Bosch IP video products

it Guida alla sicurezza informatica

Sommario

1 Finalità del documento e destinatari

La tecnologia è in evoluzione e a volte il suo sviluppo avviene a velocità impressionanti. Le rapide innovazioni dell'intelligenza artificiale (AI) e dell'Internet delle cose (IoT), e il loro elevato utilizzo (AIoT), modificano il profilo di rischio di prodotti e servizi. Gli attacchi malevoli intenzionali diventano sempre più fattibili e la probabilità di subirne aumenta costantemente a causa della maggiore connettività. Fornire prodotti e servizi sicuri e affidabili ai clienti è l'obiettivo di Bosch.

La presente guida ha lo scopo di assistere gli integratori nell'evoluzione dei prodotti video IP Bosch per un miglior allineamento alle esistenti strategie e procedure di sicurezza di rete dei clienti.

La presente guida tratta:
- Informazioni critiche sulle caratteristiche e principi di base dei dispositivi video IP Bosch
- Funzioni specifiche che possono essere modificate o disabilitate
- Funzioni specifiche che possono essere attivate e utilizzate
- Best practice relative ai sistemi video e alla sicurezza

La presente guida si concentra soprattutto sull'utilizzo di Configuration Manager per eseguire le configurazioni trattate. Nella maggior parte dei casi, tutte le configurazioni possono essere eseguite utilizzando BVMS Configuration Client, Configuration Manager e l'interfaccia Web integrata di un dispositivo video.

2 Concetto di sicurezza e relative considerazioni

I prodotti video IP sono sempre più comuni negli odierni ambienti di rete e, come per qualsiasi dispositivo IP che si trova in una rete, gli amministratori IT e i responsabili della sicurezza hanno il diritto di conoscere le impostazioni e le caratteristiche complete di un dispositivo.

Quando si utilizzano dispositivi video IP Bosch, la prima linea di difesa è costituita dai dispositivi stessi. Encoder e telecamere Bosch sono fabbricati in un ambiente sicuro e controllato che viene costantemente ispezionato. La scrittura dei dispositivi è possibile solamente tramite il caricamento di un firmware valido, specifico per la serie hardware e il chipset.

La maggior parte dei dispositivi video IP Bosch è dotata di un chip di sicurezza integrato che offre funzionalità simili alla smartcard di crittografia e al Trusted Platform Module, in breve TPM. Questo chip funziona come una "cassaforte", per la protezione di certificati, chiavi, licenze, ecc. dall'accesso non autorizzato anche quando la telecamera è fisicamente aperta per l'accesso.

I dispositivi video IP Bosch sono stati sottoposti a più di trentamila (30.000) test di vulnerabilità e penetrazione eseguiti dai fornitori indipendenti di servizi di protezione. Fino a ora, non vi sono stati cyberattacchi riusciti contro un dispositivo adeguatamente protetto.

3 Installazione sicura

3.1 Server e dispositivi di archiviazione

Tutti i componenti del server (ad esempio i server BVMS Management Server e Video Recording Manager) e i dispositivi di archiviazione devono essere installati in un'area protetta. L'accesso all'area protetta deve essere assicurato con un sistema di controllo degli accessi e deve essere monitorato. Il gruppo utenti che può accedere alla sala server centrale deve essere limitato a un piccolo gruppo di persone.
Sebbene i server e i dispositivi di archiviazione siano installati in un'area protetta, devono essere protetti dall'accesso non autorizzato.

Fare riferimento a

- *Protezione avanzata dei server, pagina 33*
- *Protezione avanzata dell'archiviazione, pagina 32*

3.2 Telecamere e dispositivi edge

Per l'installazione di telecamere e dispositivi edge, è necessario scegliere una posizione di installazione e un orientamento di montaggio sicuri. In teoria, la posizione non deve consentire interferenze intenzionali né accidentali.

4 Configurazione sicura

4.1 Assegnazione degli indirizzi IP

Tutti i dispositivi video IP Bosch vengono attualmente forniti con impostazione di fabbrica per accettare un indirizzo IP DHCP.
Se non vi sono server DHCP disponibili nella rete attiva in cui viene distribuito un dispositivo (se esegue il firmware 6.32 o successivo) il dispositivo stesso applica automaticamente un indirizzo link-locale compreso nell'intervallo tra 169.254.1.0 e 169.254.254.255 o 169.254.0.0/16.
Mentre con i firmware precedenti, assegna automaticamente l'indirizzo IP predefinito 192.168.0.1.
Sono disponibili diversi strumenti che possono essere utilizzati per eseguire l'assegnazione dell'indirizzo IP ai dispositivi video IP Bosch, tra cui:

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

Tutti gli strumenti software offrono la possibilità di assegnare un singolo indirizzo IPv4 statico nonché una gamma di indirizzi IPv4 contemporaneamente a più dispositivi. Questo comprende la subnet mask e l'indirizzamento gateway predefinito.
Tutti gli indirizzi IPv4 e i valori di subnet mask devono essere inseriti nella cosiddetta "notazione del punto decimale".

Avviso!
Uno dei primi passi per limitare le possibilità di cyberattacchi interni su una rete, eseguito da dispositivi di rete non autorizzati connessi localmente, è limitare gli indirizzi IP non utilizzati disponibili. Ciò avviene utilizzando IPAM (**IP A**ddress **M**anagement), in combinazione con il subnetting dell'intervallo degli indirizzi IP che verranno utilizzati.

Per subnetting si intende l'operazione di "prendere in prestito" dei bit dalla parte host di un indirizzo IP per suddividere una rete di grandi dimensioni in diverse reti più piccole. Quanto maggiore è il numero di bit presi in prestito, tanto maggiore è il numero di reti che è possibile creare, ma ciascuna rete supporta un numero inferiore di indirizzi host.

Suffisso	Host	CIDR	Preso in prestito	Binario
.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**

A partire dal 1993, l'Internet Engineering Task Force (IETF) ha introdotto un nuovo concetto di allocazione dei blocchi indirizzi IPv4 in modo più flessibile rispetto a quello utilizzato nella precedente architettura di indirizzamento "classful network". Il nuovo metodo è denominato "Classless Inter-Domain Routing" (CIDR) ed è utilizzato anche con gli indirizzi IPv6.

Le classful network IPv4 sono indicate come classi A, B e C, rispettivamente con numeri di bit 8, 16 e 24, e classe D, utilizzata per l'indirizzamento multicast.

Esempio:
Per un esempio di facile comprensione, verrà utilizzato uno scenario con indirizzo di classe C. La subnet mask predefinita di un indirizzo di classe C è 255.255.255.0. Tecnologicamente, questa maschera non è stata sottoposta a subnetting, quindi l'intero ottetto finale è disponibile per l'indirizzamento host valido. Quando si prendono in prestito i bit dall'indirizzo host, sono disponibili le seguenti opzioni maschera nell'ottetto finale:
.128, .192, .224, .240, .248 e .252.

Se si utilizza la subnet mask 255.255.255.240 (4 bit), si creano 16 reti più piccole che supportano 14 indirizzi host per ogni subnet.
- ID subnet 0:
  intervallo indirizzi host da 192.168.1.1 a 192.168.1.14. Indirizzo broadcast 192.168.1.15
- ID subnet 16:
  intervallo indirizzi host da 192.168.1.17 a 192.168.1.30. Indirizzo di trasmissione 192.168.1.31
- ID subnet: 32, 64, 96, ecc.

Per reti più grandi potrebbe essere necessaria la successiva classe di rete maggiore B oppure definire un blocco CIDR adeguato.

Esempio:
Prima di distribuire la rete di videosorveglianza, si esegue un semplice calcolo di quanti dispositivi IP saranno necessari nella rete, per prevedere lo spazio per espansioni future:
- 20 workstation video
- 1 server centrale
- 1 VRM Server
- 15 iSCSI Storage Arrays
- 305 telecamere IP

Totale = 342 indirizzi IP necessari

Tenendo conto del numero calcolato di 342 indirizzi IP, come minimo occorre un schema indirizzi IP di classe B per accogliere tale numero indirizzi IP. Utilizzando la subnet mask predefinita Classe B 255.255.0.0 è possibile usare 65534 indirizzi IP disponibili all'interno della rete.

In alternativa, è possibile organizzare la rete usando un blocco CIDR con 23 bit utilizzati come prefisso, fornendo uno spazio di 512 indirizzi o 510 host.

Mediante la suddivisione di una rete di grandi dimensioni in parti più piccole, con un semplice subnetting o specificando un blocco CIDR, è possibile ridurre il rischio.

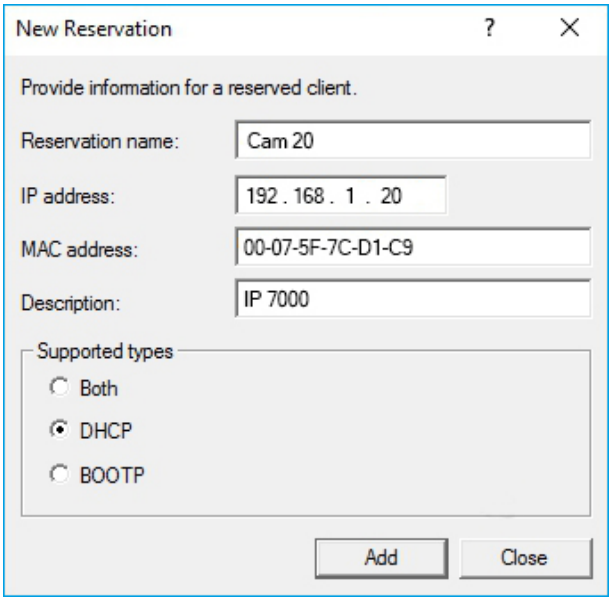
Esempio:

	Standard	Con subnet
Intervallo indirizzi IP	172.16.0.0 - 172.16.255.255	172.16.8.0 - 172.16.9.255
Subnet mask	255.255.0.0	255.255.254.0
Notazione CIDR	172.16.0.0/16	172.16.8.0/23
Numero di subnet	1	128
Numero di host	65.534	510
Indirizzi in eccesso	65.192	168

4.1.1 DHCP gestione

IPAM può utilizzare DHCP come un potente strumento per il controllo e l'utilizzo degli indirizzi IP nel proprio ambiente. DHCP può essere configurato per l'utilizzo di una gamma specifica di indirizzi IP. Può inoltre essere configurato per escludere un intervallo di indirizzi.

In caso di utilizzo di DHCP, per la distribuzione dei dispositivi video la cosa migliore potrebbe essere configurare delle prenotazioni di indirizzi senza scadenza sulla base dell'indirizzo MAC di ciascun dispositivo.



Avviso!
Anche prima di utilizzare la gestione indirizzi IP per tracciare l'utilizzo degli indirizzi IP, una best practice di gestione della rete è limitare l'accesso alla rete stessa tramite la protezione porte su edge switch, ad esempio, solo un indirizzo MAC specifico può accedere tramite una porta specifica.

4.2 Account e password utente

Tutti gli encoder e le telecamere video IP Bosch sono dotati di tre account utente integrati:

– **live**
  Questo account utente standard consente solo di accedere allo streaming video live.

– **user**
  Questo account utente più avanzato consente di accedere al video live e registrato e ai controlli telecamera come PTZ.
  Questo account non consente l'accesso alle impostazioni di configurazione.
– **service**
  Questo account amministratore consente l'accesso a tutti i menu del dispositivo e alle impostazioni di configurazione.

È necessario assegnare una password per ciascun account utente.
L'assegnazione delle password è un passaggio fondamentale per la protezione di qualunque dispositivo di rete. Si consiglia vivamente di assegnare delle password a tutti i dispositivi video di rete installati.

Avviso!
A partire dalla versione firmware 6.30, la gestione utente è stata migliorata per una maggiore flessibilità al fine di consentire la creazione di altri utenti con password proprie. I livelli account precedenti rappresentano ora i livelli dei gruppi utenti.
A partire dalla versione firmware 6.32 sono stati introdotti criteri più severi per le password (per ulteriori dettagli, vedere *Assegnazione di password tramite la pagina web del dispositivo, pagina 12*).

4.2.1 Assegnazione di password

Le password possono essere assegnate in diversi modi, in base alle dimensioni del sistema di sicurezza video e al software in uso. In applicazioni più ridotte, comprendenti solo pochi telecamere, le password possono essere impostate utilizzando la pagina web del dispositivo o Bosch Configuration Manager, poiché supporta comodamente la configurazione di dispositivi multipli contemporaneamente e comprende una procedura guidata di configurazione.

Avviso!
Come indicato precedentemente, la protezione tramite password è fondamentale per la protezione dei dati da possibili cyber-attacchi. Ciò si applica a tutti i dispositivi di rete dell'infrastruttura di sicurezza completa. La maggior parte delle organizzazioni applica già dei criteri per password complesse, ma se si lavora con una nuova installazione senza criteri, di seguito vengono indicate alcune best practice per l'implementazione della protezione tramite password:
- Le password devono avere una lunghezza compresa tra 8 e 12 caratteri.
- Le password devono contenere lettere maiuscole e minuscole.
- Le password devono contenere almeno un carattere speciale.
- Le password devono contenere almeno una cifra.

Esempio:
Utilizzo della passphrase "to be or not to be" e delle nostre regole di base per la generazione di una password efficace.
– 2be0rnOt!t0Be

Avviso!
Vi sono alcune restrizioni nell'utilizzo dei caratteri speciali, ad esempio: "@", "&", "<", ">", ":" nelle password a causa del loro significato specifico in XML e altri linguaggi markup. Sebbene l'interfaccia web li accetti, altri software di gestione e configurazione potrebbero negare l'accettazione.

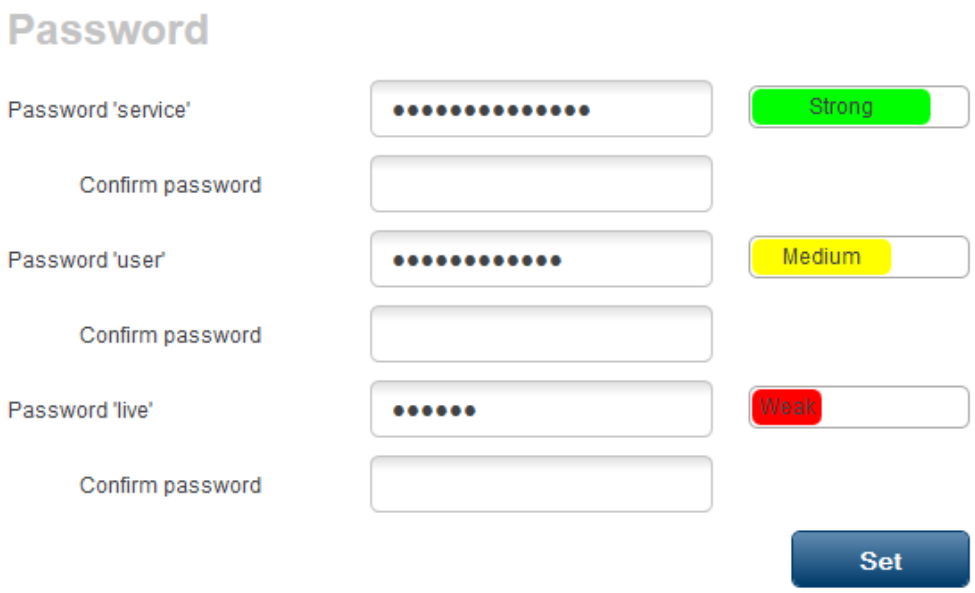
4.2.2 Assegnazione di password tramite la pagina web del dispositivo

1. Dalla pagina web del dispositivo, andare alla pagina **Configurazione** .
2. Selezionare il menu **Generale** e il sottomenu **Gestione utenti** (Nota: prima della versione firmware 6.30, il sottomenu **Gestione utenti** veniva chiamato **Password**).

Al primo accesso alla pagina web di una telecamera, all'utente è richiesto di assegnare delle password per garantire la protezione minima.
Questo verrà costantemente ripetuto a ogni ricarica delle pagine web delle telecamere finché non viene impostata una password. Facendo clic su **OK** si viene automaticamente portati al menu **Gestione utenti** .

Il firmware 6.30 ha la possibilità di attivare una casella di controllo **Non mostrare...**. Questa opzione è stata rimossa nel firmware 6.32 per evitare di falle nella sicurezza.

1. Selezionare il menu **Gestione utenti** e immettere e confermare la password desiderata per ciascuno dei tre account.
   Nota bene:
   - Le password devono essere assegnate prima al massimo livello di accesso (**Password "service"**).
   - Dal firmware versione 6.20 e successive, un nuovo indicatore denominato "indicatore di sicurezza delle password" fornisce suggerimenti relativi alla potenziale sicurezza delle password. Si tratta di uno strumento di supporto e non garantisce che una password corrisponda effettivamente alle esigenze di protezione di un'installazione.
2. Fare clic su **Imposta** per premere e salvare le modifiche.



L'**Gestione utenti** introdotto con la versione firmware 6.30 garantisce una maggiore flessibilità per creare utenti liberamente denominati con una propria password. I livelli account precedenti rappresentano ora i livelli dei gruppi utenti.

Gli utenti precedenti esistono ancora, ancora utilizzando le password assegnate con il firmware precedente, poiché non è possibile eliminarli né cambiare il livello del relativo gruppo utenti.

Le password possono essere assegnate o modificare facendo clic su o .
Finché tutti gli utenti non dispongono di una protezione tramite password, viene visualizzato un messaggio di avviso.

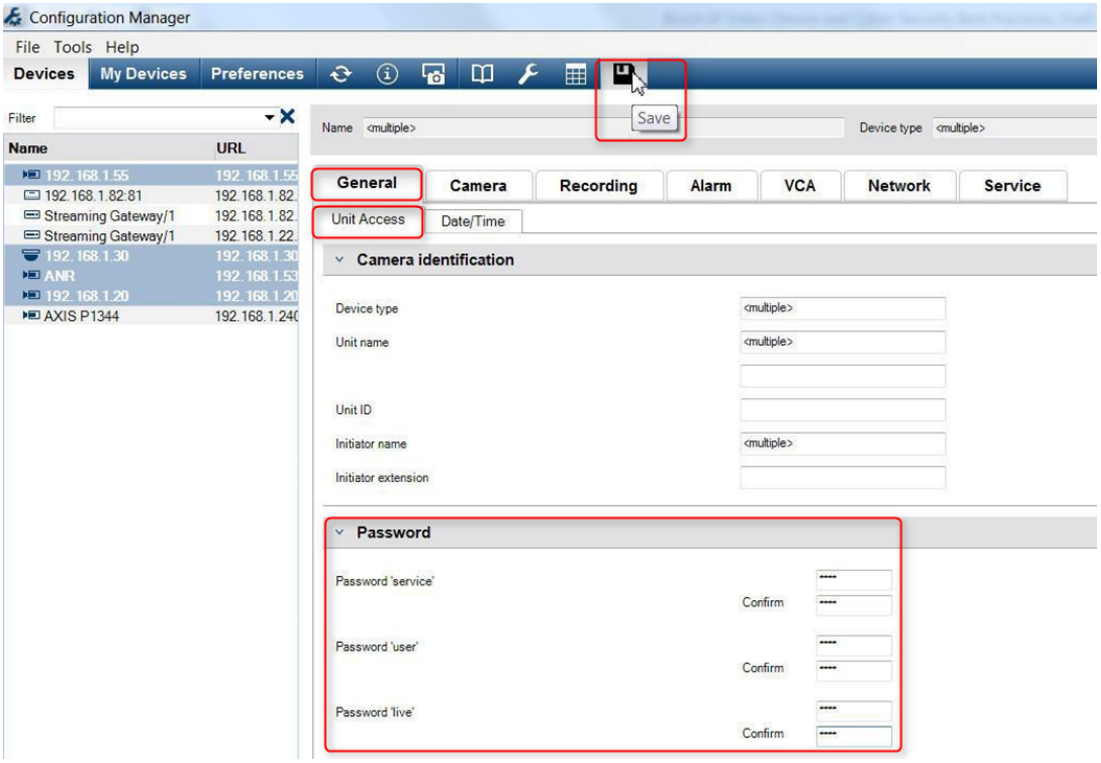
1. Per aggiungere un nuovo utente, fare clic su **Aggiungi**.
   Viene visualizzata una finestra a comparsa.
2. Immettere le nuove credenziali assegnare il gruppo utenti.
3. Fare clic su **Imposta** per salvare le modifiche.

Avviso!
Con la versione firmware 6.32 è stata inoltre introdotto un criterio più rigoroso per le password.
Le password richiedono ora una lunghezza minima di 8 caratteri.

4.2.3 Assegnazione di password tramite Configuration Manager

Utilizzando Bosch Configuration Manager, le password possono essere facilmente applicate a uno o più dispositivi contemporaneamente.

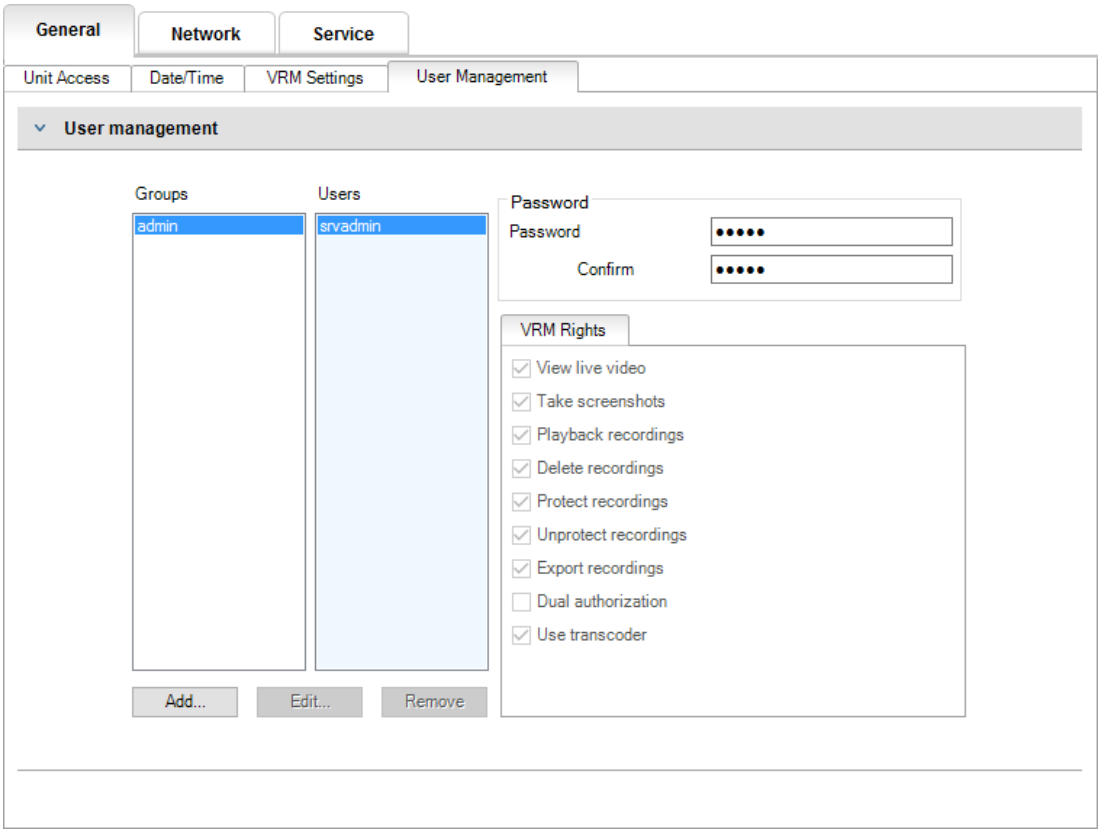
1. Nel campo Configuration Manager selezionare uno o più dispositivi.
2. Selezionare la scheda **Generale** , quindi selezionare **Accesso all'unità**.
3. Nel menu **Password** , immettere e confermare la password desiderata per ciascuno dei tre account (**Password "service"**, **Password "user"** e **Password "live"**).
4. Fare clic su per premere e salvare le modifiche.



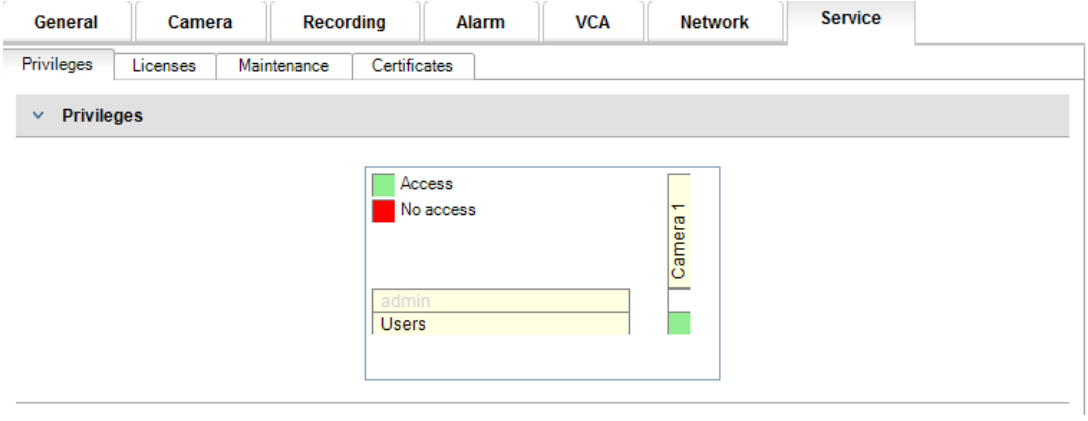
Nelle installazioni più grandi che vengono gestite da BVMS o da Video Recording Manager installato in un apparecchio di registrazione, le password globali possono essere applicate a tutti i dispositivi video IP che vengono aggiunti al sistema. Ciò consente una facile gestione e garantisce un livello di sicurezza standard attraverso l'intero sistema video di rete.

4.2.4 Assegnazione di password per l'installazione stand-alone di VRM

Video Recording Manager fornisce una gestione utente per migliorare flessibilità e sicurezza. Per impostazione predefinita, non vi sono password assegnate ad alcuno degli account utente. L'assegnazione delle password è un passaggio fondamentale per la protezione di qualunque dispositivo di rete. Si consiglia vivamente di assegnare delle password a tutti i dispositivi video di rete installati.
Lo stesso vale per gli utenti di Video Recording Manager.



Inoltre, ai membri di un gruppo utenti possono essere assegnati l'accesso a determinate telecamere e dei privilegi. In questo modo è possibile ottenere una gestione dei diritti basata sugli utenti.



4.2.5 Assegnazione di password tramite BVMS (su DIVAR IP o stand-alone)

Protezione dei dispositivi mediante password

Le telecamere e gli encoder, gestiti da BVMS, possono essere protetti dall'accesso non autorizzato mediante protezione con password.

Le password per gli account utente integrati di encoder/telecamere possono essere configurate tramite BVMS Configuration Client.

Per impostare una password per gli account utente integrati in BVMS Configuration Client:

1. Nella struttura ad albero dei dispositivi, selezionare l'encoder desiderato.
2. Fare clic con il pulsante destro del mouse sull'encoder e fare clic su **Modifica password....**
3. Immettere una password per i tre account utente predefiniti live, user e service.

Protezione con password predefinita

BVMS versione 5.0 e superiore consente di implementare password globali su tutti i dispositivi in un sistema video con un massimo di 2000 telecamere IP. Questa funzione è accessibile tramite BVMS Configuration Wizard quando si lavora con apparecchi di registrazione DIVAR IP 3000 o DIVAR IP 7000 oppure attraverso BVMS Configuration Client in qualsiasi sistema.

Per accedere al menu delle password globali in BVMS Configuration Client:

1. Nel menu **Hardware**, fare clic su **Proteggi dispositivi con la password predefinita....**.
2. Nel campo **Password predefinita globale**, inserire una password e selezionare **Applica protezione tramite password all'attivazione**.

Dopo il salvataggio e l'attivazione delle modifiche al sistema, la password inserita viene applicata agli account live, user e service di tutti i dispositivi, incluso l'account amministratore di Video Recording Manager.

Avviso!

I dispositivi hanno già delle password impostate in uno degli account, esse non verranno sovrascritte.

Ad esempio, se la password è impostata per service, ma non per live e user, la password globale verrà configurata solo per gli account live e user.

Configurazione BVMS e impostazioni VRM

Per impostazione predefinita, BVMS utilizza l'account amministratore integrato **srvadmin** per la connessione a Video Recording Manager con protezione tramite password. Per evitare l'accesso non autorizzato a Video Recording Manager, l'account amministratore **srvadmin** è protetto da una password complessa.

Per modificare la password dell'account **srvadmin** in BVMS Configuration Client:

1. Nella struttura ad albero dei dispositivi, selezionare il dispositivo VRM.
2. Fare clic con il pulsante destro del mouse sul dispositivo VRM e fare clic su **Cambia password VRM.**
   Viene visualizzata la finestra di dialogo **Modifica password...**.
3. Immettere una nuova password per l'account **srvadmin** e fare clic su **OK**.

Comunicazione crittografata alle telecamere
A partire da BVMS versione 7.0, i dati video live e la comunicazione di controllo tra la telecamera e il BVMS Operator Client, Configuration Client, Management Server e Video Recording Manager possono essere crittografati.
Dopo aver abilitato la connessione sicura nella finestra di dialogo **Modifica encoder**, il server BVMS, Operator Client e Video Recording Manager utilizzeranno una connessione HTTPS sicura per connettersi a una telecamera o a un encoder.
La stringa di connessione utilizzata internamente a BVMS passerà invece da rcpp://a.b.c.d (connessione RCP+ semplice sulla porta 1756) a https://a.b.c.d (connessione HTTPS sulla porta 443).
Per i dispositivi di versioni precedenti che non supportano HTTPS, la stringa di connessione rimane invariata (RCP+).

Se si seleziona la comunicazione HTTPS, essa utilizzerà HTTPS (TLS) per la crittografia di tutte le comunicazioni di controllo e i carichi video tramite il motore di crittografia del dispositivo. Quando si utilizza TLS, tutte le comunicazioni di controllo HTTPS e il carico video vengono crittografati con una chiave di crittografia AES lunga fino a 256 bit.
Per abilitare la comunicazione crittografata in BVMS Configuration Client:
1. Nella struttura ad albero dei dispositivi, selezionare l'encoder/la telecamera desiderati.
2. Fare clic con il pulsante destro del mouse sull'encoder/telecamera e fare clic su **Modifica encoder**.
3. Nella finestra di dialogo **Modifica encoder**, abilitare **Connessione protetta.**
4. Salvare e attivare la configurazione.

Dopo aver attivato la connessione sicura all'encoder è possibile disattivare gli altri protocolli (vedere *Utilizzo generico della porta di rete e trasmissione video, pagina 17*).

Avviso!
BVMS supporta solo la porta HTTPS predefinita 443. L'utilizzo di porte diverse non è supportato.

4.3 Accesso ai dispositivi di protezione avanzata

Tutti i dispositivi video IP Bosch sono dotati di pagine web multifunzione integrate. Le pagine web specifiche di un dispositivo supportano le funzioni video live e riproduzione nonché alcune impostazioni di configurazione specifiche che potrebbero non essere accessibili tramite un sistema di gestione video. Gli account utente integrati fungono da accesso alle diverse sezioni delle pagine web dedicate. Sebbene l'accesso alle pagine Web non possa essere completamene disabilitato tramite la pagina Web stessa (potrebbe essere utilizzato Configuration Manager), vi sono alcuni metodi per celare la presenza dell'accesso limitato al dispositivo e gestire l'utilizzo delle porte video.

4.3.1 Utilizzo generico della porta di rete e trasmissione video

Tutti i dispositivi video IP Bosch utilizzano Remote Control Protocol Plus (RCP+) per rilevamento, controllo e comunicazioni. RCP+ è un protocollo Bosch proprietario che utilizza porte statiche specifiche per rilevare e comunicare con i dispositivi video IP Bosch - 1756, 1757 e 1758. Quando si utilizza BVMS o un altro sistema di gestione video di terze parti con dispositivi video IP Bosch integrati tramite il Bosch VideoSDK, le porte elencate devono essere accessibili sulla rete per un corretto funzionamento dei dispositivi video IP.

È possibile riprodurre video dai dispositivi in diversi modi: UDP (dinamico), HTTP (80) o HTTPS (443).
L'utilizzo porta HTTP e HTTPS può essere modificato (vedere *Utilizzo porta HTTP, HTTPS e video, pagina 18*). Prima di apportare modifica alle porte, deve essere configurata la forma comunicazione desiderata con un dispositivo. È possibile accedere al menu di comunicazione tramite Configuration Manager.

1. In Configuration Manager, selezionare il dispositivo desiderato.
2. Selezionare la scheda **Generale** , quindi selezionare **Accesso all'unità**.
3. Individuare la parte **Accesso al dispositivo** della pagina.

4. Nell'elenco **Protocollo**, selezionare il protocollo desiderato:

– RCP+
– HTTP (predefinito)
– HTTPS

Se si seleziona la comunicazione HTTPS, la comunicazione tra Configuration Manager e i dispositivi video utilizzerà HTTPS (TLS) per la crittografia del payload con una chiave di crittografia AES lunga fino a 256 bit. Si tratta di una funzione gratuita di base. Quando si utilizza TLS, tutti le comunicazioni di controllo HTTPS e il payload video sono crittografati tramite il motore di crittografia del dispositivo.

Avviso!
La crittografia è specifica per il "percorso di trasmissione". Quando il video viene ricevuto da un decoder software o hardware video, il flusso viene decodificato in modo permanente.

4.3.2 Versione TLS minima

Alcuni client meno recenti potrebbero richiedere l'utilizzo di versioni di TLS meno recenti e meno sicure. Tuttavia, se possibile, si raccomanda di definire una versione minima per TLS in modo da evitare che i client forzino il dispositivo in una modalità di accesso meno sicura. Selezionare come versione minima la versione di TLS più alta possibile.

Avviso!
Quando si definisce il livello minimo di sicurezza per accedere ai dispositivi da un software client, verificare che tutte le porte e i protocolli che consentono un livello di accesso inferiore sono disattivati o disabilitati nei dispositivi.

4.3.3 Utilizzo porta HTTP, HTTPS e video

L'utilizzo delle porte HTTP e HTTPS su tutti i dispositivi può essere modificato o disattivato. La comunicazione crittografata può essere imposta disabilitando la porta RCP+ nonché la porta HTTP, forzando l'uso della crittografia per tutte le comunicazioni. Se viene disattivato l'utilizzo della porta HTTP, HTTPS rimane attivo e qualsiasi tentativo di disattivarlo non riesce.

1. In Configuration Manager, selezionare il dispositivo desiderato.
2. Selezionare la scheda **Rete**, quindi selezionare **Accesso rete**.
3. Individuare la parte **Dettagli** della pagina.

4. Nella parte **Dettagli** , modificare le porte HTTP e browser HTTPS e la porta RCP+ porta tramite il menu a discesa:
   - Modifica porte browser HTTP: 80 o porte da 10000 a 10100
   - Modifica porte browser HTTPS: 443 o porte da 10443 a 10543
   - Porta RCP+ 1756: **On** o **Off**

Avviso!
Nella versione firmware versione 6.1x, se la porta HTTP viene disabilitata viene effettuato un tentativo di accesso alla pagina web del dispositivo, la richiesta viene indirizzata alla porta HTTPS attualmente definita.
La funzione di reindirizzamento è omessa nella versione firmware 6.20 e successive. Se la porta HTTP viene disabilitata e la porta HTTPS è stata modificata per utilizzare una porta diversa dalla 443, l'accesso alle pagine web può essere effettuato solamente andando all'indirizzo IP dei dispositivi più la porta assegnata.

Esempio:
https://192.168.1.21:10443. Qualsiasi tentativo di connessione all'indirizzo predefinito non riesce.

4.3.4 Software video e selezione porta

La regolazione di tali impostazioni influenza inoltre la porta che viene utilizzata per la trasmissione video quando si utilizza un software di gestione video nella propria LAN.
Se tutti i dispositivi video IP sono impostati sulla porta HTTP 10000, ad esempio, e BVMS Operator Client è configurato per "TCP tunneling", tutte le trasmissioni video della rete vengono effettuate attraverso la porta HTTP 10000.

Avviso!
Le modifiche alle impostazioni delle porte nei dispositivi devono corrispondere a quelle del sistema di gestione e dei relativi componenti nonché nel client.

Avviso!
A seconda dello scenario di distribuzione e degli obiettivi di sicurezza dell'installazione, le best practice possono variare. La disabilitazione e il reindirizzamento dell'utilizzo porte di HTTP o HTTPS presentano dei vantaggi. Modificare la porta in uno dei due protocolli può contribuire a evitare di fornire informazioni a strumenti di rete come NMAP (Network Mapper, scanner di sicurezza gratuito). Applicazioni come NMAP sono solitamente utilizzate come strumenti di ricognizione per identificare i punti deboli di qualsiasi dispositivo su una rete. Questa tecnica, combinata con l'implementazione di password complesse contribuisce alla sicurezza generale del sistema.

4.3.5 Tunneling SSH

Per l'accesso a dispositivi in remoto con BVMS Operator Client tramite reti pubbliche, BVMS fornisce tunneling SSH (Secure Shell) per garantire una comunicazione sicura (crittografata).

Il tunneling SSH crea un tunnel crittografato stabilito mediante una connessione protocollo/socket SSH. Questo tunnel crittografato è in grado di trasportare sia il traffico crittografato che quello non crittografato. L'implementazione SSH di Bosch utilizza anche Omni-Path, un protocollo di comunicazione a bassa latenza e prestazioni elevate sviluppato da Intel.

Per ulteriori informazioni su come configurare il servizio SSH in BVMS, consultare la documentazione di BVMS.
Per ulteriori informazioni su come configurare sistemi DIVAR IP per un accesso remoto sicuro con BVMS Operator Client, consultare la documentazione DIVAR IP.

4.3.6 Accesso Telnet

Telnet è un protocollo di livello applicazione che fornisce una comunicazione ai dispositivi tramite una sessione terminale virtuale per finalità di manutenzione e risoluzione dei problemi. Tutti i dispositivi video IP Bosch sono compatibili con Telnet e per impostazione predefinita il supporto Telnet è attivato nelle versioni firmware fino a 6.1x. A partire dal firmware versione 6.20 in poi, la porta Telnet è disabilitata per impostazione predefinita.

Avviso!
Dal 2011 si è verificato un aumento dei cyberattacchi che utilizzano il protocollo Telnet. Nell'ambiente odierno, le best practice indicano che occorre disabilitare il supporto Telnet su tutti i dispositivi se non in caso di necessità per manutenzione o risoluzione dei problemi.

1. In Configuration Manager, selezionare il dispositivo desiderato.
2. Selezionare la scheda **Rete**, quindi selezionare **Accesso rete**.
3. Individuare la parte **Dettagli** della pagina.

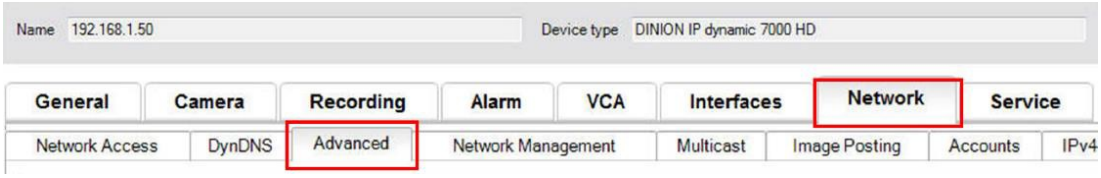
4. Nella parte **Dettagli**, attivare o disattivare **Supporto Telnet** tramite il menu a discesa.

Avviso!
A partire dal firmware versione 6.20, Telnet viene inoltre supportato anche tramite le cosiddette "Web socket", che utilizzano connessioni HTTPS sicure. Le Web socket non utilizzano la porta Telnet standard e forniscono un modo sicuro per accedere all'interfaccia riga di comando del dispositivo IP, se necessario.

4.3.7 RTSP: Real Time Streaming Protocol

Real Time Streaming Protocol (RTSP) è il componente video principale utilizzato dal protocollo ONVIF per fornire flusso video e controllo dei dispositivi ai sistemi di gestione video compatibili con ONVIF. RTSP viene inoltre utilizzato da varie applicazioni video di terze parti per funzioni di streaming base e, in alcuni casi, può essere utilizzato la risoluzione dei problemi dei dispositivi e di rete. Tutti i dispositivi video IP Bosch sono in grado di fornire flussi mediante il protocollo RTSP.
I servizi RTSP possono essere facilmente modificati tramite il Configuration Manager.

1. In Configuration Manager, selezionare il dispositivo desiderato.
2. Selezionare la scheda **Rete**, quindi selezionare **Avanzate**.



3. Individuare la parte **RTSP** della pagina.
4. Nel menu a discesa **Porta RTSP** , disattivare o modificare il servizio RSTP:
   - Porta RTSP predefinita: 554
   - Modifica porta RTSP: da 10554 a 10664

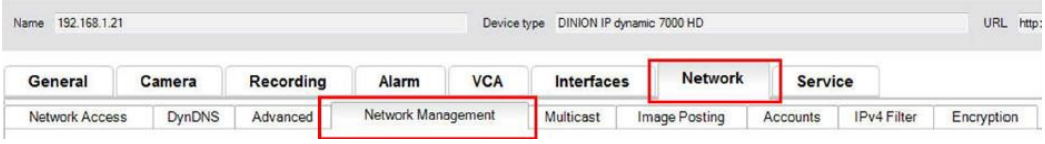
Avviso!
Recentemente vi sono state segnalazioni di cyberattacchi mediante buffer RTSP stack overflow. Gli attacchi sono stati creati per colpire i dispositivi di fornitori specifici. La best practice prevede la disabilitazione del servizio se non viene da un sistema di gestione video conforme con ONVIF o per lo streaming in tempo reale di base.
In alternativa, e se il client destinatario lo consente, la comunicazione RTSP possa essere incanalata utilizzando una connessione HTTPS, che al momento rappresenta l'unico modo per trasmettere dati RTSP crittografati.

Avviso!
Per ulteriori informazioni su RTSP, consultare la nota di applicazione *RTSP usage with Bosch VIP Devices* (Utilizzo di RTSP con dispositivi VIP Bosch) nel catalogo dei prodotti Bosch Security Systems online al seguente link:
https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf

4.3.8 UPnP: Universal Plug and Play

I dispositivi video IP Bosch sono in grado di comunicare con i dispositivi di rete tramite **UPnP**. Questa funzione viene utilizzata principalmente nei sistemi di dimensioni più piccole con un basso numero di telecamere, in cui le telecamere compaiono automaticamente nella directory di rete del PC e sono quindi facilmente reperibili. Tuttavia, ciò avviene per tutti i dispositivi nella rete.
UPnP può essere disattivato utilizzando Configuration Manager.

1. In Configuration Manager, selezionare il dispositivo desiderato.
2. Selezionare la scheda **Rete**, quindi selezionare **Gestione di rete**.



3. Individuare la parte **UPnP** della pagina.
4. Nel menu a discesa **UPnP**, selezionare **Off** per disattivare **UPnP**.

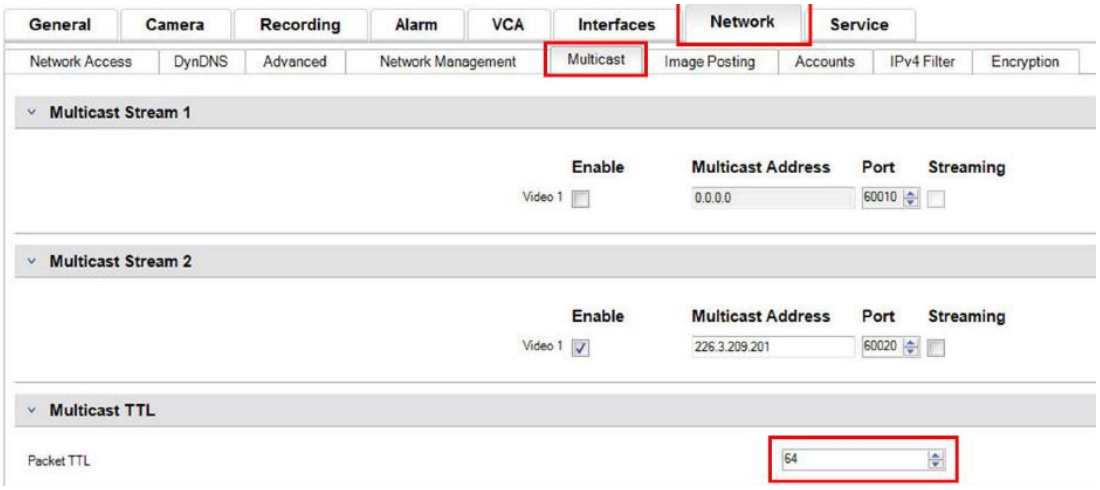
Avviso!
UPnP non deve essere utilizzato in installazioni di grandi dimensioni a causa del numero elevato di notifiche di registrazione e del rischio potenziale di accesso indesiderato o attacco.

4.3.9 Multicasting

Tutti i dispositivi video IP Bosch sono in grado di fornire video sia "Multicast on Demand" sia "Multicast Streaming". Mentre le trasmissioni video unicast sono basate sulla destinazione, multicast è basato sulla sorgente e ciò può comportare problemi di sicurezza a livello di rete,

tra cui: controllo dell'accesso, attendibilità del centro gruppi e attendibilità del router. Sebbene la configurazione del router non rientri nell'ambito di questo manuale, vi è una soluzione di sicurezza che può essere implementata dal dispositivo video IP stesso.
La definizione TTL (time-to-live) specifica dove e in che misura il traffico multicast è autorizzato a scorrere all'interno di una rete, con ogni hop che riduce il TTL di uno. Durante la configurazione dei dispositivi video IP per l'uso multicast, è possibile modificare il pacchetto TTL del dispositivo.

1. In Configuration Manager, selezionare il dispositivo desiderato.
2. Selezionare la scheda **Rete**, quindi selezionare **Multicast**.
3. Individuare la parte **TTL Multicast** della pagina.
4. Regolare le **Pacchetto TTL** impostazioni utilizzando i seguenti valori TTL e i limiti di ambito:
   - Valore TTL 0 = limitato all'host locale
   - Valore TTL 1 = limitato alla stessa subnet
   - Valore TTL 15 = limitato allo stesso sito
   - Valore TTL 64 (predefinito) = limitato alla stessa area
   - Valore TTL 127 = mondiale
   - Valore TTL 191 = mondiale con banda limitata
   - Valore TTL 255 = dati illimitati

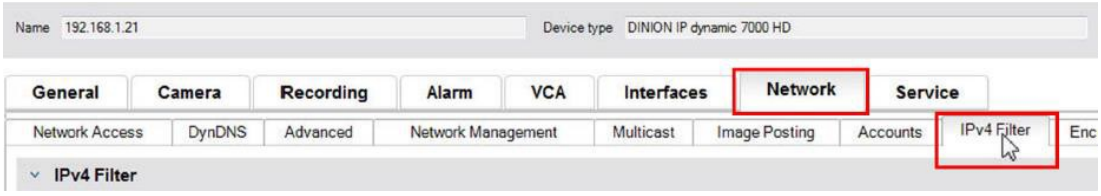


Avviso!
Quando si utilizzano i dati di videosorveglianza, la best practice prevede di regolare le impostazioni TTL su 15, limitato allo stesso sito. O meglio, se si conosce esattamente numero massimo di hop, utilizzarlo come valore TTL.

4.3.10 Filtro IPv4

È possibile limitare l'accesso a qualsiasi dispositivo video IP Bosch tramite una funzione chiamata filtro IPv4. Il filtro IPv4 utilizza i principi fondamentali del "subnetting" per definire fino a due intervalli di indirizzi IP consentiti. Una volta definito, esso nega l'accesso da qualsiasi indirizzo IP al di fuori di tali intervalli.

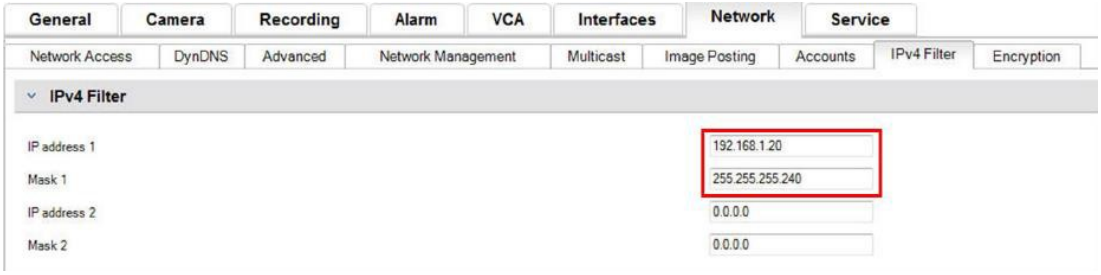
1. In Configuration Manager, selezionare il dispositivo desiderato.
2. Selezionare la scheda **Rete**, quindi selezionare **Filtro IPv4**.



Avviso!
Per configurare correttamente questa funzione, è necessario disporre delle nozioni di base sul subnetting o avere accesso a un calcolatore subnet. L'inserimento di valori errati in questa impostazione può limitare l'accesso al dispositivo stesso e rendere necessario eseguire un ripristino delle impostazioni predefinite di fabbrica per riottenere l'accesso.

3. Per aggiungere una regola filtro, immettere due valori:
   - Immettere un indirizzo IP di base che si trova all'interno della regola subnet creata. L'indirizzo IP di base indica quale subnet viene autorizzata e deve rientrare nell'intervallo desiderato.
   - Inserire una subnet mask che definisca gli indirizzi IP a cui il dispositivo video IP accetta la comunicazione.

Nell'esempio seguente sono stati immessi il **Indirizzo IP 1** di 192.168.1.20 e il **Filtro 1** di 255.255.255.240. Questa impostazione limita l'accesso dai dispositivi che rientrano nell'intervallo IP definito tra 192.168.1.16 e 192.168.1.31.



Durante l'utilizzo della funzione **Filtro IPv4** i dispositivi possono essere scansionati tramite RCP+, ma l'accesso alle impostazioni di configurazione e video non è possibile tramite client che non rientrano nell'intervallo di indirizzi IP consentiti. Ciò comprende l'accesso tramite browser web.
Non è necessario che il dispositivo video IP stesso si trovi nell'intervallo degli indirizzi consentiti.

Avviso!
In base alla configurazione del proprio sistema, utilizzando l'opzione **Filtro IPv4** è possibile la visibilità indesiderata dei dispositivi in una rete. Se si attiva questa funzione, assicurarsi di annotare le impostazioni per riferimento futuro.
Tenere presente che il dispositivo rimarrà comunque accessibile tramite IPv6, quindi il filtro IPv4 risulta ragionevole solo nelle reti IPv4 pure.

4.3.11 SNMP

Simple Network Management Protocol (SNMP) è un protocollo comune per monitorare lo stato di salute di un sistema. Tale sistema di monitoraggio in genere dispone di un server di gestione centralizzata che raccoglie tutti i dati provenienti dai dispositivi e i componenti compatibili del sistema.
SNMP fornisce due metodi per rilevare lo stato di salute del sistema:
- Il server di gestione di rete può interrogare lo stato di salute di un dispositivo tramite le richieste SNMP.

– I dispositivi possono informare attivamente il server di gestione di rete sullo stato di salute del proprio sistema in caso di condizioni di errore o allarme inviando trap SNMP al server SNMP. Tali trap devono essere configurate all'interno del dispositivo.

SNMP consente anche la configurazione di alcune variabili all'interno di componenti e dispositivi.
Le informazioni, quali messaggi sono supportati da un dispositivo e quali trap può inviare, si ricavano dalla Management Information Base, il cosiddetto file MIB, un file fornito insieme a un prodotto per la facile integrazione in un sistema di monitoraggio di rete.

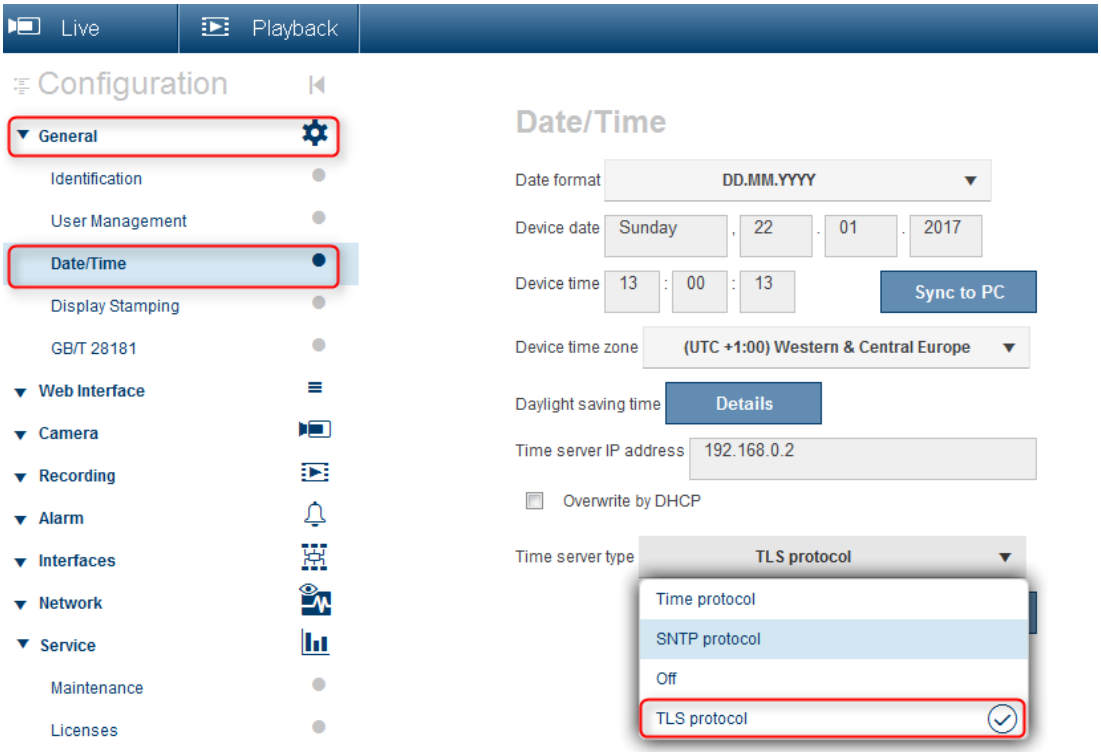
Esistono tre diversi versioni del protocollo SNMP:
– SNMP versione 1
  SNMP versione 1 (SNMPv1) è l'implementazione iniziale del protocollo SNMP. Viene utilizzato ampiamente ed è di fatto diventato il protocollo standard per la gestione e il monitoraggio di rete.
  Ma SNMPv1 è ora esposto a minacce a causa della mancanza di funzioni per la sicurezza. Esso utilizza solamente delle "*community string*" come un tipo di password, trasmessa come testo chiaro.
  Quindi, SNMPv1 deve essere utilizzato solamente se è possibile accertare che la rete è fisicamente protetta dall'accesso non autorizzato.
– SNMP versione 2
  SNMP versione 2 (SNMPv2) comprende dei miglioramenti in termini sicurezza e riservatezza, tra gli altri, e introduce una richiesta "bulk" per il recupero di grandi volumi di dati in un'unica richiesta. Tuttavia, l'approccio di sicurezza è stato ritenuto decisamente troppo complesso, ostacolandone l'accettazione.
  Quindi, è stato presto sostituito dalla versione SNMPv2c, che corrisponde a SNMPv2, ma senza il controverso modello di protezione, tornando invece al metodo "community-based" di SNMPv1, analogamente lacunoso in termini di sicurezza.
– SNMP versione 3
  SNMP versione 3 (SNMPv3) aggiunge soprattutto miglioramenti in termini di protezione e configurazione remota. Essi comprendono miglioramenti della riservatezza tramite la crittografia dei pacchetti, integrità dei messaggi e autenticazione.
  Inoltre, considera la distribuzione di SNMP su larga scala.

Avviso!
Sia SNMPv1 sia SNMPv2c sono ormai esposti a minacce a causa la mancanza di funzioni di sicurezza. Utilizzano solo "community string" come un tipo di password, trasmesse come testo chiaro.
Di conseguenza, è opportuno utilizzare SNMPv1 o SNMPv2c solo se è possibile assicurarsi che la rete è fisicamente protetta dall'accesso non autorizzato.
Attualmente, le telecamere Bosch supportano solo SNMPv1. Assicurarsi di avere disattivato SNMP, se non in uso.

4.3.12 Base oraria protetta

In aggiunta al Network Time Protocol e a SNTP, entrambi protocolli non protetti, con FW 6.20 è stata introdotta una terza modalità per il client del server di riferimento orario con utilizzo del protocollo TLS. Questo metodo è comunemente noto anche come *TLS-Date*.

In questa modalità, qualsiasi server HTTPS arbitrario può essere utilizzato come server di riferimento orario. Il valore orario viene ricavato come effetto collaterale dal processo handshake HTTPS. La trasmissione TLS è protetta. Un root certificate opzionale per il server HTTPS può essere caricato nell'archivio certificati della telecamera per autenticare il server.



Avviso!
Verificare che l'indirizzo IP del server di riferimento orario inserito disponga esso stesso di una base oraria stabile e non compromessa.

4.3.13 Servizi basati su cloud

Tutti i dispositivi video IP Bosch possono comunicare con servizi basati sul cloud Bosch come Remote Portal. A seconda dell'area di distribuzione, ciò consente ai dispositivi video IP di utilizzare servizi come Remote Device Management o Cloud VMS per inoltrare gli allarmi e altri dati a una postazione centrale.
Per ulteriori informazioni, consultare la Bosch Building Technologies Knowledge Base: https://community.boschsecurity.com.

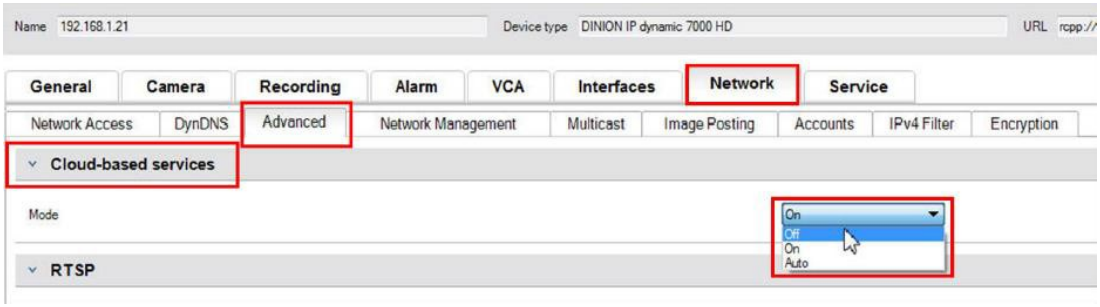
Sono disponibili tre modalità di funzionamento per servizi basati sul cloud:

- **On**:
  il dispositivo video interroga costantemente il server cloud.
- **Auto** (valore predefinito):
  i dispositivi video effettuano alcuni tentativi di interrogare il server cloud e, in caso di esito negativo, smettono di tentare di raggiungere il server cloud.
- **Off**:
  non viene eseguita alcuna interrogazione.

I servizi basati sul cloud possono essere facilmente disattivati mediante Configuration Manager.

1. In Configuration Manager, selezionare il dispositivo desiderato.

2. Selezionare la scheda **Rete**, quindi selezionare la scheda **Avanzate**.
3. Individuare la sezione **Servizi basati su cloud** della pagina e selezionare **Off** dall'elenco.



Avviso!
Se vengono utilizzati servizi Bosch basati sul cloud, mantenere la configurazione predefinita. In tutti gli altri casi, impostare la modalità dei servizi basati sul cloud su **Off**.

4.4 Protezione avanzata delle telecamere IP

Le telecamere IP Bosch vengono consegnate con una configurazione predefinita che consente una facile integrazione in ambienti diversi.
In base all'ambiente di destinazione e al livello di sicurezza previsto, potrebbe essere necessario modificare alcune impostazioni della telecamera in modo da aumentare la sicurezza informatica e dei dati.
Tuttavia, l'ambiente operativo potrebbe prevedere delle limitazioni, come l'utilizzo di un determinato protocollo o di una determinata funzione che garantiscono una minore protezione (ad esempio SNMPv1).

4.4.1 Livelli di protezione avanzata

Vengono definiti due livelli di protezione avanzata: *elevato* e *rigoroso*.
Il livello di protezione avanzata *rigoroso* rappresenta il modo più sicuro per configurare un dispositivo, ma potrebbe causare limitazioni all'utilizzo del dispositivo, poiché prevede la disabilitazione di funzioni come il rilevamento automatico di un dispositivo. Per ciascuna funzione, è necessario valutare se è possibile applicare l'impostazione *elevata* o *rigorosa*.

4.4.2 Panoramica della protezione avanzata

Rete - Servizi di rete	Standard	Elevato	Rigoroso
HTTP	Abilitato	Disabilitato	Disabilitato
HTTPS	Abilitato	Abilitato	Abilitato
RTSP	Abilitato	Opzionale	Disabilitato
RCP	Abilitato	Disabilitato	Disabilitato
SNMPv1	Disabilitato	Disabilitato	Disabilitato
SNMPv3	Disabilitato	Abilitato	Abilitato
iSCSI	Abilitato	Opzionale	Disabilitato
UPnP	Disabilitato	Disabilitato	Disabilitato
Server NTP	Disabilitato	Disabilitato	Disabilitato
Discovery	Abilitato	Abilitato	Disabilitato

Rete - Servizi di rete	Standard	Elevato	Rigoroso
ONVIF Discovery	Abilitato	Abilitato	Disabilitato
GBT/28181	Disabilitato	Disabilitato	Disabilitato
Meccanismo di ripristino password	Abilitato	Disabilitato	Disabilitato
Risposta ping	Abilitato	Abilitato	Disabilitato
RTSPS	Abilitato	Abilitato	Abilitato
HTTP	Abilitato	Disabilitato	Disabilitato

Rete - Accesso rete	Standard	Elevato	Rigoroso
Versione TLS minima	1.0	1.2	1.2
HSTS	Disabilitato	Abilitato	Abilitato

Rete - Avanzate	Standard	Elevato	Rigoroso
802.1x	Disabilitato	Opzionale	Abilitato
Syslog	Disabilitato	TCP	TLS

Rete - Gestione di rete	Standard	Elevato	Rigoroso
Modalità SNMPv3	Disabilitato	SHA1 / AES	SHA1 / AES

Rete - Filtro IPv4	Standard	Elevato	Rigoroso
Filtro IPv4	Disabilitato	Abilitato	Abilitato

Generale - Data/ora	Standard	Elevato	Rigoroso
Data/ora (client NTP)	Disabilitato	SNTP/data TLS	Data TLS

Connettività - Servizi cloud	Standard	Elevato	Rigoroso
Remote Portal	Disabilitato	Abilitato	Abilitato

Assistenza - Registrazione	Standard	Elevato	Rigoroso
Tenuta software	Disabilitato	Abilitato	Abilitato

4.4.3 Descrizione delle funzioni e consigli sulla protezione avanzata

HTTP
HTTP viene abilitato per impostazione predefinita, ma non crittografato; pertanto, credenziali o impostazioni vengono trasferite non crittografate, se in uso.
Consiglio: il protocollo HTTP semplice deve essere disabilitato in modo da poter utilizzare il protocollo HTTPS crittografato, soprattutto se la rete non è attendibile.

HTTPS
HTTPS è crittografato e deve costituire la scelta predefinita per l'accesso all'interfaccia web o all'API RCP basata sul web. Si consiglia l'utilizzo dei propri certificati e PKI.
Consiglio: HTTPS è il protocollo sicuro predefinito utilizzato per la configurazione ed è opportuno che rimanga abilitato.

RTSP
RTSP viene utilizzato per flusso video, ma in genere non crittografato. Se il software che riceve il flusso video è in grado di utilizzare RTSPS, si consiglia di disabilitare la modalità RTSP semplice. Quando si utilizzano altri componenti Bosch (ad esempio decoder/BVMS/VRM/ DIVAR IP) è possibile abilitare una crittografia proprietaria di Bosch per RTSP, rendendo la trasmissione sicura.
Consiglio: utilizzare un approccio basato sui rischi se il video può essere trasmesso non crittografato o tramite crittografia Bosch. Se possibile, utilizzare il protocollo RTSPS crittografato.

RCP
Il Remote Control Protocol Plus proprietario di Bosch è il protocollo di configurazione per le telecamere IP Bosch. Il protocollo RCP semplice non è crittografato, pertanto le impostazioni vengono trasferite non crittografate. Tutti gli strumenti Bosch utilizzano ora la comunicazione RCP su HTTPS per un certo periodo di tempo, ma questo protocollo potrebbe essere necessario per gli strumenti di script o strumenti di integrazione di terze parti che si basano ancora su di esso.
Consiglio: disabilitare RCP se non utilizzato da sistemi precedenti o strumenti di terze parti.

SNMPv1
SNMP è il protocollo di monitoraggio della rete comune utilizzato per richieste di informazioni sull'integrità di un dispositivo o per inviare trap a un ricevitore remoto, ma non è crittografato.
Consiglio: mantenerlo disabilitato se non necessario per il monitoraggio dell'integrità o altri motivi di compatibilità. Se possibile, utilizzare SNMPv3.

SNMPv3
SNMPv3 è il successore di SNMPv1 e può essere ugualmente utilizzato crittografato.
Consiglio: scelta consigliata se è necessario implementare il monitoraggio di SNMP.

iSCSI
Disabilita il server iSCSI interno utilizzato per rendere accessibili le registrazioni interne della telecamera tramite iSCSI. iSCSI è un protocollo non crittografato.
Consiglio: disabilitare il server iSCSI se non utilizzano sulla telecamera.

UPnP
Rendere la telecamera rilevabile tramite protocollo UPnP.
Consiglio: disabilitare UPnP se non necessario.

Server NTP
Abilitare un server NTP sulla telecamera per consentire ad altri dispositivi o telecamere di sincronizzare l'ora. Se possibile, un dispositivo dedicato dovrebbe fungere da riferimento temporale alla rete della telecamera consentendo la separazione dei servizi. Se non sono disponibili altri dispositivi, una telecamera può fungere da riferimento orario.
Consiglio: è opportuno disabilitare il server NTP, se non necessario.

Discovery
Utilizzo di un meccanismo proprietario di Bosch per rendere le telecamere rilevabili da un software Bosch, ad esempio Configuration Manager.
Consiglio: quando si utilizzano indirizzi IP dinamici, questa funzione deve rimanere abilitata. Quando si opera in un ambiente con indirizzi IP fissi, questa funzione può essere disabilitata.

ONVIF Discovery
Supporto del rilevamento dei dispositivi telecamera tramite il protocollo ONVIF Discovery
Consiglio: quando si utilizzano indirizzi IP dinamici e strumenti compatibili con ONVIF, questa funzione deve rimanere abilitata. Quando si opera in un ambiente fisso con indirizzi IP fissi, questa funzione può essere disabilitata.

GBT/28181
GBT/28181 è uno standard cinese per l'interoperabilità tra dispositivi diversi.
Consiglio: mantenerlo disabilitato se non necessario.

Meccanismo di ripristino password
Poiché è possibile che le telecamere IP siano installate in postazioni molto remote, è difficile eseguire le operazioni di manutenzione o un ripristino di fabbrica nel caso in cui l'accesso alla telecamera sia stato bloccato. Bosch offre la possibilità di ripristinare la password di una telecamera tramite la procedura "Challenge & Response" basata su un meccanismo sicuro a chiave pubblica/privata.
Consiglio: se questa funzione non è necessaria, si consiglia di disabilitarla.

Risposta ping
Consente di configurare se la telecamera risponde alle richieste ping nella rete. Può aiutare nell'esecuzione del debugging. In una rete con sicurezza elevata, questa opzione può essere disabilitata per evitare l'enumerazione del dispositivo tramite ping sweep, sebbene vi siano molti altri metodi di rilevamento dei dispositivi utilizzabili da un malintenzionato.
Consiglio: approccio basato sui rischi, può essere disabilitato per reti con sicurezza elevata.

RTSPS
RTSPS è la versione crittografata di RTSP ed è utilizzato per il flusso video. Se il software ricevente lo supporta, è sempre preferibile l'utilizzo di RTSPS rispetto al protocollo RTSP semplice. Poiché molti client RTSP non supportano la variante sicura, RTSP è ancora abilitato per la sicurezza di primo livello.
Consiglio: utilizzare RTSPS, se possibile.

Versione TLS minima
Le telecamere IP non consentono connessioni SSLv3 non sicure o obsolete. TLS 1.0 e 1.1 sono considerate versioni obsolete da IETF e sono noti potenziali problemi di sicurezza (BEAST, FREAK).
Le telecamere CPP4, CPP6, CPP7 e CPP7.3 supportano il protocollo TLS 1.2 sicuro, che è opportuno impostare come versione minima richiesta.
Le telecamere CPP13 e CPP14 non consentono versioni TLS precedenti alla 1.2. Supportano inoltre la specifica TLS 1.3 più recente.
Consiglio: impostare la versione TLS minima su 1.2.

HSTS
HTTP Strict Transport Security (HSTS) è un criterio impostato da un sito Web per la protezione da attacchi man-in-the-middle e attacchi di downgrade del protocollo. Permette al sito Web di comunicare al browser di consentire esclusivamente le connessioni HTTPS all'interno di questa connessione e di non consentire connessioni HTTP non crittografate.
Consiglio: abilitare HSTS sulla telecamera.

802.1x
802.1x è uno standard per il controllo dell'accesso di rete (Network Access Control, NAC). Permette ai dispositivi di effettuare l'autenticazione nella rete, concedendo l'accesso alla rete solo ai dispositivi autenticati. Le telecamere IP Bosch supportano 802.1x sia con l'autenticazione mediante password che con quella basata su certificato; quest'ultima è il metodo preferito. Per utilizzare 802.1x, lo switch di rete deve supportare questo standard ed è necessario un server di autenticazione.
Consiglio: se l'infrastruttura di rete lo consente, utilizzare l'autenticazione di rete con 802.1x.

Syslog
Poiché la telecamera dispone di uno spazio limitato per i messaggi di registro, è necessario inviare i messaggi di registro a una postazione centrale e analizzarli in tale postazione per rilevare eventuali attacchi o configurazioni errate.
Consiglio: utilizzare TCP Syslog per evitare di perdere messaggi a causa della perdita di pacchetti. Utilizzare Syslog con TLS per crittografare e autenticare i messaggi.

Modalità SNMPv3
SNMPv3 è il successore di SNMPv1 e consente l'autenticazione e il trasferimento sicuro delle informazioni.
Consiglio: quando si utilizza SNMPv3, utilizzare SHA1 come protocollo di autenticazione e AES come protocollo di privacy (se supportato).

Filtro IP
Nel filtro IP è possibile definire diversi indirizzi IP (host singoli o subnet di rete) a cui è consentito accedere alla telecamera. Si consiglia di definire qui i computer o le reti che accedono alla telecamera.
Consiglio: si consiglia di utilizzare il filtro IP per definire le reti o gli host consentiti.

Data/Ora
Per avere le indicazioni di data e ora corrette in registri e dati video, si consiglia di sincronizzare l'ora con un server di riferimento orario centrale. A tale scopo, è possibile utilizzare SNTP e la data TLS. Il vantaggio di SNTP è una sincronizzazione più precisa dell'ora. Il vantaggio della data TLS è la possibilità di verificare la presenza di un certificato corretto; di conseguenza, è la soluzione più sicura.
Consiglio: utilizzare un metodo sicuro di sincronizzazione dell'ora, con SNTP o con la data TLS.

Servizi basati su cloud
Bosch offre i propri servizi basati sul cloud per la gestione delle telecamere tramite il cloud Bosch (Remote Portal). I servizi cloud non si connettono automaticamente a Remote Portal e sono disabilitati per impostazione predefinita. Per poter utilizzare tale funzionalità, è necessario innanzitutto che ciascuna telecamera sia connessa a Remote Portal. Sono state prese tutte le precauzioni per proteggere la connessione tra Remote Portal e la telecamera quindi, se necessario, è possibile utilizzare Remote Portal in qualsiasi ambiente.
Consiglio: Remote Portal può essere utilizzato se la soluzione cloud è in uso.

Tenuta software
Dopo aver completato la configurazione di una telecamera IP, è necessario che le impostazioni del dispositivo non vengano modificate. È possibile abilitare un sigillo software per ricevere una notifica in caso di modifiche della configurazione del dispositivo.
Consiglio: abilitare il sigillo software se non sono presenti modifiche della configurazione in sospeso.

4.4.4 Strategia Defense in Depth

La strategia Defense in Depth si riferisce a un approccio di sicurezza a più livelli, in cui nessuna singola misura da sola è responsabile della sicurezza di un prodotto; per utilizzare impropriamente un prodotto, un malintenzionato deve violare più livelli. Al lancio di ogni nuova versione del prodotto, viene valutato se sono necessarie nuove funzionalità per ridurre il rischio di nuovi attacchi o per aumentare la sicurezza generale del prodotto.
Di seguito è fornita una panoramica delle principali funzioni di sicurezza della telecamera IP.

- **Firma del firmware**
  Ogni file di aggiornamento del firmware è crittografato e firmato da un certificato Bosch. È possibile installare sulle telecamere solo gli aggiornamenti pubblicati da Bosch, evitando l'installazione di firmware dannoso.
- **Secure Boot**
  Le telecamere delle piattaforme CPP13, CPP14 o più recenti presentano un meccanismo Secure Boot. Secure Boot verifica l'integrità dell'intero sistema, a partire dal bootloader e continuando con il firmware stesso sulle telecamere, ogni fase del processo di avvio verifica quella successiva, iniziando con una radice di attendibilità hardware non modificabile. Ciò impedisce che un malintenzionato modifichi il bootloader o il firmware sul dispositivo.
- **Login Firewall**
  Per proteggere da attacchi brute force alle password e al contempo consentire agli amministratori di effettuare l'accesso e di proteggere da attacchi DoS (Denial of Service), Login Firewall controlla i tentativi di accesso in base all'analisi del comportamento e ai blocchi dinamici oppure consente l'accesso in base agli indirizzi IP.

– **Autenticazione telecamera**
Per identificare e autenticare in modo univoco una telecamera, durante la produzione viene creato un certificato del dispositivo Bosch su ciascuna telecamera. Questo certificato può essere utilizzato per verificare se si sta comunicando con un dispositivo Bosch originale. Inoltre, è possibile caricare o creare sulla telecamera certificati personalizzati per fornire l'integrazione con un ambiente PKI per la protezione da attacchi man-in-the-middle.

4.5 Protezione avanzata dell'archiviazione

Poiché e telecamere o gli encoder IP Bosch sono in grado di stabilire una sessione iSCSI direttamente in un'unità iSCSI e scrivere i dati video in un'unità iSCSI, le unità iSCSI devono essere collegate alla stessa LAN o WAN delle periferiche Bosch.
Per evitare l'accesso non autorizzato ai dati video registrati, le unità iSCSI devono essere protette dall'accesso non autorizzato:

– Usare autenticazione password tramite CHAP per garantire che solo i dispositivi conosciuti siano autorizzati ad accedere alla destinazione iSCSI. Impostare una password CHAP nella destinazione iSCSI e immettere la password così configurata nella configurazione VRM. La password CHAP è valida per VRM e viene inviata automaticamente a tutti i dispositivi. Se una password CHAP viene utilizzata in un ambiente BVMS VRM, tutti i sistemi di archiviazione devono essere configurati per utilizzare la stessa password.
– Eliminare tutti i nomi utente predefiniti e password dal iSCSI di destinazione.
– Utilizzare una password complessa per gli account utente amministratore del iSCSI di destinazione.
– Disabilitare l'accesso amministrativo tramite Telnet alle destinazioni iSCSI. Utilizzare invece l'accesso SSH.
– Proteggere l'accesso della console alla destinazione iSCSI tramite password complessa.
– Disattivare le schede di interfaccia di rete non utilizzate.
– Monitorare lo stato del sistema di archivi iSCSI tramite strumenti di terze parti per identificare le anomalie.

4.5.1 Impostazione di una password CHAP su dispositivi iSCSI

Quando si imposta una password CHAP globale in BVMS Configuration Client, tale password viene trasferita automaticamente a tutti gli encoder, i decoder e i dispositivi VSG.
Per alcuni dispositivi iSCSI, questa funzione non è supportata. Su tali dispositivi è necessario impostare la password CHAP manualmente.

Avviso!
È necessario impostare la password CHAP globale sui dispositivi iSCSI prima di aggiungerli a BVMS.
Non è possibile aggiungere dispositivi iSCSI a una configurazione BVMS in cui è già attivata la password CHAP globale.

Per impostare manualmente una password CHAP su un dispositivo iSCSI (ad esempio DIVAR IP) basato su una versione recente del sistema operativo Microsoft Windows Server:

1. Aprire **Server Manager** e passare a **Servizi file e archiviazione > iSCSI.**
2. Nell'elenco **DESTINAZIONI iSCSI**, fare clic con il pulsante destro del mouse sulla destinazione iSCSI desiderata, quindi fare clic su **Proprietà**.
Viene visualizzata la finestra di dialogo **Proprietà**.

3. Nella finestra di dialogo **Proprietà**, fare clic su **Sicurezza**, quindi selezionare la casella di controllo **Abilita CHAP**.
4. Immettere quanto segue:
   – **Nome utente:** user
   – **Password:** immettere la password CHAP globale, come specificato in BVMS Configuration Client (nel menu **Hardware > Proteggi sistemi di archiviazione iSCSI con password CHAP...**).
5. Fare clic su **OK**.
   La password CHAP viene assegnata alla destinazione iSCSI.

4.6 Protezione avanzata dei server

4.6.1 Impostazioni consigliate dell'hardware server

– Il BIOS del server offre la possibilità di impostare una password di livello inferiore. Tali password consentono di impedire alle persone di avviare il computer, avviare da dispositivi rimovibili e modificare le impostazioni BIOS o UEFI (Unified Extensible Firmware Interface) senza autorizzazione.
– Per evitare il trasferimento di dati al server, le porte USB e le unità CD/DVD devono essere disabilitate.
  Inoltre, le porte NIC inutilizzate devono essere disabilitate e le porte di gestione come l'interfaccia HP ILO (HP Integrated Lights-Out) o le porte console devono essere disabilitate o protette da password.

4.6.2 Impostazioni di protezione consigliate per il sistema operativo Windows

I server devono far parte di un dominio Windows.
Grazie all'integrazione dei server in un dominio Windows, le autorizzazioni utente sono assegnate agli utenti di rete gestiti da un server centrale. Dal momento che questi account utente spesso implementano regole sulla forza e la scadenza delle password, l'integrazione può migliorare la protezione sugli account locali che non prevedono tali limitazioni.

4.6.3 Aggiornamenti di Windows

Le patch e gli aggiornamenti software Windows devono essere installati e devono rimanere aggiornati. Gli aggiornamenti Windows includono spesso patch per vulnerabilità di sicurezza individuate di recente, ad esempio la vulnerabilità Heartbleed SSL, che ha interessato milioni di computer in tutto il mondo. È opportuno installare le patch per tali problemi significativi devono.

4.6.4 Installazione del software antivirus

Installare il software antivirus e antispyware e tenerlo aggiornato.

4.6.5 Impostazioni consigliate per il sistema operativo Windows

Le seguenti impostazioni dei criteri di gruppo locale sono le impostazioni di gruppo consigliate in un sistema operativo Windows Server. Per modificare i criteri del computer locale predefiniti, utilizzare l'Editor Criteri di gruppo locali.
È possibile aprire il Local Group Policy Editor tramite la riga di comando o utilizzando Microsoft Management Console (MMC).

Per aprire il Local Group Policy Editor dalla riga di comando:

- Fare clic su **Start**, nella casella di ricerca **Start** digitare **gpedit.msc**, quindi premere Invio.

Per aprire il Local Group Policy Editor come snap-in MMC:

1. Fare clic su **Start**, nella casella di ricerca **Start** , digitare **mmc**, quindi premere Invio.
2. Nella finestra di dialogo **Aggiungi o rimuovi snap-in**, fare clic su **Editor oggetti Criteri di gruppo**, quindi fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Selezione oggetto Criteri di gruppo**, fare clic su **Sfoglia**.
4. Fare clic su **Questo computer** di modificare l'oggetto criteri di gruppo locale o fare clic su **Utenti** per modificare gli oggetti Amministratore, Non amministratore o Criteri di gruppo locale per singolo utente.
5. Fare clic su **Fine.**

4.6.6 Attivazione del controllo account utente sul server

Criteri del computer locale -> Configurazione computer -> Impostazioni di Windows -> Impostazioni di sicurezza -> Criteri locali -> Opzioni di sicurezza

Controllo account utente: modalità Approvazione amministratore per l'account amministratore predefinito	Abilitato
Controllo account utente: consenti alle applicazioni con accesso all'interfaccia utente di richiedere l'elevazione senza utilizzare il desktop protetto	Disabilitato
Controllo account utente: comportamento della richiesta di elevazione dei privilegi per gli amministratori in modalità Approvazione amministratore	Richiedi consenso
Controllo account utente: comportamento della richiesta di elevazione dei privilegi per gli utenti standard	Richiedi credenziali sul desktop sicuro
Controllo account utente: rileva installazione applicazioni e richiedi elevazione	Abilitato
Controllo account utente: eleva solo file eseguibili firmati e convalidati	Disabilitato
Controllo account utente: esegui tutti gli amministratori in modalità Approvazione amministratore	Abilitato
Controllo account utente: alla richiesta di elevazione passa al desktop protetto	Abilitato
Controllo account utente: virtualizza errori di scrittura su file e nel Registro di sistema in percorsi distinti per ogni utente	Abilitato

Criteri del computer locale -> Configurazione computer -> Modelli amministrativi -> Componenti di Windows -> Interfaccia utente delle credenziali

Enumera account amministratore nell'elevazione dei privilegi	Disabilitato

4.6.7 Disattivare l'AutoPlay

Criteri del computer locale -> Computer configurazione -> Modelli amministrativi -> Componenti di Windows -> Criteri AutoPlay

Disattiva AutoPlay	Abilitate tutte le unità

Comportamento predefinito di AutoRun	Abilitato, non eseguire comandi di esecuzione automatica
Disattiva AutoPlay per dispositivi non di volume	Abilitato

4.6.8 Dispositivi esterni

Criteri del computer locale -> Configurazione computer -> Impostazioni di Windows -> Impostazioni di sicurezza -> Criteri locali -> Opzioni di sicurezza

Dispositivi: consenti il disinserimento senza dover effettuare l'accesso	Disabilitato
Dispositivi: è consentita la formattazione e la rimozione dei supporti rimovibili	Amministratori
Dispositivi: non consentire agli utenti di installare i driver della stampante	Abilitato
Dispositivi: limita accesso al CD-ROM agli utenti che hanno effettuato l'accesso locale	Abilitato
Dispositivi: limita accesso al disco floppy agli utenti che hanno effettuato l'accesso locale	Abilitato

4.6.9 Configurazione dell'assegnazione diritti utente

Criteri del computer locale -> Configurazione computer -> Impostazioni di Windows -> Impostazioni di protezione -> Criteri locali -> Assegnazione diritti utente

Accesso a Gestione credenziali come chiamante trusted	Nessuno
Accedi al computer dalla rete	Utenti autenticati
Agire come parte del sistema operativo	Nessuno
Aggiungi workstation al dominio	Nessuno
Consenti accesso tramite Servizi Desktop remoto	Amministratori, utenti desktop remoti
Modifica dell'orario di sistema	Amministratori
Modifica del fuso orario	Amministratori, assistenza locale
Creare un file pagina	Amministratori
Creare un oggetto token	Nessuno
Creazione di oggetti condivisi permanentemente	Nessuno
Nega accesso al computer dalla rete	Accesso anonimo, gruppo Guest
Nega accesso come processo batch	Accesso anonimo, gruppo Guest
Nega accesso come servizio	Nessuno

Nega accesso locale	Accesso anonimo, gruppo Guest
Nega accesso tramite Servizi Desktop remoto	Accesso anonimo, Guest
Impostazione account computer ed utente a tipo trusted per la delega	Nessuno
Arresto forzato da un sistema remoto	Amministratori
Generazione di controlli di protezione	Assistenza locale, assistenza di rete
Aumento della priorità di pianificazione	Amministratori
Carica e scarica driver dispositivi	Amministratori
Modifica delle etichette di oggetti	Nessuno
Modifica dei valori di ambiente firmware	Amministratori
Esecuzione attività di manutenzione volume	Amministratori
Creazione di profilo del singolo processo	Amministratori
Rimozione del computer dall'alloggiamento	Amministratori
Ripristino di file e directory	Amministratori
Arresto del sistema	Amministratori
Sincronizzazione dei dati dell'Active Directory	Nessuno
Acquisizione proprietà di file o di altri oggetti	Amministratori

4.6.10 Salvaschermo

– Attivare lo screen saver protetto da password e definire il tempo di timeout:
Criteri del computer locale -> Configurazione utente -> Modelli amministrativi -> Pannello di controllo -> Personalizzazione

Abilita screen saver	Abilitato
Proteggi screen saver con password	Abilitato
Timeout screen saver	1800 secondi

4.6.11 Attiva le impostazioni dei criteri password

– L'abilitazione delle impostazioni dei criteri password garantisce che le password utente rispondano ai requisiti minimi

Criteri del computer locale -> Impostazioni di Windows -> Impostazioni di sicurezza -> Criteri account -> Criteri password

Imponi cronologia delle password	10 password memorizzate
Validità massima password	90 giorni
Validità minima password	1 giorno
Lunghezza minima password	10 caratteri

La password deve essere conforme con i requisiti di complessità	Abilitato
Archiviare le password utilizzando la crittografia reversibile per tutti gli utenti del dominio	Disabilitato

4.6.12 Disabilita i servizi Windows non essenziali

– La disabilitazione dei servizi Windows non essenziali consente un maggiore livello di sicurezza e riduce al minimo i punti di attacco.

Servizio Gateway di livello applicazione	Disabilitato
Gestione applicazione	Disabilitato
Browser computer	Disabilitato
Manutenzione collegamenti distribuiti client	Disabilitato
Host provider di individuazione funzioni	Disabilitato
Pubblicazione risorse per individuazione	Disabilitato
Accesso dispositivo Human Interface	Disabilitato
Condivisione connessione Internet (ICS)	Disabilitato
Mapper individuazione topologia livelli di collegamento	Disabilitato
Utilità di pianificazione classi multimediali	Disabilitato
File offline	Disabilitato
Auto Connection Manager di Accesso remoto	Disabilitato
Gestione connessione accesso remoto	Disabilitato
Routing e accesso remoto	Disabilitato
Rilevamento hardware shell	Disabilitato
Helper console di amministrazione speciale	Disabilitato
Individuazione SSDP	Disabilitato

4.6.13 Account utente sistema operativo Windows

Gli account utente del sistema operativo Windows devono essere protetti da password complesse.
I server sono normalmente gestiti e manutenuti con account amministratore Windows, assicurarsi che vengano utilizzate password complesse per gli account amministratore.

Le password devono contenere caratteri di tre delle seguenti categorie:
– Caratteri alfabetici maiuscoli di lingue europee (da A a Z, con segni diacritici, caratteri greci e cirillici)
– Caratteri alfabetici minuscoli di lingue europee (da a a z, ß, con segni diacritici, caratteri greci e cirillici)
– Cifre a base 10 (0-9)
– Caratteri non alfanumerici: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

– Qualsiasi carattere Unicode classificato come carattere alfabetico, ma che non è maiuscolo o minuscolo. Ciò comprende i Unicode delle lingue asiatiche.

Uso del blocco account Windows per ostacolare la riuscita dei tentativi di scoprire le password.
Il consiglio di Windows 8.1 Security Baselines è 10/15/15:
– 10 tentativi non riusciti
– Durata del blocco 15 minuti
– Ripristino del contatore dopo 15 minuti

Criteri del computer locale -> Configurazione computer -> Impostazioni di Windows -> Impostazioni di sicurezza -> Criteri account -> Criterio di blocco account

Durata blocco account	Durata blocco account
Soglia blocco account 15 minuti 10 tentativi di accesso falliti	Soglia blocco account 15 minuti 10 tentativi di accesso falliti
Reimposta blocco account dopo	Reimposta blocco account dopo

– Assicurarsi che tutte le password predefinite del server e del sistema operativo Windows siano sostituite con nuove password complesse.

4.6.14 Attiva firewall sul server

▸ Abilitare la comunicazione della porta standard BVMS secondo le porte BVMS.

Avviso!
Per l'utilizzo e le impostazioni delle porte pertinenti, consultare la documentazione su BVMS. Assicurarsi di controllare nuovamente le impostazioni nel caso di aggiornamenti di firmware o software.

4.7 Protezione avanzata dei client Windows

4.7.1 Windows Workstation

I sistemi operativi Windows desktop, utilizzati per applicazioni BVMS Client come BVMS Operator Client o Configuration Client, vengono installati all'esterno dell'area protetta. È necessario eseguire una protezione avanzata delle workstation per proteggere i dati video, i documenti e altre applicazioni dall'accesso non autorizzato.
Le seguenti impostazioni devono essere applicate o selezionate.

4.7.2 Impostazioni consigliate hardware Windows Workstation

– Impostare una password BIOS/UEFI per impedire che le persone lancino sistemi operativi alternativi.
– Per evitare il trasferimento di dati al client, le porte USB e l'unità CD/DVD devono essere disabilitate. Inoltre, occorre disabilitare le porte NIC inutilizzate.

4.7.3 Impostazioni di protezione consigliate per il sistema operativo Windows

– La workstation deve far parte di un dominio Windows.
L'integrazione della workstation in un dominio Windows, le relative impostazioni di sicurezza possono essere gestite in modo centralizzato.
– Aggiornamenti Windows
Tenersi aggiornati con le patch e gli aggiornamenti software per il sistema operativo Windows.

– Installazione del software Antivirus
  Installare il software antivirus e antispyware e mantenerlo aggiornato.

4.7.4 Impostazioni consigliate per il sistema operativo Windows

Le seguenti impostazioni dei criteri di gruppo locale sono le impostazioni di gruppo consigliate in un sistema operativo Windows Server. Per modificare i criteri del computer locale predefiniti, utilizzare l'Editor Criteri di gruppo locali.
È possibile aprire il Local Group Policy Editor tramite la riga di comando o utilizzando Microsoft Management Console (MMC).

Per aprire il Local Group Policy Editor dalla riga di comando:

- Fare clic su **Start**, nella casella di ricerca **Start** digitare **gpedit.msc**, quindi premere Invio.

Per aprire il Local Group Policy Editor come snap-in MMC:

1. Fare clic su **Start**, nella casella di ricerca **Start** , digitare **mmc**, quindi premere Invio.
2. Nella finestra di dialogo **Aggiungi o rimuovi snap-in**, fare clic su **Editor oggetti Criteri di gruppo**, quindi fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Selezione oggetto Criteri di gruppo**, fare clic su **Sfoglia**.
4. Fare clic su **Questo computer** di modificare l'oggetto criteri di gruppo locale o fare clic su **Utenti** per modificare gli oggetti Amministratore, Non amministratore o Criteri di gruppo locale per singolo utente.
5. Fare clic su **Fine.**

4.7.5 Attivazione del controllo account utente sul server

Criteri del computer locale -> Configurazione computer -> Impostazioni di Windows -> Impostazioni di sicurezza -> Criteri locali -> Opzioni di sicurezza

Controllo account utente: modalità Approvazione amministratore per l'account amministratore predefinito	Abilitato
Controllo account utente: consenti alle applicazioni con accesso all'interfaccia utente di richiedere l'elevazione senza utilizzare il desktop protetto	Disabilitato
Controllo account utente: comportamento della richiesta di elevazione dei privilegi per gli amministratori in modalità Approvazione amministratore	Richiedi consenso
Controllo account utente: comportamento della richiesta di elevazione dei privilegi per gli utenti standard	Richiedi credenziali sul desktop sicuro
Controllo account utente: rileva installazione applicazioni e richiedi elevazione	Abilitato
Controllo account utente: eleva solo file eseguibili firmati e convalidati	Disabilitato
Controllo account utente: esegui tutti gli amministratori in modalità Approvazione amministratore	Abilitato
Controllo account utente: alla richiesta di elevazione passa al desktop protetto	Abilitato
Controllo account utente: virtualizza errori di scrittura su file e nel Registro di sistema in percorsi distinti per ogni utente	Abilitato

Criteri del computer locale -> Configurazione computer -> Modelli amministrativi -> Componenti di Windows -> Interfaccia utente delle credenziali

Enumera account amministratore nell'elevazione dei privilegi	Disabilitato

4.7.6 Disattivare l'AutoPlay

Criteri del computer locale -> Computer configurazione -> Modelli amministrativi -> Componenti di Windows -> Criteri AutoPlay

Disattiva AutoPlay	Abilitate tutte le unità
Comportamento predefinito di AutoRun	Abilitato, non eseguire comandi di esecuzione automatica
Disattiva AutoPlay per dispositivi non di volume	Abilitato

4.7.7 Dispositivi esterni

Criteri del computer locale -> Configurazione computer -> Impostazioni di Windows -> Impostazioni di sicurezza -> Criteri locali -> Opzioni di sicurezza

Dispositivi: consenti il disinserimento senza dover effettuare l'accesso	Disabilitato
Dispositivi: è consentita la formattazione e la rimozione dei supporti rimovibili	Amministratori
Dispositivi: non consentire agli utenti di installare i driver della stampante	Abilitato
Dispositivi: limita accesso al CD-ROM agli utenti che hanno effettuato l'accesso locale	Abilitato
Dispositivi: limita accesso al disco floppy agli utenti che hanno effettuato l'accesso locale	Abilitato

4.7.8 Configurazione dell'assegnazione diritti utente

Criteri del computer locale -> Configurazione computer -> Impostazioni di Windows -> Impostazioni di protezione -> Criteri locali -> Assegnazione diritti utente

Accesso a Gestione credenziali come chiamante trusted	Nessuno
Accedi al computer dalla rete	Utenti autenticati
Agire come parte del sistema operativo	Nessuno
Aggiungi workstation al dominio	Nessuno
Consenti accesso tramite Servizi Desktop remoto	Amministratori, utenti desktop remoti
Modifica dell'orario di sistema	Amministratori
Modifica del fuso orario	Amministratori, assistenza locale

Creare un file pagina	Amministratori
Creare un oggetto token	Nessuno
Creazione di oggetti condivisi permanentemente	Nessuno
Nega accesso al computer dalla rete	Accesso anonimo, gruppo Guest
Nega accesso come processo batch	Accesso anonimo, gruppo Guest
Nega accesso come servizio	Nessuno
Nega accesso locale	Accesso anonimo, gruppo Guest
Nega accesso tramite Servizi Desktop remoto	Accesso anonimo, Guest
Impostazione account computer ed utente a tipo trusted per la delega	Nessuno
Arresto forzato da un sistema remoto	Amministratori
Generazione di controlli di protezione	Assistenza locale, assistenza di rete
Aumento della priorità di pianificazione	Amministratori
Carica e scarica driver dispositivi	Amministratori
Modifica delle etichette di oggetti	Nessuno
Modifica dei valori di ambiente firmware	Amministratori
Esecuzione attività di manutenzione volume	Amministratori
Creazione di profilo del singolo processo	Amministratori
Rimozione del computer dall'alloggiamento	Amministratori
Ripristino di file e directory	Amministratori
Arresto del sistema	Amministratori
Sincronizzazione dei dati dell'Active Directory	Nessuno
Acquisizione proprietà di file o di altri oggetti	Amministratori

4.7.9 Salvaschermo

– Attivare lo screen saver protetto da password e definire il tempo di timeout:
Criteri del computer locale -> Configurazione utente -> Modelli amministrativi -> Pannello di controllo -> Personalizzazione

Abilita screen saver	Abilitato
Proteggi screen saver con password	Abilitato
Timeout screen saver	1800 secondi

4.7.10 Attiva le impostazioni dei criteri password

– L'abilitazione delle impostazioni dei criteri password garantisce che le password utente rispondano ai requisiti minimi

Criteri del computer locale -> Impostazioni di Windows -> Impostazioni di sicurezza -> Criteri account -> Criteri password

Imponi cronologia delle password	10 password memorizzate
Validità massima password	90 giorni
Validità minima password	1 giorno
Lunghezza minima password	10 caratteri
La password deve essere conforme con i requisiti di complessità	Abilitato
Archiviare le password utilizzando la crittografia reversibile per tutti gli utenti del dominio	Disabilitato

4.7.11 Disabilita i servizi Windows non essenziali

– La disabilitazione dei servizi Windows non essenziali consente un maggiore livello di sicurezza e riduce al minimo i punti di attacco.

Servizio Gateway di livello applicazione	Disabilitato
Gestione applicazione	Disabilitato
Browser computer	Disabilitato
Manutenzione collegamenti distribuiti client	Disabilitato
Host provider di individuazione funzioni	Disabilitato
Pubblicazione risorse per individuazione	Disabilitato
Accesso dispositivo Human Interface	Disabilitato
Condivisione connessione Internet (ICS)	Disabilitato
Mapper individuazione topologia livelli di collegamento	Disabilitato
Utilità di pianificazione classi multimediali	Disabilitato
File offline	Disabilitato
Auto Connection Manager di Accesso remoto	Disabilitato
Gestione connessione accesso remoto	Disabilitato
Routing e accesso remoto	Disabilitato
Rilevamento hardware shell	Disabilitato
Helper console di amministrazione speciale	Disabilitato
Individuazione SSDP	Disabilitato

4.7.12 Account utente sistema operativo Windows

Gli account utente del sistema operativo Windows devono essere protetti da password complesse.

I server sono normalmente gestiti e manutenuti con account amministratore Windows, assicurarsi che vengano utilizzate password complesse per gli account amministratore.

Le password devono contenere caratteri di tre delle seguenti categorie:
- Caratteri alfabetici maiuscoli di lingue europee (da A a Z, con segni diacritici, caratteri greci e cirillici)
- Caratteri alfabetici minuscoli di lingue europee (da a a z, ß, con segni diacritici, caratteri greci e cirillici)
- Cifre a base 10 (0-9)
- Caratteri non alfanumerici: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Qualsiasi carattere Unicode classificato come carattere alfabetico, ma che non è maiuscolo o minuscolo. Ciò comprende i Unicode delle lingue asiatiche.

Uso del blocco account Windows per ostacolare la riuscita dei tentativi di scoprire le password.
Il consiglio di Windows 8.1 Security Baselines è 10/15/15:
- 10 tentativi non riusciti
- Durata del blocco 15 minuti
- Ripristino del contatore dopo 15 minuti

Criteri del computer locale -> Configurazione computer -> Impostazioni di Windows -> Impostazioni di sicurezza -> Criteri account -> Criterio di blocco account

Durata blocco account	Durata blocco account
Soglia blocco account 15 minuti 10 tentativi di accesso falliti	Soglia blocco account 15 minuti 10 tentativi di accesso falliti
Reimposta blocco account dopo	Reimposta blocco account dopo

- Assicurarsi che tutte le password predefinite del server e del sistema operativo Windows siano sostituite con nuove password complesse.
- Disattivare gli account inutilizzati del sistema operativo Windows.
- Disabilitare l'accesso desktop remoto alla workstation client.
- Eseguire la workstation senza diritti di amministratore per evitare che gli utenti standard modifichino le impostazioni del sistema.

4.7.13 Attiva firewall nella workstation

▸ Abilitare la comunicazione della porta standard BVMS secondo le porte BVMS.

Avviso!
Per l'utilizzo e le impostazioni delle porte pertinenti, consultare la documentazione su BVMS. Assicurarsi di controllare nuovamente le impostazioni nel caso di aggiornamenti di firmware o software.

4.8 Protezione accesso alla rete

Attualmente molti sistemi di videosorveglianza IP vengono distribuiti nell'infrastruttura di rete esistente del cliente solamente come "un'altra applicazione IT".
Sebbene ciò abbia dei vantaggi in termini di costi e manutenzione, questo tipo di distribuzione espone inoltre il sistema di sicurezza a minacce indesiderate, comprese quelle interne.
Occorre adottare provvedimenti adeguati per evitare situazioni quali la divulgazione del video di un evento in Internet o sui social media. Eventi di questo tipo potrebbero non solo rappresentare una violazione della privacy, ma potenzialmente danneggiare l'azienda.

Sono disponibili due tecnologie principali per creare una "rete nella rete". La scelta di una delle due da parte degli architetti dell'infrastruttura IT è strettamente legata all'infrastruttura di rete esistente, alle apparecchiature di rete distribuite e alle funzionalità e alla topologia richieste dalla rete.

4.8.1 VLAN: Virtual LAN

Una Virtual LAN viene creata suddividendo una LAN in più segmenti. La segmentazione di rete viene effettuata tramite la configurazione di uno switch di rete o di un router. Una VLAN presenta il vantaggio che la risorsa può essere indirizzata senza cambiare il cablaggio dei collegamenti dei dispositivi di rete.
La qualità dei programmi di assistenza, applicati a segmenti specifici come per la videosorveglianza, potrebbero non solo incrementare la sicurezza, ma anche le prestazioni.

Le VLAN vengono implementate su data link layer (OSI layer 2) e presentano un'analogia con il subnetting IP (vedere *Assegnazione degli indirizzi IP, pagina 8*) che è simile sul layer di rete (OSI layer 3).

4.8.2 VPN: Virtual Private Network

Una Virtual Private Network è una rete (privata) separata che si estende spesso su reti pubbliche o su Internet. Sono disponibili vari protocolli per creare una VPN, in genere un tunnel che trasporta il traffico protetto. Le reti virtuali private potrebbero essere progettate come tunnel "point-to-point", collegamenti "any-to-any" o connessioni multipunto. Le VPN possono essere distribuite con comunicazioni crittografate o semplicemente fare affidamento su una comunicazione sicura all'interno della VPN stessa.

Le VPN possono essere utilizzate per collegare siti remoti tramite connessioni Wide Area Network (WAN), proteggendo al contempo la privacy e aumentando la sicurezza all'interno di una rete locale LAN (Local Area Network). Poiché una VPN funge da rete separata, tutti i dispositivi aggiunti alla VPN funzioneranno in modo continuo, come se fossero su una rete tipica. Una VPN non solo aggiunge un ulteriore layer di protezione per un sistema di sorveglianza, ma presenta inoltre il vantaggio aggiuntivo di segmentare il traffico commerciale nelle reti di produzione e il traffico video.

Avviso!
Se applicabile, le VLAN o VPN aumentano il livello di sicurezza del sistema di sorveglianza se combinate nell'infrastruttura IT esistente.

Oltre a proteggere il sistema di sorveglianza dagli accessi non autorizzati nell'infrastruttura IT condivisa, occorre in primo luogo considerare chi deve essere autorizzato ad accedere alla rete.

4.8.3 Disabilitare le porte di commutazione inutilizzate

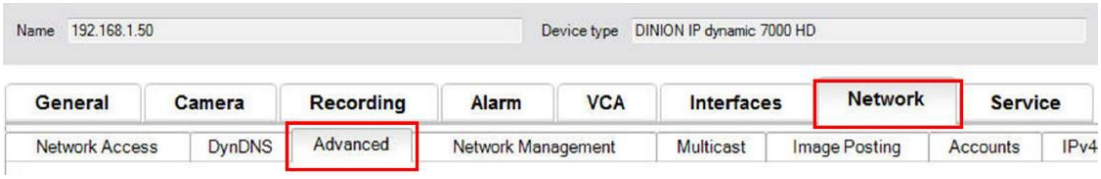
La disattivazione delle porte di rete inutilizzate garantisce che i dispositivi non autorizzati non accedano alla rete. Ciò di riduce il rischio che qualcuno tenti di accedere a una subnet di sicurezza collegando il proprio dispositivo in uno switch o in una presa di rete inutilizzata. La possibilità di disabilitare porte specifiche è un'opzione comune negli switch gestiti, sia a basso costo sia aziendali.

4.8.4 Reti protette 802.1x

Tutti i dispositivi video IP Bosch possono essere configurati come client 802.1x. Ciò consente loro di autenticarsi in server RADIUS e partecipare in una rete protetta. Prima di inserire i dispositivi video nella rete protetta, è necessario collegarsi direttamente al dispositivo video dal computer portatile di un tecnico per immettere credenziali valide come descritto nella procedura riportata di seguito.

I servizi 802.1x possono essere facilmente configurati tramite Configuration Manager.

1. In Configuration Manager, selezionare il dispositivo desiderato.
2. Selezionare la scheda **Rete**, quindi selezionare **Avanzate**.



3. Individuare la parte **802.1x** della pagina.
4. Nel menu a discesa **802.1x** selezionare **On.**
5. Inserire un **Identità** e **Password valido.**
6. Salva modifiche.
7. Disconnettere e collocare i dispositivi nella rete protetta.

Avviso!
802.1x in sé e per sé non fornisce una comunicazione sicura tra il supplicant e il server di autenticazione .
Di conseguenza, il nome utente e la password possono essere "annusate" dalla rete. 802.1x può utilizzare EAP-TLS per garantire una comunicazione sicura.

Extensible Authentication Protocol - Transport Layer Security
L'Extensible Authentication Protocol (EAP) fornisce supporto per metodi di autenticazione multipli. Transport Layer Security (TLS) consente l'autenticazione reciproca, la negoziazione di suite di cifre con protezione dell'integrità e lo scambio di chiavi tra due punti finali. EAP-TLS include il supporto per l'autenticazione reciproca basata su certificati e la derivazione delle chiavi. In altre parole, EAP-TLS incapsula il processo nel quale sia il server sia client si inviano reciprocamente un certificato.

Avviso!
Consultare il Technical White Paper specifico *Network Authentication - 802.1x - Secure the Edge of the Network*, disponibile nel catalogo prodotti Bosch Security Systems online all'indirizzo:
http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

5 Funzionamento sicuro

5.1 Separazione della rete

Se possibile, il dispositivo deve essere utilizzato in una rete separata (ad esempio mediante l'utilizzo di VLAN) con restrizioni di accesso per limitare il traffico broadcast e proteggere il dispositivo da attacchi di rete.

5.2 Archiviazione sicura delle chiavi in set di credenziali hardware

Per proteggere le chiavi private provenienti dai certificati in modo ottimale, è necessario memorizzarle in un componente hardware o in un set di credenziali hardware. Questi chip forniscono protezione dall'accesso non autorizzato a chiavi private anche quando il dispositivo è fisicamente aperto per l'accesso.
Nelle telecamere Bosch, tali chiavi sono memorizzate in un coprocessore di crittografia o in un Secure Element (SE) separato. Entrambi forniscono un'archiviazione sicura e funzioni di crittografia che non espongono mai le chiavi private nella memoria o in posizioni da cui potrebbero essere potenzialmente recuperate.
Su workstation e server, generalmente è disponibile un chip TPM (Trusted Platform Module). È necessario configurare le funzioni e le librerie di crittografia per l'utilizzo dell'archiviazione TPM, ove possibile.

5.3 Certificati univoci dei dispositivi

Sebbene un certificato predefinito autofirmato sia in genere disponibile per ogni dispositivo compatibile con TLS o HTTPS, è opportuno non considerare tale certificato di per sé sufficiente per l'autenticazione, in quanto non protegge da attacchi man-in-the-middle (MITM).

Se i dispositivi sono distribuiti in un ambiente in cui sono necessari passaggi aggiuntivi per convalidare l'identità di ciascun singolo dispositivo video IP, è possibile generare e caricare nuovi certificati e chiavi private nei dispositivi video stessi. È possibile ottenere nuovi certificati da un'autorità di certificazione (CA, Certificate Authority) oppure possono essere generati con un kit di strumenti OpenSSL.

Se i dispositivi vengono utilizzati in reti pubbliche, si consiglia di ottenere i certificati da un'autorità di certificazione pubblica o di farli firmare da tale autorità, che è inoltre in grado di verificare origine e validità, ovvero l'attendibilità, del certificato del dispositivo.

Da anni, tutte le telecamere Bosch sono dotate di un certificato di dispositivo univoco preinstallato e di una chiave privata, derivata dal certificato radice di Bosch e installata in un ambiente di produzione sicuro, a prova che la telecamera è un dispositivo originale Bosch. Questo certificato viene utilizzato per le connessioni HTTPS automaticamente e può essere utilizzato per identificare e autenticare un dispositivo verificando la catena di certificati fino al certificato radice di Bosch.

Avviso!
Per autenticare un singolo dispositivo, è opportuno utilizzare certificati. Si consiglia di generare un certificato specifico per dispositivo, derivato da un certificato principale.

La variante più sicura di una distribuzione di certificati consiste nel generare una richiesta di firma del certificato (CSR) sul dispositivo e di richiedere un certificato a un'autorità di certificazione interna o esterna.
Con una richiesta di firma del certificato, il dispositivo mantiene interna la chiave privata ed espone solo il resto del certificato che deve essere firmato dall'autorità di certificazione. La chiave privata viene memorizzata in modo sicuro nel Secure Element (SE) della telecamera o, ad esempio, nel modulo TPM (Trusted Platform Module) del dispositivo.
Pertanto, ogni volta che un dispositivo offre la possibilità di una CSR, questo è il metodo da preferire per la creazione di un certificato.

È possibile caricare i certificati su un dispositivo utilizzando la pagina Web di un dispositivo video o mediante Configuration Manager.

Caricamento dei certificati tramite la pagina Web del dispositivo
È possibile caricare i certificati utilizzando la pagina web dispositivo di un dispositivo video. Sulla pagina Web del dispositivo, sulla pagina **Certificati**, è possibile aggiungere nuovi certificati, eliminarli e definirne l'utilizzo.

Caricamento dei certificati mediante Configuration Manager
In Configuration Manager, i certificati possono essere facilmente caricati in dispositivi singoli o contemporaneamente in dispositivi multipli.
Per caricare i certificati:
1. In Configuration Manager selezionare uno o più dispositivi.
2. Fare clic con il pulsante destro del mouse su **Caricamento file**, quindi fare clic su **Certificato SSL...**.
   Si apre una finestra di Windows Explorer per individuare il certificato per il caricamento.

Per i sistemi di piccole dimensioni, Configuration Manager fornisce una funzione di supporto denominata **MicroCA**, che consente di creare o utilizzare una CA radice e derivare da essa i certificati dei dispositivi oppure di utilizzarla per firmare le richieste di firma del certificato dei dispositivi, anche per più dispositivi contemporaneamente. Per ulteriori informazioni, consultare il Manuale utente di Configuration Manager.

Fare riferimento a
– *Creazione di attendibilità con i certificati, pagina 48*

5.4 Controllo dei file di registro

Il monitoraggio dei file di registro è una parte importante dell'attività di manutenzione o analisi della sicurezza. Il controllo periodico dei file di registro consente di rivelare problemi di configurazione o violazioni della sicurezza quali falsi accessi.
Per l'analisi dei file di registro e la loro memorizzazione a lungo termine, si consiglia di inviare i file di registro del dispositivo a un server syslog o a un sistema SIEM poiché, ad esempio, una telecamera riserverà una determinata quantità fissa di spazio alla registrazione interna ma, se tale spazio viene esaurito, sovrascriverà i registri meno recenti.

5.5 Sistema SIEM

Il sistema SIEM (Security Information and Event Management) viene utilizzato per raccogliere e analizzare le informazioni provenienti da dispositivi e sistemi diversi. È possibile integrare i dispositivi con un sistema SIEM inviando i registri tramite il protocollo syslog. L'analisi di questi registri consente di eseguire la manutenzione e di rilevare errori di configurazione o attacchi sul dispositivo (ad esempio falsi accessi).

5.6 PKI

L'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure) si riferisce ai sistemi necessari per generare e gestire certificati digitali. Per HTTPS, l'autenticazione di rete con 802.1x, l'autenticazione degli utenti con certificati e altre funzioni di crittografia, è possibile installare sul dispositivo certificati personalizzati.

5.7 AD FS

Active Directory Federation Services (AD FS) è un servizio offerto da Microsoft che consente l'autenticazione a una Active Directory locale (tramite un server AD FS) o al cloud Azure. Oltre all'autenticazione degli utenti locale con password o autenticazione basata su certificato, è possibile integrare i dispositivi in un dominio Active Directory con AD FS per l'autenticazione e la gestione dell'accesso degli utenti in modo centralizzato.

5.8 Funzionamento sicuro di telecamere IP

5.8.1 Creazione di attendibilità con i certificati

Tutte le telecamere IP Bosch che eseguono FW 6.10 o successivo utilizzano un archivio certificati, che si trova nel menu **Assistenza** della configurazione telecamera.
All'archivio è possibile aggiungere certificati di server specifici, certificati client e certificati attendibili.
Per aggiungere un certificato all'archivio:

1. Dalla pagina web del dispositivo, andare alla pagina **Configurazione** .
2. Selezionare il menu **Assistenza** e il sottmenu **Certificati** .
3. Nella sezione **Elenco file** , fare clic su **Aggiungi**.
4. Caricare i certificati desiderati.
   Al termine del caricamento, i certificati compaiono nella sezione **Elenco utiilizzi**.
5. Nella sezione **Elenco utiilizzi** , selezionare il certificato desiderato.
6. Per attivare l'utilizzo dei certificati è necessario riavviare la telecamera. Per riavviare la telecamera, fare clic su **Imposta**.

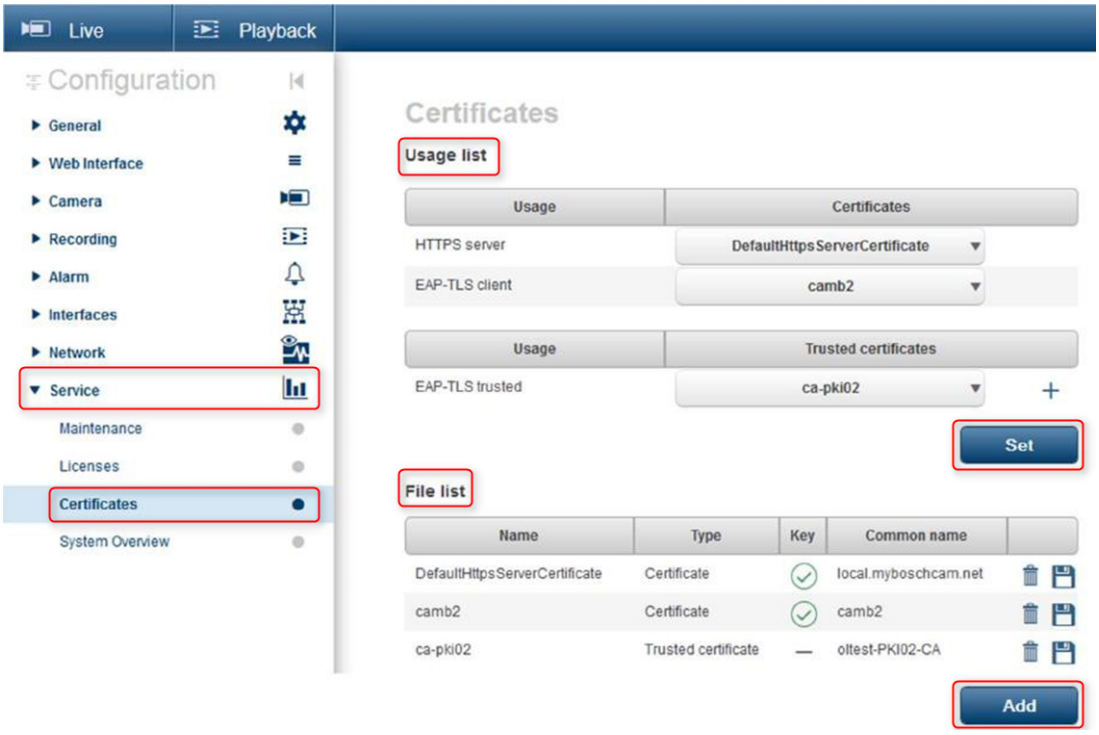


Figura 5.1: Esempio: certificati EAP/TLS memorizzati in una telecamera Bosch (FW6.11)

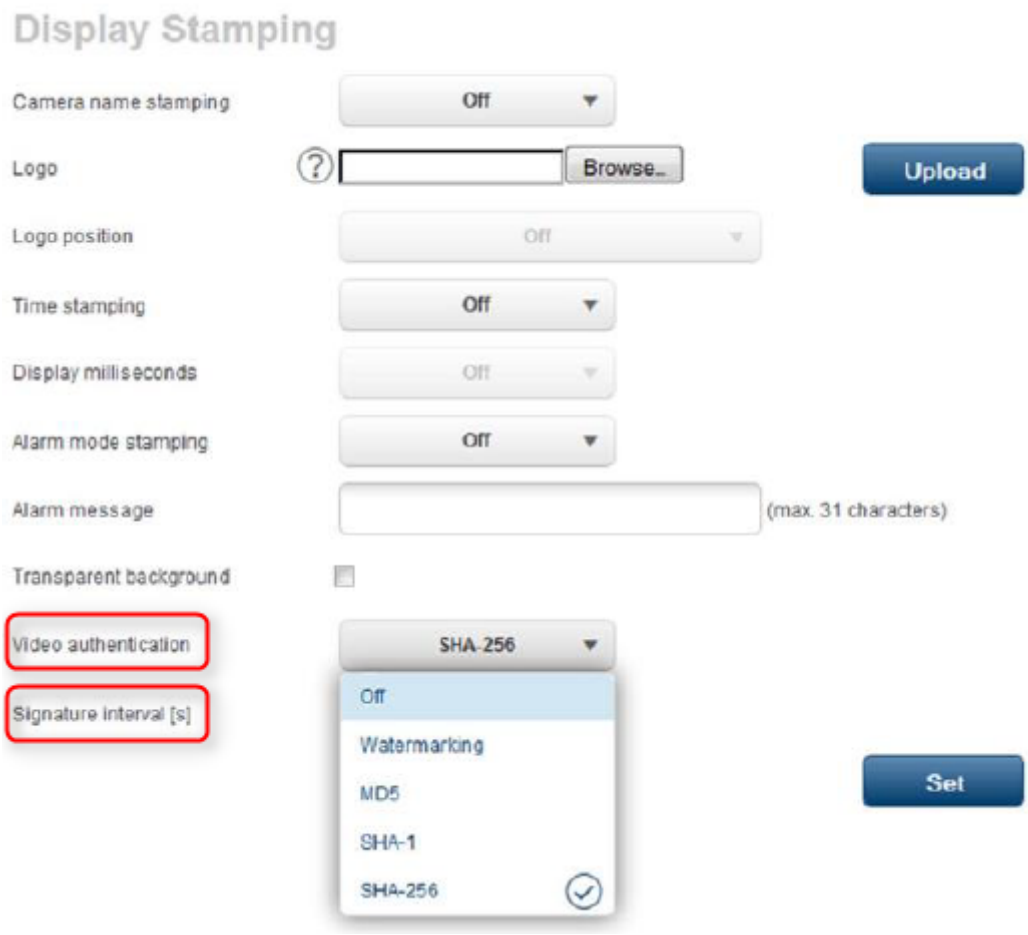
I certificati sono accettati nel formato *.pem, *.cer o *.crt e devono essere codificati a base 64. Possono essere caricati come unico file combinato, o suddivisi in certificati e chiavi parziali e caricati in quest'ordine come file separati da ricombinare automaticamente.

A partire dal firmware versione 6.20 sono supportate le chiavi private PKCS #8 protette da password (crittografia AES), da caricare in formato *.pem codificato a base 64.

5.8.2 Autenticazione video

Quando i dispositivi di un sistema sono stati correttamente protetti e autenticati, è opportuno tenere d'occhio anche i dati video da essi forniti. Il metodo è denominato autenticazione video.
L'autenticazione video è limitata esclusivamente ai metodi di convalida dell'autenticità del video. L'autenticazione video non riguarda in alcun modo la trasmissione di video o dati.
Prima della pubblicazione firmware 5.9, il watermarking avveniva mediante un semplice algoritmo di checksum attraverso il flusso video. Quando si utilizza il watermarking di base non vi è utilizzo di certificati o crittografia. Un checksum è una misurazione di base della "Data Fixity" di un file, con verifica dell'integrità del file stesso.
Per configurare l'autenticazione video, ad esempio nel browser web:

1. Andare al menu **Generale** , quindi selezionare **Visualizza indicatore**.
2. Nel menu a discesa **Autenticazione video**, selezionare l'opzione desiderata:
   I firmware versione 5,9 e successiva fornisce tre opzioni di autenticazione video oltre al classico watermarking:
   - MD5: message digest che produce un valore hash a 128 bit.
   - SHA-1: progettato dalla United States National Security Agency ed è uno U.S. Federal Information Processing Standard pubblicato dal NIST degli Stati Uniti. SHA-1 produce un valore hash a 160 bit.
   - SHA-256: l'algoritmo SHA-256 genera un hash quasi univoco, di dimensioni fise di 256 bit (32 byte).



Avviso!
l'hash è una funzione unidirezionale: non è possibile la decodifica.

Quando si utilizza l'autenticazione video, l'hash avviene per ogni pacchetto di flusso video. Questi hash sono incorporati nel flusso di video e codificati a propria volta insieme ai dati video. Ciò garantisce l'integrità del contenuto del flusso.

Gli vengono firmati a intervalli regolari, definiti dall'intervallo di firma, utilizzando la chiave privata del certificato memorizzato nel TPM del dispositivo. Le registrazioni allarme le modifiche ai blocchi nelle registrazioni iSCSI si chiudono sempre con una firma che garantisce l'autenticità continua del video.

Avviso!
Il calcolo della firma digitale richiede una potenza di elaborazione che potrebbe influenzare le prestazioni generali di una telecamera, se effettuato troppo spesso. Pertanto è opportuno selezionare un intervallo ragionevole.

Poiché hash e firme digitali sono incorporate nel flusso video, essi vengono inoltre memorizzati nella registrazione, consentendo l'autenticazione video anche riproduzione ed esportazione.

6 Gestione dell'aggiornamento della sicurezza

Prima di utilizzare il dispositivo per la prima volta, accertarsi di installare la versione più recente del software in uso. Per garantire funzionamento, compatibilità, prestazioni e sicurezza costanti, aggiornare regolarmente il software per tutta la durata operativa del dispositivo. Attenersi alle istruzioni fornite nella documentazione del prodotto relative agli aggiornamenti del software.
Ulteriori informazioni sono disponibili tramite i collegamenti seguenti:

- Informazioni generali: https://www.boschsecurity.com/xc/en/support/product-security/
- Avvertenze per la sicurezza, un elenco di vulnerabilità individuate e soluzioni proposte: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch declina ogni responsabilità per danni provocati dall'utilizzo dei prodotti con componenti software obsoleti.

Le versioni più recenti del firmware e del software sono disponibili nel download store Bosch Security and Safety Systems:
https://downloadstore.boschsecurity.com/
Per i dispositivi connessi a Remote Portal, gli utenti possono ricevere una notifica via e-mail sugli aggiornamenti firmware disponibili tramite il servizio Remote Alert.
Pacchetti di download più completi sono distribuiti tramite il catalogo dei prodotti Bosch Security and Safety Systems:
https://www.boschsecurity.com

7 Monitoraggio della sicurezza

Poiché i requisiti cambiano continuamente, la sicurezza non è mai garantita al 100%. Pertanto, presso Bosch viene istituito un processo strutturato di gestione degli incidenti e delle vulnerabilità che consente di gestire in modo professionale i potenziali incidenti e vulnerabilità di sicurezza dei prodotti.

La gestione sistematica professionale delle vulnerabilità di sicurezza segnalate e la trasparenza nei confronti dei nostri clienti sono aspetti di fondamentale importanza per noi. Per questo motivo analizziamo in modo approfondito tutte le segnalazioni di vulnerabilità. Viene eseguita una valutazione delle vulnerabilità di sicurezza dei prodotti in base al Common Vulnerability Scoring System (CVSS). CVSS è uno standard di settore aperto e libero per la valutazione della gravità delle vulnerabilità di sicurezza dei sistemi. I punteggi sono calcolati in base a una formula che dipende da diverse metriche che indicano approssimativamente il grado di facilità di violazione e l'impatto di violazione. I punteggi vanno da 0 a 10, che indica la gravità maggiore.

In caso di vulnerabilità confermata, informiamo i clienti dell'individuazione di una vulnerabilità di sicurezza nel prodotto o nella soluzione e del relativo rimedio mediante la pubblicazione di un avviso di sicurezza. Tutti gli avvisi di sicurezza contengono:
- Descrizione della vulnerabilità con riferimento CVE (Common Vulnerabilities and Exposures) e punteggio CVSS.
- Identificativo dei prodotti e delle versioni software/hardware interessati noti.
- Informazioni su fattori di riduzione dei danni e soluzioni alternative.
- Tempistiche e posizione delle correzioni disponibili o di altre misure correttive.

L'elenco degli avvisi di sicurezza pubblicati sono disponibili sul nostro sito Web all'indirizzo https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html. Qualora si ritenga di aver identificato una vulnerabilità o qualsiasi altro problema di sicurezza correlato a un prodotto o servizio Bosch, contattare il Bosch Product Security Incident Response Team (PSIRT): https://psirt.bosch.com.

8 Smaltimento e rimozione delle autorizzazioni sicuri

In un determinato momento del ciclo di vita di un prodotto o sistema, potrebbe essere necessario sostituire o rimuovere un dispositivo o un componente. Poiché il dispositivo o il componente può contenere dati sensibili, ad esempio credenziali o certificati, assicurarsi di eliminare questi dati in modo completo e sicuro.

Per la maggior parte dei dispositivi, è possibile ripristinare i valori predefiniti di fabbrica.
A tale scopo, per la maggior parte degli encoder e delle telecamere IP, è possibile utilizzare il pulsante di ripristino. Prima di scollegare dalla rete i dispositivi che non dispongono di un pulsante di ripristino, utilizzare la funzione di ripristino dei valori predefiniti di fabbrica tramite l'interfaccia Web.
Tutti i nomi utente e le rispettive password verranno eliminati e verranno ripristinate le impostazioni predefinite di fabbrica. Vengono eliminati anche tutti i certificati e le rispettive chiavi memorizzate nel TPM o nel Secure Element.

Per ripristinare i valori predefiniti di fabbrica di altri dispositivi, potrebbero essere disponibili opzioni diverse. Per le procedure di smaltimento corrette, consultare le istruzioni riportate nella rispettiva documentazione per l'utente.
Anche in server e workstation potrebbero essere memorizzati certificati e credenziali.
Utilizzare gli strumenti e i metodi adeguati per assicurarsi che i dati pertinenti siano eliminati in modo sicuro durante la rimozione delle autorizzazioni o prima dello smaltimento.

Si consiglia di ripristinare i dispositivi ai valori predefiniti di fabbrica anche nel caso in cui debbano essere spostati in un'altra installazione in cui vengono utilizzati altri certificati o credenziali.

Avviso!
Per le procedure di smaltimento corrette, consultare le istruzioni riportate nella rispettiva documentazione per l'utente.

9 Informazioni aggiuntive

Per ulteriori informazioni, download del software e documentazione, consultare la rispettiva pagina del prodotto nel catalogo dei prodotti:
http://www.boschsecurity.com

Glossario

802.1x

Lo standard IEEE 802.1x fornisce un metodo generale per l'autenticazione e l'autorizzazione su reti IEEE-802. L'autenticazione viene eseguita tramite un autenticatore, che controlla le informazioni di autenticazione trasmesse mediante un server apposito (vedere server RADIUS) ed approva o rifiuta di conseguenza l'accesso ai servizi offerti (LAN, VLAN o WLAN).

autenticazione

Processo di verifica dell'autenticità di un flusso video. Il processo di autenticazione può essere avviato dell'utente. Se vengono rilevati dati non autentici, viene visualizzato un messaggio.

DHCP

Acronimo di Dynamic Host Configuration Protocol: utilizza un apposito server per abilitare l'assegnazione dinamica di un indirizzo IP ed altri parametri di configurazione sui computer in una rete (Internet o LAN)

dispositivo

Componente hardware, ad esempio telecamera, encoder/decoder, NVR, DiBos, matrice analogica, bridge ATM/POS.

Gruppo utenti

Utilizzato per definire attributi utente comuni, ad esempio autorizzazioni, privilegi e priorità PTZ. Diventando membro di un gruppo, un utente eredita automaticamente tutti gli attributi del gruppo.

HTTP

Acronimo di Hypertext Transfer Protocol: protocollo per la trasmissione di dati su una rete

HTTPS

Acronimo di Hypertext Transfer Protocol Secure: codifica ed autentica le comunicazioni tra server Web e browser

Indirizzo IPv4

Numero a 4 byte che definisce in modo univoco ciascuna unità su Internet. Viene normalmente scritto in notazione decimale con punti di separazione, ad esempio "209.130.2.193"

LAN

Acronimo di Local Area Network. È una rete che collega dispositivi in un'area geografica limitata.

Maschera di rete

Maschera che indica la porzione di un indirizzo IP che rappresenta l'indirizzo di rete e la porzione che identifica l'indirizzo dell'host. Viene normalmente scritta in notazione decimale con punti di separazione, ad esempio "255.255.255.192".

Multicast

Comunicazione tra un unico ricetrasmettitore e più destinatari su una rete tramite la distribuzione di un unico flusso di dati sulla rete a diversi destinatari all'interno di un gruppo definito. Per il funzionamento di questo tipo di comunicazione è necessaria una rete conforme a multicast con l'implementazione dei protocolli UDP ed IGMP.

ONVIF

Acronimo di Open Network Video Interface Forum. Standard globale per prodotti video di rete. I dispositivi conformi ONVIF sono in grado di scambiare video in diretta, audio, metadati ed informazioni di controllo, garantendo rilevamento e connessione automatica alle applicazioni di rete, ad esempio ai sistemi di gestione video.

protezione avanzata

Processo di aumento della sicurezza di un sistema utilizzando solo software dedicati necessari per il funzionamento dei sistemi, applicando specifiche impostazioni di protezione e rimuovendo software non obbligatori.

RCP+

Remote Control Protocol: protocollo proprietario di Bosch che utilizza porte statiche specifiche per il rilevamento e la comunicazione con i dispositivi video IP Bosch

RTSP

Acronimo di Real Time Streaming Protocol. Protocollo di rete che consente di controllare la trasmissione continua di dati audio/video o software su reti IP.

Server RADIUS

Acronimo di Remote Authentication Dial-In User Service. Protocollo client-server per l'autenticazione, l'autorizzazione e la gestione degli account degli utenti con connessione remota per le reti di computer. RADIUS è lo standard di fatto per l'autenticazione centralizzata delle connessioni remote tramite modem, ISDN, VPN, LAN Wireless (vedere 802.1x) e DSL.

SNMP

Acronimo di Simple Network Management Protocol: un protocollo per la gestione della rete e per la gestione ed il monitoraggio dei componenti di rete

SSL

Acronimo di Secure Sockets Layer; un protocollo di crittografia obsoleto per la trasmissione dei dati nelle reti basate su IP (vedere TLS).

TCP

Transmission Control Protocol. Protocollo di comunicazione orientato alla connessione, utilizzato per trasmettere dati in una rete IP. Offre una trasmissione dati affidabile ed ordinata.

Telnet

Protocollo di accesso che consente agli utenti di accedere ad un computer remoto (host) su Internet

TLS

Transport Layer Security. TLS 1.0 e 1.1 sono sviluppi avanzati dello standard SSL 3.0 (vedere SSL). I dispositivi moderni utilizzano TLS 1.2 o 1.3

TTL

Acronimo di Time-To-Live, ciclo di vita di un pacchetto dati nei trasferimenti tra postazioni

UDP

Acronimo di User Datagram Protocol. Protocollo privo di connessione utilizzato per scambiare dati in una rete IP. UDP è più efficiente del protocollo TCP nella trasmissione video grazie a un minore sovraccarico.

VPN

Una VPN (Virtual Private Network) implementa una rete privata all'interno di una rete pubblica, ad esempio Internet. Il traffico di rete nella VPN è crittografato, quindi protetto da rischi di spionaggio.

Wide Area Network (WAN)

Collegamento a lunga distanza utilizzato per la connessione di reti locali distanti tra loro

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

Building solutions for a better life.

202302092000