



Guia de segurança de dados e vídeo IP da Bosch



BOSCH

pt-BR

Conteúdo

1	Introdução	5
2	Dispositivos de vídeo IP da Bosch	6
3	Atribuição de endereços IP	7
3.1	Gerenciamento do DHCP	9
4	Contas de usuário e senhas	10
4.1	Aplicação de senhas	10
4.2	Página da Web do dispositivo	11
4.3	Gerenciador de configuração	13
4.4	DIVAR IP 2000/DIVAR IP 5000	13
4.5	Instalação independente do VRM	14
4.6	Bosch Video Management System (Sistema de Gerenciamento de Vídeos da Bosch)	15
4.6.1	Bosch VMS/DIVAR IP 3000/DIVAR IP 7000: proteção por senha do dispositivo	15
4.6.2	Bosch VMS/DIVAR IP 3000/DIVAR IP 7000: proteção por senha padrão	15
4.6.3	Configuração do Bosch VMS e definições do VRM	16
4.6.4	Bosch VMS/DIVAR IP 3000/DIVAR IP 7000: comunicação criptografada para câmeras	17
5	Proteção de acesso a dispositivo	19
5.1	Uso geral da porta de rede e transmissão de vídeo	19
5.1.1	Uso das portas HTTP, HTTPS e de vídeo	20
5.1.2	Software de vídeo e seleção de porta	20
5.1.3	Acesso Telnet	21
5.1.4	RTSP: Real Time Streaming Protocol	22
5.1.5	UPnP: Universal Plug and Play	23
5.1.6	Multicasting	23
5.1.7	Filtragem de IPv4	24
5.1.8	SNMP	25
5.2	Base temporal segura	26
5.3	Serviços com base na nuvem	27
6	Proteção de armazenamento	29
7	Proteção de servidores	30
7.1	Servidores Windows	30
7.1.1	Configurações recomendadas de hardware do servidor	30
7.1.2	Configurações de segurança recomendadas do sistema operacional Windows	30
7.1.3	Atualizações do Windows	30
7.1.4	Instalação de software antivírus	30
7.1.5	Configurações recomendadas do sistema operacional Windows	30
7.1.6	Ativar Controle de Conta de Usuário no servidor	31
7.1.7	Desativar Reprodução Automática	31
7.1.8	Dispositivos Externos	32
7.1.9	Configuração de atribuição de direitos do usuário	32
7.1.10	Protetor de tela	33
7.1.11	Ativar configurações de política de senha	33
7.1.12	Desativar serviços não essenciais do Windows	34
7.1.13	Contas de usuário do sistema operacional Windows	34
7.1.14	Ativar firewall no servidor	35
8	Proteção de clientes	36
8.1	Estações de Trabalho do Windows	36
8.1.1	Configurações recomendadas do hardware de Estação de Trabalho do Windows	36
8.1.2	Configurações de segurança recomendadas do sistema operacional Windows	36

8.1.3	Configurações recomendadas do sistema operacional Windows	36
8.1.4	Ativar Controle de Conta de Usuário no servidor	36
8.1.5	Desativar Reprodução Automática	37
8.1.6	Dispositivos Externos	37
8.1.7	Configuração de atribuição de direitos do usuário	38
8.1.8	Protetor de tela	39
8.1.9	Ativar configurações de política de senha	39
8.1.10	Desativar serviços não essenciais do Windows	39
8.1.11	Contas de usuário do sistema operacional Windows	40
8.1.12	Ativar firewall na estação de trabalho	41
9	Proteção do acesso à rede	42
9.1	VLAN: Virtual LAN	42
9.2	VPN: Virtual Private Network	42
9.3	Desativar portas de switches não usadas	43
9.4	Redes protegidas 802.1x	43
9.4.1	Protocolo de Autenticação Extensível - Transport Layer Security (TLS)	43
10	Criação de confiança com certificados	44
10.1	Protegido em um Módulo de plataforma confiável (TPM) seguro	44
10.2	Certificados TLS	45
10.2.1	Página da Web do dispositivo	45
10.2.2	Gerenciador de configuração	45
11	Autenticação de vídeo	47

1 Introdução

Embora todas as organizações no ambiente atual possam ter procedimentos e políticas de segurança cibernética no local, os padrões podem variar de organização para organização com base em muitos fatores, como tamanho, região e setor.

Em fevereiro de 2014, o National Institute of Standards and Technology (NIST) introduziu a Cyber Security Framework. Essa estrutura é baseada na Executive Order 13636 e foi criada utilizando as normas, diretrizes e melhores práticas existentes. Ela foi desenvolvida especificamente para reduzir riscos cibernéticos a infraestruturas críticas e seus dispositivos e dados conectados à rede. Essa estrutura está projetada para ajudar as organizações a entender riscos de segurança cibernética externos e internos e é aplicável a organizações de qualquer porte categorizadas entre a Camada 1 (Parcial) e a Camada 4 (Adaptável).

Este documento educativo foi escrito para auxiliar integradores a solidificar produtos de vídeo IP da Bosch para melhor aderirem a políticas e procedimentos de segurança de rede existentes de seus 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 Bosch Configuration Manager para executar as configurações discutidas. Na maioria dos casos, todas as configurações podem ser executadas utilizando o Bosch Video Management System Configuration Client, o Bosch Configuration Manager e a interface da Web integrada de um dispositivo de vídeo.

2 Dispositivos de vídeo IP da Bosch

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 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:

- Auxiliar de IP
- Bosch Configuration Manager
- Bosch Video Management System Configuration Client
- Bosch Video Management System 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".

Nota!

Dica de segurança de dados nº 1

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, ou **IP Address Management**, 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	.11111110
.252	4	/30	2	.11111100
.248	8	/29	3	.11111000
.240	16	/28	4	.11110000
.224	32	/27	5	.11100000
.192	64	/26	6	.11000000
.128	128	/25	7	.10000000

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.

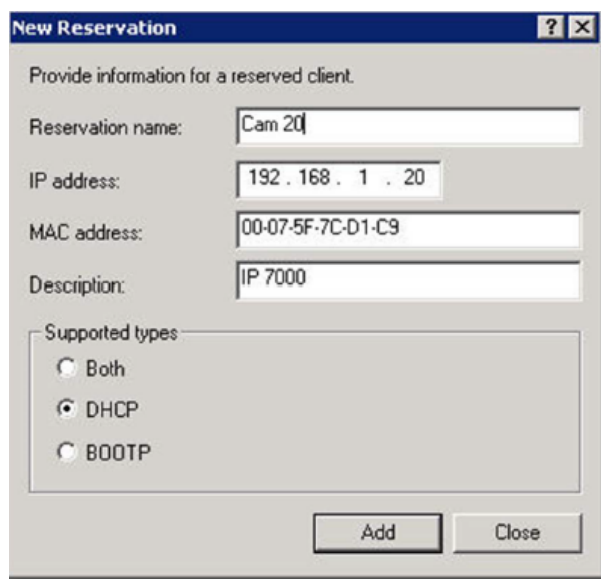
Exemplo:

	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

3.1**Gerenciamento do DHCP**

O IPAM pode utilizar o DHCP 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.

**Nota!****Dica de segurança de dados nº 2**

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 Contas de usuário e senhas

Todos os dispositivos de vídeo 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.

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 que sejam atribuídas senhas a todos os dispositivos de vídeo em rede instalados.



Nota!

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 *Página da Web do dispositivo, Página 11*).

4.1 Aplicação 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.



Nota!

Dica de segurança de dados nº 3

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

**Nota!**

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 aceite esses caracteres, outros softwares de configuração e gerenciamento poderão recusar a aceitação.

4.2

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.

Password

Password 'service'	<input type="password"/>	Strong
Confirm password	<input type="password"/>	
Password 'user'	<input type="password"/>	Medium
Confirm password	<input type="password"/>	
Password 'live'	<input type="password"/>	Weak
Confirm password	<input type="password"/>	
<input type="button" value="Set"/>		



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.

User Management

 Please make sure that all users are password protected.

User name	Group	Type	
service	service	Password	 
user	user	Password	 
live	live	Password	 

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.

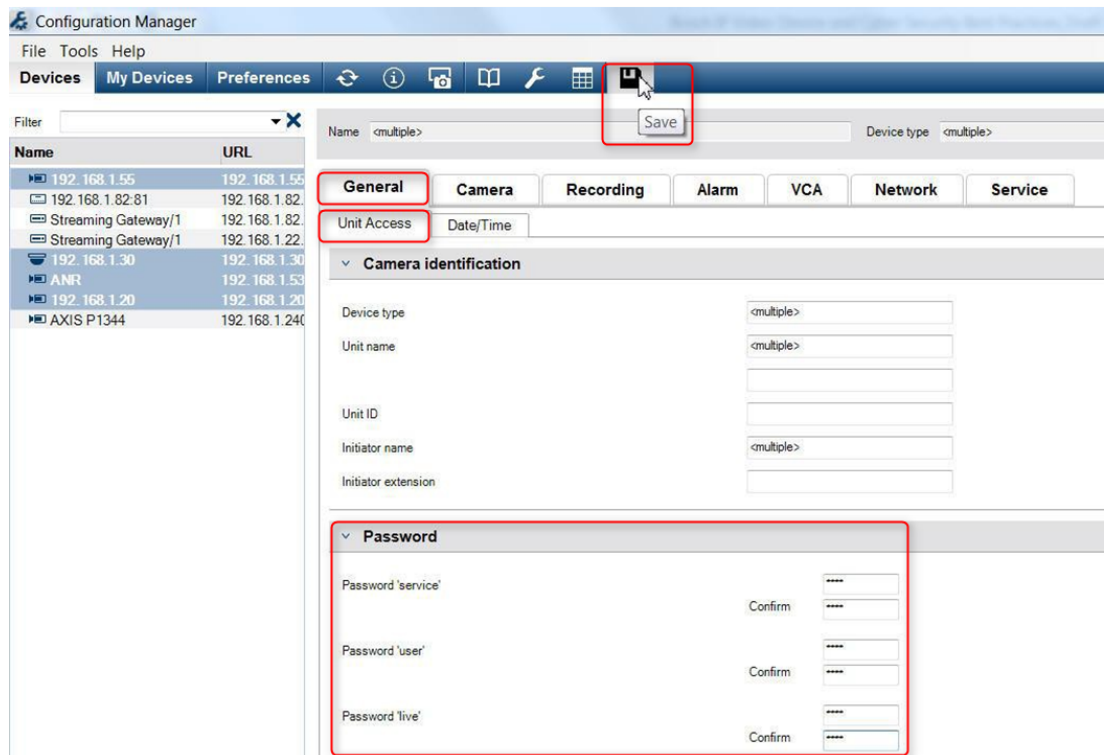
**Nota!**

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.

4.3 Gerenciador de configuração

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 Bosch Video Management System 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.

4.4 DIVAR IP 2000/DIVAR IP 5000

Os aparelhos de gravação DIVAR IP são equipados com um Configuration Wizard (Assistente de configuração) fácil de usar. A atribuição de uma senha de administrador em todo o sistema é obrigatória ao configurar o sistema. Essa senha é atribuída à conta service de todas as câmeras de vídeo IP adicionadas ao sistema. O recurso para adicionar uma senha de conta

user também é fornecido pelo Configuration Wizard (Assistente de configuração), mas a implementação não é obrigatória. O indicador de intensidade de senha está usando um algoritmo semelhante, assim como quando as páginas da Web da câmera estão sendo usadas.

4.5 Instalação independente do VRM

O Bosch 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.

The screenshot displays the 'User Management' configuration page. It features a sidebar with 'Groups' and 'Users' lists. The 'Groups' list contains 'admin', and the 'Users' list contains 'srvadmin'. Below these lists are buttons for 'Add...', 'Edit...', and 'Remove'. To the right, there are input fields for 'Password' and 'Confirm', both masked with dots. Below these is a 'VRM Rights' section with a list of permissions, each with a checkbox: 'View live video', 'Take screenshots', 'Playback recordings', 'Delete recordings', 'Protect recordings', 'Unprotect recordings', 'Export recordings', 'Dual authorization', and 'Use transcoder'. The 'Dual authorization' checkbox is unchecked, while the others are checked.

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.

The screenshot displays the 'Privileges' configuration page. It features a sidebar with 'Privileges', 'Licenses', 'Maintenance', and 'Certificates' tabs. The 'Privileges' tab is selected, showing a table with columns for 'Access' (green for Access, red for No access) and 'Camera 1'. The table lists 'admin' and 'Users' under the 'Users' column, both with 'Access' status.

4.6 Bosch Video Management System (Sistema de Gerenciamento de Vídeos da Bosch)

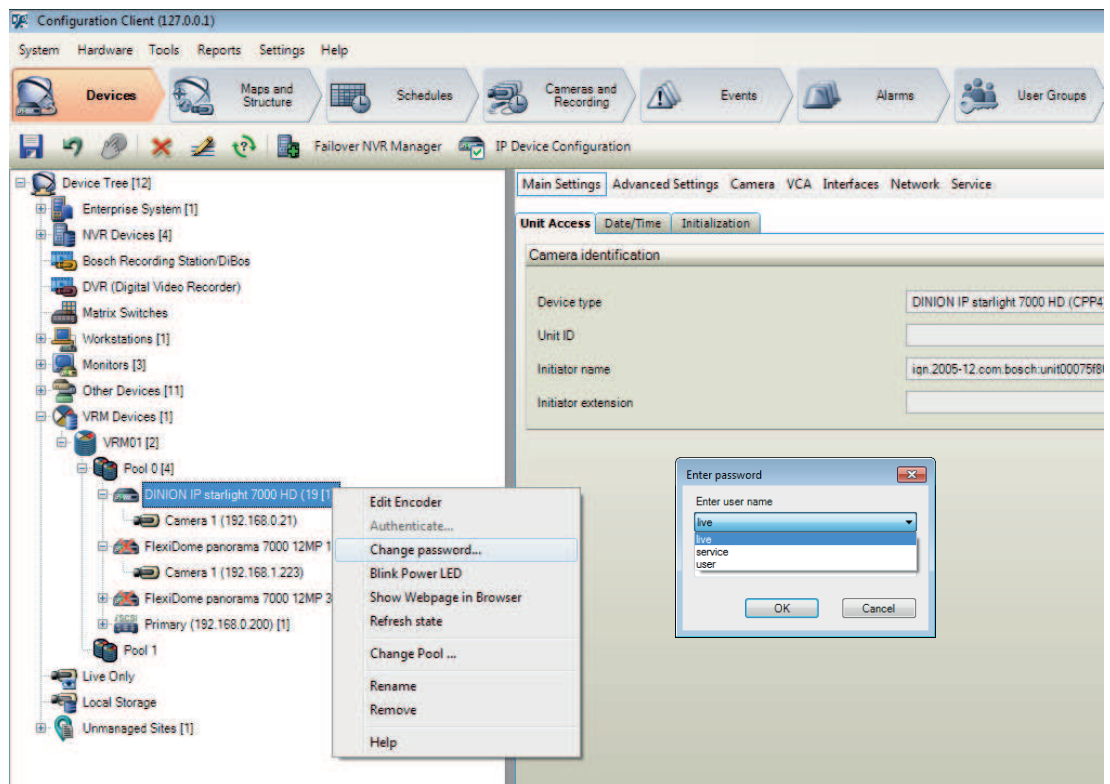
4.6.1 Bosch VMS/DIVAR IP 3000/DIVAR IP 7000: proteção por senha do dispositivo

Câmeras e codificadores, gerenciados por um Bosch Video Management System, 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 Bosch Video Management System.

Para definir uma senha para as contas de usuário integradas no Bosch Video Management System 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.



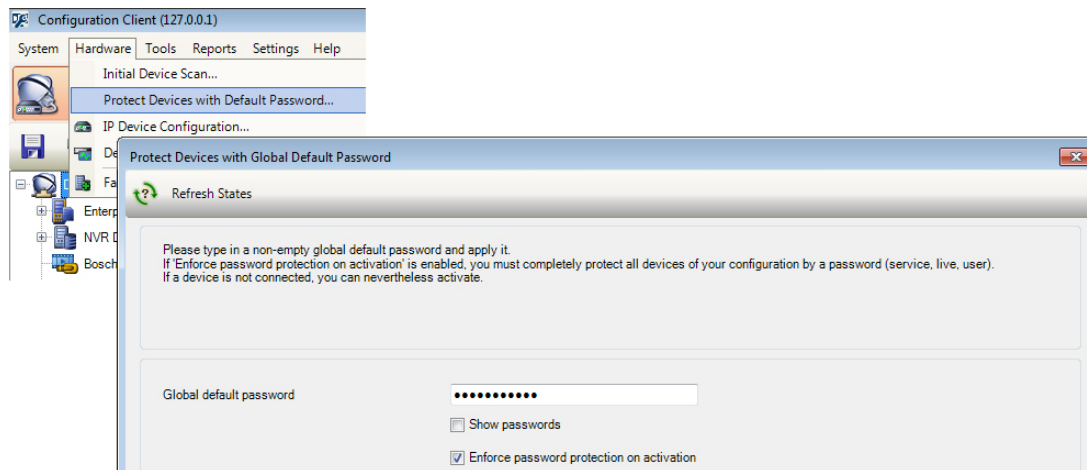
4.6.2 Bosch VMS/DIVAR IP 3000/DIVAR IP 7000: proteção por senha padrão

O Bosch Video Management System 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 Bosch Video Management System Configuration Wizard ao trabalhar com os aparelhos de gravação DIVAR IP 3000 ou DIVAR IP 7000 ou por meio do Configuration Client do Bosch Video Management System em qualquer sistema.

Para acessar o menu de senhas globais no Configuration Client do Bosch Video Management System:

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 a protecção por palavra-passe durante a activação** (Impor protecção 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.

**Nota!**

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.

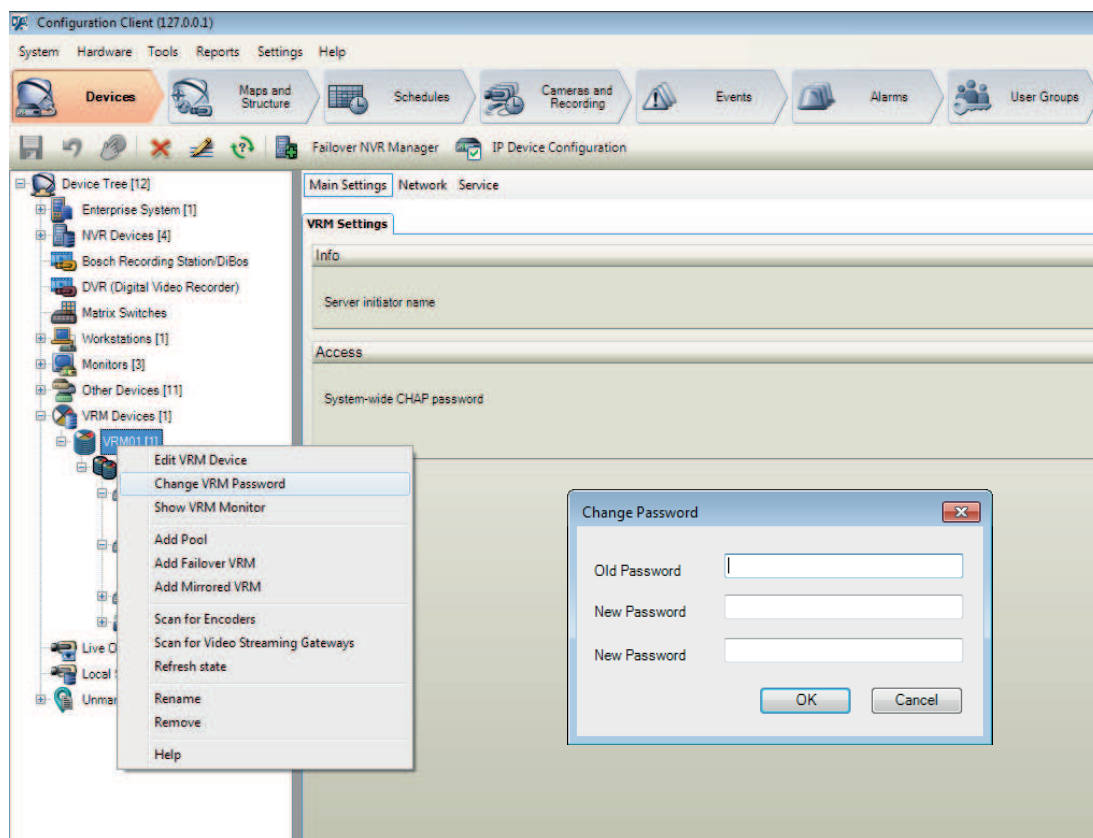
4.6.3

Configuração do Bosch VMS e definições do VRM

Por padrão, o Bosch Video Management System usa a conta de administração integrada **srvadmin** para conectar ao Video Recording Manager com uma protecção por senha. Por evitar o acesso não autorizado ao Video Recording Manager, a senha de administração **srvadmin** deverá ser protegida por uma senha complexa.

Para alterar a senha da conta **srvadmin** no Configuration Client do Bosch Video Management System:

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**.



4.6.4

Bosch VMS/DIVAR IP 3000/DIVAR IP 7000: comunicação criptografada para câmeras

Desde o Bosch Video Management System 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 Bosch Video Management System pode ser criptografada.

Depois de ativar a conexão segura na caixa de diálogo **Editar Codificador**, o Bosch Video Management System 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 Bosch Video Management System 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).

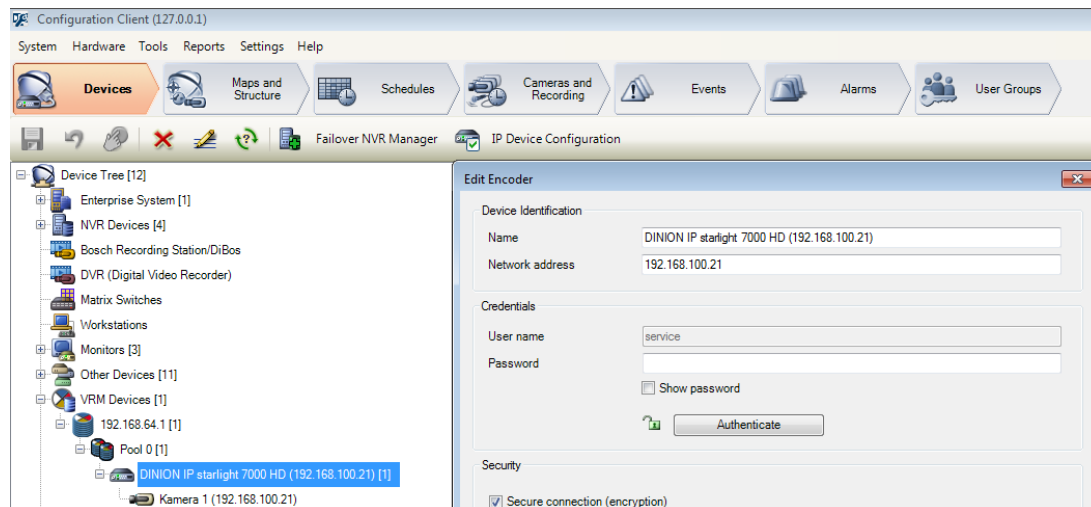
Para dispositivos legados que não são compatíveis com HTTPS, a cadeia de conexão permanece inalterada (RCP+).

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 Bosch Video Management System:

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 (criptação) (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 19).

**Nota!**

O Bosch VMS é compatível apenas com a porta 443 padrão do HTTPS. O uso de portas diferentes não é permitido.

5 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.

5.1 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+) 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 Bosch Video Management System 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 20*). 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.

**Nota!**

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.

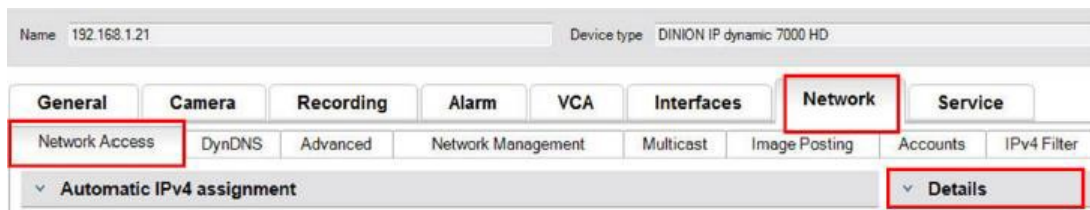
**Nota!****Dica de segurança de dados nº 4**

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.

5.1.1**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)**

**Nota!**

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.

5.1.2**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 Bosch Video Management System estiver configurado para "TCP tunneling" (Túnel TCP), todas as transmissões de vídeo na rede serão feitas pela porta HTTP 10000.

**Nota!**

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

**Nota!****Dica de segurança de dados nº 5**

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.

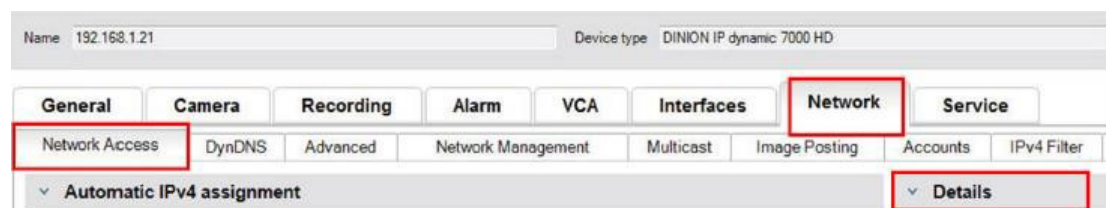
5.1.3**Acesso Telnet**

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.

**Nota!****Dica de segurança de dados nº 6**

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.

**Nota!****Dica de segurança de dados nº 7**

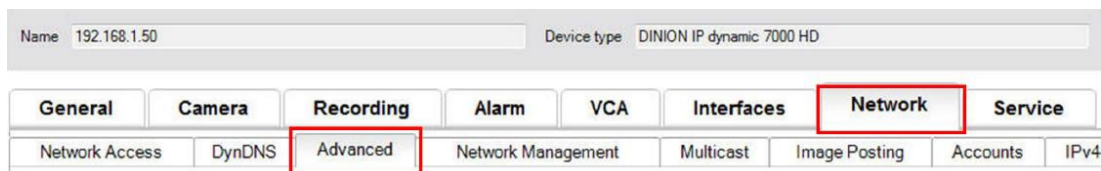
Desde a versão de firmware 6.20, o Telnet também é suportado por meio dos assim-chamados "soquetes da Web", os quais usam conexões HTTPS seguras. Os soquetes da Web não estão usando a porta Telnet padrão e oferecem uma maneira segura de acessar a interface de linha de comando do dispositivo IP, se necessário.

5.1.4**RTSP: Real Time Streaming Protocol**

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

**Nota!****Dica de segurança de dados nº 8**

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.

**Nota!**

Para obter mais detalhes sobre o RTSP, consulte a nota do serviço técnico "Uso do RTSP com dispositivos Bosch VIP" no catálogo de produtos online do Bosch Security Systems no link a seguir:

http://resource.boschsecurity.com/documents/RTSP_VIP_Configuration_Note_enUS_9007200806939915.pdf

5.1.5

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**.



Nota!

Dica de segurança de dados nº 9

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.

5.1.6

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 (time-to-live, vida útil) 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

The screenshot shows the 'Network' configuration page. The 'Multicast' sub-tab is selected. It displays settings for two multicast streams and the TTL value.

Stream	Enable	Multicast Address	Port	Streaming
Multicast Stream 1	<input type="checkbox"/>	0.0.0.0	60010	<input type="checkbox"/>
Multicast Stream 2	<input checked="" type="checkbox"/>	226.3.209.201	60020	<input type="checkbox"/>

Multicast TTL: Packet TTL is set to 64.

Nota!**Dica de segurança de dados nº 10**

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.

5.1.7**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).

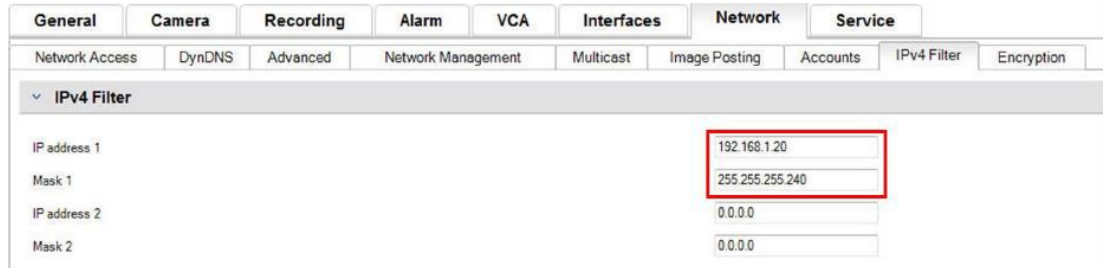
The screenshot shows the 'IPv4 Filter' configuration page. The 'Network' tab is selected, and the 'IPv4 Filter' sub-tab is active. The 'Name' field contains '192.168.1.21' and the 'Device type' is 'DINION IP dynamic 7000 HD'.

Nota!

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.

Nota!

Dica de segurança de dados nº 11



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.

5.1.8

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.

Nota!**Dica de segurança de dados nº 12**

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 deve ser usado apenas quando é possível assegurar que a rede está fisicamente protegida contra acesso não autorizado.

Até a data atual, as câmeras Bosch são compatíveis apenas com SNMPv1. Desative o protocolo SNMP caso não o utilize.

5.2

Base temporal segura

Além do protocolo Time e SNTP, 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.

**Nota!****Dica de segurança de dados nº 13**

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

5.3

Serviços com base na nuvem

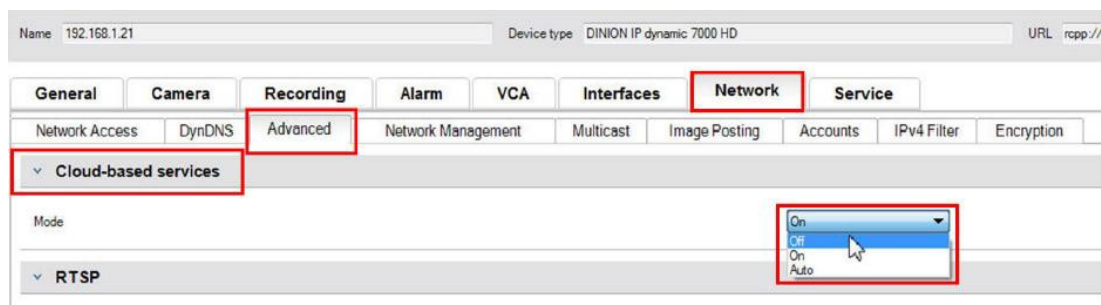
Todos os dispositivos de vídeo IP da Bosch podem se comunicar com os **Serviços com base na nuvem** da Bosch. Dependendo da região de implantação, isso permite que os dispositivos de vídeo IP encaminhem alarmes e outros dados para uma estação central.

Existem três modos de operação para os **Serviços com base na nuvem**:

- **On** (Ativado):
O dispositivo de vídeo sondará constantemente o Servidor de nuvem.
- **Auto** (Automático) (default):
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 com base na nuvem** podem ser facilmente desativados 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 **Serviços com base na nuvem** (Serviços com base na nuvem) da página.
4. No menu suspenso, selecione **Off** (Desativado).

**Nota!****Dica de segurança de dados nº 14**

Se você estiver utilizando os **Serviços com base na nuvem** da Bosch, mantenha a configuração padrão.

Em todos os outros casos, alterne o modo de **Serviços com base na nuvem** para **Off** (Desativado).



6 Proteção de armazenamento

As unidades de armazenamento iSCSI devem ser instaladas na área segura. O acesso à área segura deve ser garantido com um sistema de controle de acesso e deve ser monitorado. O grupo de usuários, que tem acesso à sala do servidor central, deve ser limitado a um grupo pequeno de pessoas.

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:

- Por padrão, as unidades iSCSI concedem a todos os inicializadores de iSCSI acesso aos LUNs da iSCSI. Para garantir que apenas os componentes da solução Bosch Video Management (câmeras, codificadores, estações de trabalho e servidores) tenham permissão para acessar os LUNs da iSCSI, o mapeamento padrão de LUNs poderá ser desativado.
Para permitir acesso dos dispositivos aos destinos de iSCSI de um Bosch Video Management System, os Nomes qualificados de iSCSI de todos os componentes no Bosch Video Management System precisam estar configurados em todos os destinos de iSCSI. Isso causa esforços durante a instalação, mas minimiza o risco de perda, fuga ou manipulação de dados de vídeo.
- Use a autenticação de senha por meio do CHAP para garantir que apenas dispositivos conhecidos tenham permissão para acessar o destino da iSCSI. Configure uma senha do CHAP 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 a senha do CHAP for usada em um ambiente VRM do Bosch Video Management System, 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 por meio do 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.

7 Proteção de servidores

7.1 Servidores Windows

Todos os componentes de servidor, como o Bosch VMS Management Server e o servidor Video Recording Manager devem ser colocados em uma área segura. O acesso à área segura deve ser garantido com um sistema de controle de acesso e deve ser monitorado. O grupo de usuários, que tem acesso à sala do servidor central, deve ser limitado a um grupo pequeno de pessoas.

Embora o hardware do servidor esteja instalado em uma área segura, o hardware deverá estar protegido contra acesso não autorizado.

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.1.4 Instalação de software antivírus

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

7.1.5 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 de Grupo Locais (LCP) 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**.

7.1.6

Ativar Controle de Conta de Usuário no servidor

LCP -> 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

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

Enumerar contas de administrador na elevação	Desativado
--	------------

7.1.7

Desativar Reprodução Automática

LCP -> 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
---	---------

7.1.8

Dispositivos Externos

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

Dispositivos: permitir desencanaixe 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

7.1.9

Configuração de atribuição de direitos do usuário

LCP -> 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
Fazer backup de arquivos e pastas	Administradores
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
Depurar programas	Ninguém
Negar acesso a este computador pela rede	Logon Anônimo, Convidado
Negar logon como um trabalho em lotes	Logon Anônimo, Convidado
Negar logon como um serviço	Ninguém
Negar logon local	Logon Anônimo, 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
Gerenciar a auditoria e o log de segurança	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
Traçar um perfil do desempenho do sistema	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

7.1.10**Protetor de tela**

- Ative o protetor de tela protegido por senha e defina o tempo limite:
LCP -> 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

7.1.11**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.

LCP -> 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

7.1.12**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
Áudio do Windows	Desativado
Construtor de Pontos de Extremidade de Áudio do Windows	Desativado

7.1.13**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

LCP -> 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.

7.1.14

Ativar firewall no servidor

- ▶ Ative a comunicação da porta padrão do Bosch VMS de acordo com as portas do Bosch VMS.



Nota!

Dica de segurança de dados nº 15

Consulte a documentação de instalação e do usuário do Bosch VMS para obter as configurações de porta e o uso relevantes. Verifique novamente as configurações sobre atualizações de firmware ou software.

8 Proteção de clientes

8.1 Estações de Trabalho do Windows

Os sistemas operacionais para desktop Windows, usados para aplicativos do Bosch VMS, como o Bosch VMS Operator Client ou o Configuration Client, são instalados fora da área segura. As estações de trabalho precisam 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.

8.1.1 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.

8.1.2 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.

8.1.3 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 de Grupo Locais (LCP) 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**.

8.1.4 Ativar Controle de Conta de Usuário no servidor

LCP -> 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

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

Enumerar contas de administrador na elevação	Desativado
--	------------

8.1.5

Desativar Reprodução Automática

LCP -> 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

8.1.6

Dispositivos Externos

LCP -> 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
---	---------

8.1.7

Configuração de atribuição de direitos do usuário

LCP -> 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
Fazer backup de arquivos e pastas	Administradores
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
Depurar programas	Ninguém
Negar acesso a este computador pela rede	Logon Anônimo, Convidado
Negar logon como um trabalho em lotes	Logon Anônimo, Convidado
Negar logon como um serviço	Ninguém
Negar logon local	Logon Anônimo, 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
Gerenciar a auditoria e o log de segurança	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

Traçar um perfil do desempenho do sistema	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

8.1.8

Protetor de tela

- Ative o protetor de tela protegido por senha e defina o tempo limite:
LCP -> 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

8.1.9

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.

LCP -> 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

8.1.10

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
Áudio do Windows	Desativado
Construtor de Pontos de Extremidade de Áudio do Windows	Desativado

8.1.11

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

LCP -> 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.

8.1.12

Ativar firewall na estação de trabalho

- ▶ Ative a comunicação da porta padrão do Bosch VMS de acordo com as portas do Bosch VMS.



Nota!

Dica de segurança de dados nº 16

Consulte a documentação de instalação e do usuário do Bosch VMS para obter as configurações de porta e o uso relevantes. Verifique novamente as configurações sobre atualizações de firmware ou software.

9 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.

9.1 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 7*) que é similar na camada de rede (camada 3 de OSI).

9.2 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.



Nota!

Dica de segurança de dados nº 17

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.

9.3 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.

9.4 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.



Nota!

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.

9.4.1 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 enviam certificado um ao outro.



Nota!

Dica de segurança de dados nº 18

Consulte o Whitepaper técnico específico "Network Authentication - 802.1x – Secure the Edge of the Network", disponível no catálogo de produtos on-line do Bosch Security Systems em:

http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

10 Criação de confiança com certificados

Todas as câmeras IP da Bosch que 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 reiniciada. Para reinicializar a câmera, clique em **Definir**.

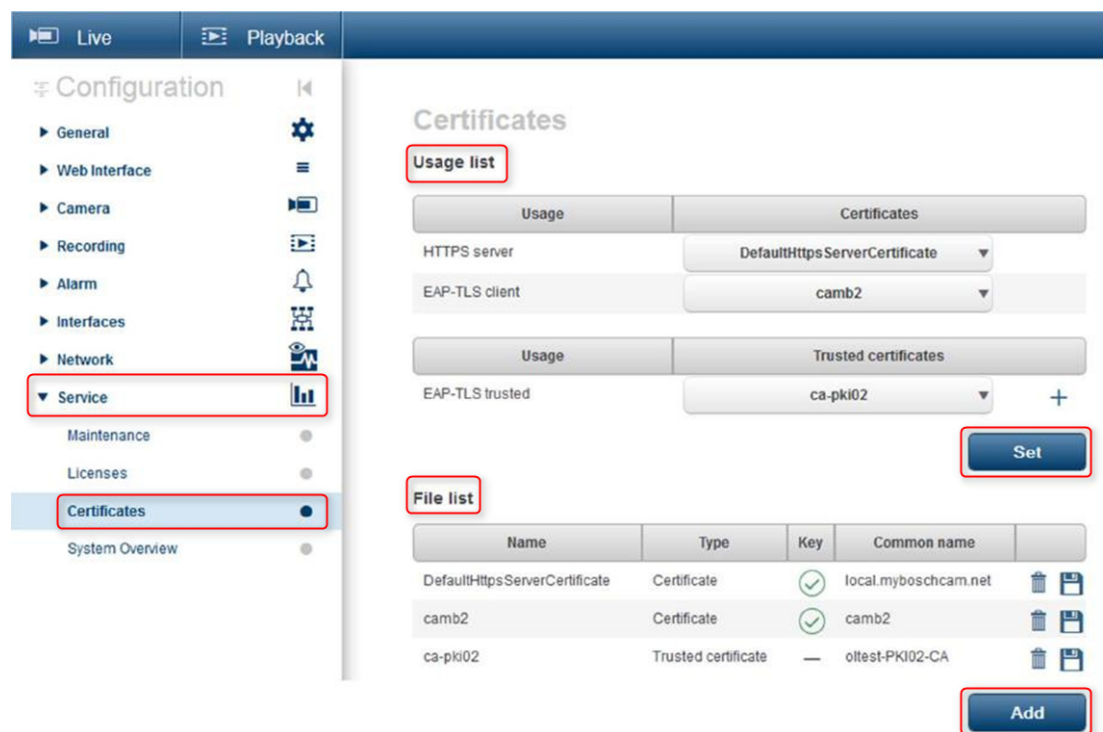


Figura 10.1: Exemplo: Certificados EAP/TLS armazenados em uma câmera Bosch (FW 6.11)

10.1 Protegido em um Módulo de plataforma confiável (TPM) seguro

As chaves são armazenadas em um chip, como se estivessem sendo usadas em SmartCards criptográficos, também chamados "Módulo de plataforma confiável", ou TPM. Esse chip funciona como um cofre para dados críticos, protegendo certificados, chaves, licenças contra o acesso não autorizado mesmo quando a câmera está fisicamente aberta para obter acesso.

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.

10.2 Certificados TLS

Todos os dispositivos de vídeo da Bosch que executam o firmware até FW 6.1x são fornecidos com um certificado TLS pré-instalado e com a chave privada que está sendo usada para conexões HTTPS automaticamente. O certificado e a chave padrão são significativos para fins de teste apenas, uma vez que todos os dispositivos são fornecidos com o mesmo certificado padrão.

Desde o FW 6.20, um certificado TLS autoassinado específico do dispositivo é criado automaticamente quando necessário para conexões HTTPS, permitindo autenticação exclusiva. Esse certificado autoassinado pode ser renovado manualmente, basta excluí-lo. O dispositivo mesmo criará um novo certificado assim que for necessário.

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 (CA) ou eles podem ser criados com um OpenSSL Toolkit, por exemplo.

10.2.1 Página da Web do dispositivo

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

Veja também

– Criação de confiança com certificados, Página 44

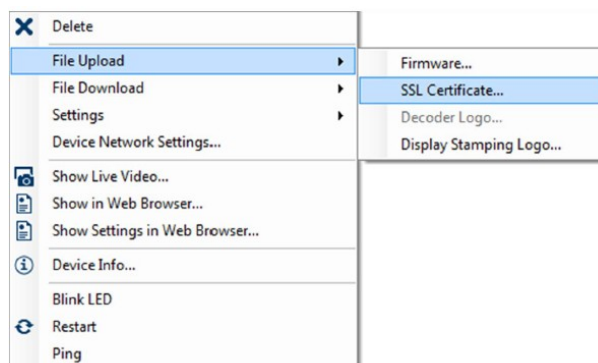
10.2.2 Gerenciador de configuração

No Configuration Manager (Gerenciador de configuração, os certificados podem ser facilmente carregados para um ou vários dispositivos simultaneamente.

Para carregar certificados:

1. No Configuration Manager (Gerenciador de configuração), 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.



**Nota!**

Os certificados podem ser carregados usando o Configuration Manager (Gerenciador de configuração), mas a definição de uso deve ser especificada por meio da página da Web **Certificados** (Certificados).

**Nota!****Dica de segurança de dados nº 19**

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

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.

11 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.

Display Stamping

Camera name stamping: Off

Logo: ? [] Browse... Upload

Logo position: Off

Time stamping: Off

Display milliseconds: Off

Alarm mode stamping: Off

Alarm message: (max. 31 characters)

Transparent background: ☐

Video authentication: SHA-256

Signature interval [s]:

Set

**Nota!**

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.

**Nota!**

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.

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2017