulte as instruções na respectiva documentação do usuário para conhecer os procedimentos corretos de descarte.
Servidores e estações de trabalho também podem ter certificados e credenciais armazenados. Use as ferramentas e métodos adequados para garantir que seus dados relevantes sejam excluídos com segurança durante o descomissionamento ou antes do descarte.

Recomenda-se também redefinir os dispositivos para o padrão de fábrica caso eles devam ser movidos para outra instalação que possa usar outras credenciais ou certificados.

Aviso!
Consulte as instruções na respectiva documentação do usuário para conhecer os procedimentos corretos de descarte.

9 Informações adicionais

Para mais informações, download de software e documentação, acesse a página do produto correspondente no catálogo de produtos:
http://www.boschsecurity.com

Glossário

802.1x

O padrão IEEE 802.1x fornece um método geral para autenticação e autorização em redes IEEE-802. A autenticação é realizada por meio do autenticador, que verifica as informações de autenticação transmitidas usando um servidor de autenticação (consulte servidor RADIUS) e aprova ou nega o acesso aos serviços oferecidos (LAN, VLAN ou WLAN) de maneira adequada.

autenticação

Processo de verificação da autenticidade de um fluxo de vídeo. O usuário pode iniciar um processo de autenticação. Se forem encontrados dados não autênticos, uma mensagem será exibida.

DHCP

Dynamic Host Configuration Protocol: usa um servidor apropriado para permitir a atribuição dinâmica de um endereço IP e outros parâmetros de configuração para computadores em uma rede (Internet ou LAN)

dispositivo

Componente de hardware como câmera, codificador/decodificador, NVR, DiBos, matriz analógica, ponte ATM/POS.

Endereço IPv4

Um número de 4 bytes que define exclusivamente cada unidade na Internet. Geralmente é escrito em notação decimal com pontos (por exemplo, "209.130.2.193")

Grupo de usuários

Grupos de usuários são usados para definir atributos de usuários comuns, como permissões, privilégios e prioridade de PTZ. Ao se tornar membro de um grupo, um usuário herda automaticamente todos os atributos do grupo.

HTTP

Hypertext Transfer Protocol: protocolo para transmissão de dados através de uma rede

HTTPS

Hypertext Transfer Protocol Secure (Protocolo de Transferência de Hipertexto Seguro): criptografa e autentica a comunicação entre o servidor Web e o navegador

LAN

Local Area Network. É uma rede que conecta dispositivos dentro de uma área geográfica confinada.

Máscara de rede

Uma máscara que explica qual parte de um endereço IP é o endereço de rede e qual parte é o endereço do host. Geralmente é escrito em notação decimal com pontos (por exemplo, "255.255.255.192").

Multicast

Comunicação entre um único transceptor e vários receptores em uma rede pela distribuição de um único fluxo de dados na rede para vários receptores em um grupo definido. O requisito para a operação multicast é uma rede compatível com multicast com implementação do protocolo UDP e do protocolo IGMP.

ONVIF

Open Network Video Interface Forum (Fórum Aberto de Interface de Vídeo em Rede). Padrão global para produtos de vídeo em rede. Os dispositivos compatíveis com ONVIF podem fazer a troca de vídeos ao vivo, áudio, metadados e informações de controle e garantem que sejam descobertos e conectados automaticamente a aplicações de rede, como sistemas de gerenciamento de vídeo.

proteção

Processo de aumentar a segurança de um sistema usando apenas software dedicado necessário para a operação do sistema, aplicando configurações de proteção específicas e removendo software não obrigatório.

RCP+

Remote Control Protocol: um protocolo de propriedade da Bosch que usa portas estáticas específicas para detectar e se comunicar com dispositivos de vídeo IP da Bosch

RTSP

Real Time Streaming Protocol (Protocolo de Transmissão em Tempo Real). Um protocolo de rede que permite controlar a transmissão contínua de dados audiovisuais ou software em redes baseadas em IP.

Servidor RADIUS

Remote Authentication Dial-In User Service: um protocolo cliente/servidor para autenticação, autorização e contabilização de usuários com conexões dial-up em uma rede de computadores. RADIUS é o padrão de fato para autenticação central de conexões dial-up via Modem, ISDN, VPN, LAN sem fio (consulte 802.1x) e DSL.

SNMP

Simple Network Management Protocol (Protocolo Simples de Gerenciamento de Redes); um protocolo de gerenciamento de rede usado para administrar e monitorar componentes de rede

SSL

Secure Sockets Layer (Camada Segura de Soquetes); um protocolo de criptografia desatualizado para transmissão de dados em redes baseadas em IP (consulte TLS).

TCP

Transmission Control Protocol (Protocolo de Controle de Transmissão). Protocolo de comunicação baseado em conexão usado para transmitir dados por uma rede IP. Oferece uma transmissão de dados confiável e ordenada.

Telnet

Protocolo de login com o qual os usuários podem acessar um computador remoto (Host) na Internet

TLS

Transport Layer Security (Segurança da Camada de Transporte). TLS 1.0 e 1.1 são os desenvolvimentos avançados padrão do SSL 3.0 (consulte SSL). Dispositivos modernos usam TLS 1.2 ou 1.3

TTL

Time-To-Live; ciclo de vida de um pacote de dados em transferências de estação

UDP

User Datagram Protocol (Protocolo de Datagrama do Usuário). Um protocolo sem conexão usado para trocar dados em uma rede IP. O UDP é mais eficiente que o TCP para transmissão de vídeo devido à menor sobrecarga.

VPN

Uma rede privada virtual (virtual private network, VPN) implementa uma rede privada dentro de uma rede pública, como a Internet. O tráfego de rede dentro da VPN é criptografado e, portanto, protegido contra espionagem.

Wide Area Network

Uma rede de longa distância usada para estender ou conectar redes locais localizadas remotamente

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com

Building solutions for a better life.

202302091957