Bosch IP video products

de Leitfaden zu Cybersicherheit

Inhaltsverzeichnis

1 Zweck des Dokuments und Zielgruppe

Die Technologie entwickelt sich mit – manchmal unglaublicher – Geschwindigkeit weiter. Die rasanten Fortschritte bei der Künstlichen Intelligenz (KI) und dem Internet der Dinge (IoT) sowie deren massive Nutzung (AIoT) verändern das Risikoprofil von Produkten und Dienstleistungen. Vorsätzliche böswillige Angriffe werden durch mehr Konnektivität leichter möglich und wahrscheinlicher. Die Bereitstellung sicherer und zuverlässiger Produkte und Dienstleistungen für Kunden ist das Ziel von Bosch.

Dieses Handbuch soll Integratoren dabei helfen, Bosch IP-Videoprodukte so zu härten, dass sie die bestehenden Netzwerksicherheitsrichtlinien und -verfahren ihrer Kunden besser einhalten.

Dieses Handbuch behandelt:
- wichtige Informationen zu Funktionen und Grundlagen von Bosch IP-Videogeräten
- bestimmte Funktionen, die geändert oder deaktiviert werden können
- bestimmte Funktionen, die aktiviert und verwendet werden können
- bewährte Methoden zu Videosystemen und -sicherheit

Dieses Handbuch konzentriert sich in erster Linie auf die Verwendung von Configuration Manager zur Durchführung der besprochenen Konfigurationen. In den meisten Fällen können alle Konfigurationen über BVMS Configuration Client, Configuration Manager und die integrierte Webschnittstelle eines Videogeräts vorgenommen werden.

2 Sicherheitskonzept und Überlegungen

IP-Videoprodukte gehören in der heutigen Netzwerkumgebung zunehmend zur Standardausrüstung, und wie bei jedem IP-Gerät in einem Netzwerk müssen IT-Administratoren und Sicherheitsmanager alle Funktionen und Eigenschaften eines Geräts kennen.

Bei der Verwendung von Bosch IP-Videogeräten sind die Geräte selbst sozusagen der erste Schutzschild. Bosch Encoder und Kameras werden in einer kontrollierten, sicheren Umgebung hergestellt, die regelmäßig geprüft wird. Die Geräte können nur über einen gültigen Firmware-Upload mit Daten beschrieben werden, der spezifisch für Hardwareserie und Chipsatz ist.

Die meisten Bosch IP-Videogeräte sind mit einem integrierten Sicherheitschip ausgestattet, der Funktionen ähnlich denen von Crypto-SmartCards und das sogenannte Trusted Platform Module bietet, kurz TPM. Dieser Chip ist wie ein Tresor für wichtige Daten und schützt Schlüssel, Lizenzen usw. selbst dann vor unbefugtem Zugriff, wenn die Kamera physisch geöffnet wird.

Bosch IP-Videogeräte wurden über 30.000 Anfälligkeits- und Penetrationstests ausgesetzt, die von unabhängigen Sicherheitsanbietern durchgeführt wurden. Bisher wurden keine erfolgreichen Cyber-Attacken auf ein ordnungsgemäß geschütztes Gerät gemeldet.

3 Sichere Installation

3.1 Server und Speichergeräte

Alle Serverkomponenten (z.B. BVMS Management Server and Video Recording Manager Server) und Speichergeräte sollten in einem sicheren Bereich installiert werden. Der Zugang zum gesicherten Bereich muss mit einem Zutrittskontrollsystem kontrolliert und überwacht werden. Die Benutzergruppe, die Zugang zum zentralen Serverraum hat, muss auf eine kleine Personengruppe begrenzt sein.
Obwohl die Server und Speichergeräte in einem sicheren Bereich installiert sind, müssen sie vor unbefugtem Zugriff geschützt werden.

Siehe

- *Härten von Servern, Seite 33*
- *Härten des Speichers, Seite 32*

3.2 Kameras und dezentrale Geräte

Für die Installation von Kameras und dezentralen Geräten sollten Sie einen sicheren Installationsort und die Montageausrichtung wählen. Im Idealfall ist dies ein Montageort, an dem das Gerät weder vorsätzlich noch unbeabsichtigt manipuliert werden kann.

4 Sichere Konfiguration

4.1 Zuweisen von IP-Adressen

Alle Bosch IP-Videogeräte befinden sich derzeit im Auslieferungszustand und sind bereit, eine DHCP IP-Adresse zu akzeptieren.
Wenn in dem aktiven Netzwerk, in dem ein Gerät eingesetzt wird, kein DHCP-Server verfügbar ist, wendet das Gerät – wenn es mit Firmware 6.32 oder höher läuft – automatisch eine link-lokale Adresse aus dem Bereich 169.254.1.0 bis 169.254.254.255 oder 169.254.0.0/16 an.
Mit früherer Firmware weist sich das Gerät die Standard-IP-Adresse 192.168.0.1 zu.
Man kann Bosch IP-Videogeräten mit mehreren Tools eine IP-Adresse zuweisen, einschließlich:

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

Alle Software-Tools ermöglichen das Zuweisen einer einzelnen statischen IPv4-Adresse sowie einer Reihe von IPv4-Adressen für mehrere Geräte gleichzeitig. Dazu gehören die Subnetzmaske und die Standard-Gateway-Adressierung.
Alle Werte für IPv4-Adressen und Subnetzmasken müssen in der sogenannten Dezimalpunktschreibweise eingegeben werden.

Hinweis!
Einer der ersten Schritte zum Minimieren einer internen Cyber-Attacke auf ein Netzwerk durch nicht autorisierte, lokal angeschlossene Netzwerkgeräte ist die Einschränkung der verfügbaren, nicht verwendeten IP-Adressen. Dies erfolgt mithilfe von **IP A**ddress **M**anagement (kurz „IPAM") in Verbindung mit dem Subnetting des verwendeten IP-Adressbereichs.

Beim Subnetting werden Bits vom Host-Abschnitt einer IP-Adresse „geliehen", um ein großes Netzwerk in mehrere kleinere Netzwerke aufzuteilen. Je mehr Bits geliehen werden, desto mehr Netzwerke können erstellt werden, aber jedes Netzwerk unterstützt weniger Host-Adressen.

Suffix	Hosts	CIDR	Geliehen	Binär
.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**

1993 führte die Internet Engineering Task Force (IETF) eines neues Konzept, mit dem IPv4-Adressblöcke flexibler als in der vorherigen Netzklassen-Adressierungsarchitektur zugewiesen werden können. Die neue Methode heißt „Classless Inter-Domain Routing" (CIDR) und wird auch mit IPv6-Adressen verwendet.

IPv4-Netzklassen sind in die Klassen A, B und C mit einer Netzlänge von 8, 16 bzw. 24 Bit und die Klasse D aufgeteilt, die für Multicast-Adressierung verwendet wird.

Beispiel:
Für dieses einfache Beispiel verwenden wir ein Adressszenario der Klasse C. Die Standard-Subnetzmaske einer Adresse der Klasse C ist 255.255.255.0. Bisher wurde bei dieser Maske noch kein Subnetting vorgenommen, darum steht das gesamte letzte Oktett für eine gültige Host-Adressierung zur Verfügung. Wenn wir Bits von der Host-Adresse leihen, haben wir im letzten Oktett die folgenden Möglichkeiten:
.128, .192, .224, .240, .248 und .252.

Wenn die Subnetzmaske 255.255.255.240 (4 Bits) verwendet wird, erstellen wir 16 kleinere Netzwerke, die 14 Host-Adressen pro Subnetz unterstützen.
- Subnetz-ID 0:
  Host-Adressbereich 192.168.1.1 bis 192.168.1.14. Broadcast-Adresse 192.168.1.15
- Subnetz-ID 16:
  Host-Adressbereich 192.168.1.17 bis 192.168.1.30. Broadcast-Adresse 192.168.1.31
- Subnetz-IDs: 32, 64, 96 etc.

Für größere Netzwerke ist die nächstgrößere Netzklasse B erforderlich, oder es muss ein entsprechender CIDR-Block definiert werden.

Beispiel:
Vor der Implementierung Ihres Videoüberwachungsnetzwerks führen Sie eine einfache Berechnung der für das Netzwerk erforderlichen IP-Geräte durch, um Raum für zukünftiges Wachstum zu lassen:
- 20 Video-Arbeitsstation
- 1 zentraler Server
- 1 VRM-Server
- 15 iSCSI-Speicherarrays
- 305 IP-Kameras

Gesamt = 342 IP-Adressen erforderlich

Berücksichtigt man die berechnete Anzahl von 342 IP-Adressen, benötigen wir mindestens ein IP-Adressschema der Klasse B, um so viele IP-Adressen bereitstellen zu können. Die Verwendung der Standard-Subnetzmaske 255.255.0.0 für Klasse B ermöglicht die Verwendung von 65534 IP-Adressen innerhalb des Netzwerks.

Alternativ kann das Netzwerk auch mit einem CIDR-Block mit 23 Bits als Präfix geplant werden, was eine Adresskapazität von 512 Adressen bzw. 510 Hosts bietet.

Indem man ein großes Netzwerks durch Subnetting in kleinere Netzwerke aufteilt oder einen CIDR-Block definiert, können Sie dieses Risiko verringern.

Beispiel:

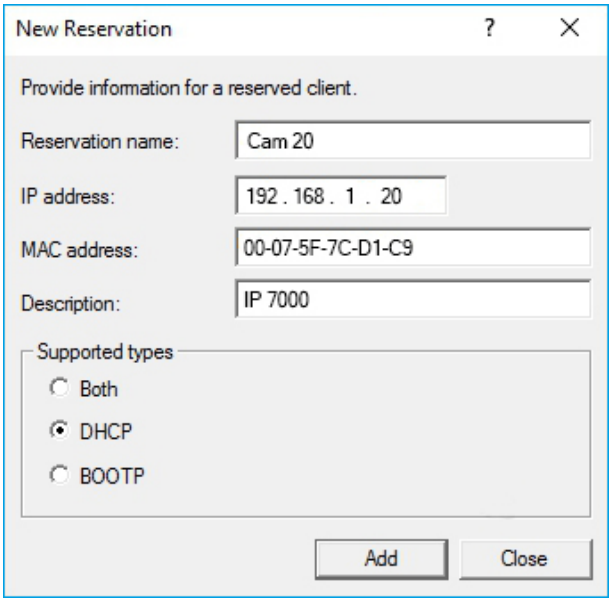
	Standard	**Subnetted**
IP-Adressbereich	172.16.0.0 - 172.16.255.255	172.16.8.0 - 172.16.9.255
Subnetzmaske	255.255.0.0	255.255.254.0

CIDR-Notation	172.16.0.0/16	172.16.8.0/23
Anzahl von Subnetzen	1	128
Anzahl der Hosts	65.534	510
Zusätzliche Adressen	65.192	168

4.1.1 Verwaltender DHCP

IPAM kann DHCP als leistungsstarkes Werkzeug für die Kontrolle und Verwendung von IP-Adressen in Ihrer Umgebung nutzen. DHCP kann so konfiguriert werden, dass ein bestimmter Bereich von IP-Adressen verwendet wird. Es kann auch zum Ausschließen eines Adressbereichs konfiguriert werden.

Wenn Sie DHCP verwenden, wird bei der Implementierung von Videogeräten angeraten, nicht ablaufende Adressreservierungen auf Basis der MAC-Adresse jedes Geräts zu konfigurieren.



Hinweis!
Selbst vor dem Einsatz von IPAM zur Nachverfolgung der IP-Adressverwendung besteht eine bewährte Methode in der Netzwerkverwaltung darin, den Netzwerkzugriff über die Port-Sicherheit auf Edge-Switches zu beschränken, damit beispielsweise nur eine bestimmte MAC-Adresse über einen bestimmten Port Zugriff hat.

4.2 Benutzerkonten und Passwörter

Alle Bosch IP-Videokameras und Encoder werden mit drei integrierten Benutzerkonten geliefert:

- **live**
  Dieses Standardbenutzerkonto ermöglicht nur den Zugriff auf Live-Video-Streaming.
- **user**
  Dieses erweiterte Benutzerkonto ermöglicht den Zugriff auf Live- und aufgezeichnete Videos und Kamerasteuerungsoptionen wie die PTZ-Steuerung.
  Mit diesem Konto hat man keinen Zugriff auf Konfigurationseinstellungen.
- **service**
  Dieses Administratorkonto bietet Zugriff auf alle Gerätemenüs und Konfigurationseinstellungen.

Für jedes der Benutzerkonten muss ein Passwort vergeben werden.
Das Zuweisen von Passwörtern ist ein wichtiger Schritt zum Schutz jedes Netzwerkgeräts. Es wird dringend empfohlen, allen installierten Netzwerkvideogeräten ein Passwort zuzuweisen.

Hinweis!
Bei Firmware-Version 6.30 wurde die Benutzerverwaltung flexibler gestaltet, damit weitere Benutzer und Benutzernamen mit eigenen Passwörtern erstellt werden können. Die früheren Kontoebenen entsprechen jetzt den Benutzergruppenebenen.
Bei Firmware-Version 6.32 wurde eine strengere Passwortrichtlinie eingeführt (weitere Informationen finden Sie unter *Zuweisen von Passwörtern über die Gerätewebseite, Seite 11*).

4.2.1 Zuweisen von Passwörtern

Passwörter können abhängig von der Größe des Videoüberwachungssystems und der verwendeten Software auf verschiedene Arten zugewiesen werden. Bei kleineren Anlagen mit nur wenigen Kameras können Passwörter entweder über die Webseite des Geräts oder Bosch Configuration Manager (unterstützt die gleichzeitige Konfiguration von mehreren Geräten und verfügt über einen Konfigurationsassistenten) zugewiesen werden.

Hinweis!
Wie bereits erwähnt, ist ein Passwortschutz sehr wichtig, um Daten vor potenziellen Cyber-Attacken zu schützen. Dies gilt für alle Netzwerkgeräte in der gesamten Sicherheitsinfrastruktur. Die meisten Unternehmen haben bereits Richtlinien für sichere Passwörter, aber wenn Sie mit einer neuen Anlage ohne festgelegte Richtlinien arbeiten, sollten Sie einige der folgenden bewährten Methoden für den Passwortschutz befolgen:
– Passwörter sollten eine Länge von 8 bis 12 Zeichen haben.
– Passwörter sollten sowohl Groß- als auch Kleinbuchstaben enthalten.
– Passwörter sollten mindestens ein Sonderzeichen enthalten.
– Passwörter sollten mindestens eine Zahl enthalten.

Beispiel:
Wir verwenden den Satz „Sein oder Nichtsein” und wenden unsere Grundregeln zur Erstellung eines sicheren Passworts darauf an:
– S3!n/N!chts3!n

Hinweis!
Bei der Verwendung von Sonderzeichen (z. B. @ & < > :) in Passwörtern gibt es Einschränkungen, da sie eine besondere Bedeutung bei XML und anderen Auszeichnungssprachen haben. Die Webschnittstelle akzeptiert diese Sonderzeichen zwar, bei anderen Verwaltungs- und Konfigurationssoftwares ist dies aber möglicherweise nicht der Fall.

4.2.2 Zuweisen von Passwörtern über die Gerätewebseite

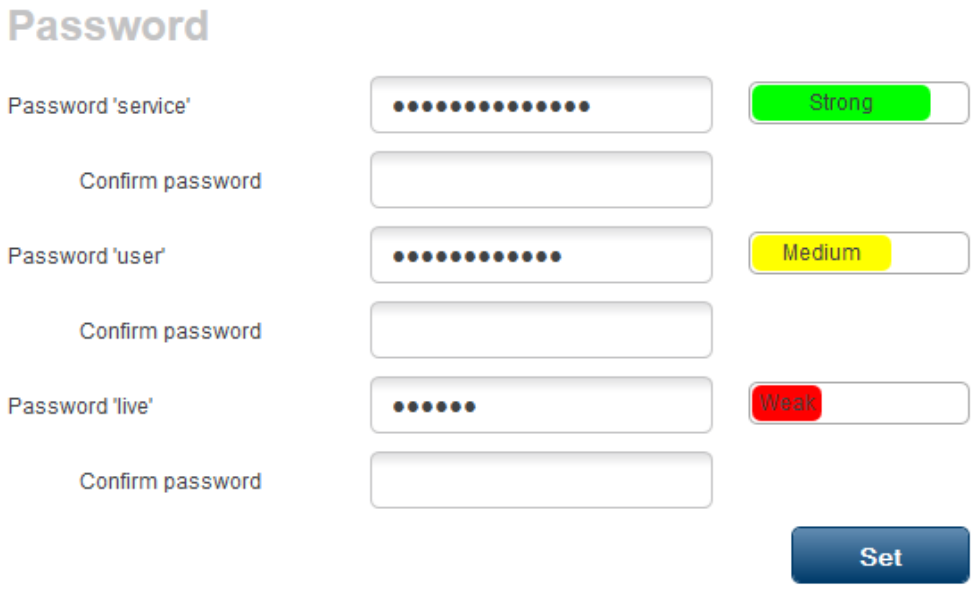
1. Navigieren Sie in der Webseite des Geräts zur Seite **Konfiguration**.
2. Wählen Sie das Menü **Allgemein** und das Untermenü **Benutzerverwaltung** aus (Hinweis: Vor Firmware-Version 6.30 hatte das Untermenü **Benutzerverwaltung** den Namen **Passwort**).

Beim erstmaligen Öffnen der Webseite einer Kamera wird der Benutzer darauf hingewiesen, dass er ein Passwort zuweisen muss, damit der Mindestschutz gewährleistet ist.

Solange kein Passwort festgelegt ist, wird dieser Hinweis bei jeder Aktualisierung der Webseite der Kamera angezeigt. Bei einem Klick auf **OK** werden Sie automatisch zum Menü **Benutzerverwaltung** weitergeleitet.

Bei Firmware-Version 6.30 gab es die Möglichkeit, ein Kontrollkästchen **Nicht anzeigen ...** zu aktivieren. Diese Option wurde in Firmware-Version 6.32 aus Sicherheitsgründen entfernt.

1. Wählen Sie das Menü **Benutzerverwaltung** aus, geben Sie das gewünschte Passwort für jedes der drei Konten ein und bestätigen Sie es.
   Hinweis:
   - Passwörter müssen zuerst für die höchste Zugriffsebene (**Passwort 'service'**) zugewiesen werden.
   - Ab Firmware-Version 6.20 wurde eine neue Anzeige hinzugefügt, die die Stärke des ausgewählten Passworts angibt. Sie ist jedoch lediglich eine Hilfsmittel und garantiert nicht, dass ein Passwort wirklich die Sicherheitsanforderungen einer Anlage erfüllt.
2. Klicken Sie auf **Setzen**, um die Änderungen zu speichern.



Bei Firmware-Version 6.30 wurde die **Benutzerverwaltung** flexibler gestaltet, damit Benutzer mit frei wählbaren Namen und eigenen Passwörtern erstellt werden können. Die ehemaligen Kontoebenen wurden durch die Benutzergruppenebenen ersetzt.

Die ehemaligen Benutzer sind noch vorhanden und verwenden weiterhin die Passwörter, die ihnen mit einer früheren Firmware zugewiesen wurden. Sie können aber nicht gelöscht werden, und auch ihre Benutzergruppenebene kann nicht geändert werden.

Passwörter können mit einem Klick auf oder  zugewiesen oder geändert werden. Solange nicht allen Benutzern ein Passwort zugewiesen wurde, wird eine Warnmeldung angezeigt.

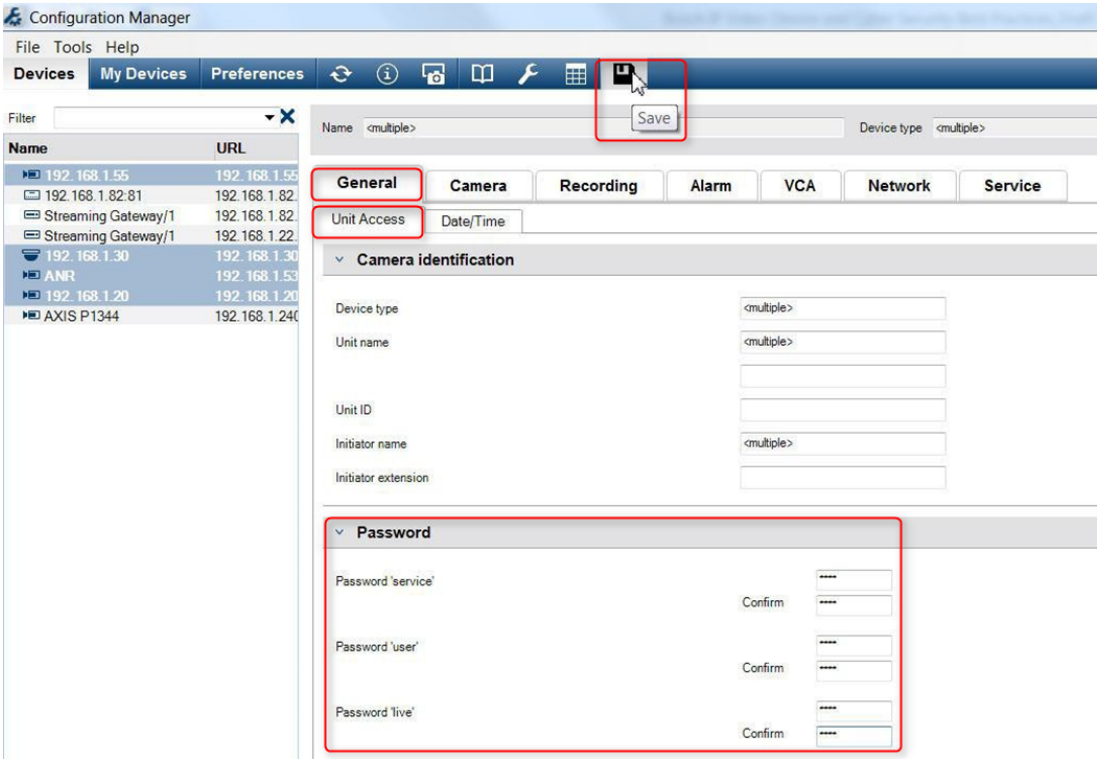
1. Um einen neuen Benutzer hinzuzufügen, klicken Sie auf **Hinzufügen**.
   Ein Popup-Fenster wird angezeigt.
2. Geben Sie die neuen Anmeldeinformationen ein und weisen Sie eine Benutzergruppe zu.
3. Klicken Sie auf **Setzen**, um die Änderungen zu speichern.

Hinweis!
Bei Firmware-Version 6.32 wurde außerdem eine strengere Passwortrichtlinie eingeführt. Passwörter müssen nun eine Mindestlänge von 8 Zeichen haben.

4.2.3 Zuweisen von Passwörtern mithilfe von Configuration Manager

Mit Bosch Configuration Manager können einem oder mehreren Geräten gleichzeitig Passwörter zugewiesen werden.

1. Wählen Sie im Configuration Manager ein oder mehrere Geräte aus.
2. Wählen Sie die Registerkarte **Allgemein** aus und wählen Sie dann **Gerätezugriff** aus.
3. Geben Sie im Menü **Passwort** das gewünschte Passwort für jedes der drei Konten ein und bestätigen Sie es (**Passwort 'service'**, **Passwort 'user'**und **Passwort 'live'**).
4. Klicken Sie auf  , um die Änderungen zu speichern.



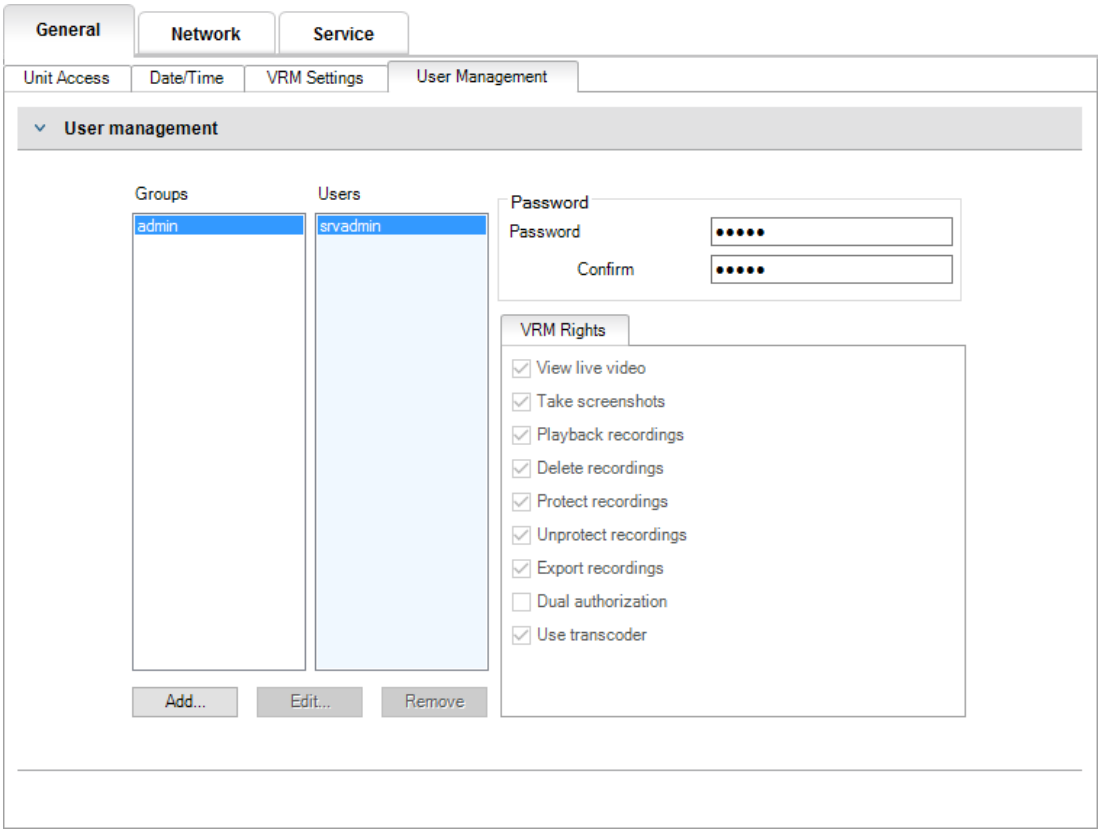
Bei größeren Anlagen, die entweder vom BVMS oder Video Recording Manager (auf einem Aufzeichnungsgerät installiert) verwaltet werden, können allen IP-Videogeräten im System globale Passwörter zugewiesen werden. Dies ermöglicht eine einfache Verwaltung und gewährleistet ein standardisiertes Sicherheitsniveau im gesamten Netzwerkvideosystem.

4.2.4 Zuweisen von Passwörtern für die eigenständige VRM Installation

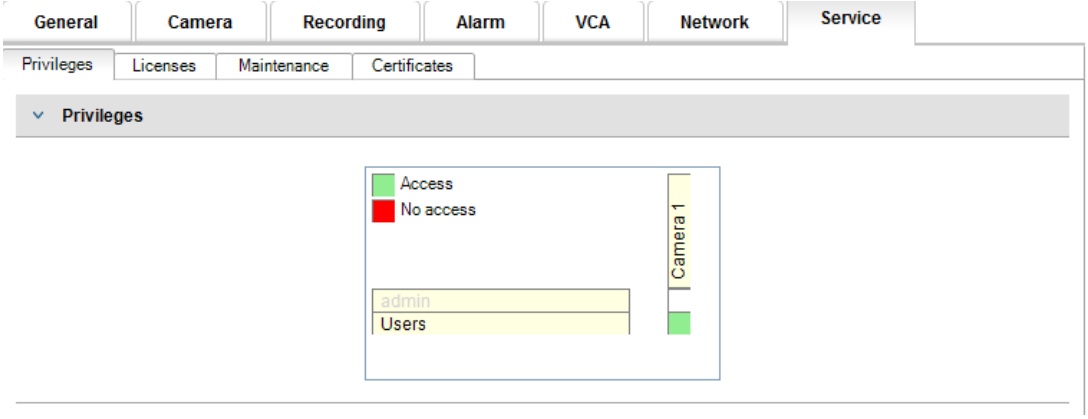
Der Video Recording Manager bietet eine Benutzerverwaltung für mehr Flexibilität und Sicherheit.

Standardmäßig ist keinem der drei Benutzerkonten ein Passwort zugewiesen. Das Zuweisen von Passwörtern ist ein wichtiger Schritt zum Schutz jedes Netzwerkgeräts. Es wird dringend empfohlen, allen installierten Netzwerkvideogeräten ein Passwort zuzuweisen.

Dasselbe gilt für die Benutzer des Video Recording Manager.



Darüber hinaus kann Mitgliedern einer Benutzergruppe der Zugriff auf bestimmte Kameras und Berechtigungen zugewiesen werden. So wird eine detaillierte benutzerbasierte Rechteverwaltung erzielt.



4.2.5 Zuweisen von Passwörtern mit BVMS (auf DIVAR IP oder eigenständiges System)

Geräte-Passwortschutz

Kameras und Encoder, die von BVMS verwaltet werden, können durch den Passwortschutz vor unbefugtem Zugriff geschützt werden.

Passwörter für die integrierten Benutzerkonten von Encodern/Kameras können mit dem BVMS Configuration Client konfiguriert werden.

Gehen Sie wie folgt vor, um ein Passwort für die integrierten Benutzerkonten mit BVMS Configuration Client festzulegen:

1. Wählen Sie im Gerätebaum den gewünschten Encoder aus.
2. Klicken Sie mit der rechten Maustaste auf den Encoder und klicken Sie auf **Passwort ändern...**.
3. Geben Sie ein Passwort für die drei integrierten Benutzerkonten live, user und service ein.

Standard-Passwortschutz

Mit BVMS ab Version 5.0 können Sie in einem Videosystem mit bis zu 2000 IP-Kameras globale Passwörter auf allen Geräten implementieren. Der Zugriff auf diese Funktion erfolgt entweder über den BVMS Configuration Wizard bei der Arbeit mit DIVAR IP 3000 oder DIVAR IP 7000 Aufzeichnungsgeräten oder über den BVMS Configuration Client auf jedem System.

Gehen Sie wie folgt vor, um im BVMS Configuration Client auf das Menü für globale Passwörter zuzugreifen:

1. Klicken Sie im Menü **Hardware** auf **Geräte mit Standardpasswort schützen...**.
2. Geben Sie im Feld **Globales Standardpasswort** ein Passwort ein und wählen Sie **Passwortschutz bei Aktivierung erzwingen** aus.

Nach dem Speichern und Aktivieren der Systemänderungen wird das eingegebene Passwort für die live-, user- und service-Konten aller Geräte und das Administratorkonto von Video Recording Manager übernommen.

Hinweis!

Wenn bei den Geräten bereits Passwörter für ein oder mehrere Konten festgelegt wurden, werden sie nicht überschrieben.

Wenn z. B. bereits ein Passwort für service, aber nicht für live und user festgelegt wurde, wird das globale Passwort nur für die live- und user-Konten konfiguriert.

BVMS Konfiguration und VRM-Einstellungen

Standardmäßig verwendet das BVMS das integrierte Administratorkonto **srvadmin** für die passwortgeschützte Verbindung mit Video Recording Manager. Um unbefugten Zugriff auf den Video Recording Manager zu vermeiden, sollte das **srvadmin** Administratorkonto mit einem komplexen Passwort geschützt werden.

Gehen Sie wie folgt vor, um das Passwort für das **srvadmin**-Konto in BVMS Configuration Client zu ändern:

1. Wählen Sie im Gerätebaum das VRM-Gerät aus.
2. Klicken Sie mit der rechten Maustaste auf das VRM-Gerät und klicken Sie dann auf **VRM-Passwort ändern**.
   Das Dialogfeld **Passwort ändern...** wird angezeigt.
3. Geben Sie ein neues Passwort für das **srvadmin**-Konto an und klicken Sie auf **OK**.

Verschlüsselte Kommunikation mit Kameras
Seit BVMS Version 7.0 kann die Live-Videodaten- und Steuerungskommunikation zwischen Kamera und BVMS Operator Client, Configuration Client, Management Server und Video Recording Manager verschlüsselt werden.
Nach der Aktivierung der sicheren Verbindung im Dialogfeld **Encoder bearbeiten** verwenden der BVMS-Server, Operator Client und Video Recording Manager eine sichere HTTPS-Verbindung für die Verbindung mit einer Kamera oder einem Encoder.
Die intern verwendete Verbindungszeichenfolge von BVMS ändert sich von rcpp://a.b.c.d (einfache RCP+-Verbindung an Port 1756) zu https://a.b.c.d (HTTPS-Verbindung an Port 443). Für ältere Geräte, die HTTPS nicht unterstützen, bleibt die Verbindungszeichenfolge unverändert (RCP+).

Bei Auswahl der HTTPS-Kommunikation wird HTTPS (TLS) zur Verschlüsselung der gesamten Steuerungskommunikation und Video-Nutzdaten über das Verschlüsselungsmodul im Gerät verwendet. Bei der Verwendung von TLS werden die gesamte HTTPS-Steuerungskommunikation und Video-Nutzdaten mit einem AES-Verschlüsselungscode mit einer Länge von bis zu 256 Bits verschlüsselt.
Gehen Sie wie folgt vor, um die verschlüsselte Kommunikation in BVMS Configuration Client zu aktivieren:

1. Wählen Sie im Gerätebaum den gewünschten Encoder/die gewünschte Kamera aus.
2. Klicken Sie mit der rechten Maustaste auf den Encoder/die Kamera und klicken Sie auf **Encoder bearbeiten**.
3. Aktivieren Sie im Dialogfeld **Encoder bearbeiten** die Option **Sichere Verbindung**.
4. Speichern und aktivieren Sie die Konfiguration.

Nach der Aktivierung der sicheren Verbindung zum Encoder können andere Protokolle deaktiviert werden (siehe *Allgemeine Netzwerk-Portverwendung und Videoübertragung, Seite 17*).

Hinweis!
BVMS unterstützt nur den Standard-HTTPS-Port 443. Die Verwendung anderer Ports wird nicht unterstützt.

4.3 Härten des Gerätezugriffs

Alle Bosch-IP-Videogeräte verfügen über eine integrierte Mehrzweck-Webseite. Die gerätespezifische Webseite unterstützt sowohl Live- als auch Videowiedergabefunktionen und einige bestimmte Konfigurationseinstellungen, die möglicherweise nicht über ein Videomanagementsystem zugänglich sind. Die integrierten Benutzerkonten dienen als Zugriff auf die verschiedenen Bereiche der speziellen Webseiten. Der Webseitenzugriff kann nicht vollständig über die Webseite selbst deaktiviert werden – dafür kann der Configuration Manager verwendet werden –, dort stehen aber mehrere Methoden zur Verfügung, um das Vorhandensein des Geräts zu tarnen, den Zugriff einzuschränken und die Video-Portverwendung zu verwalten.

4.3.1 Allgemeine Netzwerk-Portverwendung und Videoübertragung

Alle Bosch IP-Videogeräte nutzen das Remote Control Protocol Plus (RCP+) für Detektion, Steuerung und Kommunikation. RCP+ ist ein proprietäres Bosch-Protokoll, das bestimmte statische Ports (1756, 1757 und 1758) verwendet, um Bosch IP-Videogeräte zu erkennen und mit ihnen zu kommunizieren. Bei der Arbeit mit dem BVMS oder einem anderen Drittanbieter-

Videomanagementsystem, das Bosch IP-Videogeräte über das Bosch VideoSDK integriert hat, müssen die aufgeführten Ports im Netzwerk erreichbar sein, damit die IP-Videogeräte ordnungsgemäß funktionieren.

Videos können auf verschiedene Arten von den Geräten gestreamt werden: UDP (Dynamic), HTTP (80), oder HTTPS (443).
Die HTTP- und HTTPS-Portverwendung kann geändert werden (siehe *HTTP-, HTTPS- und Video-Portverwendung, Seite 19*). Vor dem Bearbeiten eines Ports muss die gewünschte Kommunikationsart zu einem Gerät konfiguriert werden. Über den Configuration Manager kann auf das Menü „Kommunikation” zugegriffen werden.

1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.
2. Wählen Sie die Registerkarte **Allgemein** aus und wählen Sie dann **Gerätezugriff** aus.
3. Suchen Sie auf der Seite den Abschnitt **Geräte-Zugriff**.

4. Wählen Sie das gewünschte Protokoll in der Liste **Protokoll** aus:

– RCP+
– HTTP (Standard)
– HTTPS

Bei Auswahl der HTTPS-Kommunikation wird bei der Kommunikation zwischen Configuration Manager und Videogeräten HTTPS (TLS) verwendet, um die Nutzdaten mit einem AES-Verschlüsselungscode mit einer Länge von bis zu 256 Bits zu verschlüsseln. Dies ist eine kostenlose Grundfunktion. Bei der Verwendung von TLS werden die gesamte HTTPS-Steuerungskommunikation und alle Video-Nutzdaten über das Verschlüsselungsmodul im Gerät verschlüsselt.

Hinweis!
Die Verschlüsselung gilt speziell für den „Übertragungsweg“. Nachdem ein Video von einem Software- oder Hardware-Decoder empfangen wurde, wird der Stream dauerhaft entschlüsselt.

4.3.2 Minimale TLS-Version

Einige ältere Clients müssen möglicherweise ältere und weniger sichere TLS-Versionen verwenden. Definieren Sie jedoch nach Möglichkeit eine Mindestversion für TLS, um zu vermeiden, dass Clients das Gerät in einen weniger sicheren Zugriffsmodus zwingen. Wählen Sie die höchstmögliche TLS-Version als Mindestversion.

Hinweis!
Wenn Sie das Mindestsicherheitsniveau für den Zugriff auf Geräte von einer Client-Software festlegen, achten Sie darauf, dass alle Ports und Protokolle, die eine niedrigere Zugriffsebene ermöglichen, bei den Geräten deaktiviert oder ausgeschaltet sind.

4.3.3 HTTP-, HTTPS- und Video-Portverwendung

HTTP und HTTPS Portnutzung auf allen Geräten kann geändert oder ausgeschaltet werden. Die verschlüsselte Kommunikation kann durch das Deaktivieren des RCP+- und HTTP-Ports erzwungen werden. So wird die Verschlüsselung der gesamten Kommunikation erreicht. Wenn die HTTP-Portverwendung ausgeschaltet ist, bleibt HTTPS eingeschaltet und alle Versuche, es auszuschalten, schlagen fehl.

1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.
2. Wählen Sie die Registerkarte **Netzwerk** aus und wählen Sie dann **Netzwerkzugriff** aus.
3. Suchen Sie auf der Seite den Abschnitt **Details**.

4. Bearbeiten Sie im Abschnitt **Details** die HTTP- und HTTPS-Browser-Ports und den RCP+-Port über das Dropdown-Menü:
   - HTTP-Browser-Portmodifizierung: 80 oder Ports 10000 bis 10100
   - HTTPS-Browser-Portmodifizierung: 443 oder Ports 10443 bis 10543
   - RCP+-Port 1756: **Ein** oder **Aus**

Hinweis!
Wenn der HTTP-Port bei Firmware-Version 6.1x deaktiviert ist und versucht wird, auf die Webseite des Geräts zuzugreifen, wird die Anforderung zum aktuell definierten HTTPS-Port weitergeleitet.
Die Weiterleitungsfunktion ist ab Firmware-Version 6.20 nicht mehr vorhanden. Wenn der HTTP-Port deaktiviert ist und der HTTPS-Port so geändert wurde, dass ein anderer Port als Port 443 verwendet wird, kann man nur auf die Webseiten zugreifen, indem man zur Geräte-IP-Adresse plus zugewiesenem Port navigiert.

Beispiel:
https://192.168.1.21:10443. Alle Versuche, eine Verbindung mit der Standardadresse herzustellen, schlagen fehl.

4.3.4 Video-Software und Portauswahl

Das Anpassen dieser Einstellungen beeinflusst auch, welcher Port für die Videoübertragung verwendet wird, wenn in Ihrem LAN eine Videomanagementsoftware genutzt wird.
Wenn zum Beispiel alle IP-Videogeräte auf den HTTP-Port 10000 eingestellt sind und das BVMS Operator Client für „TCP-Tunnelung“ konfiguriert ist, dann erfolgen alle Videoübertragungen im Netzwerk über den HTTP-Port 10000.

Hinweis!
Änderungen an den Port-Einstellungen von Geräten müssen mit den Einstellungen im Managementsystem und seinen Komponenten sowie der Clients übereinstimmen.

Hinweis!
Abhängig vom Implementierungsszenario und dem Sicherheitsmodell der Anlage können die bewährten Methoden variieren. Das Deaktivieren und Weiterleiten der HTTP- oder HTTPS-Ports hat seine Vorteile. Das Wechseln des Port-Protokolls kann dabei helfen, dass keine Informationen an Netzwerk-Tools wie NMAP (Network Mapper, kostenloser Sicherheitsscanner) weitergegeben werden. Anwendungen wie NMAP werden in der Regel als Erkundungstool zur Identifizierung von Schwachstellen bei Geräten in einem Netzwerk verwendet. Dieses Verfahren in Kombination mit dem Einsatz von starken Passwörtern trägt zur Gesamtsicherheit des Systems bei.

4.3.5 SSH Tunnelung

Für den Zugriff auf ein Remote-Gerät mit dem BVMS Operator Client über öffentliche Netzwerke bietet BVMS Secure Shell (SSH) Tunnelung, um eine sichere (verschlüsselte) Kommunikation zu gewährleisten.
Bei der SSH-Tunnelung wird ein verschlüsselter Tunnel über eine SSH-Protokoll/Socket-Verbindung aufgebaut. Dieser verschlüsselte Tunnel ermöglicht verschlüsselten und unverschlüsselten Datenverkehr. Die Bosch SSH-Implementierung nutzt außerdem das Omni-Path-Protokoll, ein von Intel entwickeltes, hochleistungsfähiges Kommunikationsprotokoll mit niedriger Latenz.

Weitere Informationen zur Konfiguration des SSH-Dienstes finden Sie in BVMS der BVMS-Dokumentation.
Weitere Informationen über die Konfiguration von DIVAR IP Systemen für einen sicheren Fernzugriff mit BVMS Operator Client finden Sie in der DIVAR IP-Dokumentation.

4.3.6 Telnet-Zugriff

Telnet ist ein Protokoll der Anwendungsschicht, das die Kommunikation mit Geräten über eine virtuelle Terminalsitzung zu Wartungs- und Fehlerbehebungszwecken ermöglicht. Alle Bosch IP-Videogeräte sind Telnet-fähig und die Telnet-Unterstützung ist bei Firmware-Versionen bis 6.1x standardmäßig eingeschaltet. Ab Firmware-Version 6.20 ist der Telnet-Port standardmäßig deaktiviert.

Hinweis!
Seit 2011 wird ein Anstieg der Cyber-Attacken über das Telnet-Protokoll verzeichnet. Mittlerweile hat sich bewährt, die Telnet-Unterstützung bei allen Geräten zu deaktivieren, bis sie für Wartung oder Fehlerbehebung benötigt wird.

1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.
2. Wählen Sie die Registerkarte **Netzwerk** aus und wählen Sie dann **Netzwerkzugriff** aus.
3. Suchen Sie auf der Seite den Abschnitt **Details**.

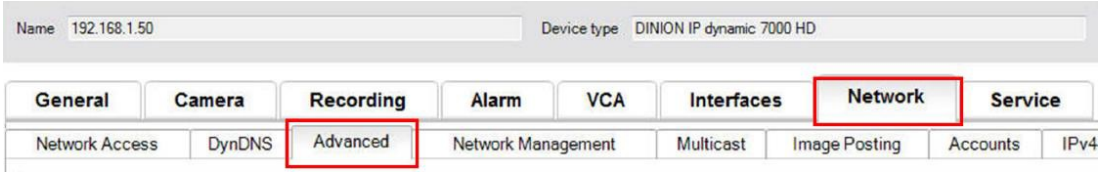
4. Im Abschnitt **Details** können Sie **Telnet-Unterstützung** mit dem Dropdown-Menü auf **Ein** oder **Aus** festlegen.

Hinweis!
Seit Firmware-Version 6.20 wird Telnet auch über sogenannte WebSockets unterstützt, die sichere HTTPS-Verbindungen verwenden. WebSockets verwenden den Standard-Telnet-Port nicht und bieten bei Bedarf eine sichere Möglichkeit für den Zugriff auf die Kommandozeilenschnittstelle des IP-Geräts.

4.3.7 RTSP: Real Time Streaming Protocol

Das Real Time Streaming Protocol (RTSP) ist die primäre Videokomponente, die vom ONVIF-Protokoll verwendet wird, um Video-Streaming und Gerätesteuerung für ONVIF-konforme Videomanagementsysteme bereitzustellen. RTSP wird auch von verschiedenen Drittanbieter-Videoanwendungen für grundlegende Streamingfunktionen verwendet und kann in manchen Fällen für die Geräte- und Netzwerkfehlerbehebung eingesetzt werden. Alle Bosch IP-Videogeräte können Streams über RTSP bereitstellen.
RTSP-Dienste können ganz einfach mit dem Configuration Manager bearbeitet werden.

1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.
2. Wählen Sie die Registerkarte **Netzwerk** aus und wählen Sie dann **Erweitert** aus.



3. Suchen Sie auf der Seite den Abschnitt **RTSP**.
4. Schalten Sie den RTSP-Dienst im Dropdown-Menü **RTSP-Port** aus oder bearbeiten Sie ihn:
   - Standard-RTSP-Port: 554
   - RTSP-Portmodifizierung: 10554 bis 10664

Hinweis!
In letzter Zeit wurde über Cyber-Attacken berichtet, die über RTSP-Buffer-Overflows durchgeführt wurden. Diese Angriffe waren gezielt auf Geräte bestimmter Hersteller programmiert. Es hat sich bewährt, den Dienst zu deaktivieren, wenn er nicht von einem ONVIF-kompatiblen Videomanagementsystem oder für grundlegendes Streaming in Echtzeit verwendet wird.
Alternativ und wenn der empfangende Client es ermöglicht, kann die RTSP-Kommunikation mit einer HTTPS-Verbindung getunnelt werden. Dies ist aktuell die einzige Möglichkeit zur Verschlüsselung der RTSP-Datenübertragung.

Hinweis!
Weitere Einzelheiten zu *RTSP finden Sie im Anwendungshinweis* RTSP-Nutzung mit Bosch VIP-Geräten im Online-Produktkatalog von Bosch Security Systems unter dem folgenden Link:
https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf

4.3.8 UPnP: Universal Plug and Play

Bosch IP-Videogeräte können über **UPnP** mit Netzwerkgeräten kommunizieren. Diese Funktion wird vor allem in kleineren Systemen mit nur wenigen Kameras eingesetzt, wo die Kameras automatisch im Netzwerkverzeichnis des PC angezeigt und somit leicht gefunden werden können. Dies passiert allerdings auch bei jedem anderen Gerät im Netzwerk.
UPnP kann mit dem Configuration Manager ausgeschaltet werden.

1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.

2. Wählen Sie die Registerkarte **Netzwerk** aus und wählen Sie dann **Netzwerk-Verwaltung** aus.

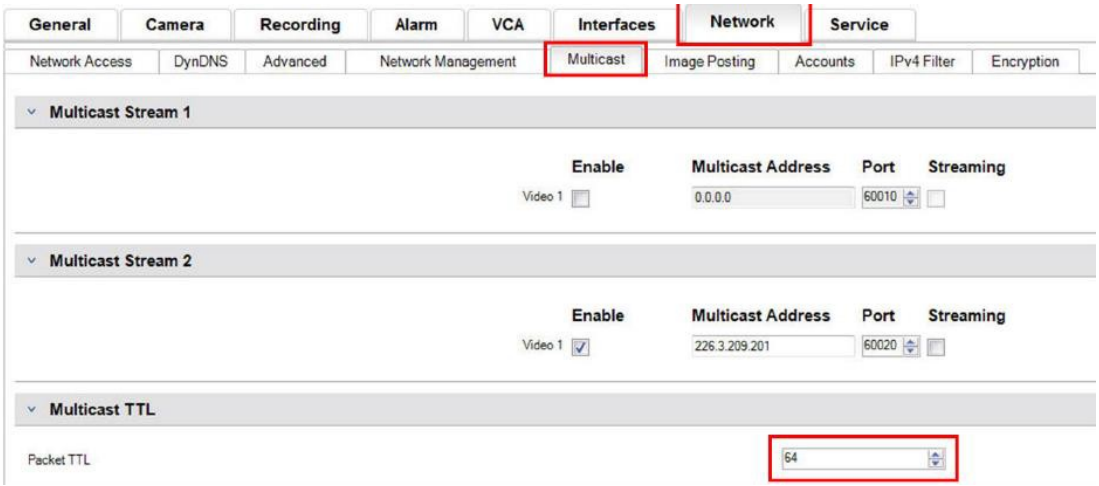
3. Suchen Sie auf der Seite den Abschnitt **UPnP**.
4. Wählen Sie im Dropdown-Menü **UPnP** die Option **Aus** aus, um **UPnP** zu deaktivieren.

Hinweis!
UPnP sollte wegen der zahlreichen Registrierungsnachrichten und der potenziellen Gefahr eines unbefugten Zugriffs oder einer Attacke nicht in großen Anlagen verwendet werden.

4.3.9 Multicasting

Alle Bosch IP-Videogeräte sind in der Lage, sowohl „Multicast on Demand“ als auch „Multicast Streaming" Video bereitzustellen. Während Unicast-Videoübertragungen zielbasiert sind, ist Multicast quellenbasiert. Dies kann zu Sicherheitsproblemen auf der Netzwerkebene führen, einschließlich: Gruppenzutrittskontrolle, Vertrauen von Gruppenzentren und Vertrauen von Routern. Die Routerkonfiguration ist nicht Gegenstand dieses Handbuchs, doch es gibt eine Sicherheitslösung, die vom IP-Videogerät selbst implementiert werden kann.
TTL (time-to-live) scoping definiert, wo und wie weit der Multicast-Verkehr innerhalb eines Netzwerks fließen darf, wobei jeder Hop die TTL um eins verringert. Bei der Konfiguration der IP-Videogeräte für die Multicast-Verwendung kann das Paket-TTL des Geräts geändert werden.

1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.
2. Wählen Sie die Registerkarte **Netzwerk** aus und wählen Sie dann **Multicast** aus.
3. Suchen Sie auf der Seite den Abschnitt **Multicast TTL**.
4. Passen Sie die **Paket-TTL**-Einstellungen mithilfe der folgenden TTL-Werte und Scoping-Einschränkungen an:
   - TTL-Wert 0 = auf lokalen Host beschränkt
   - TTL Wert 1 = auf dasselbe Subnetz beschränkt
   - TTL-Wert 15 = auf denselben Standort beschränkt
   - TTL-Wert 64 (Standard) = auf dieselbe Region beschränkt
   - TTL-Wert 127 = weltweit
   - TTL-Wert 191 = weltweit mit begrenzter Bandbreite
   - TTL-Wert 255 = uneingeschränkte Daten

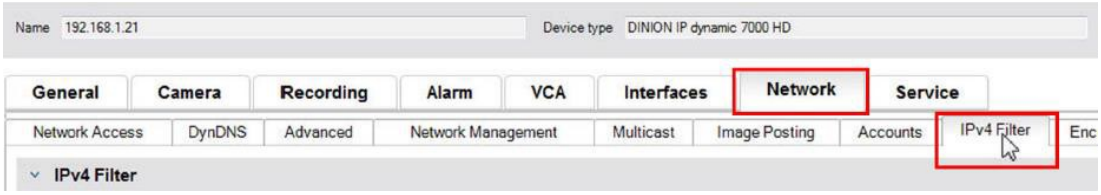


Hinweis!
Beim Umgang mit Videoüberwachungsdaten hat es sich bewährt, den TTL-Wert auf 15 (selber Standort) festzulegen. Ideal: Wenn Sie die genaue Maximalanzahl an Hops kennen, können Sie sie als TTL-Wert verwenden.

4.3.10 IPv4-Filter

Sie können den Zugriff auf jedes Bosch IP-Videogerät mit der IPv4-Filter-Funktion einschränken. Die IPv4-Filterung nutzt die grundlegenden Subnetting-Funktionen zur Definition von bis zu zwei zulässigen IP-Adressbereichen. Nach der Definition wird der Zugriff von einer beliebigen IP-Adresse außerhalb dieser Bereiche verweigert.

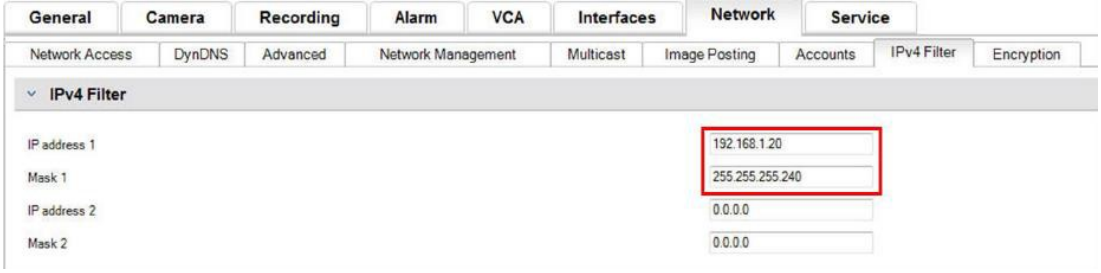
1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.
2. Wählen Sie die Registerkarte **Netzwerk** aus und wählen Sie dann **IPv4-Filter** aus.



Hinweis!
Um diese Funktion erfolgreich konfigurieren zu können, müssen Sie über grundlegende Subnetting-Kenntnisse verfügen oder Zugriff auf einen Subnet-Rechner haben. Werden bei dieser Einstellung falsche Werte eingegeben, kann der Zugriff auf das Gerät verweigert werden, und das Gerät muss möglicherweise auf die Standardeinstellungen zurückgesetzt werden, um wieder darauf zugreifen zu können.

3. Nehmen Sie zwei Eingaben vor, um eine Regel hinzuzufügen:
   - Geben Sie eine Basis-IP-Adresse an, die innerhalb der von Ihnen erstellten Subnetz-Regel liegt.
     Die Basis-IP-Adresse gibt an, welches Subnetz Sie erlauben. Es muss im gewünschten Bereich liegen.
   - Geben Sie eine Subnetzmaske an, die die IP-Adressen definiert, mit denen das IP-Videogerät eine Kommunikation akzeptiert.

Im folgenden Beispiel wurden die **IP-Adresse 1** 192.168.1.20 und die **Ausblendung 1** 255.255.255.240 eingegeben. Diese Einstellung schränkt den Zugriff von Geräten ein, die innerhalb des festgelegten IP-Adressbereichs von 192.168.1.16 bis 192.168.1.31 liegen.



Beim Einsatz der **IPv4-Filter**-Funktion können Geräte über RCP+ gefunden werden, aber der Zugriff auf Konfigurationseinstellungen und Video ist nicht über Clients möglich, die außerhalb des zulässigen IP-Adressbereichs liegen. Dazu zählt auch der Zugriff über einen Webbrowser. Das IP-Videogerät selbst muss sich nicht im zulässigen Adressbereich befinden.

Hinweis!
Abhängig von der Konfiguration Ihres Systems kann der Einsatz der **IPv4-Filter**-Funktion die unerwünschte Sichtbarkeit von Geräten in einem Netzwerk reduzieren. Wenn Sie diese Funktion aktivieren, dokumentieren Sie die Einstellungen für spätere Zwecke.
Beachten Sie, dass der Zugriff auf das Gerät über IPv6 immer noch möglich ist. Die IPv4-Filterung ist also nur in reinen IPv4-Netzwerken sinnvoll.

4.3.11 SNMP

Simple Network Management Protocol (SNMP) ist ein gängiges Protokoll zur Überwachung des Gesundheitszustands eines Systems. Ein solches Überwachungssystem beinhaltet in der Regel einen zentralen Verwaltungsserver, der alle Daten der kompatiblen Komponenten und Geräte des Systems sammelt.
SNMP bietet zwei Methoden zur Ermittlung des Systemzustands:

- Der Netzwerkverwaltungsserver kann den Zustand eines Geräts über SNMP-Anforderungen abrufen.
- Geräte können den Netzwerkverwaltungsserver bei Fehler- oder Alarmbedingungen aktiv über ihren Systemzustand benachrichtigen, indem sie SNMP-Traps an den SNMP-Server senden. Solche Traps müssen im Gerät konfiguriert werden.

SNMP ermöglicht außerdem die Konfiguration einiger Variablen in Geräten und Komponenten. Die Informationen darüber, welche Nachrichten ein Gerät unterstützt und welche Traps es senden kann, werden aus der Management Information Base (die sogenannte MIB-Datei) abgeleitet. Diese Datei wird für die problemlose Integration in ein Netzwerküberwachungssystem mit dem Produkt geliefert.

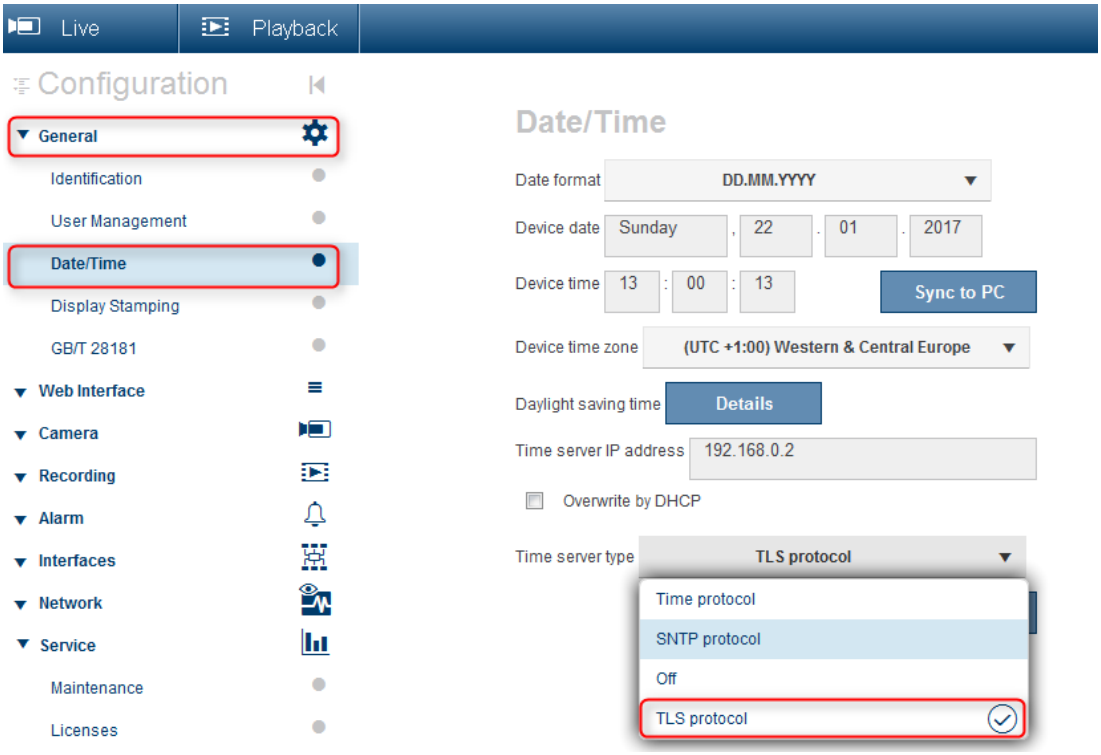
Es gibt drei verschiedene SNMP-Versionen:

- SNMP-Version 1
  Die SNMP-Version 1 (SNMPv1) ist die erste SNMP-Implementierung. Sie wird sehr häufig verwendet und ist de facto zum Standardprotokoll für die Netzwerkverwaltung und -überwachung geworden.
  Aufgrund der mangelnden Sicherheitsfunktionen ist die Verwendung von SNMPv1 aber riskant. Es verwendet nur *Community-Strings* als eine Art von Passwörtern, die als Klartext übertragen werden.
  SNMPv1 sollte also nur verwendet werden, wenn sichergestellt werden kann, dass das Netzwerk physisch gegen unberechtigten Zugriff geschützt ist.
- SNMP-Version 2
  Bei SNMP-Version 2 (SNMPv2) wurden u. a. Verbesserungen bei Sicherheit und Vertraulichkeit und eine Bulk-Anforderung eingeführt, mit der große Datenmengen in einer einzigen Anforderung abgerufen werden können. Ihr Sicherheitsansatz galt jedoch als viel zu komplex und die Akzeptanz war dementsprechend niedrig.
  Sie wurde bald von der Version SNMPv2c verdrängt, die bis auf das kontroverse Sicherheitsmodell SNMPv2 entspricht, die Community-basierte Methode von SNMPv1 einsetzt und darum hinsichtlich Sicherheit ähnlich mangelhaft ist.
- SNMP-Version 3
  Bei SNMP-Version 3 (SNMPv3) wurden hauptsächlich Verbesserungen bei Sicherheit und Fernkonfiguration hinzugefügt. Dazu zählen bessere Vertraulichkeit bei der Verschlüsselung von Paketen, Nachrichtenintegrität und Authentifizierung.
  Ziel war auch die umfassende Implementierung von SNMP.

Hinweis!
Die Verwendung von SNMPv1 und SNMPv2c ist wegen der mangelnden Sicherheitsfunktionen riskant. Beide verwenden nur „Community-Strings” als eine Art von Passwörtern, die als Klartext übertragen werden.
Daher sollte SNMPv1 oder SNMPv2c nur dann verwendet werden, wenn sichergestellt ist, dass das Netzwerk physisch vor unbefugtem Zugriff geschützt ist.
Bosch Kameras unterstützen derzeit nur SNMPv1. Stellen Sie sicher, dass SNMP ausgeschaltet ist, wenn Sie es nicht verwenden.

4.3.12 Sichere Zeitbasis

Zusätzlich zu Time Protocol und SNTP, die beide nicht gesicherte Protokolle sind, wurde mit FW 6.20 ein dritter Modus für den Timeserver-Client eingeführt, der das TLS-Protokoll verwendet. Diese Methode wird auch als *TLS-Datum* bezeichnet.
In diesem Modus kann jeder beliebige HTTPS-Server als Zeitserver verwendet werden. Der Zeitwert wird als Nebeneffekt vom HTTPS-Handshake-Vorgang abgeleitet. Die Übertragung ist TLS-gesichert. Ein optionales Root-Zertifikat für den HTTPS-Server kann im Zertifikatspeicher der Kamera gespeichert werden, um den Server zu authentifizieren.



Hinweis!
Stellen Sie sicher, dass die eingegebene IP-Adresse des Zeitservers eine stabile und unverfälschte Zeitbasis hat.

4.3.13 Cloud-basierte Dienste

Alle Bosch IP-Videogeräte können mit Cloud-basierten Diensten von Bosch wie Remote Portal kommunizieren. Je nach Einsatzgebiet können IP-Videogeräte damit Dienste wie Remote Device Management oder Cloud VMS nutzen, um Alarme und andere Daten an eine zentrale Station weiterzuleiten.

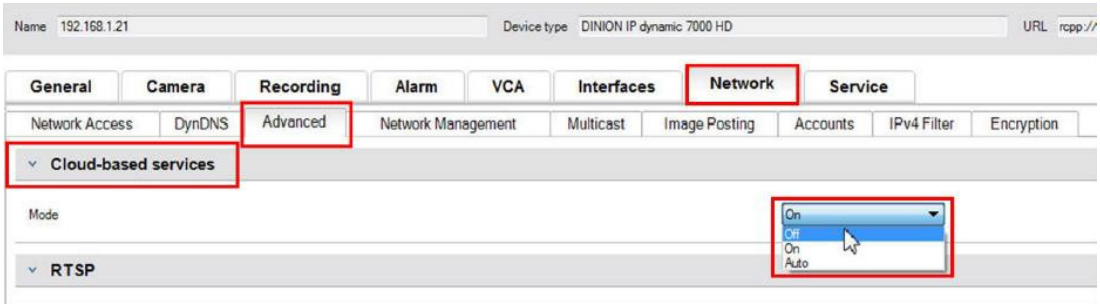
Weitere Informationen finden Sie in der Bosch Building Technologies Knowledge Base: https://community.boschsecurity.com.

Es gibt drei Betriebsmodi für Cloud-basierte Dienste:

– **Ein**:
  Das Videogerät fragt ständig den Cloud-Server ab.
– **Auto** (Standard):
  Die Videogeräte werden einige Male versuchen, den Cloud-Server abzufragen. Wenn dies nicht gelingt, wird der Versuch, den Cloud-Server zu erreichen, eingestellt.
– **Aus**:
  Es wird kein Polling durchgeführt.

Cloud-basierte Dienste können mit dem Configuration Manager einfach ausgeschaltet werden.

1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.
2. Wählen Sie das **Netzwerk** aus und wählen Sie dann die Registerkarte **Erweitert**.
3. Suchen Sie den Abschnitt **Cloud-basierte Dienste** auf der Seite und wählen Sie in der Liste **Aus**.



Hinweis!
Wenn Sie die Cloud-basierten Dienste von Bosch nutzen, behalten Sie die Standardkonfiguration bei.
In allen anderen Fällen schalten Sie den Modus für Cloud-basierte Dienste auf **Aus**.

4.4 Härten von IP-Kameras

Die IP-Kameras von Bosch werden mit einer Standardkonfiguration geliefert, die eine einfache Integration in verschiedene Umgebungen ermöglicht.
Je nach Zielumgebung und beabsichtigter Sicherheitsstufe kann es erforderlich sein, einige Kameraeinstellungen zu ändern, um die Cyber- und Datensicherheit zu erhöhen.
Es kann jedoch Einschränkungen in der Betriebsumgebung geben, die die Verwendung eines bestimmten Protokolls oder einer Funktion vorschreiben, die weniger sicher ist (zum Beispiel SNMPv1).

4.4.1 Härtungsstufen

Es sind zwei Härtungsstufen definiert: *erhöht* und *strikt*.
Die *strikte* Härtungsstufe bietet die sicherste Möglichkeit, ein Gerät einzurichten, schränkt aber möglicherweise die Nutzung des Geräts ein, da Funktionen wie die automatische Erkennung eines Geräts deaktiviert sind. Für jedes Merkmal sollte geprüft werden, ob die Einstellung *erhöht* und *strikt* angewendet werden kann.

4.4.2 Übersicht über die Härtungen

Netzwerk - Netzwerk-Dienste	Standard	Erhöht	Strikt
HTTP	Aktiviert	Deaktiviert	Deaktiviert
HTTPS	Aktiviert	Aktiviert	Aktiviert
RTSP	Aktiviert	Optional	Deaktiviert
RCP	Aktiviert	Deaktiviert	Deaktiviert
SNMPv1	Deaktiviert	Deaktiviert	Deaktiviert
SNMPv3	Deaktiviert	Aktiviert	Aktiviert
iSCSI	Aktiviert	Optional	Deaktiviert
UPnP	Deaktiviert	Deaktiviert	Deaktiviert
NTP-Server	Deaktiviert	Deaktiviert	Deaktiviert
Discovery	Aktiviert	Aktiviert	Deaktiviert
ONVIF Discovery	Aktiviert	Aktiviert	Deaktiviert
GBT/28181	Deaktiviert	Deaktiviert	Deaktiviert
Mechanismus zum Zurücksetzen des Passworts	Aktiviert	Deaktiviert	Deaktiviert
Ping-Antwort	Aktiviert	Aktiviert	Deaktiviert
RTSPS	Aktiviert	Aktiviert	Aktiviert
HTTP	Aktiviert	Deaktiviert	Deaktiviert

Netzwerk - Netzwerkzugriff	Standard	Erhöht	Strikt
Minimale TLS-Version	1.0	1.2	1.2
HSTS	Deaktiviert	Aktiviert	Aktiviert

Netzwerk - Erweitert	Standard	Erhöht	Strikt
802.1x	Deaktiviert	Optional	Aktiviert
Syslog	Deaktiviert	TCP	TLS

Netzwerk - Netzwerk-Verwaltung	Standard	Erhöht	Strikt
SNMPv3-Modus	Deaktiviert	SHA1 / AES	SHA1 / AES

Netzwerk - IPv4-Filter	Standard	Erhöht	Strikt
IPv4Filter	Deaktiviert	Aktiviert	Aktiviert

Allgemein - Datum/ Zeit	Standard	Erhöht	Strikt
Datum/Zeit (NTP Client)	Deaktiviert	SNTP- / TLS-Datum	TLS-Datum

Konnektivität - Cloud-Dienste	Standard	Erhöht	Strikt
Remote Portal	Deaktiviert	Aktiviert	Aktiviert

Service - Protokollierung	Standard	Erhöht	Strikt
Software-Versiegelung	Deaktiviert	Aktiviert	Aktiviert

4.4.3 Funktionsbeschreibung und Härtungsempfehlungen

HTTP

HTTP ist standardmäßig aktiviert, aber unverschlüsselt, so dass Anmeldedaten oder Einstellungen unverschlüsselt übertragen werden, wenn sie verwendet werden.
Empfehlung: Einfaches HTTP sollte zugunsten des verschlüsselten HTTPS deaktiviert werden, insbesondere wenn das Netzwerk nicht vertrauenswürdig ist.

HTTPS

HTTPS ist verschlüsselt und sollte die Standardwahl für den Zugriff auf die Weboberfläche oder auf die webbasierte RCP-API sein. Die Verwendung einer eigenen PKI und von Zertifikaten wird empfohlen.
Empfehlung: HTTPS ist das standardmäßig für die Konfiguration verwendete sichere Protokoll und sollte aktiviert bleiben.

RTSP

RTSP wird für Video-Streaming verwendet, aber normalerweise unverschlüsselt. Wenn die Software, die den Video-Stream empfängt, in der Lage ist, RTSPS zu verwenden, empfiehlt es sich, einfaches RTSP zu deaktivieren. Bei Verwendung anderer Bosch Komponenten (z.B. Decoder/BVMS/VRM/DIVAR IP) kann eine Bosch-eigene Verschlüsselung für RTSP aktiviert werden, die die Übertragung sicher macht.
Empfehlung: Risikobasierter Ansatz, wenn das Video unverschlüsselt oder mit Bosch Verschlüsselung übertragen werden kann. Wenn möglich, verwenden Sie verschlüsseltes RTSPS.

RCP
Das von Bosch entwickelte Remote Control Protocol plus ist das Konfigurationsprotokoll für Bosch IP-Kameras. Einfaches RCP ist unverschlüsselt, so dass die Einstellungen unverschlüsselt übertragen werden. Alle Bosch-Tools verwenden seit einiger Zeit RCP über HTTPS, aber es kann sein, dass Integrationstools von Drittanbietern oder Skripting-Tools, die noch auf dieses Protokoll angewiesen sind, es benötigen.
Empfehlung: Deaktivieren Sie RCP, wenn es nicht von Tools von Drittanbietern oder Legacy-Systemen verwendet wird.

SNMPv1
SNMP ist das gängige Netzwerküberwachungsprotokoll, das verwendet wird, um Gesundheitsinformationen eines Geräts abzufragen oder Traps an einen entfernten Empfänger zu senden, allerdings unverschlüsselt.
Empfehlung: Lassen Sie die Funktion deaktiviert, wenn sie nicht für die Gesundheitsüberwachung oder aus anderen Kompatibilitätsgründen benötigt wird. Verwenden Sie nach Möglichkeit SNMPv3.

SNMPv3
SNMPv3 ist der Nachfolger von SNMPv1 und kann auch verschlüsselt verwendet werden.
Empfehlung: Empfohlen, wenn eine SNMP-Überwachung durchgeführt werden muss.

iSCSI
Deaktiviert den internen iSCSI-Server, der verwendet wird, um interne Aufnahmen auf der Kamera über iSCSI zugänglich zu machen. iSCSI ist ein unverschlüsseltes Protokoll.
Empfehlung: Deaktivieren Sie den iSCSI-Server, wenn er nicht auf der Kamera verwendet wird.

UPnP
Die Kamera über das UPnP Protokoll auffindbar machen.
Empfehlung: Deaktivieren Sie UPnP, wenn Sie es nicht benötigen.

NTP-Server
Aktivieren Sie einen NTP-Server auf der Kamera, damit andere Geräte oder Kameras die Zeit synchronisieren können. Wenn möglich, sollte ein dediziertes Gerät die Zeit für das Kameranetzwerk bereitstellen, um eine Trennung der Dienste zu ermöglichen. Wenn kein anderes Gerät verfügbar ist, kann die Zeit mit einer Kamera gemessen werden.
Empfehlung: NTP-Server sollte bei Bedarf deaktiviert werden.

Discovery
Verwendung eines Bosch-eigenen Mechanismus, um Kameras durch eine Bosch-Software auffindbar zu machen, wie z.B. Configuration Manager.
Empfehlung: Wenn Sie mit dynamischen IP-Adressen arbeiten, sollte diese Funktion aktiviert bleiben. Wenn Sie in einer Umgebung mit festen IP-Adressen arbeiten, können Sie diese Funktion deaktivieren.

ONVIF Discovery
Unterstützung der Erkennung von Kameraregeräten über das ONVIF Discovery-Protokoll

Empfehlung: Wenn Sie mit dynamischen IP-Adressen und ONVIF-kompatiblen Tools arbeiten, sollte diese Funktion aktiviert bleiben. Wenn Sie in einer festen Umgebung mit festen IP-Adressen arbeiten, können Sie diese Funktion deaktivieren.

GBT/28181
GBT/28181 ist ein chinesischer Standard für die Interoperabilität zwischen verschiedenen Geräten.
Empfehlung: Deaktiviert lassen, wenn nicht benötigt.

Mechanismus zum Zurücksetzen des Passworts
IP-Kameras können an sehr abgelegenen Orten montiert werden, was es schwierig macht, Wartungsarbeiten oder einen Werksreset durchzuführen, falls der Zugang zur Kamera gesperrt wurde. Bosch bietet die Möglichkeit, das Passwort einer Kamera über einen Challenge-Response-Mechanismus zurückzusetzen, der auf einem sicheren Public/Private-Key-Mechanismus basiert.
Empfehlung: Wenn Sie diese Funktion nicht benötigen, empfehlen wir Ihnen, sie zu deaktivieren.

Ping-Antwort
Legt fest, ob die Kamera auf Ping-Anfragen im Netzwerk antwortet. Kann bei der Fehlersuche helfen. In einem hochsicheren Netzwerk kann diese Funktion deaktiviert werden, um die Auflistung von Geräten über den Ping Sweep zu vermeiden, obwohl es mehrere andere Möglichkeiten der Geräteerkennung gibt, die von einem Angreifer verwendet werden können.
Empfehlung: Risikobasierter Ansatz, kann für hochsichere Netzwerke deaktiviert werden.

RTSPS
RTSPS ist die verschlüsselte Version von RTSP und wird für Video-Streaming verwendet. Wenn die Empfangssoftware dies unterstützt, sollte RTSPS immer gegenüber einfachem RTSP bevorzugt werden. Da viele RTSP-Clients die sichere Variante nicht unterstützen, ist RTSP weiterhin für die Sicherheitsstufe 1 aktiviert.
Empfehlung: Verwenden Sie nach Möglichkeit RTSPS.

Minimale TLS-Version
IP-Kameras erlauben keine unsicheren SSLv3 oder älteren Verbindungen. TLS 1.0 und 1.1 sind von der IETF veraltet und es sind potenzielle Sicherheitsprobleme bekannt (BEAST, FREAK). CPP4-, CPP6-, CPP7- und CPP7.3-Kameras unterstützen das sichere TLS 1.2, das als Mindestversion eingestellt werden sollte.
CPP13 und CPP14 Kameras lassen keine TLS-Versionen vor 1.2 zu. Sie unterstützen auch die neuere TLS1.3-Spezifikation.
Empfehlung: Setzen Sie die minimale TLS Version auf 1.2.

HSTS
HTTP Strict Transport Security (HSTS) ist eine Richtlinie, die von einer Website zum Schutz vor Man-in-the-Middle-Angriffen und Protokoll-Downgrade-Angriffen festgelegt wurde. Sie ermöglicht es der Website, dem Browser mitzuteilen, dass er nur HTTPS Verbindungen innerhalb dieser Verbindung zulässt und keine unverschlüsselten HTTP-Verbindungen erlaubt.
Empfehlung: Aktivieren Sie HSTS auf der Kamera.

802.1x
802.1x ist ein Standard für die Netzwerkzugangskontrolle (NAC). Sie ermöglicht es Geräten, sich im Netzwerk zu authentifizieren und nur authentifizierten Geräten Zugang zum Netzwerk zu gewähren. Bosch IP-Kameras unterstützen 802.1x entweder mit Passwort oder zertifikatsbasierter Authentifizierung, wobei die zertifikatsbasierte Authentifizierung die bevorzugte Methode ist. Zur Verwendung von 802.1x muss der Netzwerk-Switch diesen Standard unterstützen, und ein Authentifizierungsserver wird benötigt.
Empfehlung: Wenn die Netzwerkinfrastruktur es zulässt, verwenden Sie die Netzwerkauthentifizierung mit 802.1x.

Syslog
Da die Kamera nur einen begrenzten Speicherplatz für Protokollmeldungen bietet, sollten die Protokollmeldungen an eine zentrale Stelle gesendet und dort analysiert werden, um Angriffe oder Fehlkonfigurationen zu erkennen.
Empfehlung: Verwenden Sie TCP Syslog, um den Verlust von Nachrichten aufgrund von Paketverlusten zu vermeiden. Verwenden Sie Syslog mit TLS, um Nachrichten zu verschlüsseln und zu authentifizieren.

SNMPv3-Modus
SNMPv3 ist der Nachfolger von SNMPv1 und ermöglicht eine sichere Authentifizierung und Übertragung von Informationen.
Empfehlung: Wenn Sie SNMPv3 verwenden, benutzen Sie SHA1 als Authentifizierungsprotokoll und AES als Datenschutzprotokoll (falls unterstützt).

IP-Filter
Im IP-Filter können mehrere IP-Adressen (einzelne Hosts oder Netzwerk-Subnetze) definiert werden, die auf die Kamera zugreifen dürfen. Es wird empfohlen, hier die Computer oder Netzwerke zu definieren, die auf die Kamera zugreifen.
Empfehlung: Es wird empfohlen, den IP-Filter zu verwenden, um erlaubte Hosts oder Netzwerke zu definieren.

Datum/Uhrzeit
Um den korrekten Zeitstempel auf Protokollen und Videodaten zu erhalten, empfiehlt es sich, die Zeit mit einem zentralen Zeitserver zu synchronisieren. Sowohl das SNTP- als auch das TLS-Datum können dafür verwendet werden. Der Vorteil von SNTP ist eine präzisere Zeitsynchronisation. Der Vorteil des TLS-Datums ist die Möglichkeit, auf ein korrektes Zertifikat zu prüfen, wodurch es die sicherere Lösung ist.
Empfehlung: Verwenden Sie eine sichere Methode zur Zeitsynchronisation, entweder mit SNTP oder TLS.

Cloud-basierte Dienste
Bosch bietet seine eigenen Cloud-basierten Dienste zur Verwaltung von Kameras über die Bosch Cloud an (Remote Portal). Die Cloud-Dienste stellen nicht automatisch eine Verbindung zu Remote Portal her und sind standardmäßig deaktiviert. Jede Kamera muss zuerst mit Remote Portal verbunden werden, wenn sie verwendet werden soll. Es wurden alle Vorkehrungen getroffen, um die Verbindung zwischen Remote Portal und Kamera zu sichern, so dass Remote Portal bei Bedarf in jeder Umgebung eingesetzt werden kann.

Empfehlung: Der Einsatz von Remote Portal kann abhängig davon sein, ob Cloud-Lösung verwendet wird.

Software-Versiegelung
Nach einer abgeschlossenen Konfiguration einer IP-Kamera sollten sich die Einstellungen des Geräts nicht mehr ändern. Ein Softwaresiegel kann aktiviert werden, um Sie über Änderungen der Gerätekonfiguration zu informieren.
Empfehlung: Aktivieren Sie die Softwareversiegelung, wenn keine Konfigurationsänderungen anstehen.

4.4.4 Defense in Depth

„Defense in Depth“ bezieht sich auf einen mehrschichtigen Sicherheitsansatz, bei dem keine einzelne Maßnahme allein für die Sicherheit eines Produkts verantwortlich ist, sondern es mehrere Schichten gibt, die ein Angreifer durchbrechen muss, um ein Produkt auszunutzen. Bei jeder Veröffentlichung eines Produkts wird geprüft, ob neue Funktionen erforderlich sind, um neue Angriffe abzuschwächen oder die allgemeine Sicherheit des Produkts zu erhöhen. Hier finden Sie einen Überblick über die wichtigsten Sicherheitsfunktionen der IP-Kamera.

- **Firmware-Signierung**
  Jede Firmware-Update-Datei ist verschlüsselt und mit einem Bosch-Zertifikat signiert. Es können nur von Bosch veröffentlichte Updates auf den Kameras installiert werden, um die Installation bösartiger Firmware zu verhindern.
- **Sicherer Start**
  Kameras der Plattformen CPP13, CPP14 oder neuer verfügen über einen Secure Boot-Mechanismus. Secure Boot prüft die Integrität des gesamten Systems, angefangen beim Bootloader bis hin zur Firmware auf den Kameras. Jeder Schritt des Bootvorgangs prüft den nächsten, beginnend mit einer unveränderlichen Hardware-Root of Trust. Dies verhindert, dass ein Angreifer den Bootloader oder die Firmware des Geräts verändern kann.
- **Anmeldung Firewall**
  Zum Schutz vor Brute-Force-Passwörtern, aber auch um Administratoren die Anmeldung zu ermöglichen und vor Denial-of-Service-Angriffen (DoS) zu schützen, prüft die Login-Firewall Anmeldeversuche auf der Grundlage einer Verhaltensanalyse und blockiert oder erlaubt den Zugriff dynamisch auf der Grundlage von IP-Adressen.
- **Kamera-Authentifizierung**
  Um eine Kamera eindeutig zu identifizieren und zu authentifizieren, wird während der Produktion für jede Kamera ein Bosch Gerätezertifikat erstellt. Mit diesem Zertifikat können Sie überprüfen, ob Sie mit einem echten Bosch Gerät kommunizieren. Darüber hinaus können benutzerdefinierte Zertifikate hochgeladen oder auf der Kamera erstellt werden, um die Integration in eine PKI-Umgebung zum Schutz vor Man-in-the-Middle-Angriffen zu ermöglichen.

4.5 Härten des Speichers

Da Bosch IP-Kameras oder Encoder eine iSCSI-Sitzung direkt mit einem iSCSI-Laufwerk herstellen und Videodaten auf ein iSCSI-Laufwerk schreiben können, müssen die iSCSI-Einheiten sich im selben LAN oder WAN wie die Bosch-Peripheriegeräte befinden.
Um unbefugten Zugriff auf die aufgezeichneten Videodaten zu vermeiden, müssen die iSCSI-Einheiten gegen unbefugten Zugriff geschützt werden:

- Verwenden Sie die Passwort-Authentifizierung über CHAP, um sicherzustellen, dass nur bekannte Geräte Zugriff auf das iSCSI-Ziel haben. Richten Sie beim iSCSI-Ziel ein CHAP-Passwort ein und geben Sie das konfigurierte Passwort in der VRM-Konfiguration ein. Das

CHAP-Passwort ist für VRM gültig und wird automatisch an alle Geräte gesendet. Wenn ein CHAP-Passwort in einer BVMS VRM-Umgebung verwendet wird, müssen alle Speichersysteme für die Verwendung desselben Passworts konfiguriert werden.
- Entfernen Sie alle Standard-Benutzernamen und -Passwörter vom iSCSI-Ziel.
- Verwenden Sie starke Passwörter für die Administrator-Benutzerkonten des iSCSI-Ziels.
- Deaktivieren Sie den administrativen Zugriff über Telnet auf die iSCSI-Ziele. Verwenden Sie stattdessen den SSH-Zugang.
- Schützen Sie den Konsolenzugriff auf das iSCSI-Ziel mit einem starken Passwort.
- Deaktivieren Sie nicht verwendete Netzwerkkarten.
- Überwachen Sie den Systemstatus von iSCSI-Speichern mit Drittanbietertools, um Abweichungen zu identifizieren.

4.5.1 Einrichten eines CHAP-Passworts auf iSCSI-Geräten

Wenn Sie ein globales CHAP-Passwort in BVMS Configuration Client festlegen, wird dieses Passwort automatisch an alle Encoder, Decoder und VSG-Geräte übertragen.
Für einige iSCSI-Geräte wird diese Funktion nicht unterstützt. Sie müssen das CHAP-Passwort auf diesen Geräten manuell festlegen.

Hinweis!
Sie müssen das globale CHAP-Passwort auf den iSCSI-Geräten festlegen, bevor Sie sie zu BVMS hinzufügen.
iSCSI-Geräte können nicht zu einer BVMS-Konfiguration hinzugefügt werden, in der das globale CHAP-Passwort bereits aktiviert ist.

So legen Sie manuell ein CHAP-Passwort auf einem iSCSI-Gerät (z.B. DIVAR IP) fest, das auf einer aktuellen Version des Betriebssystems Microsoft Windows Server basiert:

1. Öffnen Sie den **Server Manager,** und navigieren Sie zu **Datei- und Speicherdienste > iSCSI**.
2. Klicken Sie in der Liste **ISCSI TARGETS** mit der rechten Maustaste auf das gewünschte iSCSI-Ziel und klicken Sie auf **Eigenschaften**.
   Das Dialogfeld **Eigenschaften** wird angezeigt.
3. Klicken Sie im Dialogfeld **Eigenschaften** auf **Sicherheit** und aktivieren Sie dann das Kontrollkästchen **CHAP aktivieren**.
4. Geben Sie Folgendes ein:
   - **Benutzername:** Benutzer
   - **Passwort:** Geben Sie das globale CHAP-Passwort ein, wie es im BVMS Configuration Client angegeben ist (unter dem Menü **Hardware > iSCSI-Speicher mit CHAP-Passwort schützen...**).
5. Klicken Sie auf **OK**.
   Das CHAP-Passwort wird dem iSCSI-Ziel zugewiesen.

4.6 Härten von Servern

4.6.1 Empfohlene Einstellungen für die Server-Hardware

- Das Server-BIOS bietet die Möglichkeit, Passwörter für niedrigere Ebenen festzulegen. Mit diesen Passwörtern kann man verhindern, dass Personen ohne Genehmigung den Computer starten, von Wechseldatenträgern booten und BIOS- oder UEFI-Einstellungen (Unified Extensible Firmware Interface) ändern.

– Um Datenübertragungen zum Server zu verhindern, müssen die USB-Anschlüsse und das CD/DVD-Laufwerk deaktiviert werden.
  Darüber hinaus müssen die nicht genutzten Anschlüsse an der Netzwerkkarte deaktiviert werden und Verwaltungsports wie die HP ILO-Schnittstelle (HP Integrated Lights-Out) oder Konsolenports müssen entweder deaktiviert oder passwortgeschützt werden.

4.6.2 Empfohlene Sicherheitseinstellungen für das Windows-Betriebssystem

Server müssen Teil einer Windows-Domäne sein.
Durch die Integration von Servern in eine Windows-Domäne werden Netzwerkbenutzern Benutzerberechtigungen zugewiesen, die von einem zentralen Server verwaltet werden. Da diese Benutzerkonten häufig Regeln für Passwortstärke und -ablauf einsetzen, kann diese Integration die Sicherheit im Vergleich zu lokalen Konten verbessern, die diese Einschränkungen nicht haben.

4.6.3 Windows-Updates

Die Windows-Software-Patches und -Updates werden installiert und bleiben auf dem neuesten Stand. Windows-Updates enthalten oft Patches für neu entdeckte Sicherheitslücken, wie z.B. die Heartbleed SSL-Schwachstelle, von der Millionen von Computern weltweit betroffen waren. Updates für derart erhebliche Probleme müssen installiert werden.

4.6.4 Installation von Antivirenprogrammen

Installieren Sie Antiviren- und Antispywareprogramme und halten Sie sie auf dem neuesten Stand.

4.6.5 Empfohlene Einstellungen für das Windows-Betriebssystem

Die folgenden lokalen Gruppenrichtlinieneinstellungen sind empfohlene Gruppeneinstellungen in einem Windows-Serverbetriebssystem. Um die standardmäßigen Local Computer Policies (LCP) zu ändern, verwenden Sie den Editor für lokale Gruppenrichtlinien.
Sie können den Editor für lokale Gruppenrichtlinien mit der Kommandozeile oder über die Microsoft Management Console (MMC) öffnen.

Gehen Sie wie folgt vor, um den Editor für lokale Gruppenrichtlinien über die Kommandozeile zu öffnen:

- Klicken Sie auf **Start**, geben Sie im **Start**-Suchfeld **gpedit.msc** ein und drücken Sie die Eingabetaste.

Gehen Sie wie folgt vor, um den Editor für lokale Gruppenrichtlinien als MMC-Snap-In zu öffnen:

1. Klicken Sie auf **Start**, geben Sie im **Start**-Suchfeld **mmc** ein und drücken Sie die Eingabetaste.
2. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** auf **Gruppenrichtlinienobjekt-Editor** und klicken Sie dann auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt auswählen** auf **Durchsuchen**.
4. Klicken Sie auf **Dieser Computer**, um das lokale Gruppenrichtlinienobjekt zu bearbeiten, oder klicken Sie auf **Benutzer**, um lokale Gruppenrichtlinienobjekte für Administratoren, Nicht-Administratoren oder einzelne Benutzer zu bearbeiten.
5. Klicken Sie auf **Fertig stellen**.

4.6.6 Aktivieren der Benutzerkontensteuerung auf dem Server

Lokale Computerrichtlinien -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen

Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administratorkonto	Aktiviert
Benutzerkontosteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern	Deaktiviert
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorgenehmigungsmodus	Eingabeaufforderung zur Zustimmung
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer	Eingabeaufforderung zu Anmeldeinformationen auf dem sicheren Desktop
Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern	Aktiviert
Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und validiert sind	Deaktiviert
Benutzerkontensteuerung: Alle Administratoren im Administratorgenehmigungsmodus ausführen	Aktiviert
Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln	Aktiviert
Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren	Aktiviert

Lokale Computerrichtlinien -> Computerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> Benutzerschnittstellen für Anmeldeinformationen

Bei Ausführung mit erhöhten Rechten Administratorkonten auflisten	Deaktiviert

4.6.7 Deaktivieren der automatischen Wiedergabe

Lokale Computerrichtlinien -> Computerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> AutoPlay-Richtlinien

Autoplay deaktivieren	Alle Laufwerke aktiviert
AutoAusführen-Standardverhalten	Aktiviert, keine AutoAusführen-Befehle ausführen
Automatische Wiedergabe für andere Geräte als Volumes deaktivieren	Aktiviert

4.6.8 Externe Geräte

Lokale Computerrichtlinien -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen

Geräte: Entfernen ohne vorherige Anmeldung erlauben	Deaktiviert
Geräte: Formatieren und Auswerfen von Wechselmedien zulassen	Administratoren

Geräte: Anwendern das Installieren von Druckertreibern nicht erlauben	Aktiviert
Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert

4.6.9 Konfiguration des Zuweisens von Benutzerrechten

Lokale Computerrichtlinien -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Zuweisung von Benutzerrechten

Auf Anmeldeinformations-Manager als vertrauenswürdigem Aufrufer zugreifen	Niemand
Auf diesen Computer vom Netzwerk aus zugreifen	Authentifizierte Benutzer
Einsetzen als Teil des Betriebssystems	Niemand
Hinzufügen von Arbeitsstationen zur Domäne	Niemand
Anmelden über Remotedesktopdienste zulassen	Administratoren, Remotedesktopbenutzer
Ändern der Systemzeit	Administratoren
Ändern der Zeitzone	Administratoren, lokaler Dienst
Erstellen einer Auslagerungsdatei	Administratoren
Erstellen eines Tokenobjekts	Niemand
Erstellen von dauerhaft freigegebenen Objekten	Niemand
Zugriff vom Netzwerk auf diesen Computer verweigern	Anonyme Anmeldung, Gästegruppe
Anmelden als Batchauftrag verweigern	Anonyme Anmeldung, Gästegruppe
Anmelden als Dienst verweigern	Niemand
Lokal anmelden verweigern	Anonyme Anmeldung, Gästegruppe
Anmelden über Remotedesktopdienste verweigern	Anonyme Anmeldung, Gast
Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird	Niemand
Erzwingen des Herunterfahrens von einem Remotesystem aus	Administratoren
Generieren von Sicherheitsüberwachungen	Lokaler Dienst, Netzwerkdienst
Anheben der Zeitplanungspriorität	Administratoren
Laden und Entfernen von Gerätetreibern	Administratoren

Verändern einer Objektbezeichnung	Niemand
Verändern der Firmwareumgebungsvariablen	Administratoren
Durchführen von Volumewartungsaufgaben	Administratoren
Erstellen eines Profils für einen Einzelprozess	Administratoren
Entfernen des Computers von der Dockingstation	Administratoren
Wiederherstellen von Dateien und Verzeichnissen	Administratoren
Herunterfahren des Systems	Administratoren
Synchronisieren von Verzeichnisdienstdaten	Niemand
Übernehmen des Besitzes von Dateien und Objekten	Administratoren

4.6.10 Bildschirmschoner

– Aktivieren Sie den passwortgeschützten Bildschirmschoner und legen Sie die Timeout-Zeit fest:
Lokale Computerrichtlinien -> Benutzerkonfiguration -> Administrative Vorlagen -> Systemsteuerung -> Personalisierung

Bildschirmschoner aktivieren	Aktiviert
Kennwortschutz für den Bildschirmschoner verwenden	Aktiviert
Bildschirmschoner-Zeitlimit	1800 Sekunden

4.6.11 Aktivieren der Kennwortrichtlinieneinstellungen

– Das Aktivieren der Kennwortrichtlinieneinstellungen stellt sicher, dass Benutzerkennwörter die Mindestanforderungen für Kennwörter erfüllen.

Lokale Computerrichtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> Kontorichtlinien -> Passwortrichtlinie

Kennwortchronik erzwingen	10 gespeicherte Kennwörter
Maximales Kennwortalter	90 Tage
Minimales Kennwortalter	1 Tag
Minimale Kennwortlänge	10 Zeichen
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwort mit umkehrbarer Verschlüsselung für alle Benutzer in der Domäne speichern	Deaktiviert

4.6.12 Deaktivieren von nicht grundlegenden Windows-Diensten

– Das Deaktivieren von nicht grundlegenden Windows-Diensten ermöglicht eine höhere Sicherheitsstufe und minimiert die Angriffspunkte.

Gatewaydienst auf Anwendungsebene	Deaktiviert
Anwendungsverwaltung	Deaktiviert
Computersuchdienst	Deaktiviert

Client für die Überwachung verteilter Verknüpfungen	Deaktiviert
Funktionssuchanbieter-Host	Deaktiviert
Funktionssuche-Ressourcenveröffentlichung	Deaktiviert
Zugriff auf Eingabegeräte	Deaktiviert
Gemeinsame Nutzung der Internetverbindung	Deaktiviert
Verbindungsschicht-Topologieerkennungs-Zuordnungsprogramm	Deaktiviert
Multimediaklassenplaner	Deaktiviert
Offlinedateien	Deaktiviert
Verwaltung für automatische RAS-Verbindung	Deaktiviert
RAS-Verbindungsverwaltung	Deaktiviert
Routing und Remotezugriff	Deaktiviert
Shellhardwareerkennung	Deaktiviert
Hilfsprogramm für spezielle Verwaltungskonsole	Deaktiviert
SSDP-Suche	Deaktiviert

4.6.13 Benutzerkonten beim Windows-Betriebssystem

Die Benutzerkonten beim Windows-Betriebssystem müssen mit komplexen Passwörtern geschützt werden.
Server werden normalerweise mit Windows-Administratorkonten verwaltet und gewartet. Achten Sie darauf, dass starke Passwörter für die Administratorkonten verwendet werden.

Die Passwörter müssen Zeichen aus drei der folgenden Kategorien enthalten:
- Großbuchstaben aus europäischen Sprachen (A-Z, mit diakritischen, griechischen und kyrillischen Zeichen)
- Kleinbuchstaben aus europäischen Sprachen (a-z und ß, mit diakritischen, griechischen und kyrillischen Zeichen)
- Ziffern zur Basis 10 (0-9)
- Sonderzeichen: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Jedes Unicode-Zeichen, das als Buchstabe eingestuft wird, aber weder Groß- noch Kleinbuchstabe ist. Dies beinhaltet Unicode-Zeichen aus asiatischen Sprachen.

Die Verwendung der Windows Kontosperrung minimiert die Erfolgsrate für Attacken, bei denen Passwörter durch Raten ermittelt werden.
Die Empfehlung von Windows 8.1 Security Baselines ist 10/15/15:
- 10 ungültige Versuche
- 15 Minuten Sperrung
- Zurücksetzen des Zählers nach 15 Minuten

Lokale Computerrichtlinien -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Kontorichtlinien -> Richtlinie zur Kontosperrung

Kontosperrdauer	Kontosperrdauer

15 Minuten Kontensperrungsschwelle, 10 fehlgeschlagene Anmeldeversuche	15 Minuten Kontensperrungsschwelle, 10 fehlgeschlagene Anmeldeversuche
Zurücksetzungsdauer des Kontosperrungszählers	Zurücksetzungsdauer des Kontosperrungszählers

– Stellen Sie sicher, dass alle Standardpasswörter auf dem Server und dem Windows-Betriebssystem mit neuen, starken Passwörtern ersetzt werden.

4.6.14 Aktivieren der Firewall auf dem Server

▸ Aktivieren Sie die Kommunikation des BVMS-Standardports entsprechend den BVMS-Ports.

Hinweis!
Lesen Sie in der BVMS-Dokumentation nach, wie Sie die Ports einstellen und verwenden. Denken Sie daran, die Einstellungen nach Aktualisierungen der Firmware oder Software erneut zu überprüfen.

4.7 Härten von Windows-Clients

4.7.1 Windows-Arbeitsstationen

Die Windows Desktop-Betriebssysteme, die für BVMS Client-Anwendungen wie den BVMS Operator Client oder Configuration Client verwendet werden, sind außerhalb des gesicherten Bereichs installiert. Die Arbeitsstationen müssen gehärtet werden, um die Videodaten, die Dokumente und andere Anwendungen vor unbefugtem Zugriff zu schützen.
Die folgenden Einstellungen sollten angewendet oder überprüft werden.

4.7.2 Empfohlene Einstellungen für die Windows-Arbeitsstation-Hardware

– Legen Sie ein BIOS-/UEFI-Passwort fest, um zu verhindern, dass Personen alternative Betriebssysteme starten.
– Deaktivieren Sie die USB-Anschlüsse und das CD/DVD-Laufwerk, um Datenübertragungen zum Client zu verhindern. Außerdem müssen alle nicht genutzten Anschlüsse an der Netzwerkkarte deaktiviert werden.

4.7.3 Empfohlene Sicherheitseinstellungen für das Windows-Betriebssystem

– Die Arbeitsstation muss Teil einer Windows-Domäne sein.
  Durch die Integration der Arbeitsstation in eine Windows-Domäne können sicherheitsrelevante Einstellungen zentral verwaltet werden.
– Windows-Updates
  Bleiben Sie mit Softwarepatches und Aktualisierungen für das Windows Betriebssystem auf dem neuesten Stand.
– Installation von Antivirenprogrammen
  Installieren Sie Antiviren- und Antispywareprogramme und halten Sie sie auf dem neuesten Stand.

4.7.4 Empfohlene Einstellungen für das Windows-Betriebssystem

Die folgenden lokalen Gruppenrichtlinieneinstellungen sind empfohlene Gruppeneinstellungen in einem Windows-Serverbetriebssystem. Um die standardmäßigen Local Computer Policies (LCP) zu ändern, verwenden Sie den Editor für lokale Gruppenrichtlinien.
Sie können den Editor für lokale Gruppenrichtlinien mit der Kommandozeile oder über die Microsoft Management Console (MMC) öffnen.

Gehen Sie wie folgt vor, um den Editor für lokale Gruppenrichtlinien über die Kommandozeile zu öffnen:

- Klicken Sie auf **Start**, geben Sie im **Start**-Suchfeld **gpedit.msc** ein und drücken Sie die Eingabetaste.

Gehen Sie wie folgt vor, um den Editor für lokale Gruppenrichtlinien als MMC-Snap-In zu öffnen:

1. Klicken Sie auf **Start**, geben Sie im **Start**-Suchfeld **mmc** ein und drücken Sie die Eingabetaste.
2. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** auf **Gruppenrichtlinienobjekt-Editor** und klicken Sie dann auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt auswählen** auf **Durchsuchen**.
4. Klicken Sie auf **Dieser Computer**, um das lokale Gruppenrichtlinienobjekt zu bearbeiten, oder klicken Sie auf **Benutzer**, um lokale Gruppenrichtlinienobjekte für Administratoren, Nicht-Administratoren oder einzelne Benutzer zu bearbeiten.
5. Klicken Sie auf **Fertig stellen**.

4.7.5 Aktivieren der Benutzerkontensteuerung auf dem Server

Lokale Computerrichtlinien -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen

Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administratorkonto	Aktiviert
Benutzerkontosteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern	Deaktiviert
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorgenehmigungsmodus	Eingabeaufforderung zur Zustimmung
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer	Eingabeaufforderung zu Anmeldeinformationen auf dem sicheren Desktop
Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern	Aktiviert
Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und validiert sind	Deaktiviert
Benutzerkontensteuerung: Alle Administratoren im Administratorgenehmigungsmodus ausführen	Aktiviert
Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln	Aktiviert
Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren	Aktiviert

Lokale Computerrichtlinien -> Computerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> Benutzerschnittstellen für Anmeldeinformationen

Bei Ausführung mit erhöhten Rechten Administratorkonten auflisten	Deaktiviert

4.7.6 Deaktivieren der automatischen Wiedergabe

Lokale Computerrichtlinien -> Computerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> AutoPlay-Richtlinien

Autoplay deaktivieren	Alle Laufwerke aktiviert
AutoAusführen-Standardverhalten	Aktiviert, keine AutoAusführen-Befehle ausführen
Automatische Wiedergabe für andere Geräte als Volumes deaktivieren	Aktiviert

4.7.7 Externe Geräte

Lokale Computerrichtlinien -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen

Geräte: Entfernen ohne vorherige Anmeldung erlauben	Deaktiviert
Geräte: Formatieren und Auswerfen von Wechselmedien zulassen	Administratoren
Geräte: Anwendern das Installieren von Druckertreibern nicht erlauben	Aktiviert
Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert

4.7.8 Konfiguration des Zuweisens von Benutzerrechten

Lokale Computerrichtlinien -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Zuweisung von Benutzerrechten

Auf Anmeldeinformations-Manager als vertrauenswürdigem Aufrufer zugreifen	Niemand
Auf diesen Computer vom Netzwerk aus zugreifen	Authentifizierte Benutzer
Einsetzen als Teil des Betriebssystems	Niemand
Hinzufügen von Arbeitsstationen zur Domäne	Niemand
Anmelden über Remotedesktopdienste zulassen	Administratoren, Remotedesktopbenutzer
Ändern der Systemzeit	Administratoren
Ändern der Zeitzone	Administratoren, lokaler Dienst
Erstellen einer Auslagerungsdatei	Administratoren
Erstellen eines Tokenobjekts	Niemand
Erstellen von dauerhaft freigegebenen Objekten	Niemand

Zugriff vom Netzwerk auf diesen Computer verweigern	Anonyme Anmeldung, Gästegruppe
Anmelden als Batchauftrag verweigern	Anonyme Anmeldung, Gästegruppe
Anmelden als Dienst verweigern	Niemand
Lokal anmelden verweigern	Anonyme Anmeldung, Gästegruppe
Anmelden über Remotedesktopdienste verweigern	Anonyme Anmeldung, Gast
Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird	Niemand
Erzwingen des Herunterfahrens von einem Remotesystem aus	Administratoren
Generieren von Sicherheitsüberwachungen	Lokaler Dienst, Netzwerkdienst
Anheben der Zeitplanungspriorität	Administratoren
Laden und Entfernen von Gerätetreibern	Administratoren
Verändern einer Objektbezeichnung	Niemand
Verändern der Firmwareumgebungsvariablen	Administratoren
Durchführen von Volumewartungsaufgaben	Administratoren
Erstellen eines Profils für einen Einzelprozess	Administratoren
Entfernen des Computers von der Dockingstation	Administratoren
Wiederherstellen von Dateien und Verzeichnissen	Administratoren
Herunterfahren des Systems	Administratoren
Synchronisieren von Verzeichnisdienstdaten	Niemand
Übernehmen des Besitzes von Dateien und Objekten	Administratoren

4.7.9 Bildschirmschoner

– Aktivieren Sie den passwortgeschützten Bildschirmschoner und legen Sie die Timeout-Zeit fest:
Lokale Computerrichtlinien -> Benutzerkonfiguration -> Administrative Vorlagen -> Systemsteuerung -> Personalisierung

Bildschirmschoner aktivieren	Aktiviert
Kennwortschutz für den Bildschirmschoner verwenden	Aktiviert
Bildschirmschoner-Zeitlimit	1800 Sekunden

4.7.10 Aktivieren der Kennwortrichtlinieneinstellungen

– Das Aktivieren der Kennwortrichtlinieneinstellungen stellt sicher, dass Benutzerkennwörter die Mindestanforderungen für Kennwörter erfüllen.

Lokale Computerrichtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> Kontorichtlinien -> Passwortrichtlinie

Kennwortchronik erzwingen	10 gespeicherte Kennwörter
Maximales Kennwortalter	90 Tage
Minimales Kennwortalter	1 Tag
Minimale Kennwortlänge	10 Zeichen
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwort mit umkehrbarer Verschlüsselung für alle Benutzer in der Domäne speichern	Deaktiviert

4.7.11 Deaktivieren von nicht grundlegenden Windows-Diensten

– Das Deaktivieren von nicht grundlegenden Windows-Diensten ermöglicht eine höhere Sicherheitsstufe und minimiert die Angriffspunkte.

Gatewaydienst auf Anwendungsebene	Deaktiviert
Anwendungsverwaltung	Deaktiviert
Computersuchdienst	Deaktiviert
Client für die Überwachung verteilter Verknüpfungen	Deaktiviert
Funktionssuchanbieter-Host	Deaktiviert
Funktionssuche-Ressourcenveröffentlichung	Deaktiviert
Zugriff auf Eingabegeräte	Deaktiviert
Gemeinsame Nutzung der Internetverbindung	Deaktiviert
Verbindungsschicht-Topologieerkennungs-Zuordnungsprogramm	Deaktiviert
Multimediaklassenplaner	Deaktiviert
Offlinedateien	Deaktiviert
Verwaltung für automatische RAS-Verbindung	Deaktiviert
RAS-Verbindungsverwaltung	Deaktiviert
Routing und Remotezugriff	Deaktiviert
Shellhardwareerkennung	Deaktiviert
Hilfsprogramm für spezielle Verwaltungskonsole	Deaktiviert
SSDP-Suche	Deaktiviert

4.7.12 Benutzerkonten beim Windows-Betriebssystem

Die Benutzerkonten beim Windows-Betriebssystem müssen mit komplexen Passwörtern geschützt werden.
Server werden normalerweise mit Windows-Administratorkonten verwaltet und gewartet. Achten Sie darauf, dass starke Passwörter für die Administratorkonten verwendet werden.

Die Passwörter müssen Zeichen aus drei der folgenden Kategorien enthalten:

– Großbuchstaben aus europäischen Sprachen (A-Z, mit diakritischen, griechischen und kyrillischen Zeichen)
– Kleinbuchstaben aus europäischen Sprachen (a-z und ß, mit diakritischen, griechischen und kyrillischen Zeichen)
– Ziffern zur Basis 10 (0-9)
– Sonderzeichen: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
– Jedes Unicode-Zeichen, das als Buchstabe eingestuft wird, aber weder Groß- noch Kleinbuchstabe ist. Dies beinhaltet Unicode-Zeichen aus asiatischen Sprachen.

Die Verwendung der Windows Kontosperrung minimiert die Erfolgsrate für Attacken, bei denen Passwörter durch Raten ermittelt werden.
Die Empfehlung von Windows 8.1 Security Baselines ist 10/15/15:
– 10 ungültige Versuche
– 15 Minuten Sperrung
– Zurücksetzen des Zählers nach 15 Minuten

Lokale Computerrichtlinien -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Kontorichtlinien -> Richtlinie zur Kontosperrung

Kontosperrdauer	Kontosperrdauer
15 Minuten Kontensperrungsschwelle, 10 fehlgeschlagene Anmeldeversuche	15 Minuten Kontensperrungsschwelle, 10 fehlgeschlagene Anmeldeversuche
Zurücksetzungsdauer des Kontosperrungszählers	Zurücksetzungsdauer des Kontosperrungszählers

– Stellen Sie sicher, dass alle Standardpasswörter auf dem Server und dem Windows-Betriebssystem mit neuen, starken Passwörtern ersetzt werden.
– Deaktivieren Sie nicht verwendete Konten des Windows-Betriebssystems.
– Deaktivieren Sie den Remotedesktopzugriff auf die Client-Arbeitsstation.
– Führen Sie die Arbeitsstation ohne Administratorrechte aus, um zu vermeiden, dass Standardbenutzer Systemeinstellungen ändern.

4.7.13 Aktivieren der Firewall auf der Arbeitsstation

▸ Aktivieren Sie die Kommunikation des BVMS-Standardports entsprechend den BVMS-Ports.

Hinweis!
Lesen Sie in der BVMS-Dokumentation nach, wie Sie die Ports einstellen und verwenden. Denken Sie daran, die Einstellungen nach Aktualisierungen der Firmware oder Software erneut zu überprüfen.

4.8 Schützen des Netzwerkzugriffs

Derzeit werden viele kleine bis mittelgroße IP-Videoüberwachungssysteme in der vorhandenen Netzwerkinfrastruktur des Kunden nur als „eine weitere IT-Anwendung“ implementiert.
Diese Art der Implementierung hat zwar Vorteile in Bezug auf Kosten und Wartung, setzt das Sicherheitssystem aber externen und internen Bedrohungen aus. Geeignete Maßnahmen müssen ergriffen werden, um unerwünschte Situationen zu vermeiden, beispielsweise das Leaken von Videos eines Ereignisses im Internet oder in sozialen Netzwerken. Solche Vorkommnisse verletzen möglicherweise nicht nur die Privatsphäre, sondern können auch dem Unternehmen schaden.

Es gibt zwei Haupttechnologien für die Erstellung eines „Netzwerks im Netzwerk”. Welche Technologie von den IT-Infrastrukturarchitekten gewählt wird, hängt in hohem Maße von der vorhandenen Netzwerkinfrastruktur, den implementierten Netzwerkgeräten, den gewünschten Funktionen und der Topologie des Netzwerks ab.

4.8.1 VLAN: Virtuelles LAN

Ein virtuelles LAN wird erstellt, indem ein LAN in mehrere Segmente unterteilt wird. Die Segmentierung des Netzwerks erfolgt über Netzwerk-Switches oder Routerkonfiguration. Ein VLAN hat den Vorteil, dass man geändertem Ressourcenbedarf ohne die Neuverkabelung der Netzwerkverbindungen von Geräten begegnen kann.
Die Qualität der Serviceschemata, die auf bestimmte Segmente wie die Videoüberwachung angewendet werden, verbessert möglicherweise nicht nur die Sicherheit, sondern auch die Leistung.

VLANs werden auf der Sicherungsschicht (OSI-Schicht 2) implementiert und haben Ähnlichkeit mit IP-Subnetting (siehe *Zuweisen von IP-Adressen, Seite 8*), das der Vermittlungsschicht (OSI-Schicht 3) ähnelt.

4.8.2 VPN: Virtual Private Network

Ein VPN ist ein getrenntes (privates) Netzwerk, das sich häufig über öffentliche Netzwerke oder das Internet erstreckt. Es stehen verschiedene Protokolle zur Verfügung, um ein VPN zu erstellen, typischerweise ein Tunnel, der den geschützten Datenverkehr überträgt. VPNs können als Point-to-Point-Tunnel, Any-to-Any-Verbindungen oder Multi-Point-Verbindungen ausgelegt sein. VPNs können mit verschlüsselter Kommunikation implementiert werden oder lediglich auf die sichere Kommunikation innerhalb des VPN selbst bauen.

VPNs können verwendet werden, um entfernte Standorte über Wide Area Network (WAN)-Verbindungen zu verbinden und gleichzeitig die Privatsphäre zu schützen und die Sicherheit innerhalb eines Local Area Network (LAN) zu erhöhen. Da ein VPN als ein separates Netzwerk fungiert, funktionieren alle Geräte im VPN wie in einem typischen Netzwerk. Ein VPN fügt einem Überwachungssystem nicht nur eine zusätzliche Schutzebene hinzu, sondern hat darüber hinaus auch den Vorteil, dass der geschäftliche und Video-Traffic eines Produktionsnetzwerks aufgeteilt werden.

Hinweis!
Falls vorhanden, erhöhen VLAN oder VPN die Sicherheit des Überwachungssystems, das in die vorhandene IT-Infrastruktur integriert ist.

Abgesehen vom Schutz des Überwachungssystems vor unbefugtem Zugriff in der gemeinsamen IT-Infrastruktur muss man überlegen, wer sich überhaupt mit dem Netzwerk verbinden darf.

4.8.3 Deaktivieren nicht verwendeter Switch-Anschlüsse

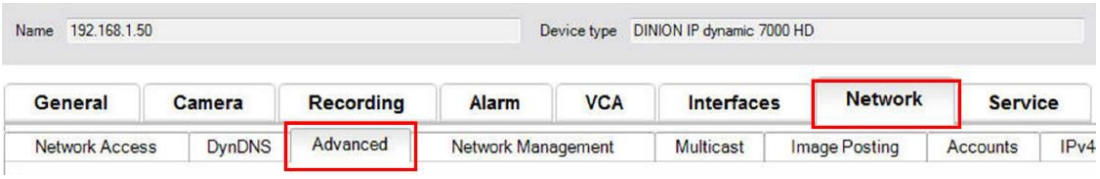
Durch das Deaktivieren nicht verwendeter Netzwerkanschlüsse wird gewährleistet, dass nicht autorisierte Geräte keinen Zugriff auf das Netzwerk erhalten. Damit kann das Risiko vermindert werden, dass jemand versucht, durch das Anschließen eines Geräts an einen Switch oder nicht verwendeten Netzwerkanschluss auf ein Sicherheitssubnetz zuzugreifen. Das Deaktivieren bestimmter Anschlüsse wird sowohl bei Low-Cost- als auch Enterprise-Systemen häufig bei managed Switches eingesetzt.

4.8.4 802.1x-geschützte Netzwerke

Alle Bosch IP-Videogeräte können als 802.1x-Clients konfiguriert werden. Dadurch können sie sich bei einem RADIUS-Server authentifizieren und an einem gesicherten Netzwerk teilnehmen. Bevor Sie die Videogeräte in einem gesicherten Netzwerk implementieren können, müssen Sie sich mit einem Techniker-Laptop direkt mit dem Videogerät verbinden, um gültige Anmeldeinformationen einzugeben (siehe folgende Anleitung).

802.1x-Dienste können einfach über den Configuration Manager konfiguriert werden.

1. Wählen Sie im Configuration Manager das gewünschte Geräte aus.
2. Wählen Sie die Registerkarte **Netzwerk** aus und wählen Sie dann **Erweitert** aus.



3. Suchen Sie auf der Seite den Abschnitt **802.1x**.
4. Wählen Sie im Dropdown-Menü **802.1x** die Option **Ein** aus.
5. Geben Sie eine gültige **Identität** und ein gültiges **Passwort** ein.
6. Speichern Sie die Änderungen.
7. Trennen Sie die Verbindung und implementieren Sie die Geräte im gesicherten Netzwerk.

Hinweis!
802.1x selbst bietet keine sichere Kommunikation zwischen dem Supplicant und Authentication-Server.
Daher können Benutzername und Passwort aus dem Netzwerk ausgespäht werden. 802.1x kann EAP-TLS für eine sichere Kommunikation verwenden.

Extensible Authentication Protocol – Transport Layer Security
Das Extensible Authentication Protocol (EAP) unterstützt mehrere Authentifizierungsmethoden. Transport Layer Security (TLS) ermöglicht die gegenseitige Authentifizierung, integritätsgeschützte Cipher Suite Negotiation und Schlüsselaustausch zwischen zwei Endpunkten. EAP-TLS unterstützt zertifikatbasierte gegenseitige Authentifizierung und Schlüsselableitung. EAP-TLS fasst also den Vorgang zusammen, bei dem sowohl Server als auch Client einander ein Zertifikat senden.

Hinweis!
Lesen Sie das spezifische Technische Whitepaper *Netzwerkauthentifizierung - 802.1x - Sichern des Netzwerkendpunkts*. Sie finden es im Online-Produktkatalog von Bosch Security Systems unter:
http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

5 Sicherer Betrieb

5.1 Trennung des Netzwerks

Sofern möglich, sollte das Gerät in einem separaten Netzwerk betrieben werden (z. B. bei Verwendung von WLNs) mit Zugangsbeschränkungen zur Begrenzung des Übertragungsverkehrs und zum Schutz des Geräts vor Netzwerkangriffen.

5.2 Sichere Schlüsselaufbewahrung im Hardware-Tresor

Private Schlüssel von Zertifikaten sind am besten geschützt, wenn sie sicher in einer Hardwarekomponente oder einem Hardware-Tresor aufbewahrt werden. Solche Chips bieten Schutz vor unbefugtem Zugriff auf private Schlüssel, selbst wenn das Gerät physisch geöffnet ist, um Zugang zu erhalten.
In Bosch Kameras werden solche Schlüssel in einem separaten Krypto-Prozessor oder Secure Element (SE) gespeichert. Beide bieten eine sichere Speicherung sowie kryptografische Funktionen, die private Schlüssel niemals an Orten oder in Speichern preisgeben, von denen sie möglicherweise abgerufen werden könnten.
Auf Arbeitsstation und Servern ist in der Regel ein Trusted Platform Module (TPM) Chip verfügbar. Kryptografische Bibliotheken und Funktionen sollten so konfiguriert werden, dass sie den TPM-Speicher verwenden, sofern dies möglich ist.

5.3 Eindeutige Gerätezertifikate

Obwohl jedes TLS- oder HTTPS-fähige Gerät in der Regel über ein selbstsigniertes Standardzertifikat verfügt, sollte dieses Zertifikat nicht als ausreichend für die Authentifizierung angesehen werden, da es keinen Schutz vor einem Man-in-the-Middle-Angriff (MITM) bietet.

Wenn Geräte in einer Umgebung implementiert werden, in der zusätzliche Schritte erforderlich sind, um die Identität jedes einzelnen IP-Videogeräts zu überprüfen, können neue Zertifikate und private Schlüssel erstellt und auf die Videogeräte hochgeladen werden. Neue Zertifikate können von einer Zertifizierungsstelle (CA) abgerufen oder mit einem OpenSSL-Toolkit erstellt werden.

Falls Geräte in öffentlichen Netzwerken verwendet werden, wird empfohlen, Zertifikate von einer öffentlichen Zertifizierungsstelle abzurufen oder eigene Zertifikate von einer solchen Stelle signieren zu lassen. Öffentliche Zertifizierungsstellen sind auch in der Lage, den Ursprung und die Gültigkeit – in anderen Worten die Vertrauenswürdigkeit – des Gerätezertifikats zu überprüfen.

Seit Jahren werden alle Bosch Kameras mit einem vorinstallierten, eindeutigen Gerätezertifikat und einem privaten Schlüssel ausgeliefert, die vom Bosch-Root-Zertifikat abgeleitet und in einer sicheren Produktionsumgebung installiert wurden, um zu beweisen, dass es sich bei der Kamera um ein „ursprünglich hergestelltes“ Bosch-Gerät handelt. Dieses Zertifikat wird automatisch für HTTPS Verbindungen verwendet und kann zur Identifizierung und Authentifizierung eines Geräts verwendet werden, indem die Zertifikatskette bis zum Bosch-Root-Zertifikat überprüft wird.

Hinweis!
Zertifikate sollten für die Authentifizierung eines einzelnen Geräts verwendet werden. Es wird empfohlen, ein spezifisches Zertifikat pro Gerät zu erstellen, das von einem Root-Zertifikat abgeleitet wird.

Die sicherste Variante eines Zertifikatseinsatzes besteht darin, auf dem Gerät eine Zertifikatsignierungsanforderung (CSR) zu erstellen und ein Zertifikat bei einer internen oder externen Zertifizierungsstelle anzufordern.
Bei einer Zertifikatsignierungsanforderung hält das Gerät den privaten Schlüssel intern und gibt nur den Rest des Zertifikats frei, um von der Zertifizierungsstelle signiert zu werden. Der private Schlüssel ist sicher im Secure Element (SE) der Kamera oder z.B. im Trusted Platform Module (TPM) des Geräts gespeichert.
Wenn ein Gerät eine CSR-Möglichkeit bietet, sollte dies daher der bevorzugte Weg sein, um ein Zertifikat zu erstellen.

Zertifikate können entweder über die Geräte-Webseite eines Videogeräts oder über den Configuration Manager auf ein Gerät hochgeladen werden.

Hochladen von Zertifikaten mit Hilfe der Geräte-Webseite
Zertifikate können über die Webseite des Videogeräts hochgeladen werden.
Auf der Geräte-Webseite können Sie auf der Seite **Zertifikate** neue Zertifikate hinzufügen und löschen und ihre Verwendung definieren.

Hochladen von Zertifikaten mit dem Configuration Manager
Im Configuration Manager können Zertifikate problemlos auf einzelne oder mehrere Geräte gleichzeitig hochgeladen werden.
Hochladen von Zertifikaten:
1. Wählen Sie im Configuration Manager ein oder mehrere Geräte aus.
2. Klicken Sie mit der rechten Maustaste und klicken Sie dann auf **Datei-Upload** und anschließend auf **SSL-Zertifikat...**.
   Ein Windows-Explorer-Fenster wird geöffnet, in dem Sie das gewünschte Zertifikat suchen können.

Für kleinere Systeme bietet der Configuration Manager eine unterstützende Funktion namens **MicroCA**, die es ermöglicht, eine Root CA zu erstellen oder zu verwenden und daraus Gerätezertifikate abzuleiten oder sie zum Signieren von Zertifikatsignierungsanforderungen der Geräte zu verwenden, auch für mehrere Geräte gleichzeitig. Weitere Einzelheiten finden Sie im Benutzerhandbuch des Configuration Manager.

Siehe
– *Vertrauen schaffen mit Zertifikaten, Seite 49*

5.4 Prüfen von Protokolldateien

Die Überwachung der Protokolldateien ist ein wichtiger Bestandteil der Sicherheitsanalyse oder der Wartungsaktivitäten. Eine regelmäßige Überprüfung der Protokolldateien kann Konfigurationsprobleme oder Sicherheitsverstöße wie falsche Anmeldungen aufdecken.
Um Protokolldateien zu analysieren und langfristig zu speichern, empfiehlt es sich, die Protokolldateien des Geräts an einen Syslog-Server oder ein SIEM-System zu senden, da eine Kamera beispielsweise einen festen Speicherplatz für die interne Protokollierung reserviert, aber ältere Protokolle überschreibt, wenn dieser Speicherplatz voll ist.

5.5 SIEM-System

Das SIEM-System (Security Information and Event Management) wird zum Sammeln und Analysieren von Informationen aus verschiedenen Geräten und Systemen verwendet. Die Geräte können in ein SIEM-System integriert werden, indem die Protokolle über das Syslog-Protokoll gesendet werden. Die Analyse dieser Protokolle kann bei der Wartung helfen und Konfigurationsfehler oder Angriffe auf das Gerät (z.B. falsche Anmeldungen) aufdecken.

5.6 PKI

Public Key Infrastructure (PKI) bezieht sich auf die Systeme, die zur Erstellung und Verwaltung digitaler Zertifikate benötigt werden. Für HTTPS, Netzwerkauthentifizierung mit 802.1x, Benutzerauthentifizierung mit Zertifikaten und andere Verschlüsselungsfunktionen können benutzerdefinierte Zertifikate auf dem Gerät installiert werden.

5.7 AD FS

Active Directory Federation Services (AD FS) ist ein von Microsoft angebotener Dienst, der die Authentifizierung bei einem lokalen Active Directory (über einen AD FS-Server) oder bei der Azure Cloud ermöglicht. Neben der lokalen Benutzerauthentifizierung mit Passwörtern oder zertifikatsbasierter Authentifizierung ist die Integration von Geräten in eine Active Directory-Domäne mit AD FS möglich, um den Benutzerzugang zentral zu authentifizieren und zu verwalten.

5.8 Sicherer Betrieb von IP-Kameras

5.8.1 Vertrauen schaffen mit Zertifikaten

Alle Bosch IP-Kameras mit Firmware-Version 6.10 oder neuer verwenden einen Zertifikatspeicher, den man im Menü **Service** der Kamerakonfiguration finden kann. Bestimmte Serverzertifikate, Client-Zertifikate und vertrauenswürdige Zertifikate können zum Speicher hinzugefügt werden.

Hinzufügen eines Zertifikats zum Speicher:

1. Navigieren Sie in der Webseite des Geräts zur Seite **Konfiguration**.
2. Wählen Sie das Menü **Service** und das Untermenü **Zertifikate** aus.
3. Klicken Sie im Abschnitt **Dateiliste** auf **Hinzufügen**.
4. Laden Sie die gewünschten Zertifikate hoch.
   Wenn der Upload abgeschlossen ist, werden die Zertifikate im Abschnitt **Nutzungsliste** angezeigt.
5. Wählen Sie im Abschnitt **Nutzungsliste** das gewünschte Zertifikat aus.
6. Die Kamera muss neu gestartet werden, damit sie die Zertifikate verwenden kann. Klicken Sie auf **Setzen**, um die Kamera neu zu starten.

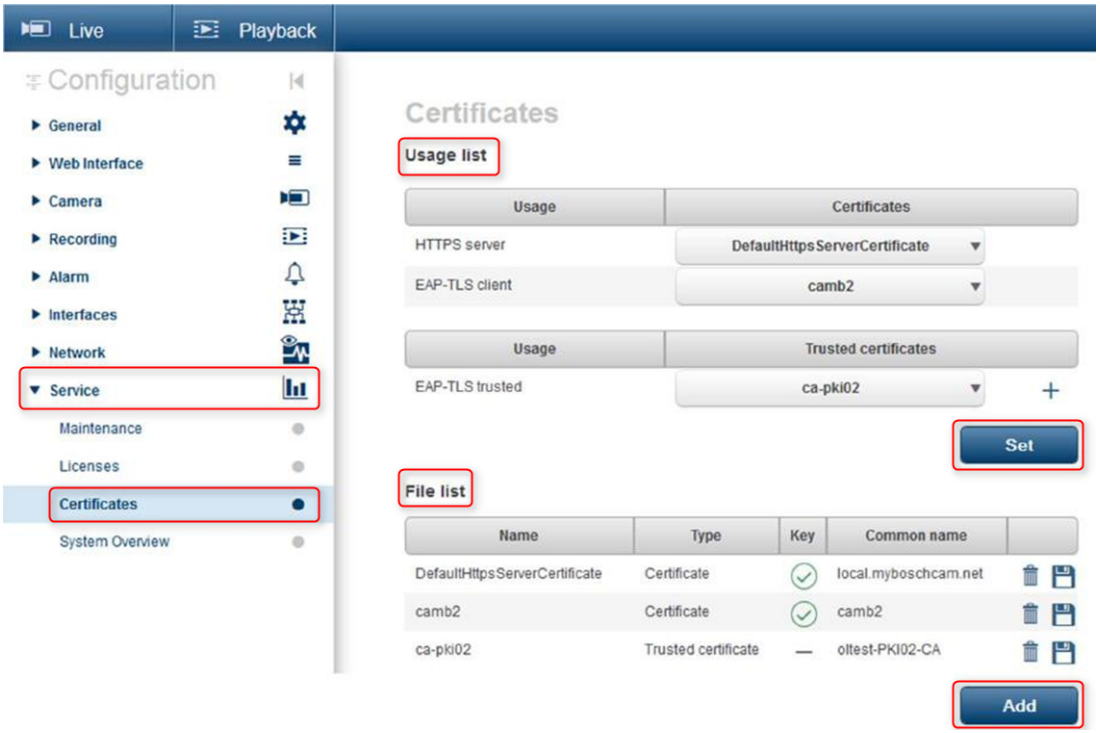


Abbildung 5.1: Beispiel: In einer Bosch Kamera (FW 6.11) gespeicherte EAP/TLS-Zertifikate

Es werden base64-codierte Zertifikate im *.pem-, *.cer- oder *.crt-Format akzeptiert. Sie können als eine kombinierte Datei hochgeladen werden, es ist aber auch der in Zertifikat- und Schlüsseldateien aufgeteilte Upload möglich. Werden die Dateien separat in dieser Reihenfolge hochgeladen, dann werden sie automatisch zusammengefügt.

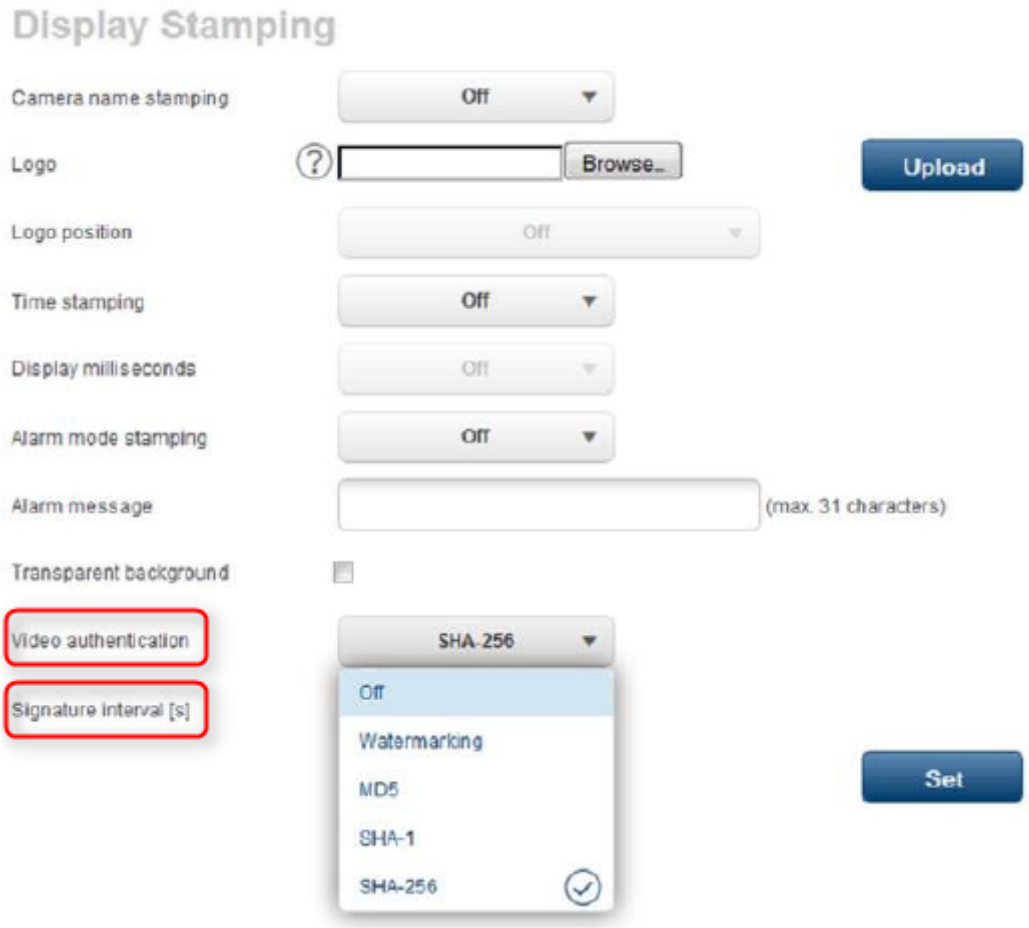
Seit Firmware-Version 6.20 werden passwortgeschützte private PKCS#8-Schlüssel (AES-verschlüsselt) unterstützt, die im base64-codierten *.pem-Format hochgeladen werden müssen.

5.8.2 Video-Authentifizierung

Sobald die Geräte in einem System geschützt und ordnungsgemäß authentifiziert sind, sollte man auch ein Auge auf die von ihnen übertragenen Videodaten haben. Diese Methode wird Video-Authentifizierung genannt.
Die Video-Authentifizierung dreht sich ausschließlich um Methoden zur Überprüfung der Authentizität der Videos. Video-Authentifizierung behandelt in keiner Weise die Übertragung von Video und Daten.
Vor der Veröffentlichung der Firmware-Version 5.9 erfolgte Watermarking durch einen einfachen Prüfsummenalgorithmus über den Video-Stream. Beim grundlegenden Watermarking werden weder Zertifikate noch Verschlüsselung verwendet. Eine Prüfsumme ist eine grundlegende Messung der „Datenbeständigkeit” einer Datei und überprüft die Integrität einer Datei.
Konfiguration der Video-Authentifizierung, z. B. im Webbrowser:

1. Navigieren Sie zum Menü **Allgemein** und wählen Sie dann **Bildeinblendungen** aus.
2. Wählen Sie im Dropdown-Menü **Video-Authentifizierung** die gewünschte Option aus:
   Ab Firmware-Version 5.9 gibt es abgesehen vom klassischen Watermarking drei weitere Optionen zur Video-Authentifizierung:
   – MD5: Message-Digest erzeugt einen 128-Bit-Hashwert.

- SHA-1: Der Secure Hash Algorithm wurde von der US-amerikanischen National Security Agency (NSA) entworfen und ist ein U.S. Federal Information Processing Standard (FIPS), der vom US-amerikanischen National Institute of Standards and Technology (NIST) veröffentlicht wird. SHA-1 erzeugt einen 160-Bit-Hashwert.
- SHA-256: Der SHA-256-Algorithmus erzeugt einen nahezu einzigartigen Hashwert mit fester Größe von 256 Bit (32 Byte).



Hinweis!
Ein Hash ist eine einseitige Funktion – es kann nicht wieder entschlüsselt werden.

Bei der Video-Authentifizierung wird jedes Paket eines Video-Streams gehasht. Diese Hashes werden im Video-Stream eingebettet und zusammen mit den Videodaten gehasht. Dadurch wird die Integrität der Streaminhalte gewährleistet.

Die Hashes werden in regelmäßigen (vom Signaturintervall definierten) Zeitabständen mit dem privaten Schlüssel des Zertifikats signiert, das im TPM des Geräts gespeichert ist. Alarmaufzeichnungen und Blockänderungen in iSCSI-Aufzeichnungen werden alle mit einer Signatur geschlossen, um die kontinuierliche Authentizität des Videos zu gewährleisten.

Hinweis!
Die Berechnung der digitalen Signatur erfordert eine Rechenleistung, die bei zu häufigem Einsatz die Gesamtleistung einer Kamera beeinflussen kann. Daher sollte ein angemessenes Intervall gewählt werden.

Da die Hashes und digitalen Signaturen im Video-Stream eingebettet sind, werden sie auch in der Aufzeichnung gespeichert, sodass die Video-Authentifizierung auch bei Wiedergabe und Exporten möglich ist.

6 Verwaltung von Sicherheitsupdates

Stellen Sie vor der Erstinbetriebnahme des Geräts sicher, dass die neueste gültige Version der Software installiert ist. Sie sollten die Software während der gesamten Betriebsdauer des Geräts immer auf dem aktuellen Stand halten, um die bestmögliche Funktionalität, Kompatibilität, Leistung und Sicherheit zu erhalten. Befolgen Sie die Anweisungen zu Softwareaktualisierungen in der Produktdokumentation.
Die folgenden Links bieten weitere Informationen:

- Allgemeine Informationen: https://www.boschsecurity.com/xc/en/support/product-security/
- Sicherheitsanweisungen, d. h. eine Liste bekannter Sicherheitslücken und vorgeschlagene Lösungen: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch haftet nicht für Schäden, die durch den Betrieb seiner Produkte mit veralteten Softwarekomponenten verursacht werden.

Die neuesten Firmware- und Softwareversionen finden Sie im Download Store von Bosch Security and Safety Systems:
https://downloadstore.boschsecurity.com/
Für Geräte, die mit Remote Portal verbunden sind, können Benutzer über den Remote Alert Service eine E-Mail-Benachrichtigung über verfügbare Firmwareupdates erhalten.
Umfangreichere Download-Pakete werden über den Produktkatalog von Bosch Security and Safety Systems vertrieben:
https://www.boschsecurity.com

7 Sicherheitsüberwachung

Da sich die Anforderungen ständig ändern, ist eine 100%ige Sicherheit niemals gewährleistet. Daher hat Bosch einen strukturierten Prozess für das Management von Schwachstellen und Zwischenfällen eingerichtet, um potenzielle Sicherheitslücken und Zwischenfälle professionell zu verwalten.

Der professionelle und systematische Umgang mit gemeldeten Sicherheitslücken sowie die Transparenz gegenüber unseren Kunden ist uns sehr wichtig. Deshalb untersuchen wir alle Berichte über Sicherheitslücken. Wir führen eine Bewertung der Sicherheitsschwachstellen von Produkten gemäß dem Common Vulnerability Scoring System (CVSS) durch. CVSS ist ein freier und offener Industriestandard zur Bewertung des Schweregrads von Sicherheitslücken in Computersystemen. Die Scores werden anhand einer Formel berechnet, die von mehreren Metriken abhängt, die die Leichtigkeit des Ausnutzens und die Auswirkungen des Ausnutzens annähern. Die Punktzahl reicht von 0 bis 10, wobei 10 die höchste Stufe ist.

Im Falle einer bestätigten Sicherheitslücke informieren wir unsere Kunden durch die Veröffentlichung eines Sicherheitshinweises über eine identifizierte Sicherheitslücke in einem Produkt oder einer Lösung und deren Behebung. Alle Sicherheitshinweise enthalten:

- Beschreibung der Sicherheitslücke mit CVE-Referenz (Common Vulnerabilities and Exposures) und CVSS-Score.
- Identität der bekannten betroffenen Produkte und Software-/Hardware-Versionen.
- Informationen über mildernde Faktoren und Umgehungsmöglichkeiten.
- Zeitplan und Ort der verfügbaren Korrekturen oder anderer Abhilfemaßnahmen.

Die Liste der veröffentlichten Sicherheitshinweise finden Sie auf unserer Website https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html.
Wann immer Sie glauben, eine Schwachstelle oder ein anderes Sicherheitsproblem im Zusammenhang mit einem Bosch Produkt oder Dienst entdeckt zu haben, wenden Sie sich an das Bosch Product Security Incident Response Team (PSIRT): https://psirt.bosch.com.

8 Sichere Entsorgung und Außerbetriebnahme

Zu einem bestimmten Zeitpunkt im Lebenszyklus eines Produkts oder eines Systems kann es notwendig sein, ein Gerät oder eine Komponente zu ersetzen oder außer Betrieb zu nehmen. Da das Gerät oder die Komponente möglicherweise sensible Daten wie Anmeldeinformationen oder Zertifikate enthält, stellen Sie sicher, dass Sie diese Daten vollständig und sicher löschen.

Sie können die meisten Geräte auf die Grundeinstellungen zurücksetzen.
Bei den meisten IP-Kameras und Encodern können Sie dafür die Reset-Taste verwenden. Für diejenigen, die keine Reset-Taste haben, verwenden Sie die werkseitig eingestellte Funktion über die Webschnittstelle, bevor Sie sie aus dem Netzwerk demontieren.
Alle Benutzer und ihre jeweiligen Passwörter werden gelöscht und die Einstellungen werden auf die Grundeinstellungen zurückgesetzt. Alle Zertifikate und die entsprechenden Schlüssel, die im TPM oder sicheren Element gespeichert waren, werden ebenfalls gelöscht.

Andere Geräte haben möglicherweise andere Optionen, um sie auf die Grundeinstellungen zurückzusetzen. Beachten Sie die Anweisungen in der jeweiligen Benutzerdokumentation für die korrekte Entsorgung.
Auf Servern und Arbeitsstationen können ebenfalls Zertifikate und Anmeldedaten gespeichert sein. Verwenden Sie die richtigen Tools und Methoden, um sicherzustellen, dass Ihre relevanten Daten bei der Stilllegung oder vor der Entsorgung sicher gelöscht werden.

Es wird empfohlen, die Geräte auf die Grundeinstellungen zurückzusetzen, auch für den Fall, dass sie in eine andere Installation verschoben werden müssen, die möglicherweise andere Anmeldedaten oder Zertifikate verwendet.

Hinweis!
Beachten Sie die Anweisungen in der jeweiligen Benutzerdokumentation für die korrekte Entsorgung.

9 Zusatzinformationen

Weitere Informationen, Software-Downloads und Dokumentation finden Sie auf der jeweiligen Produktseite im Produktkatalog:
http://www.boschsecurity.com

Glossar

802.1x

Der Standard IEEE 802.1x stellt eine allgemeine Methode für die Authentifizierung und Berechtigung in IEEE-802-Netzwerken zur Verfügung. Die Berechtigungsprüfung erfolgt durch einen Authenticator, der mittels eines Berechtigungsprüf-Servers (siehe RADIUS-Server) die übertragenen Berechtigungsinformationen prüft und den Zugriff auf die angebotenen Dienste (LAN, VLAN oder WLAN) zulässt oder abweist.

Authentifizierung

Prozess zur Authentizitätsprüfung eines Video-Streams. Der Benutzer kann eine Authentifizierung starten. Bei der Feststellung nicht authentischer Daten wird eine Meldung angezeigt.

Benutzergruppe

Mit Benutzergruppen lassen sich gemeinsame Benutzerattribute definieren, wie Berechtigungen, Rechte und Prioritäten für die PTZ-Kamerasteuerung. Durch die Mitgliedschaft in einer Gruppe erbt ein Benutzer automatisch alle Attribute dieser Gruppe.

DHCP

Dynamic Host Configuration Protocol: Nutzt einen entsprechenden Server für die dynamische Zuweisung einer IP-Adresse und anderer Konfigurationsparameter an Computer in einem Netzwerk (Internet oder LAN)

Gerät

Hardwarekomponenten wie Kamera, Encoder/Decoder, NVR, DiBos, analoge Matrix, ATM/POS-Brücke.

Härten

Verfahren zur Erhöhung der Sicherheit eines Systems, indem nur die Software verwendet wird, die für den Betrieb des Systems erforderlich ist, indem bestimmte Schutzeinstellungen vorgenommen werden und indem Software, die nicht zwingend erforderlich ist, entfernt wird.

HTTP

Hypertext Transfer Protocol: Protokoll für die Datenübertragung über ein Netzwerk

HTTPS

Hypertext Transfer Protocol Secure: Verschlüsselt und authentifiziert die Kommunikation zwischen Webserver und -browser

IPv4-Adresse

Eine 4-Byte-Nummer, durch die jedes Gerät im Internet eindeutig identifiziert wird. Sie wird normalerweise in Dezimalnotation mit Punkten zwischen den Bytes angegeben, zum Beispiel „209.130.2.193“.

LAN

Local Area Network. Dies ist ein Netzwerk, das Geräte innerhalb eines begrenzten geografischen Gebiets miteinander verbindet.

Multicast

Kommunikation zwischen einem Transceiver und mehreren Empfängern in einem Netzwerk durch Übertragung eines einzelnen Daten-Streams über das Netzwerk an eine Reihe von Empfängern in einer definierten Gruppe. Voraussetzung für das Multicasting ist ein Multicast-fähiges Netzwerk, in dem das UDP-Protokoll und das IGMP-Protokoll implementiert sind.

Netzmaske

Eine Maske, über die festgelegt wird, welcher Teil einer IP-Adresse die Netzwerkadresse ist und welcher Teil die Hostadresse bildet. Sie wird normalerweise in Dezimalnotation mit Punkten zwischen den Bytes angegeben, z. B. „255.255.255.192“

ONVIF

Open Network Video Interface Forum Globaler Standard für Netzwerkvideoprodukte. ONVIF-konforme Geräte sind in der Lage, Livevideo, Audio, Metadaten und Steuerdaten auszutauschen sowie sicherzustellen, dass sie automatisch erkannt und mit Netzwerkanwendungen verbunden werden, wie z. B. mit Videomanagementsystemen.

RADIUS-Server

Remote Authentication Dial-In User Service. Client-Server-Protokoll, das zur Berechtigungsprüfung, Berechtigung und Rechnungserstellung bei Benutzern mit Einwahlverbindungen in ein Computer-Netzwerk

dient. RADIUS ist der de-facto-Standard für die zentrale Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN, Wireless LAN (siehe 802.1x) und DSL.

RCP+

Fernsteuerungsprotokoll: ein proprietäres Bosch Protokoll, das bestimmte statische Ports zur Erkennung und Kommunikation mit Bosch IP-Videogeräten verwendet

RTSP

Real Time Streaming Protocol. Netzwerkprotokoll zur Steuerung der kontinuierlichen Übertragung von audiovisuellen Daten oder Software über IP-basierte Netzwerke.

SNMP

Simple Network Management Protocol: Protokoll für die Netzwerkverwaltung, für die Verwaltung und Überwachung von Netzwerkkomponenten

SSL

Secure Sockets Layer; ein veraltetes Verschlüsselungsprotokoll für die Datenübertragung in IP-basierten Netzwerken (siehe TLS).

TCP

Transmission Control Protocol. Verbindungsorientiertes Kommunikationsprotokoll zum Übertragen von Daten über ein IP-Netzwerk. Bietet eine zuverlässige und geordnete Datenübertragung.

Telnet

Anmeldeprotokoll, mit dem sich Benutzer an einem entfernten Rechner (Host) im Internet anmelden können

TLS

Transport Layer Security. TLS 1.0 und 1.1 sind die standardmäßigen Weiterentwicklungen von SSL 3.0 (siehe SSL). Moderne Geräte verwenden TLS 1.2 oder 1.3

TTL

Time-To-Live; Lebensdauer eines Datenpakets in Stationssprüngen

UDP

User Datagram Protocol. Verbindungsloses Protokoll für den Datenaustausch über ein IP-Netzwerk. Für die Videoübertragung ist UDP aufgrund seines geringeren Overheads effizienter als TCP.

VPN

Ein virtuelles privates Netzwerk (VPN) implementiert ein privates Netzwerk innerhalb eines öffentlichen Netzwerks, wie dem Internet. Der Netzwerkverkehr innerhalb des VPNs ist verschlüsselt und somit vor Spionage geschützt.

Wide Area Network

Eine Weitverkehrsverbindung zur Ausdehnung oder Verbindung entfernter lokaler Netzwerke

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

Building solutions for a better life.

202302091957