IQSIGHT

CYBERSECURITY GUIDEBOOK

FOR IP VIDEO PRODUCTS

4.0.1 2026-06

Visual intelligence for a world uninterrupted.

CONTENTS

This guidebook helps security integrators harden IQSIGHT IP video products within enterprise network environments. Part I covers vendor-agnostic cybersecurity principles. Parts II and III provide product-specific guidance for IQSIGHT cameras, servers, storage, and client workstations.

PART I: GENERAL CYBERSECURITY

Part I establishes the foundational cybersecurity concepts that apply to any IP video deployment, regardless of vendor.

CHAPTER 1 — THREAT LANDSCAPE

Understanding the threats facing IP video systems is the starting point for any security strategy. This chapter outlines why video systems attract attackers, the most common attack methods, and how the risk profile continues to evolve.

1.1 Why IP Video Systems Are Targets

IP video systems are high-value targets for several reasons:

- **Sensitive data** — Video footage can contain personally identifiable information, proprietary business activities, and security-relevant intelligence. Unauthorized access to live or recorded video can violate privacy regulations and expose organizations to legal liability.
- **Network foothold** — Cameras and encoders are network-connected devices that, if compromised, can serve as entry points for lateral movement into the broader enterprise network.
- **Operational disruption** — Disabling or manipulating a video surveillance system can facilitate physical security breaches, sabotage, or theft.
- **Botnet recruitment** — Inadequately secured IoT devices, including IP cameras, have historically been recruited into large-scale botnets for distributed denial-of-service (DDoS) attacks.

1.2 Common Attack Vectors

The most common attack vectors targeting IP video systems include:

- **Default or weak credentials** — Devices shipped with factory-default passwords that are never changed remain the single most exploited vulnerability.
- **Unencrypted communication** — Protocols like HTTP, RTSP, or SNMPv1 transmit data in clear text, allowing attackers to intercept credentials, configuration data, or video streams.
- **Firmware exploitation** — Unpatched firmware may contain known vulnerabilities that attackers can exploit remotely.

CHAPTER 2 — SECURITY FRAMEWORKS AND STANDARDS

Security frameworks provide structured approaches to managing cybersecurity risk across an organization. This chapter introduces the frameworks and certifications most relevant to IP video deployments, guided by current and emerging European cybersecurity regulations — particularly **NIS2**, the **Critical Entities Resilience (CER) Directive**, and the **Cyber Resilience Act (CRA)**.

These regulations establish outcome-based requirements rather than prescriptive technical controls and do not provide dedicated certification schemes or formal compliance labels. A common misconception is that organizations or products can be certified as "NIS2-compliant" or "NIS2-ready." In practice, NIS2 does not define a formal certification framework or compliance designation. Instead, organizations rely on recognized cybersecurity standards, frameworks, and independent third-party certifications to demonstrate due diligence, implement structured security measures, and support alignment with regulatory expectations.

2.1 NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework organizes security activities into five core functions:

1. **Identify** — Understand your assets, business environment, and risk tolerance. For IP video, this means maintaining an inventory of all cameras, encoders, servers, and network infrastructure.
2. **Protect** — Implement safeguards to ensure delivery of critical services. This includes access control, encryption, and device hardening (covered in Parts II and III of this guide).
3. **Detect** — Develop capabilities to identify security events. Log monitoring and SIEM integration (see Chapter 8) enable early detection.
4. **Respond** — Define processes to contain and mitigate the impact of detected incidents.
5. **Recover** — Plan for restoring capabilities after a security event, including backup and disaster recovery procedures.

Appendix B provides a mapping of this guidebook's recommendations to NIST CSF controls.

2.2 IEC 62443 — Industrial Automation Security

IEC 62443 is an international series of standards addressing cybersecurity for industrial automation and control systems (IACS). Physical security systems, including IP video surveillance, fall within its scope.

Key concepts from IEC 62443 relevant to IP video deployments:

- **Zones and conduits** — Grouping assets with similar security requirements into zones, connected by controlled conduits. This aligns with network segmentation practices (see Chapter 4).
- **Security levels** — Defining target security levels (SL 1–4) based on the threat environment, from protection against casual violation to state-sponsored attacks.
- **Product supplier requirements** — IEC 62443-4-1 defines secure development lifecycle requirements for product vendors; IEC 62443-4-2 defines component-level security requirements.

IQSIGHT has achieved certification against both standards: the product development process is certified to **IEC 62443-4-1** (secure development lifecycle), and IQSIGHT IP cameras are certified to **IEC 62443-4-2** (component-level security requirements). These certifications, issued by an accredited third-party body, confirm that security is embedded in both how the products are built and what they deliver.

2.3 CIS Benchmarks

The Center for Internet Security (CIS) publishes consensus-based security configuration guidelines, known as **CIS Benchmarks**, for hardening operating systems, applications, and network devices.

For IP video deployments, the most relevant benchmarks are:

- **CIS Microsoft Windows Server Benchmark** — Applied to BVMS and VRM servers (see Chapter 16).
- **CIS Microsoft Windows Desktop Benchmark** — Applied to operator and configuration client workstations (see Chapter 18).

CIS Benchmarks define two implementation levels: - **Level 1** — Practical settings that can be applied broadly without significant impact on functionality. - **Level 2** — Settings intended for high-security environments that may limit some functionality.

2.4 UL 2900 — Product Cybersecurity Certification

UL 2900 is a family of cybersecurity standards and certification programs designed for network-connectable products. It addresses software security, vulnerability management, and resilience against common cyber threats throughout the product lifecycle. Connected physical security technologies, including IP video systems, fall within its scope.

Key aspects of UL 2900 relevant to IP video and connected security products:

- **Secure software development** — Verification that secure coding practices, security testing, and vulnerability mitigation are embedded throughout the product development lifecycle.
- **Known vulnerability management** — Assessment of products against publicly disclosed software vulnerabilities, with requirements for timely identification, remediation, and risk management.
- **Product-level assurance** — Independent evaluation and testing of the delivered product, providing assurance beyond process-based controls alone.

IQSIGHT has achieved UL 2900 certification for selected products. Accredited third-party certification bodies issue these certifications, providing formal, auditable confirmation that the certified products meet recognized cybersecurity requirements at the product level. UL 2900 certifications complement IEC 62443-aligned development processes by independently validating the cybersecurity characteristics of delivered products.

2.5 Choosing the Right Framework

The choice of framework depends on your regulatory environment, industry sector, and deployment scale:

- **NIST CSF** is widely adopted and provides a flexible, risk-based approach suitable for most organizations.
- **IEC 62443** is particularly relevant for organizations operating in regulated industrial environments or those requiring formal security level certification.
- **CIS Benchmarks** provide actionable, technical hardening guidance and complement both NIST CSF and IEC 62443 at the implementation level.
- **UL 2900** provides independent, product-level cybersecurity certification for network-connectable devices — particularly relevant when procurement or regulatory due diligence requires auditable evidence of product security.

These frameworks are not mutually exclusive. Many organizations use NIST CSF or IEC 62443 for strategic risk management, CIS Benchmarks for tactical system hardening, and UL 2900 certifications as independent validation of product-level security.

2.6 Conclusion

NIS2, the CER Directive, and the Cyber Resilience Act approach cybersecurity and resilience from different regulatory perspectives, yet they share a common objective: ensuring that security and resilience are systematic, measurable, and demonstrable in practice. Rather than introducing standalone compliance schemes, these regulations rely on recognized standards, established processes, and independent assurance mechanisms.

Within this context, IQSIGHT's certified development processes and product certifications provide tangible alignment with regulatory intent. IEC 62443-4-1 demonstrates that cybersecurity is embedded throughout the product development lifecycle, supporting NIS2 expectations for secure development practices and the CRA principles of cybersecurity by design and by default. IEC 62443-4-2 and UL 2900 certifications extend this assurance to the products themselves, providing independently verified evidence of software robustness, vulnerability management, and operational resilience — key considerations for both NIS2 assurance expectations and CER resilience objectives.

These certifications do not constitute regulatory compliance in themselves, nor do they support formal claims of "NIS2 compliance" or "CRA compliance." Instead, they provide a coherent and auditable foundation that demonstrates how IQSIGHT translates regulatory expectations into established engineering practices, validated development processes, and resilient products. The regulations define the desired outcomes; the certifications provide practical and independently verified evidence of alignment with those outcomes.

CHAPTER 3 — ZERO TRUST ARCHITECTURE

Traditional perimeter-based security assumes that devices inside the network can be trusted. Zero Trust eliminates this assumption — every access request must be verified, regardless of network location.

3.1 Zero Trust Principles

Zero Trust is built on three core principles:

1. **Never trust, always verify** — Every device, user, and network flow must be authenticated and authorized before access is granted. A camera on the internal VLAN does not get implicit trust simply because it is "inside" the network.
2. **Least privilege** — Grant only the minimum access required for a device or user to perform its function. A camera needs to send video to the recording server — it does not need access to the corporate file share.
3. **Assume breach** — Design systems as if an attacker is already present in the network. Limit blast radius through segmentation, monitor continuously, and ensure that a single compromised device cannot lead to system-wide compromise.

3.2 Zero Trust Applied to IP Video

Applying Zero Trust to IP video deployments involves several practical measures:

- **Device identity** — Use unique device certificates (see Chapter 6) to authenticate every camera and encoder. IQSIGHT cameras ship with a unique device certificate derived from the IQSIGHT Root Certificate, enabling cryptographic device authentication.
- **Microsegmentation** — Place cameras, recording servers, and management clients in separate network segments with explicit access rules between them (see Chapter 4). A compromised camera should not be able to reach the management server directly.
- **Encrypted communication** — Enforce secure protocols for all management and video traffic. Unencrypted protocols (HTTP, RCP+, RTSP) are already disabled in favor of their encrypted equivalents (HTTPS, RTSPS). For device-level protocol configuration, see Chapter 12.
- **Continuous verification** — Monitor device behavior through syslog and SIEM integration (see Chapter 8). Use software sealing to detect unauthorized configuration changes.
- **Network access control** — Implement 802.1x to authenticate devices before granting network access (see Chapter 4).

3.3 Implementation Roadmap

Transitioning from a traditional perimeter model to Zero Trust is a phased process:

1. **Inventory and classify** — Identify all devices, users, and data flows in the video system. Map which devices communicate with which services.
2. **Segment and isolate** — Implement VLANs and firewall rules to separate video infrastructure from the corporate network. Disable unused switch ports.
3. **Authenticate everything** — Deploy device certificates, enable 802.1x, and enforce password policies across all devices and user accounts.
4. **Encrypt all traffic** — Switch all communication to encrypted protocols. Disable legacy unencrypted options.
5. **Monitor and respond** — Deploy centralized logging and SIEM integration. Establish incident response procedures.
6. **Iterate and harden** — Continuously refine access policies, review logs, apply firmware updates, and adjust segmentation as the deployment evolves.

CHAPTER 4 — NETWORK SECURITY

Network architecture is a critical layer of defense. Proper segmentation and access control reduce the blast radius of any compromise.

4.1 Network Segmentation

IP video devices should be operated in a separate network with access restrictions to limit broadcast traffic and protect the devices from network attacks. Without segmentation, the video system is exposed to threats from every other device on the network — including internal ones. A compromised or misconfigured host on the same flat network can intercept video traffic, access camera management

interfaces, or leak footage to the Internet. These risks apply to privacy, regulatory compliance, and physical security alike.

Two technologies are commonly used to create a segmented network:

- **VLANs** — A Virtual LAN subdivides a physical LAN into isolated segments through switch or router configuration, without rewiring device connections. VLANs operate at the data link layer (OSI layer 2) and complement IP subnetting at the network layer (OSI layer 3). Quality-of-service schemes applied to a video VLAN can improve both security and streaming performance.
- **VPNs** — A Virtual Private Network creates a separated (private) network that can extend across public networks or the Internet. VPNs add encryption and isolation for video traffic, and are particularly useful for connecting remote sites over WAN links.

The choice between VLANs, VPNs, or a combination of both depends on the existing network infrastructure, the deployed equipment, and the required topology.

4.2 Network Access Control with 802.1x

802.1x is an IEEE standard for port-based network access control (NAC). It ensures that only authenticated devices can communicate on the network by requiring each device (the supplicant) to present credentials to an authentication server (typically RADIUS) before the network switch grants access.

In an IP video deployment, 802.1x prevents unauthorized devices from joining the camera network — even if an attacker gains physical access to a switch port or network socket.

802.1x supports multiple authentication methods through the Extensible Authentication Protocol (EAP). The most secure option is **EAP-TLS**, which provides mutual certificate-based authentication between the device and the authentication server. With EAP-TLS, both endpoints exchange certificates, ensuring encrypted communication and eliminating the risk of credential interception.

For device-specific 802.1x configuration on IQSIGHT cameras, see the 802.1x entry in Chapter 12 — Camera Hardening.

> **NOTICE**
>
> Refer to the Technical White Paper *Network Authentication — 802.1x — Secure the Edge of the Network*, available on the IQSIGHT Security Systems online product catalog.

4.3 Multicast Security Considerations

Where unicast video transmissions are destination based, multicast is source based and this can introduce security issues at the network level, including: group access control, group center trust, and router trust. While router configuration is beyond the scope of this guide, awareness of these risks is important when designing network architecture for IP video systems.

TTL (time-to-live) scoping defines where and how far multicast traffic is allowed to flow within a network, each hop decreasing TTL by one. For video surveillance data, a best practice would be to set TTL settings to 15 (restricted to same site), or use the exact maximum number of hops as the TTL value.

For device-specific multicast configuration, see Multicast Configuration in Part II.

CHAPTER 5 — IDENTITY AND AUTHENTICATION

Strong authentication is the foundation of access control. Every device, user, and service should prove its identity before gaining access.

5.1 Password Policies and Best Practices

Password protection is critical when securing data from possible cyberattacks. This applies to all network devices in your complete security infrastructure. Most organizations already have strong password policies in place, but if you are working with a new installation with no policies in place, the following are some best practices when implementing password protection:

- Passwords should be between 8 and 12 characters in length.
- Passwords should contain both upper and lower case letters.
- Passwords should contain at least one special character.
- Passwords should contain at least one digit.

Example: Using the passphrase “to be or not to be” and the basic rules for good password generation: `2be0rnOt!t0Be`

> **NOTICE**
>
> There are some restrictions for the use of special characters such as `@`, `&`, `<`, `>`, `:` in passwords due to their dedicated meaning in XML and other markup languages. While the web interface will accept those, other management and configuration software might refuse acceptance.

For device-specific password assignment, see Camera Passwords and User Management (Part II) and BVMS and Configuration Manager (Part III).

5.2 Active Directory Federation Services

Active Directory Federation Services (AD FS) is a service offered by Microsoft, allowing authentication to a local Active Directory (using an AD FS server) or to the Azure Cloud.

Besides local user authentication with either passwords or certificate-based authentication, integration of devices into an Active Directory Domain is possible with AD FS to authenticate and manage user access centrally.

CHAPTER 6 — CRYPTOGRAPHY AND PKI

Cryptography protects data in transit and at rest. A well-managed Public Key Infrastructure ensures that devices and users can trust each other’s identities.

6.1 TLS and Encrypted Communication

HTTPS (TLS) encrypts all control communication and video payload via the encryption engine in the device. When utilizing TLS, communication is encrypted with an AES encryption key up to 256 bits in length.

IP video devices do not allow unsecure SSLv3 or older connections. TLS 1.0 and 1.1 are deprecated by the IETF and there are potential security issues known (BEAST, FREAK). Modern camera platforms support the secure TLS 1.2, which should be set as minimum required version. Newer platforms also support TLS 1.3.

> **Tip:** Set the minimum TLS version to 1.2 on all devices and enable HTTP Strict Transport Security (HSTS) to prevent protocol downgrade attacks.

6.2 PKI and Certificate Management

IQSIGHT IP cameras and video storage devices ship with a unique IQSIGHT device certificate, derived from the IQSIGHT Root Certificate and installed during production. This certificate enables HTTPS out of the box and allows verification that the device is a genuine IQSIGHT product by tracing the certificate chain back to the IQSIGHT Root Certificate.

While the factory-installed IQSIGHT certificate proves device authenticity, most enterprise deployments require certificates issued by the organization's own corporate CA. Integrating devices into the corporate PKI enables consistent trust management, certificate lifecycle control, and compliance with organizational security policies.

IQSIGHT Configuration Manager includes an integrated CA function called **MicroCA**, which can create a Root CA and derive device certificates — including for multiple devices simultaneously. MicroCA is a practical option for smaller deployments or staging environments. For production environments, use a corporate CA to issue device certificates and maintain centralized control over certificate lifecycle and revocation.

> **NOTICE**
>
> Certificates should be used to authenticate a single device. It is recommended to create a specific certificate per device

IQSIGHT cameras also support the **Simple Certificate Enrollment Protocol (SCEP)**, which automates certificate requests and renewals against a SCEP-enabled CA. This simplifies certificate rollout in larger deployments. For configuration details, see Camera Certificates and Video Authentication in Part II.

For device-specific certificate upload procedures, see Camera Certificates and Video Authentication in Part II.

6.3 Hardware Key Storage

Private keys from certificates are best protected when safely stored in a hardware component, or hardware vault. Such chips provide protection against unauthorized access to private keys even when the device is physically open to gain access.

In IQSIGHT cameras, such keys are stored in a separate crypto-coprocessor or secure element (SE). Both provide secure storage as well as cryptographic functions that never expose private keys to locations or memory where it could potentially be retrieved.

CHAPTER 7 — SUPPLY CHAIN SECURITY

Securing the supply chain ensures that devices and software have not been tampered with before deployment. A compromised device introduced during procurement or installation can undermine every other security measure.

7.1 Firmware Integrity and Signing

Firmware is the operating system of an IP video device. If an attacker can install modified firmware, they gain full control of the device.

Key protections against firmware tampering:

- **Firmware signing** — The vendor digitally signs every firmware release. The device verifies the signature before accepting an update, rejecting any firmware that has been modified or that originates from an unauthorized source. IQSIGHT cameras only accept firmware signed by a valid IQSIGHT certificate. Each update file is also encrypted, providing protection against both tampering and reverse engineering.
- **Secure Boot** — Modern camera platforms (e.g., IQSIGHT CPP13, CPP14 and newer) verify the integrity of the entire boot chain, from bootloader to application firmware, starting from an unchangeable hardware root of trust. This prevents an attacker from persistently modifying the device software.
- **Firmware source verification** — Only download firmware from official vendor channels. Verify checksums or signatures before deploying updates.

7.2 Software Signing

All IQSIGHT software products — including BVMS, Configuration Manager, and Video Recording Manager — are digitally signed with an IQSIGHT code signing certificate. This signature allows the operating system to verify that the software originates from IQSIGHT and has not been modified since it was published. Before installing or updating any IQSIGHT software, verify that the digital signature is valid and issued to IQSIGHT.

7.3 Vendor Assessment

When selecting IP video products, evaluate the vendor's security practices:

- **Vulnerability disclosure** — Does the vendor operate a Product Security Incident Response Team (PSIRT)? Are security advisories published transparently with CVE references and CVSS scores?
- **Software Bill of Materials (SBOM)** — Can the vendor provide an SBOM listing all software components, enabling assessment of exposure to known vulnerabilities in third-party libraries?
- **Security certifications** — Has the product or the vendor's development process been certified against relevant standards (e.g., IEC 62443-4-1 for secure development lifecycle)?

- **Penetration testing** — Has the product been subjected to independent security testing?

7.4 Secure Procurement and Deployment

Protect the integrity of devices from procurement through initial deployment:

- **Authorized channels** — Purchase devices only from authorized distributors to reduce the risk of counterfeit or tampered hardware.
- **Chain of custody** — Document the handling of devices from receipt to installation. Inspect packaging for signs of tampering.
- **Initial provisioning** — Change all default passwords, disable unnecessary services, and upload certificates before connecting a device to the production network. Never deploy a device with factory-default credentials.

CHAPTER 8 — MONITORING AND INCIDENT RESPONSE

Continuous monitoring detects threats early. A defined incident response process ensures swift and effective action when a security event occurs.

8.1 Log Management

Monitoring the log files is an important part of security analysis or maintenance activity. Regular review of the log files can reveal configuration problems or security violations like false logins.

To analyze log files and store them for long term it is advised to send the log files of the device to a syslog server or a SIEM system as for example a camera will reserve a fixed space for logging internally but will overwrite older logs if that space is filled. IQSIGHT cameras reserve approximately 4096 KB for internal log storage — enough for about 14.000 messages before older entries are overwritten.

The camera supports three syslog transport protocols: UDP (fast, unreliable), TCP (reliable, retransmits lost packets), and TLS (encrypted and reliable). Use TLS when the network is not fully trusted.

> **Tip:** For step-by-step syslog configuration, server setup, TLS certificate generation, and log message format details, see the Log Monitoring and Time Synchronization Guide.

8.2 SIEM Integration

Security Information and Event Management (SIEM) system is used to collect and analyze information from different devices and systems. The devices can be integrated with a SIEM system by sending the logs via syslog protocol. Analyzing these logs can help to do the maintenance and to detect configuration errors or attacks on the device (for example false logins).

8.3 Vulnerability Management and CVSS

Because requirements are constantly changing, 100% security is never guaranteed. Therefore, a structured vulnerability and incident management process is established at IQSIGHT to professionally manage potential product security vulnerabilities and incidents.

The professional systematic handling of reported security vulnerabilities as well as transparency towards customers is very important. That is why all vulnerability reports are investigated. Product security vulnerabilities are evaluated according to the Common Vulnerability Scoring System (CVSS). CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe.

In case of confirmed vulnerability, customers are informed about an identified security vulnerability in product or solution and its remediation by publishing of security advisory. All security advisories contain:

- Description of the vulnerability with Common Vulnerabilities and Exposures (CVE) reference and CVSS score.
- Identity of known affected products and software/hardware versions.
- Information on mitigating factors and workarounds.
- Location of available fixes.

Published Security Advisories and means to report a vulnerability or any other security issue related to a IQSIGHT product or service can be found at: https://www.iqsight.com/en/support/product-security/

8.4 Incident Response Process

A defined incident response process ensures that security events are handled quickly and consistently. The following lifecycle, based on NIST SP 800-61, provides a structured approach:

1. **Prepare** — Establish an incident response team with clear roles and contact information. Document escalation procedures, maintain an up-to-date asset inventory of all IP video components, and ensure that logging and monitoring are operational.
2. **Detect and analyze** — Use SIEM alerts, syslog data, and software sealing notifications to identify potential incidents. Determine the scope — which devices are affected, what type of event occurred, and whether video data or credentials may have been compromised.
3. **Contain** — Isolate affected devices to prevent lateral movement. For a compromised camera, disable its network port or move it to a quarantine VLAN. Preserve logs and forensic evidence before making changes to the device.
4. **Eradicate** — Remove the root cause. This may involve performing a factory reset, updating firmware to patch a vulnerability, revoking and replacing compromised certificates, or changing passwords across affected devices.
5. **Recover** — Restore the device to operational status. Re-provision credentials and certificates, verify firmware integrity, re-enable network access, and confirm that video recording and monitoring have resumed.
6. **Lessons learned** — Document what happened, how it was detected, how long containment took, and what could be improved. Update response procedures, hardening configurations, and monitoring rules based on the findings.

> **Tip:** Test your incident response process at least once a year with a tabletop exercise that includes a scenario specific to the video surveillance system — for example, a compromised camera or unauthorized access to recorded video.

CHAPTER 9 — LIFECYCLE MANAGEMENT

Security is not a one-time activity. Every device must be maintained through its operational life and securely decommissioned at end of life.

9.1 Security Update Management

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

IQSIGHT assumes no liability whatsoever for any damage caused by operating its products with outdated software components.

You can find the latest firmware and software versions in the IQSIGHT download store: https://downloadstore.keenfinity-group.com/

For devices connected to Remote Portal, users can receive an email notification about available firmware updates through the Remote Alert service.

Checking for Updates from the Camera
IQSIGHT cameras can check for available updates directly from the web interface:

1. Navigate to **Service** → **Maintenance**.
2. If a new update is available, it can be downloaded directly to the camera.

> **NOTICE**
>
> The camera must be able to reach `downloadstore.keenfinity-group.com` to check for updates. This may not be possible in isolated camera networks.

Installing Firmware Updates
Firmware updates can be installed through two methods:

- **Web interface** — Upload the firmware file in **Service** → **Maintenance**.
- **Configuration Manager** — Select one or more cameras, then use **File Upload** → **Firmware** to deploy updates to multiple devices simultaneously.

> **NOTICE**
>
> Each camera belongs to a specific platform (e.g., CPP7.3, CPP13, CPP14), which requires a platform-specific firmware file. The platform is shown in the camera web interface under **Service** → **System Overview**.

9.2 Configuration Backup

Maintaining configuration backups protects against accidental misconfiguration, simplifies device replacement, and enables rapid recovery after security incidents. Back up each device's configuration after initial deployment and after any significant configuration change.

IQSIGHT cameras support encrypted configuration export via the web interface and via Configuration Manager for multi-device operations. For detailed backup and restore procedures, see Configuration Backup and Restore in Part II.

9.3 Secure Disposal and Decommissioning

At a certain point in the life cycle of a product or a system, it might be necessary to replace or to take out of order a device or a component. As the device or the component may hold sensitive data, like credentials or certificates, make sure to delete these data completely and securely.

You can set the most devices to factory default.

For the most IP cameras and encoders, you can use for this the reset button. For the ones that do not have a reset button, use the factory default function via the web interface before dismounting them from the network.

All users and their respective passwords will be deleted and the settings will be set back to the factory default settings. All certificates and the respective keys that were stored in the TPM or secure element will also be deleted.

Other devices may have different options to set them to factory default. Refer to the instructions in the respective user documentation for correct disposal procedures.

Servers and workstations may also have certificates and credentials stored. Use the proper tools and methods to make sure that your relevant data is securely deleted during decommissioning or before disposal.

It is recommended to set devices to factory default also in case that they must be moved into another installation that may use other credentials or certificates.

PART II: IQSIGHT IP CAMERAS

Part II covers the security architecture, configuration, and hardening of IQSIGHT IP cameras.

CHAPTER 10 — CAMERA ARCHITECTURE AND SECURITY CONCEPTS

IQSIGHT IP cameras incorporate multiple layers of security, from hardware-level protections to application-layer controls.

10.1 Security by Design

IQSIGHT develops IP video products following a secure development lifecycle certified to **IEC 62443-4-1**. This means security is not an afterthought — it is integrated into every phase of product development:

- **Threat modeling** — Each product undergoes systematic threat modeling to identify potential attack vectors and abuse scenarios before development begins.
- **Risk analysis** — Identified threats are assessed for likelihood and impact, and mitigation measures are defined as part of the product security concept.
- **Security concept** — Every product has a documented security concept that defines its security objectives, trust boundaries, and the controls required to meet its target security level.
- **Secure implementation** — Development follows secure coding guidelines and includes automated and manual code reviews to eliminate common vulnerability classes.
- **Security testing** — IQSIGHT IP video devices are subjected to regular security testing and independent penetration testing by external security vendors throughout the product lifecycle — not just at initial release.

IQSIGHT cameras are manufactured in a controlled and audited production environment. Each device receives a unique IQSIGHT device certificate and cryptographic keys during production, stored in an onboard secure element that protects them against physical extraction.

10.2 Secure by Default

IQSIGHT IP cameras ship with a security-first default configuration that minimizes the attack surface out of the box:

- **No default password** — The camera refuses all access until the integrator sets an initial service password, preventing deployment with known credentials.
- **HTTPS enabled, HTTP disabled** — All management communication uses TLS encryption by default. Unencrypted HTTP and RCP+ are disabled.
- **Unneeded services off** — Services such as SNMPv1, iSCSI, UPnP, and GBT/28181 are disabled by default and only activated when explicitly needed.
- **TLS 1.2 minimum** — The camera rejects connections using deprecated TLS versions.

This approach follows the principle that a device should be secure from the moment it connects to the network, without requiring the integrator to disable insecure features first. For further hardening beyond the defaults, see Chapter 12 — Camera Hardening.

10.3 Defense in Depth

Defense in depth refers to a layered security approach, where no single measure alone is responsible for the security of a product, but there are multiple layers that an attacker needs to breach to exploit a product. At each release of a product, it is evaluated if new features are needed to mitigate new attacks or to increase overall security of the product.

Here is an overview of the main security functions of the IP camera:

Firmware signing — Each firmware update file is encrypted and signed by a IQSIGHT certificate. Only updates published by IQSIGHT can be installed on the cameras, avoiding installation of malicious firmware.

Secure Boot — Cameras of platforms CPP13, CPP14 or newer, feature a Secure Boot mechanism. Secure Boot checks the integrity of the whole system, starting with the bootloader and continuing with the firmware itself on the cameras, each step of the boot process is verifying the next, starting with an unchangeable hardware root of trust. This prevents an attacker from modifying bootloader or firmware on the device.

Login Firewall — To protect against password brute forcing but at the same time allowing administrators to login and to protect against Denial of Service (DoS) attacks, the login firewall checks login attempts based on behavioral analysis and dynamically blocks or allows access based on IP addresses.

Camera authentication — To uniquely identify and authenticate a camera, a IQSIGHT device certificate is created on each camera during production. This certificate can be used to check whether communicating with a genuine IQSIGHT device. In addition, custom certificates can be uploaded or created on the camera to provide integration with a PKI environment to protect against man-in-the-middle attacks.

CHAPTER 11 — CAMERA PASSWORDS AND USER MANAGEMENT

Access control starts with strong credentials and clear role separation. IQSIGHT IP cameras give integrators three authentication methods, three built-in access groups, and tools to assign and rotate credentials at scale. This chapter walks through the options and the steps required to secure access from first boot.

11.1 Authentication and Access Basics

11.1.1 Authentication Methods

IQSIGHT IP cameras support three authentication methods. Choose the option that matches your environment and your key management capabilities:

- **Local users with password authentication** — Each user holds credentials stored on the camera.
- **Local users with certificate-based authentication** — Each user presents a client certificate instead of a password. Certificates can live on a smartcard or hardware token for stronger protection.
- **Remote ADFS authentication** — The camera delegates authentication to Active Directory Federation Services (ADFS), centralizing identity in your existing directory.

11.1.2 Access Rights Groups

Every user belongs to one of three access rights groups. The groups reflect least-privilege best practice for video devices:

- **live** — View live video streams only.
- **user** — View live and recorded video and operate camera controls such as PTZ. Configuration settings remain hidden.
- **service** — Full administrator access to every menu, plus live video and PTZ control.

11.1.3 Built-in Accounts

Every IQSIGHT IP camera ships with three built-in accounts that share the names of the access groups. You cannot delete these accounts or change their group membership — they provide a predictable baseline for initial provisioning and recovery.

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

Figure 1: Built-in accounts: service, user, and live

Figure 11-1. The three built-in accounts shown in the camera's User Management table.

11.1.4 Password Policy

When you use password authentication, every password must meet all of the following requirements:

- At least 8 characters
- At least 1 number
- At least 1 special character
- Upper and lower case letters
- Different from the username

> **Tip:** The policy sets a floor, not a ceiling. Pair it with a password manager and use 16+ character random passwords for any account in the **service** group.

11.1.5 Login Timeout

Auto-logout closes the window for an unattended browser session to be hijacked. Open **Web Interface → 'Live' functions** and set **Auto logout time [min]** to the idle duration you want. The web session ends automatically once that time expires. A value of `0` disables automatic logout.

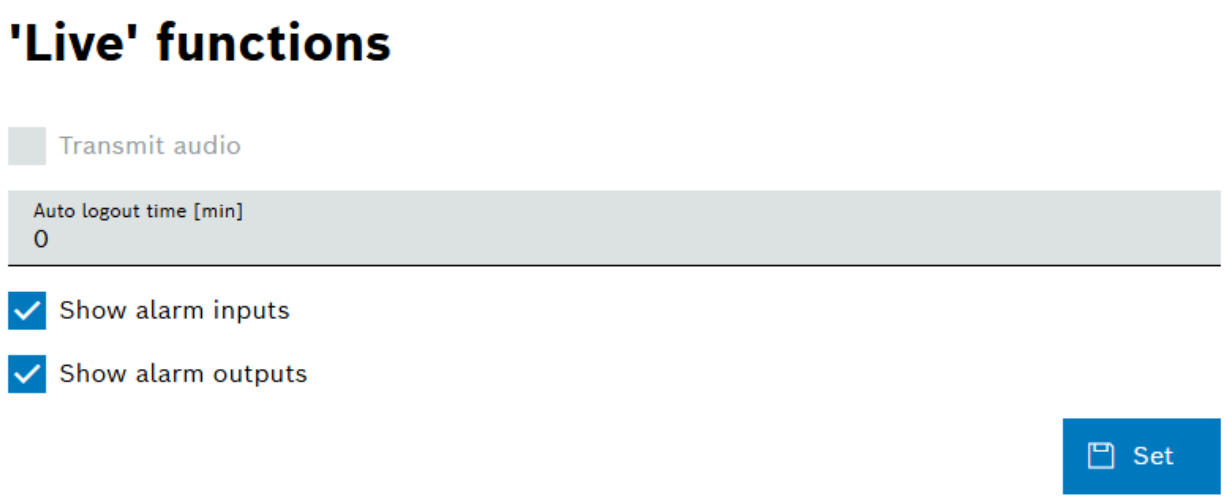

Figure 2: Auto logout time configuration in 'Live' functions

Figure 11-2. Configure the web interface auto-logout interval under 'Live' functions.

11.1.6 Login Notification

Login notifications make concurrent access visible. Enable them under **Web Interface → Appearance**. When another user — or the same account from a different location — signs in, a banner alerts anyone already logged in, so your team can spot unexpected sessions immediately.

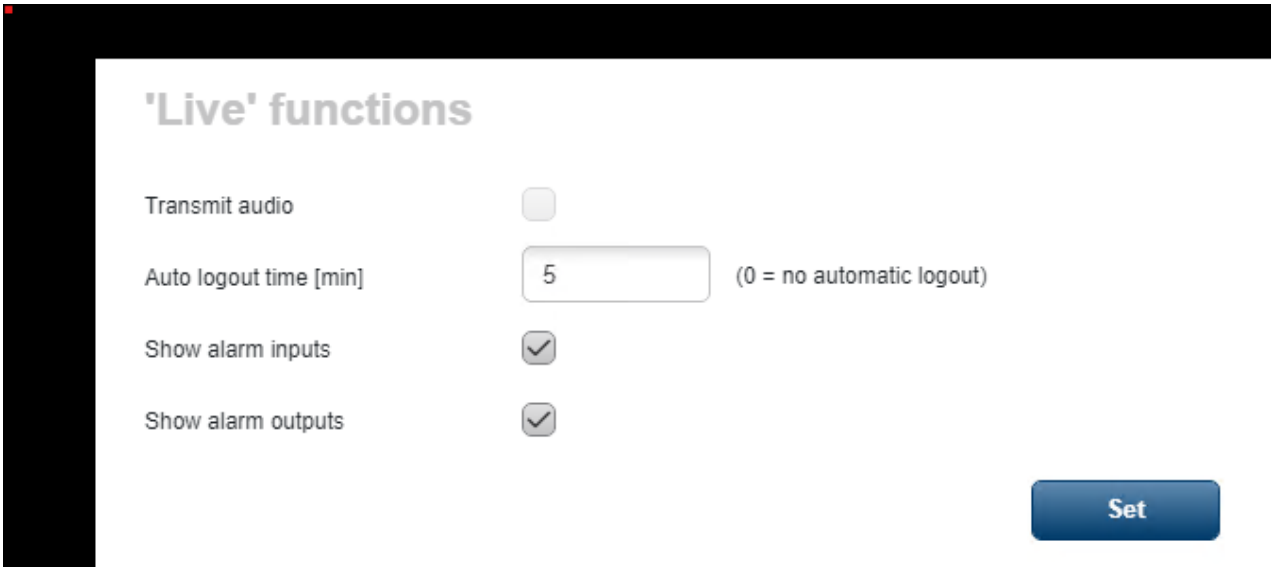

Figure 3: Login notification banner showing another user sign-in

Figure 11-3. A login notification alerts existing sessions when another user signs in.

11.2 Initial Password Assignment

At factory reset, every built-in account exists without a password and only password-based authentication is enabled. Enabling certificate or ADFS authentication requires the additional steps covered later in this chapter.

Before any other configuration, set the **service** account password. Until you do, the camera refuses every login attempt and blocks access to the web interface.

1. Browse to the camera's IP address. The **Device security** screen appears automatically.
2. Enter and confirm a strong password for the **service** account. The policy checklist turns green as each rule is satisfied.
3. Click **Set** to save.

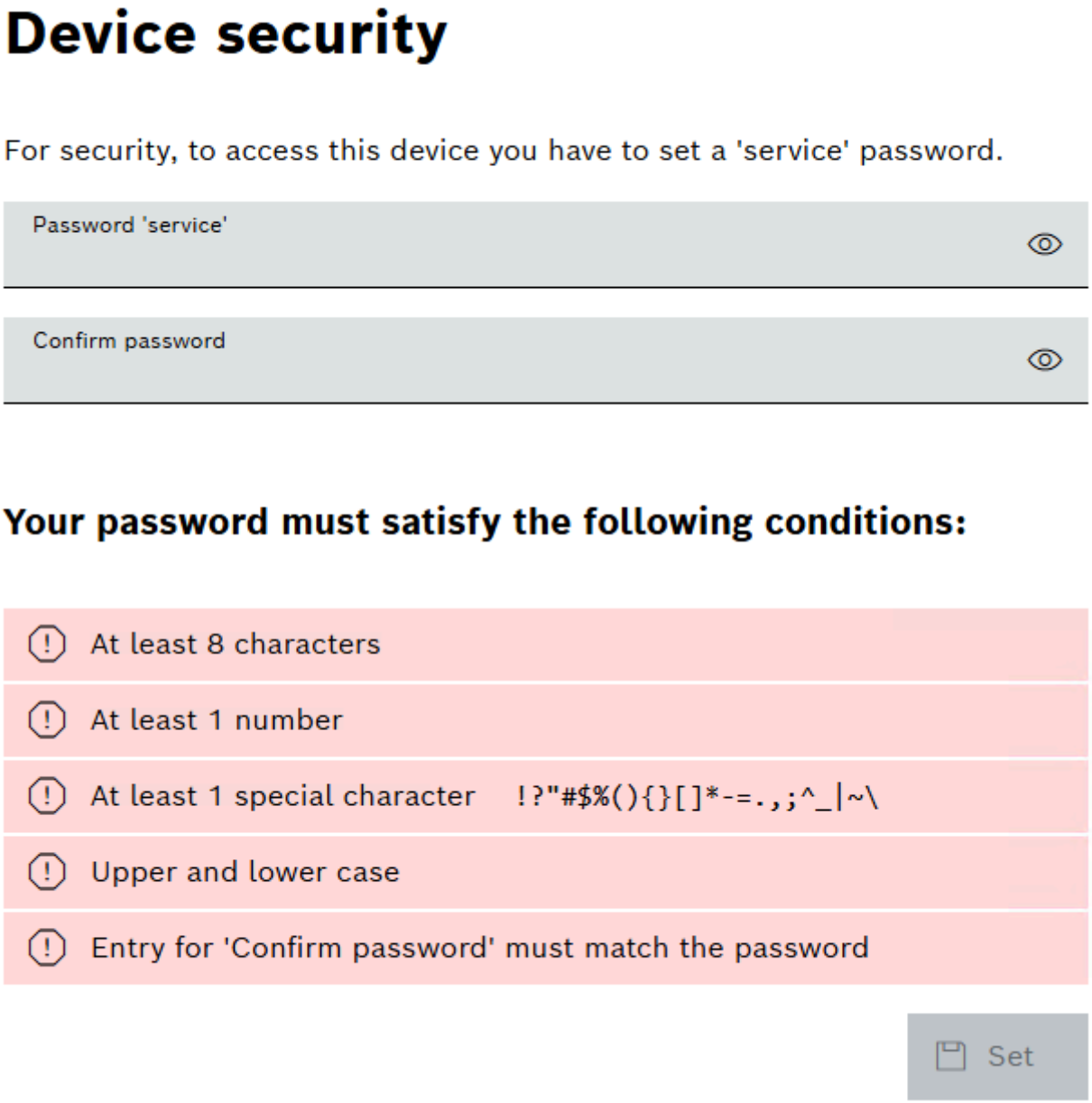

Figure 4: Device security screen for assigning the service password

Figure 11-4. The Device security screen validates every password policy rule before it lets you save.

After you sign in, immediately assign passwords to the **user** and **live** accounts. Leaving them unprotected lets an attacker view live or recorded video without touching the service account. Open **General → User Management**, click the edit icon next to each account, and set a unique password.

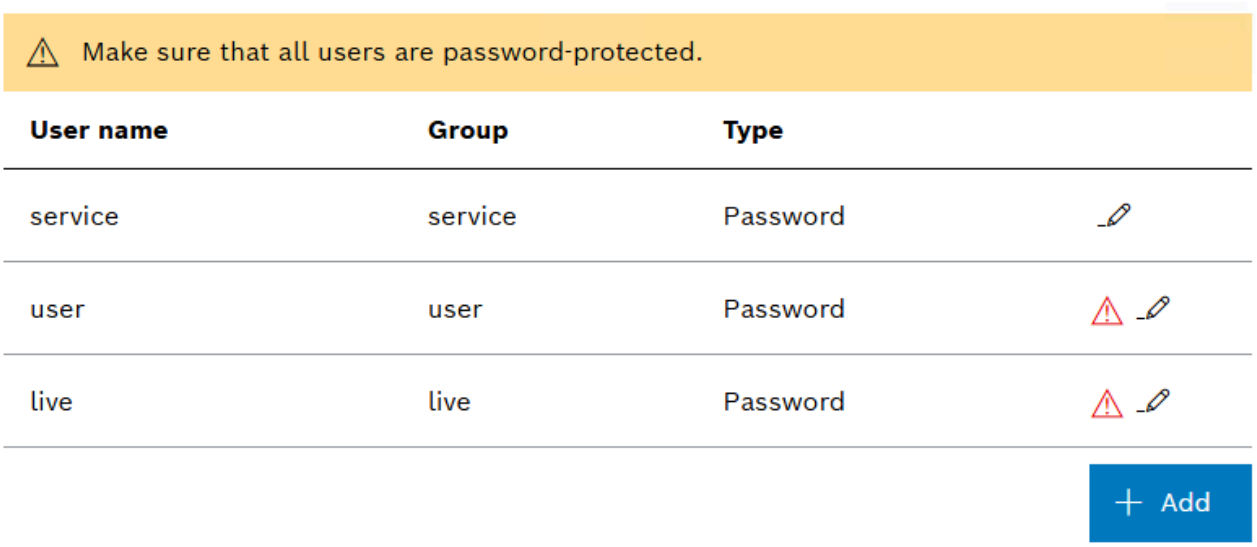

Figure 5: User Management table with a warning about unprotected accounts

Figure 11-5. A warning message remains visible in the User Management table until every account is password-protected.

> **NOTICE**
>
> Use distinct, unrelated passwords for every account and store them in a shared password manager. Reusing credentials across roles collapses the benefit of the least-privilege access groups.

11.3 Creating New User Accounts

The three built-in accounts cover initial provisioning. For everyday operation, create named accounts so that every action can be attributed to a specific person.

11.3.1 Via the Web Interface

1. Open **General → User Management**.
2. Click **Add**. The New user dialog appears.
3. Enter a **User name** of at least 4 characters. The name must be unique on the camera.
4. Choose the **Group** that matches the user's role: *live*, *user*, or *service*.
5. Choose a **Type**: *Password* or *Certificate*.
6. For password authentication, enter and confirm a password that satisfies the policy.
7. Click **Set** to save.

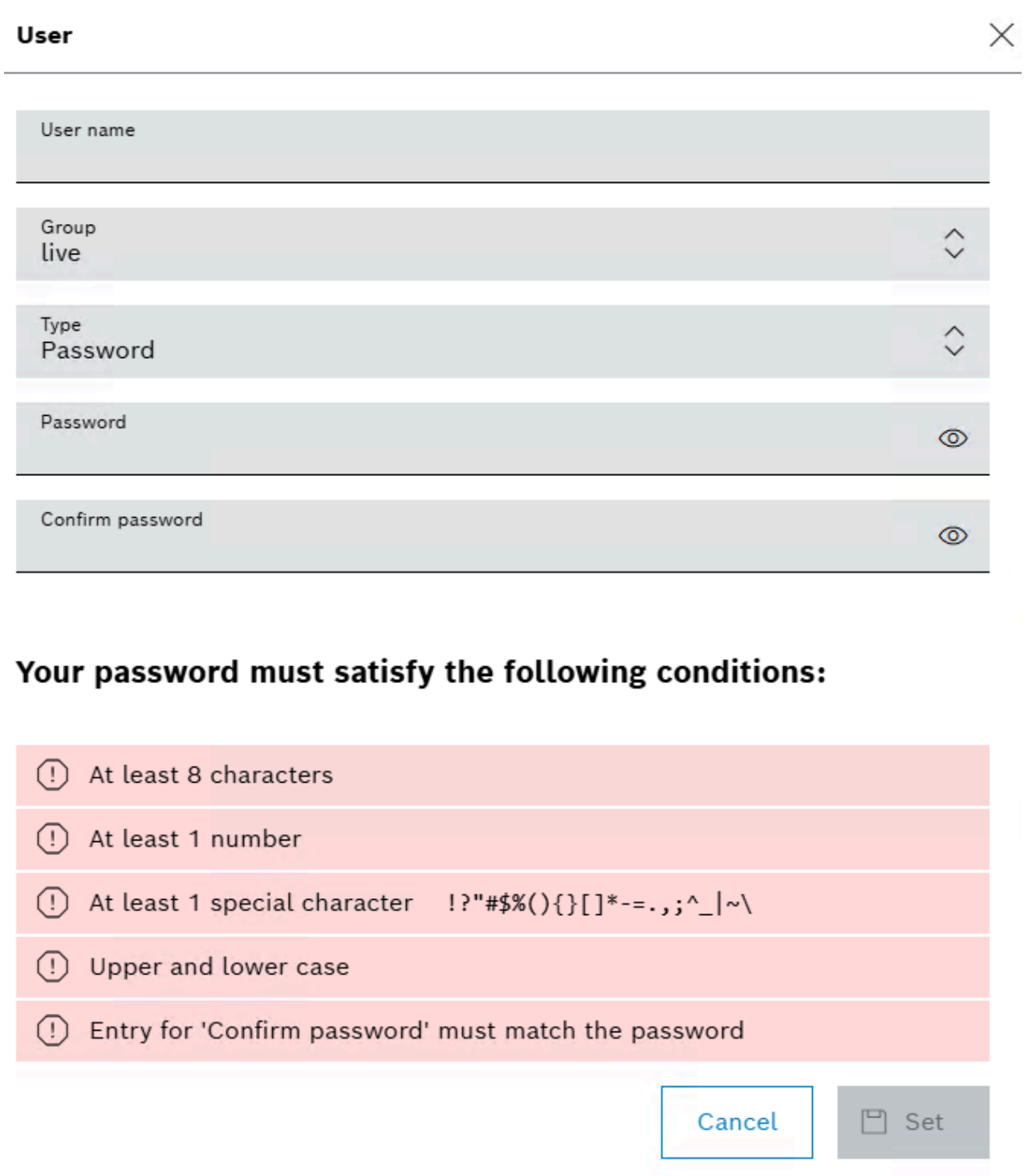

Figure 6: New user dialog with password policy checklist

Figure 11-6. Creating a new user through the camera web interface. The checklist validates every password policy rule in real time.

11.3.2 Via IQSIGHT Configuration Manager

In larger deployments managed by BVMS or VRM, Configuration Manager pushes global passwords to every IP video device on the network. That keeps credentials consistent and prevents the per-camera drift that produces orphaned or weak accounts. IQSIGHT Configuration Manager also handles small and medium deployments, applying credentials to one device or a batch at the same time.

1. In Configuration Manager, select one or more devices.
2. Open the **General** tab, then **User Management**.
3. Click the gear icon next to the account you want to update.
4. Enter the password and click the **Save** icon to push and save the change.

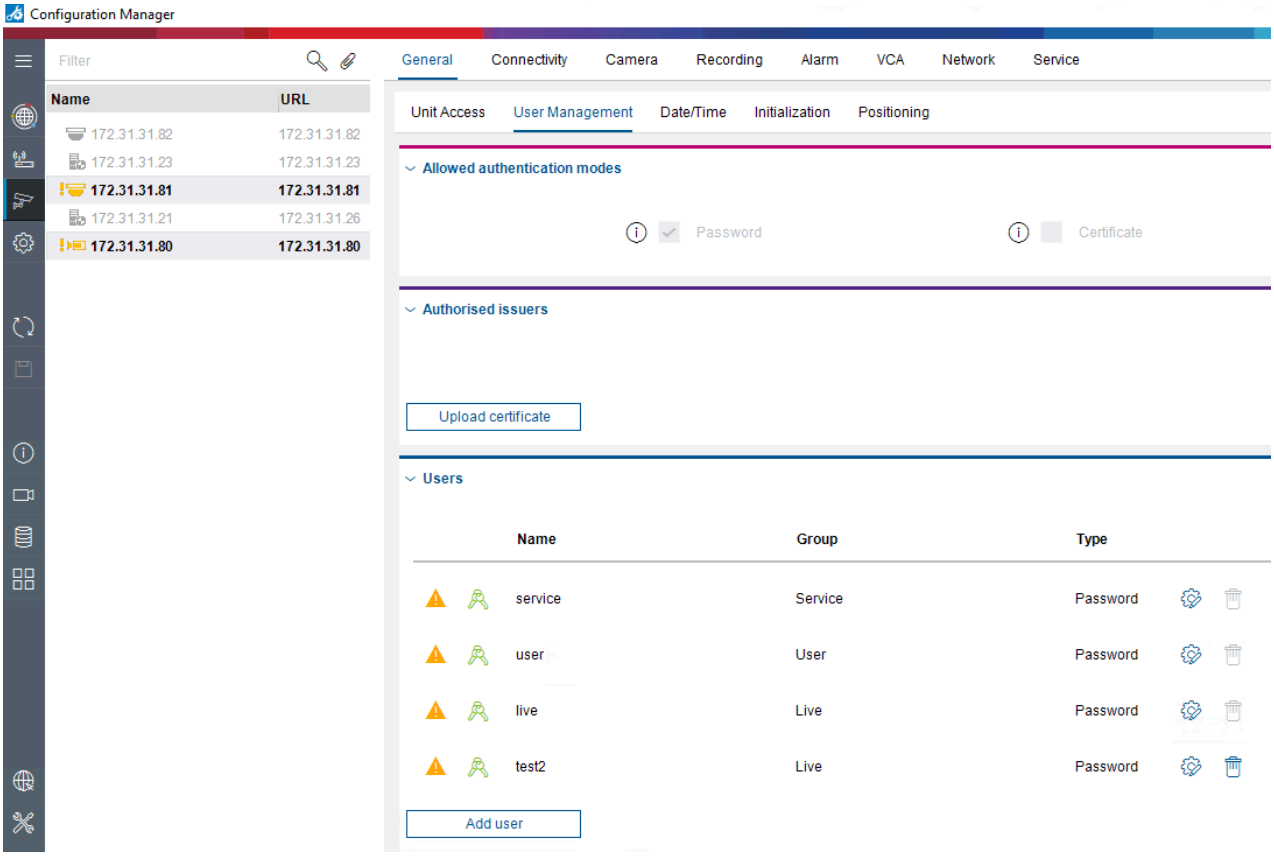

Figure 7: Configuration Manager User Management view with multiple devices

Figure 11-7. Configuration Manager applies user accounts and passwords across multiple cameras in a single operation.

11.4 Certificate-Based Authentication

Certificate-based authentication replaces the password with a client certificate that the browser — or a smartcard or hardware token — presents to the camera. Because certificates cannot be brute-forced or guessed the way a password can, this method raises the bar for attackers and removes credential reuse risk altogether.

11.4.1 Install the Certificate Authority on the Camera

1. Open **Service → Certificates** and click **Add**.
2. Upload the Certificate Authority (CA) that signs your user certificates.
3. Set the certificate **Usage** to **User authentication**.
4. Click **Set** to save.

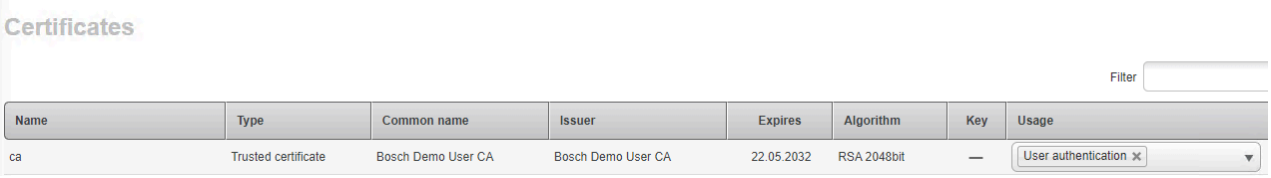

Figure 8: CA certificate entry with User authentication usage

Figure 11-8. The CA certificate in the camera's certificate store, configured for user authentication.

11.4.2 Enable Certificate Authentication

1. Open **General → User Management**.
2. Under **Authentication modes**, enable **Certificate**.
3. Click **Set** to save.
4. Reboot the camera. The new authentication mode takes effect after the restart.

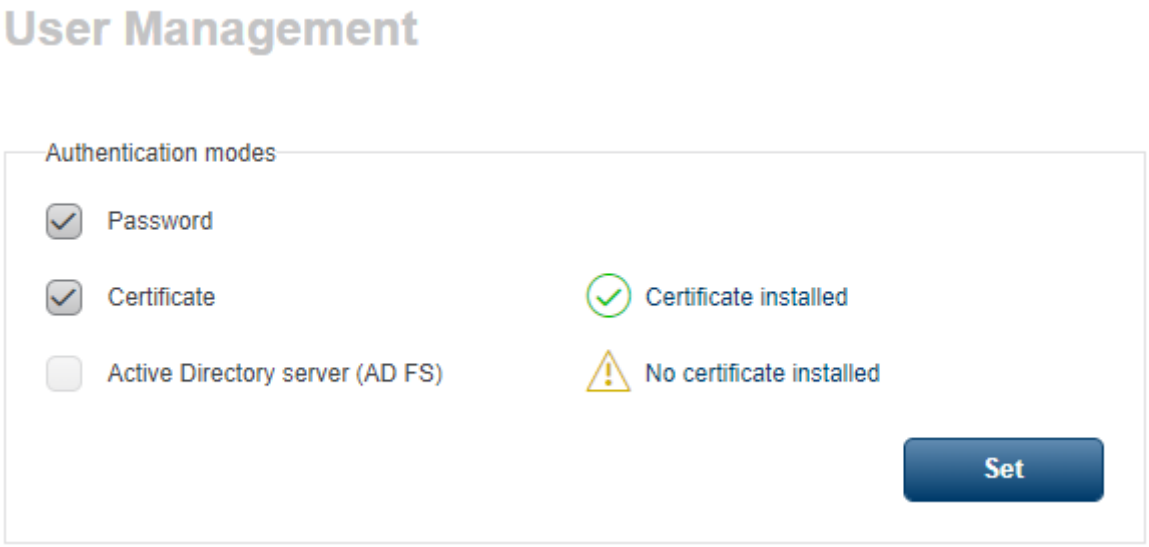

Figure 9: Authentication modes with Password and Certificate enabled

Figure 11-9. Enable the Certificate authentication mode alongside — or instead of — Password.

11.4.3 Create a Certificate-Based User

After the reboot, create the user account that the certificate will authenticate:

1. Open **General → User Management** and click **Add**.
2. Enter a **User name**, choose a **Group**, and set **Type** to **Certificate**. No password is required.
3. Click **Set** to save.

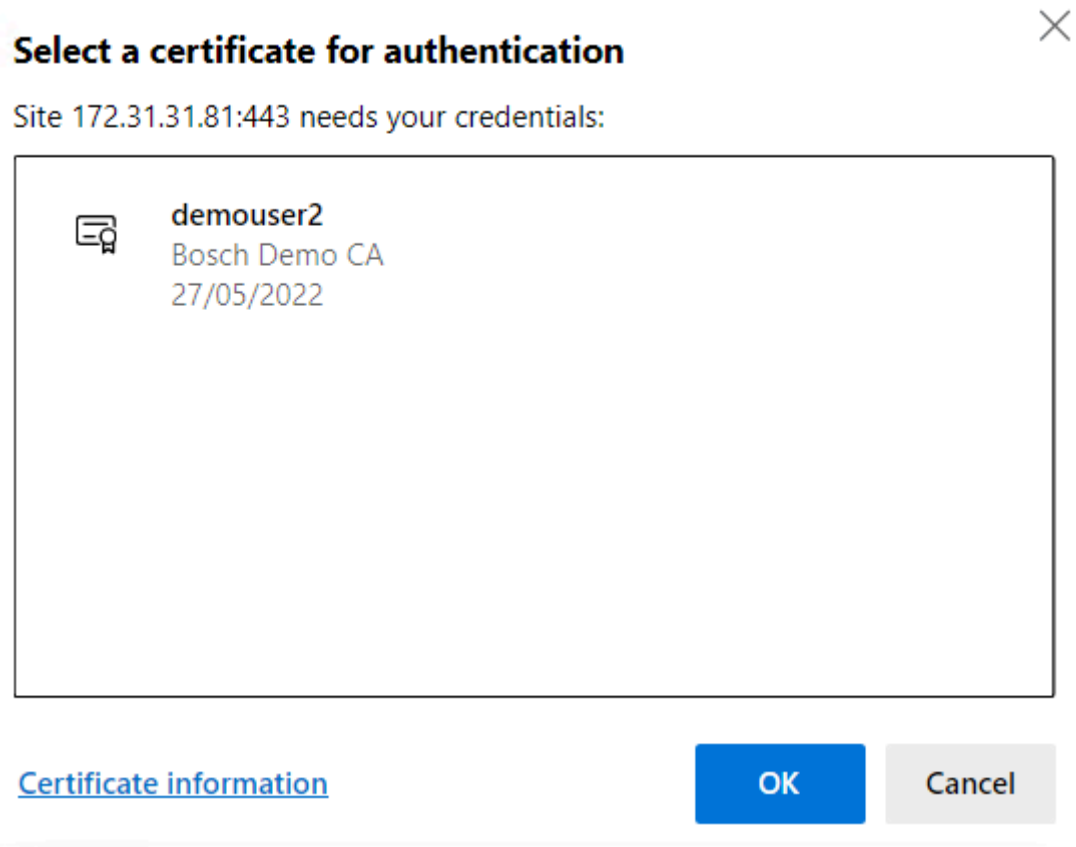

Figure 10: New user dialog with Type set to Certificate

Figure 11-10. A certificate-based user. The common name of the client certificate must match this username exactly.

NOTICE

The common name (CN) in the user's client certificate must match the username created on the camera. A mismatch blocks login even if the certificate is otherwise valid and trusted.

11.4.4 Import and Use the Client Certificate

Load the user certificate into the browser's certificate store — the Windows certificate store for Microsoft Edge, or the certificate settings for Mozilla Firefox. The next time the user opens the camera web interface, the browser presents a certificate selection dialog; select the certificate that matches the camera user, and the session begins without a password prompt.

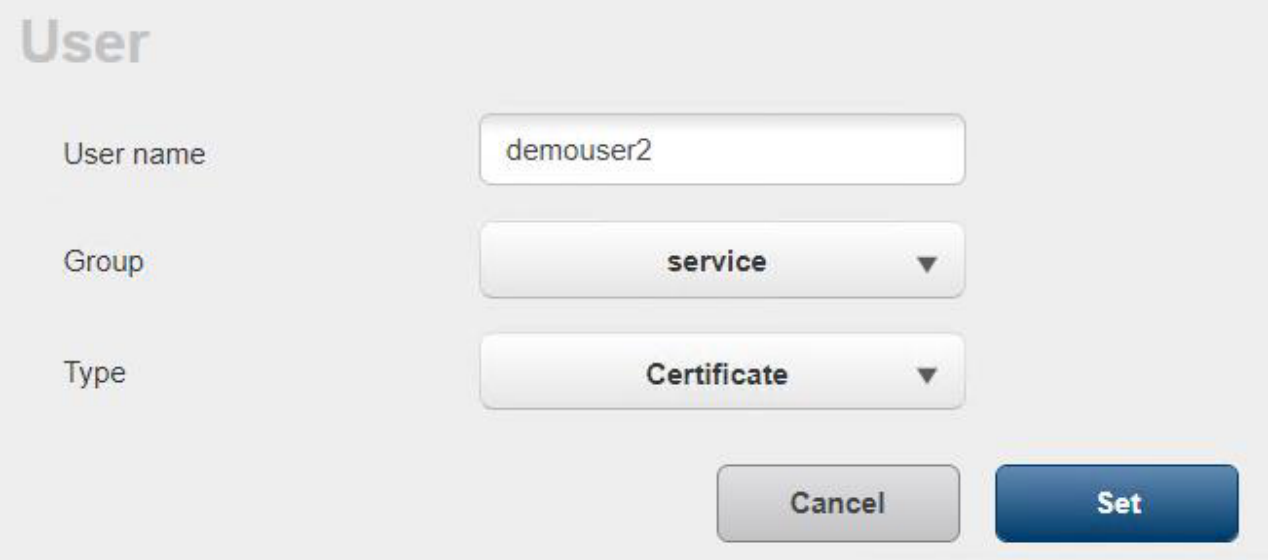

Figure 11: Browser certificate selection dialog for camera login

Figure 11-11. The browser prompts the user to select a certificate when connecting to the camera.

> **Tip:** Store user certificates on a smartcard or hardware token whenever possible. Hardware-backed keys cannot be copied off the device, which closes one of the most common credential exfiltration paths.

CHAPTER 12 — CAMERA HARDENING

Hardening reduces the attack surface by disabling unnecessary services and enforcing secure defaults.

12.1 Hardening Levels

IQSIGHT IP cameras are delivered with a secure by default configuration that allows easy integration into different environments.

Depending on the target environment and its intended security level, it might be required to change some camera settings to increase cyber and data security. However, there can be limitations of the operational environment that mandates the use of a certain protocol or a feature, which is less secure (for example SNMPv1).

There are two levels of hardening defined: *elevated* and *strict*.

Hardening level *strict* features the most secure means of setting up a device but might be limiting the usage of the device as features like auto discovery of a device are disabled. For each feature, it should be evaluated if the setting *elevated* or *strict* can be applied.

12.2 Hardening Overview Tables

Network — Network Services

Feature	Default	Elevated	Strict
HTTP	Disabled	Disabled	Disabled
HTTPS	Enabled	Enabled	Enabled
RTSP	Disabled	Optional	Disabled
RCP	Disabled	Disabled	Disabled
SNMPv1	Disabled	Disabled	Disabled
SNMPv3	Disabled	Enabled	Enabled
iSCSI	Disabled	Optional	Disabled
Discovery	Enabled	Enabled	Disabled
ONVIF Discovery	Enabled	Enabled	Disabled
Password reset mechanism	Enabled	Disabled	Disabled
Ping response	Enabled	Enabled	Disabled
RTSPS	Enabled	Enabled	Enabled

Network — Network Access

Feature	Default	Elevated	Strict
Minimum TLS version	1.2+	1.2+	1.2+
HSTS	Disabled	Enabled	Enabled

Network — Advanced

Feature	Default	Elevated	Strict
802.1x	Disabled	Optional	Enabled
Syslog	Disabled	TCP	TLS

Network — Network Management

Feature	Default	Elevated	Strict
SNMPv3 mode	Disabled	SHA1 / AES	SHA1 / AES

Network — IPv4 Filter

Feature	Default	Elevated	Strict
IPv4 filter	Disabled	Enabled	Enabled

General — Date/Time

Feature	Default	Elevated	Strict
Date/Time (NTP Client)	Disabled	SNTP / TLS Date	TLS Date

Connectivity — Cloud Services

Feature	Default	Elevated	Strict

Remote Portal	Disabled	Enabled	Enabled

Service — Logging

Feature	Default	Elevated	Strict
Software sealing	Disabled	Enabled	Enabled

12.3 Feature Descriptions and Recommendations

HTTP HTTP is enabled by default, but unencrypted, so credentials or settings are transferred unencrypted if used. *Recommendation:* Plain HTTP should remain disabled in favor of the encrypted HTTPS, especially if the network is untrusted.

HTTPS HTTPS is encrypted and should be the default choice for accessing the web interface or access the web-based RCP API. Using own PKI and certificates is recommended. *Recommendation:* HTTPS is the default secure protocol used for configuration and should remain enabled.

RTSP RTSP is used for video streaming, but normally unencrypted. If the software receiving the video stream is capable of using RTSPS, it is recommended to disable plain RTSP. When using other IQSIGHT components (for example decoders/BVMS/VRM/DIVAR IP) a IQSIGHT proprietary encryption for RTSP can be enabled, making transmission secure. *Recommendation:* Risk based approach if video can be transmitted unencrypted or via IQSIGHT encryption. If possible, use encrypted RTSPS.

RCP The IQSIGHT proprietary Remote Control Protocol plus is the configuration protocol for IQSIGHT IP cameras. Plain RCP is unencrypted, so settings are transferred unencrypted. All IQSIGHT tools now use RCP over HTTPS communication for some time, but it might be needed for 3rd party integration tools or scripting tools still relying on this protocol. *Recommendation:* Enable RCP only if used by 3rd party tools or legacy systems.

SNMPv1 SNMP is the common network monitoring protocol used to query health information of a device or send out traps to a remote receiver, but unencrypted. *Recommendation:* Keep disabled if not required for health monitoring or other compatibility reasons. Use SNMPv3 if possible.

SNMPv3 SNMPv3 is successor of SNMPv1 and can also be used encrypted. *Recommendation:* Recommended if SNMP monitoring must be implemented.

iSCSI The internal iSCSI server which is used to make internal recordings on the camera accessible via iSCSI. iSCSI is an unencrypted protocol. *Recommendation:* Keep iSCSI server disabled if not used on the camera.

Discovery Using a IQSIGHT proprietary mechanism to make cameras discoverable by a IQSIGHT software, such as Configuration Manager. *Recommendation:* When working with dynamic IP addresses this feature should remain enabled. When working in an environment with fixed IP addresses, this feature can be turned off.

ONVIF Discovery Support the discovery of camera devices via the ONVIF Discovery protocol. *Recommendation:* When working with dynamic IP addresses and ONVIF compliant tools, this feature should remain enabled. When working in a fixed environment with fixed IP addresses, this feature can be turned off.

Password reset mechanism IP cameras can be mounted in very remote locations which makes it hard to do maintenance work or a factory reset in case that the access to the camera has been locked. IQSIGHT offers the possibility to reset the password of a camera via challenge-response mechanism

based on a secure public/private key mechanism. *Recommendation:* If this feature is not needed, it is recommended to disable it.

Ping response Configures if the camera answers to ping requests in the network. Can help with debugging. In a high secure network this can be disabled to avoid device enumeration via ping sweep, although there are several other means of device discovery that can be used by an attacker. *Recommendation:* Risk based approach, can be disabled for high security networks.

RTSPS RTSPS is the encrypted version of RTSP and used for video streaming. If the receiving software supports it, RTSPS should always be preferred over plain RTSP. As many RTSP clients do not support the secure variant, RTSP is still enabled for Level 1 security. *Recommendation:* Use RTSPS if possible.

Minimum TLS version IP cameras do not allow insecure SSLv3, TLS 1.0 or TLS 1.1. They also support the newer TLS 1.3 specification. TLS 1.2+ is a setting to only enable secure TLS ciphers. If you need a broader range of TLS ciphers to be compatible to older devices you can enable TLS 1.2 as minimum version. *Recommendation:* Leave minimum TLS version to 1.2+.

HSTS HTTP Strict Transport Security (HSTS) is a policy set by a website to protect against man-in-the-middle attacks and protocol downgrade attacks. It allows the website to tell the browser to only allow HTTPS connections within this connection and not allow any unencrypted HTTP connections. *Recommendation:* Enable HSTS on the camera.

802.1x 802.1x is a standard for Network Access Control (NAC). It allows devices to authenticate in the network, granting only authenticated devices access to the network. IQSIGHT IP cameras support 802.1x either with password or certificate-based authentication, with certificate-based authentication being the preferred method. To use 802.1x the network switch must support this standard, and an authentication server is needed. *Recommendation:* If the network infrastructure allows it, use network authentication with 802.1x.

Syslog As the camera does only provide a limited space for log messages, log messages should be sent to a central location and analyzed there to detect any attacks or misconfigurations. *Recommendation:* Use TCP Syslog to avoid losing messages due to packet loss. Use Syslog with TLS to encrypt and authenticate messages.

SNMPv3 mode SNMPv3 is the successor of SNMPv1 and allows for secure authentication and transfer of information. *Recommendation:* When using SNMPv3, use SHA1 as authentication protocol and AES as privacy protocol (if supported).

IP filter In IP Filter several IP addresses (single hosts or network subnets) can be defined, that are allowed to access the camera. It is recommended to define the computers or networks accessing the camera here. *Recommendation:* It is recommended to use the IP filter to define allowed hosts or networks.

Date/Time To have the correct timestamp on logs and video data, it is recommended to synchronize the time to a central timeserver. Both, SNTP and TLS date can be used to achieve this. The advantage of SNTP is a more precise time synchronization. The advantage of TLS date is the possibility to check for a correct certificate, making it the more secure solution. *Recommendation:* Use a secure means of synchronizing time, either with SNTP or TLS date.

Cloud-based services IQSIGHT offers its own cloud-based services to manage cameras over the IQSIGHT cloud (Remote Portal). The cloud services do not automatically connect to Remote Portal and are disabled by default. Each camera needs to be connected to Remote Portal first if it should be used. Every precaution has been taken to secure the connection between Remote Portal and camera, so if

needed Remote Portal can be used in any environment. *Recommendation:* Remote Portal can be used depending on if cloud solution is in use.

Software sealing After a completed configuration of an IP camera, the settings of the device should not change. A software seal can be enabled to notify of device configuration changes. *Recommendation:* Enable software sealing if there are no pending configuration changes.

12.4 Multicast Configuration

All IQSIGHT IP video devices are capable of providing both “Multicast on Demand” or “Multicast Streaming” video. Where unicast video transmissions are destination based, multicast is source based and this can introduce security issues at the network level, including: group access control, group center trust, and router trust.

TTL (time-to-live) scoping defines where and how far multicast traffic is allowed to flow within a network, each hop decreasing TTL by one. When configuring IP video devices for multicast usage, the packet TTL of the device can be modified.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **Multicast**.
3. Locate the **Multicast TTL** portion of the page.
4. Adjust the **Packet TTL** settings using the following TTL values and Scoping Limits:
   - TTL Value 0 = Restricted to local host
   - TTL Value 1 = Restricted to same subnet
   - TTL Value 15 = Restricted to same site
   - TTL Value 64 (Default) = Restricted to same region
   - TTL Value 127 = Worldwide
   - TTL Value 191 = Worldwide with limited bandwidth
   - TTL Value 255 = Unrestricted Data

> **NOTICE**
>
> When dealing with video surveillance data, a best practice would be to set your TTL settings to 15, restricted to same site. Or better, if you know the exact maximum number of hops, use this as TTL value.

12.5 IPv4 Filtering

You can restrict access to any IQSIGHT IP video device via a feature called IPv4 filtering. IPv4 filtering utilizes the basic fundamentals of “subnetting” to define up to two allowable IP address ranges. Once defined, it denies access from any IP address outside these ranges.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select **IPv4 Filter**.

> **NOTICE**

To successfully configure this feature, you must have basic understanding of subnetting or have access to a subnet calculator. Entering incorrect values into this setting can restrict access to the device itself and a factory default reset may need to be performed to regain access.

3. To add a filter rule, make two entries:
   - Enter a base IP address that falls within the subnet rule you create. The base IP address specifies which subnet you are allowing and it must fall within the desired range.
   - Enter a subnet mask that defines the IP addresses with which the IP video device will accept communication.

Example: The IP address 1 of `192.168.1.20` and the Mask 1 of `255.255.255.240` have been entered. This setting will restrict access from devices that fall within the defined IP range of `192.168.1.16` to `192.168.1.31`.

While utilizing the IPv4 Filter feature, devices will be able to be scanned via RCP+, but access to configuration settings and video is not possible via clients that fall outside the allowed IP address range. This includes web browser access.

The IP video device itself does not need to be located in the allowed address range.

NOTICE

Based on the set-up of your system, utilizing the IPv4 Filter option can reduce unwanted visibility of devices on a network. If enabling this function, make sure to document settings for future reference. Note that the device will still be accessible via IPv6, so IPv4 filtering only makes sense in pure IPv4 networks.

12.6 SNMP Configuration

Simple Network Management Protocol (SNMP) is a common protocol to monitor the health status of a system. Such a monitoring system typically has a central management server that collects all the data from the system's compatible components and devices.

SNMP provides two methods to gain the system health status:

- The network management server can poll the health status of a device via SNMP requests.
- Devices can actively notify the network management server about their system health status in case of error or alarm conditions through sending SNMP traps to the SNMP server. Such traps must be configured inside the device.

SNMP also allows configuration of some variables inside devices and components.

The information, which messages a device supports and which traps it can send, is derived from the Management Information Base, the so-called MIB file, a file that is delivered with a product for easy integration into a network monitoring system.

There are three different versions of the SNMP protocol:

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. It is widely used and has become the de facto standard protocol for network management and monitoring. But SNMPv1 has become under threat due to its lack of security features. It only uses *community strings* as a kind

of passwords, which are transmitted in clear text. Thus, SNMPv1 shall only be used when it can be assured that the network is physically protected against unauthorized access.

SNMP version 2 (SNMPv2) included improvements in security and confidentiality, amongst others, and introduced a bulk request to retrieve large amounts of data in a single request. However, its security approach was considered way too complex, hindering its acceptance. Thus, it was soon pushed out by version SNMPv2c, which equals SNMPv2 but without its controversial security model, reverting to the community-based method from SNMPv1 instead, similarly lacking security.

SNMP version 3 (SNMPv3) mainly adds security and remote configuration enhancements. These include improvements on confidentiality by encryption of packets, message integrity and authentication. It also addresses large-scale deployment of SNMP.

> **NOTICE**
>
> Both SNMPv1 and SNMPv2c have become under threat due to their lack of security features. They only use 'community strings' as a kind of passwords, which are transmitted in clear text. Thus, SNMPv1 or SNMPv2c should only be used when it can be assured that the network is physically protected against unauthorized access.

Platform MIB Support
Full private MIB integration for both SNMPv1 and SNMPv3, including trap support.

The MIB file is included in the firmware ZIP package, available from the IQSIGHT product catalog.

Enabling SNMP

1. Open the camera web interface and log in.
2. Navigate to **Configuration** → **Network** → **Network Management**.
3. Select the desired SNMP version (v1 or v3) and click **Set**.
4. Reboot the camera.

SNMP can also be enabled via Configuration Manager.

Configuring SNMP Traps
After enabling SNMP, configure trap destinations in **Configuration** → **Network** → **Network Management**:

1. Open the **SNMP traps** select menu and choose which traps to send.
2. Specify up to two trap destination hosts to receive the trap messages.

12.7 Secure Time Synchronization

IQSIGHT cameras support three time synchronization protocols:

- **Time Protocol (RFC 868)** — Legacy protocol with 1-second precision. Use only for backward compatibility.
- **SNTP** — Standard NTP implementation with good precision. Recommended for most deployments.
- **TLS (TLS-Date)** — Derives time from a TLS handshake with any HTTPS server. No dedicated time server needed, but lower precision than SNTP.

In TLS mode, any arbitrary HTTPS server can be used as time server. The time value is derived as a side-effect from the HTTPS handshake process. The transmission is TLS secured. An optional root

certificate for the HTTPS server can be loaded to the camera's certificate store to authenticate the server.

The NTP server address can be pushed to cameras automatically via **DHCP option 42** (NTP Servers), eliminating manual configuration.

> **NOTICE**
>
> Make sure that the entered time server IP address has a stable and uncompromised time base itself.

> **Tip:** For NTP server setup instructions (Windows and Linux), DHCP configuration, and protocol comparison, see the Log Monitoring and Time Synchronization Guide.

12.8 Cloud-Based Services

All IQSIGHT IP video devices can communicate with IQSIGHT cloud-based services such as Remote Portal. Depending on the region of deployment, this allows IP video devices to use services such as Remote Device Management or Cloud VMS to forward alarms and other data to a central station.

There are three modes of operation for cloud-based services:

- **On:** The video device will constantly poll the cloud server.
- **Auto** (default): The video devices will attempt to poll the cloud server a few times, and if unsuccessful, it will cease attempting to reach the cloud server.
- **Off:** No polling is performed.

Cloud-based services can be easily turned off using Configuration Manager.

1. In the Configuration Manager, select the desired device.
2. Select the **Network** tab, then select the tab **Advanced**.
3. Locate the **Cloud-based services** section of the page and select **Off** from the list.

> **NOTICE**
>
> If you are utilizing IQSIGHT cloud-based services, keep the default configuration. In all other cases switch the cloud-based services mode to **Off**.

12.9 Configuration Sealing

After an IP camera is installed, calibrated, and configured, changes to its settings are rarely needed. **Configuration sealing** protects the device against accidental or malicious configuration changes by creating a tamper-evident seal.

Like a physical seal, the software seal can be broken — but the break is immediately detectable, and configuration changes can be traced or undone.

Enable Configuration Sealing

1. Navigate to **Service** → **Logging** → **Software Sealing**.
2. Enable the seal.

Once active, the interface shows when the seal was enabled and confirms that it is intact. If a configuration change occurs, the interface shows when the seal was broken.

Detect a Broken Seal
An attacker could attempt to disable sealing to hide their changes. Forward seal-break notifications to an external system using one or more of these methods:

1. **Syslog forwarding** — Transfer device logs to a syslog server and monitor for EMERGENCY-level messages, which identify who broke the seal and what was changed.
2. **SNMP trap** — Configure SNMP trap sending (see SNMP Configuration). A trap is sent as soon as a configuration entry changes while the seal is active.

After investigating and resolving a seal break, re-seal the configuration by unchecking and re-checking the **Enable software sealing** checkbox.

12.10 Configuration Backup and Restore

Backing up the camera configuration allows you to restore a known-good state, recover settings after a device replacement, or copy configuration to another device of the same type.

Backup and Restore via Web Interface

1. Navigate to **Service** → **Maintenance**.
2. Click **Download** next to the **Configuration** entry.
3. Enter a password when prompted — the configuration file is AES-encrypted with this password.

The exported file is saved as `rtc_image.ct`.

To restore, navigate to the same page, select the exported file via **Browse...**, click **Upload**, and enter the password.

> **NOTICE**
>
> Store the backup password in a secure location. The configuration file cannot be imported without the correct password.

> **NOTICE**
>
> The device reboots automatically after uploading a configuration file.

Backup and Restore via Configuration Manager
Configuration Manager supports backing up and restoring configurations for multiple devices simultaneously.

1. Select one or more cameras in Configuration Manager.
2. Right-click and select **Settings** → **Back Up**.
3. Choose the storage path and optionally seal the configuration(s).
4. On first use, set a password to encrypt the exported configurations.

To restore, select **Settings** → **Restore**, choose the desired configuration revision, and click **Restore**. The camera reboots automatically with the restored configuration.

> **NOTICE**
>
> The backup password must meet the same quality criteria applied to camera passwords. The password is set once and stored in the encrypted Configuration Manager data.

CHAPTER 13 — CAMERA CERTIFICATES AND VIDEO AUTHENTICATION

Certificates establish trust between cameras and management systems. Video authentication ensures the integrity of recorded footage.

13.1 Certificate Store and Management

All IQSIGHT IP cameras running use a certificate store, which can be found under the **Service** menu of the camera configuration.

Specific server certificates, client certificates and trusted certificates can be added to the store.

To add a certificate to the store:

1. On the device web page, navigate to the **Configuration** page.
2. Select the **Service** menu and the **Certificates** submenu.
3. In the **File list** section, click **Add**.
4. Upload the desired certificates. After the upload is completed, the certificates appear in the **Usage list** section.
5. In the **Usage list** section, select the desired certificate.
6. To activate the usage of the certificates the camera must be rebooted. To reboot the camera, click **Set**.

Certificates are accepted in `*.pem`, `*.cer` or `*.crt` format and must be base64-coded. They may be uploaded as one combined file, or split into certificate and key parts and uploaded in this order as separate files to be automatically re-combined.

Password-protected PKCS#8 private keys (AES-encrypted) are supported which must be uploaded in base64-coded `*.pem` format. PKCS#12 containers in `*.p12` or `*.pfx` format are also supported, with either no encryption, 3DES or AES encryption of the container.

When a certificate is added to the store, it has no usage assigned by default. The usage determines what the certificate is used for and allows assigning different certificates for different purposes. For certificates with a private key available, the following usages can be selected:

- CBS client
- EAP-TLS client
- HTTPS server
- MQTT client
- Primary Record Encryption
- SYSLOG client
- Secondary Record Encryption

- TLS-DATE client

For certificates where only the public certificate (no private key) is available:

- ADFS CA trusted
- CBS trusted
- EAP-TLS trusted
- Intermediate
- MQTT trusted
- Syslog trusted
- TLS-DATE trusted
- User Authentication trusted
- lun trusted
- rec1 trusted
- rec2 trusted

13.2 Device Certificates and CSR

All IQSIGHT cameras come with a preinstalled unique device certificate and a private key, derived from the IQSIGHT Root Certificate and installed in a secure production environment, proving the camera being an “originally manufactured” IQSIGHT device. This certificate is used for HTTPS connections automatically and can be used to identify and authenticate a device by verifying the certificate chain up to the IQSIGHT Root Certificate.

> **NOTICE**
>
> Certificates should be used to authenticate a single device. It is recommended to create a specific certificate per device, derived from a root certificate.

The most secure variant of a certificate deployment is to generate a certificate signing request (CSR) on the device and to request a certificate from an internal or external certification authority.

With a certificate signing request, the device holds the private key internal and only exposes the rest of the certificate to be signed by the certificate authority. The private key is securely stored in the Secure Element (SE) of the camera.

Therefore, whenever a device provides a CSR possibility, this should be the preferred way to create a certificate.

Generated certificates and CSRs can also be downloaded directly via HTTP(S):

- Certificate: `https://<device-ip>/cert_download/<filename>.pem?type=cert`
- CSR: `https://<device-ip>/cert_download/<filename>.pem?type=csr`

> **Tip:** The CSR and certificate download URLs enable scripted workflows — for example, using the RCP+ API to automate certificate provisioning across multiple cameras.

The camera also supports generating **self-signed certificates** directly on the device. While self-signed certificates keep keys secure in the Secure Element, they must be individually trusted by every client — making them impractical for larger deployments. Use a CA-signed certificate instead when possible.

Certificates can be uploaded to a device by either using the device web page of a video device or by using Configuration Manager.

Uploading certificates by using the device web page

Certificates can be uploaded using the device web page of a video device. On the device web page, on the **Certificates** page, new certificates can be added and deleted, and their usage can be defined.

Uploading certificates by using Configuration Manager

In Configuration Manager, certificates can be easily uploaded to individual or multiple devices simultaneously.

1. In Configuration Manager, select one or more devices.
2. Right-click and click **File Upload**, then click **SSL Certificate...**. A Windows Explorer window opens to locate the certificate for upload.

For smaller systems, Configuration Manager provides a supportive function called **MicroCA**, which allows to create or use a Root CA and derive device certificates from this, or use it for signing the devices' certificate signing requests, also for multiple devices simultaneously. For more details, refer to the Configuration Manager User manual.

Automated certificate enrollment with SCEP

IQSIGHT cameras support the **Simple Certificate Enrollment Protocol (SCEP)** for automated certificate enrollment and renewal. SCEP allows cameras to request certificates directly from a SCEP-enabled CA without manual file upload. This is particularly useful in larger deployments where manual certificate provisioning per device is impractical. Configure the SCEP server URL and challenge password in the camera's certificate settings to enable automated enrollment.

13.3 Video Authentication / Signing

Once the devices in a system are protected and authenticated correctly it is worth keeping an eye also on the video data delivered from them. The method is called video authentication.

Video authentication deals solely with methods of validating the authenticity of video. Video authentication does not deal with the transmission of video, or data, in any way.

To configure video authentication, for example in the web browser:

1. Navigate to the **Camera** menu and then select **Display stamping**.
2. In the **Video authentication** drop-down menu, select the desired option:

The firmware provides three options in video authentication besides classic watermarking:

- **MD5:** Message-digest that produces a 128-bit hash value.
- **SHA-1:** Produces a 160-bit hash value.
- **SHA-256:** SHA-256 algorithm generates an fixed size 256-bit (32-byte) hash.

> **NOTICE**
>
> Only SHA-256 is considered cryptographically secure

When utilizing video authentication, every packet of a video stream is hashed. These hashes are embedded in the video stream and hashed themselves together with the video data. This ensures integrity of the stream content.

The hashes are signed in regular periods, defined by the signature interval, using the private key of the stored certificate within the TPM of the device. Alarm recordings and block changes in iSCSI recordings are all closed with a signature to ensure continuous video authenticity.

> **NOTICE**
>
> Calculating the digital signature requires computational power which might influence the overall performance of a camera if done too often. Therefore a reasonable interval should be chosen.

Since the hashes and digital signatures are embedded in the video stream they will be also stored in the recording, allowing video authentication also for playback and exports.

CHAPTER 14 — PHYSICAL INSTALLATION

Physical security is the first line of defense. Proper installation prevents tampering and unauthorized access to camera hardware.

14.1 Installation Location and Mounting

For the installation of cameras and edge devices a secure installation location and mounting orientation should be chosen. Ideally, this is a location where the device cannot be interfered with either intentionally or accidentally.

CHAPTER 15 — CAMERA DECOMMISSIONING

When a camera is removed from service — whether for replacement, relocation, or disposal — all sensitive data must be securely deleted. IQSIGHT cameras can store credentials, certificates, configuration data, and video recordings in multiple locations. Each must be addressed during decommissioning.

15.1 Factory Reset

A factory reset restores the camera to its original state and securely deletes all user-configured data:

- All user accounts and passwords
- All configuration settings
- All certificates and private keys stored in the Secure Element (SE)

Perform a factory reset using the hardware reset button on the camera, or through the factory default function in the web interface.

> **NOTICE**

A factory reset does not affect the pre-installed IQSIGHT device certificate, which is permanently bound to the hardware. It does delete all custom certificates uploaded or generated after production.

15.2 Local Storage (SD Card)

IQSIGHT cameras with an SD card slot can store recorded video locally. This data persists through a factory reset because it resides on removable media.

- **Unencrypted storage** — If the SD card contains unencrypted recordings, you can securely erase the SD card with the integrated Wipe function, use a tool that performs a full overwrite, or physically destroy the card.
- **Encrypted storage** — When SD card encryption is enabled, the encryption key is stored in the camera's Secure Element. A factory reset deletes this key, rendering the data on the SD card unreadable. For additional assurance, remove and securely erase or destroy the card.

Tip: Enable SD card encryption during initial deployment. This ensures that a factory reset alone is sufficient to make local recordings irrecoverable, even if the SD card is not physically removed.

15.3 Cloud Storage and Remote Services

If the camera was connected to IQSIGHT cloud-based services such as Remote Portal or Cloud VMS, decommissioning must also address cloud-side data:

- **Remove the camera from Remote Portal** — Delete the device from your Remote Portal account before performing the factory reset. This removes the cloud-side association and stops any further data synchronization.
- **Review stored data** — Check whether alarms, events, or video clips were forwarded to cloud services. Delete this data from the cloud platform according to your organization's data retention policies.
- **Revoke access** — If the camera was registered with cloud services, verify that its credentials and tokens are revoked after removal.

15.4 Decommissioning Checklist

Before a camera leaves your custody:

1. Remove the camera from any cloud services (Remote Portal, Cloud VMS).
2. Remove the camera from the video management system (BVMS, VRM).
3. Wipe the SD card or remove and securely erase or destroy it.
4. Perform a factory reset via the web interface or hardware reset button.
5. Document the decommissioning, including device serial number and date.

For general decommissioning guidance applicable to all device types, see Secure Disposal and Decommissioning in Chapter 9.

PART III: IQSIGHT SERVERS, STORAGE, AND CLIENTS

Part III covers the hardening and secure configuration of server infrastructure, storage systems, and client workstations that support IQSIGHT IP video deployments.

CHAPTER 16 — HARDENING SERVERS

Servers hosting BVMS and Video Recording Manager must be hardened at both the hardware and operating system level.

16.1 Physical Security

All server components (for example BVMS Management Server and Video Recording Manager server) and storage devices should be installed in a secure area. The access to the secure area should be ensured with an access control system and should be monitored. The user group, which has access to the central server room, should be limited to a small group of persons.

Although the servers and storage devices are installed in a secure area, they have to be protected against unauthorized access.

16.2 Server Hardware Settings

- The server's BIOS offers the ability to set lower-level passwords. These passwords allow to restrict people from booting the computer, booting from removable devices, and changing BIOS or UEFI (Unified Extensible Firmware Interface) settings without permission.
- In order to prevent data transfer to the server, the USB ports and the CD/DVD drive shall be disabled. In addition the unused NIC ports shall be disabled and management ports like the HP ILO (HP Integrated Lights-Out) interface or console ports shall be either disabled or password protected.

16.3 Windows Server Hardening

Servers shall be part of a Windows Domain.

With the integration of the servers to a Windows domain, user permissions are assigned to network users managed by a central server. Since these user accounts often implement password strength and expiration rules, this integration may improve security over local accounts which do not have these restrictions.

Windows Updates

The Windows software patches and updates shall be installed and shall remain up to date. Windows updates often include patches to newly discovered security vulnerabilities, such as the Heartbleed SSL vulnerability, which affected millions of computers worldwide. Patches for these significant issues should be installed.

Anti-virus Software

Install anti-virus and anti-spyware software and keep it up to date.

16.4 CIS Benchmark Reference

For comprehensive Windows Server hardening, apply the **CIS Microsoft Windows Server Benchmark** (available at https://www.cisecurity.org/benchmark/microsoft_windows_server). The CIS Benchmark provides detailed, consensus-based security configuration guidelines covering:

- User Account Control (UAC) settings
- AutoPlay policies
- External device restrictions
- User rights assignment
- Screen saver and lockout policies
- Password policies
- Non-essential Windows services

Apply CIS Benchmark Level 1 as a baseline. For IQSIGHT BVMS servers, note the following deviations:

- BVMS services require specific Windows services to remain enabled — refer to the BVMS documentation for the list of required services.
- BVMS uses specific network ports that must remain open in the Windows Firewall (see Server Firewall Configuration).

16.5 Windows User Accounts and Lockout

The Windows Operating System user accounts have to be protected with complex passwords. Servers are normally managed and maintained with Windows administrator accounts; ensure that strong passwords are used for the administrator accounts.

Passwords must contain characters from three of the following categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: `~!@#$%^&*_-+=\` |(){}[]:;"'<>,.?/`
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase (includes Unicode characters from Asian languages)

Use of Windows Account Lockout to make it harder for password-guessing attacks to succeed. Windows 8.1 Security Baselines recommendation is 10/15/15:

Setting	Value
Account lockout duration	15 minutes
Account lockout threshold	10 failed logon attempts
Reset account lockout counter after	15 minutes

Ensure that all default passwords of the server and the Windows Operating System are replaced with new strong passwords.

16.6 Server Firewall Configuration

Enable communication of BVMS standard ports according to BVMS ports.

> **NOTICE**
>
> Refer to the BVMS documentation for relevant port settings and usage. Be sure to re-check settings on upgrades of firmware or software.

CHAPTER 17 — HARDENING STORAGE

iSCSI storage devices hold recorded video data and must be protected against unauthorized access.

17.1 iSCSI Security Best Practices

As IQSIGHT IP cameras or encoders are capable of establishing an iSCSI session directly to an iSCSI drive and write video data to an iSCSI drive, the iSCSI units have to be connected to the same LAN or WAN as the IQSIGHT peripheral devices.

To avoid unauthorized access to the recorded video data, the iSCSI units have to be protected against unauthorized access:

- Use password authentication via CHAP to ensure only known devices are allowed to access the iSCSI target. Set a CHAP password on the iSCSI target and enter the configured password in the VRM configuration. The CHAP password is valid for VRM and is sent to all devices automatically. If a CHAP password is used in a BVMS VRM environment, all storage systems have to be configured to use the same password.
- Remove all default usernames and passwords from the iSCSI target.
- Use strong password for administrative user accounts of the iSCSI target.
- Disable administrative access via Telnet to the iSCSI targets. Use SSH access instead.
- Protect console access to the iSCSI target via strong password.
- Disable unused network interface cards.
- Monitor system status of iSCSI storages via 3rd party tools to identify anomalies.

17.2 CHAP Password Configuration

When you set a global CHAP password in BVMS Configuration Client, this password is automatically transferred to all encoders, decoders and VSG devices.

For some iSCSI devices this function is not supported. You have to set the CHAP password on these devices manually.

> **NOTICE**
>
> You have to set the global CHAP password on the iSCSI devices before adding them to BVMS. iSCSI devices cannot be added to a BVMS configuration where the global CHAP password is already activated.

To manually set a CHAP password on an iSCSI device (for example DIVAR IP), which is based on a recent version of the Microsoft Windows Server operating system:

1. Open the **Server Manager** and navigate to **File and Storage Services > iSCSI**.
2. In the **ISCSI TARGETS** list, right-click the desired iSCSI target and click **Properties**.
3. In the **Properties** dialog box, click **Security**, then select the check box **Enable CHAP**.
4. Enter the following:
   - **User name:** `user`
   - **Password:** enter the global CHAP password as given in the BVMS Configuration Client (under the menu **Hardware > Protect iSCSI storages with CHAP password...**).
5. Click **OK**.

CHAPTER 18 — HARDENING WORKSTATIONS

Client workstations running BVMS Operator Client and Configuration Client require hardening to protect video data and system access.

18.1 Workstation Hardware Settings

The Windows desktop operating systems, used for BVMS Client applications like the BVMS Operator Client or Configuration Client, are installed outside of the secure area. The workstations have to be hardened to protect the video data, the documents and other applications against unauthorized access.

- Set a BIOS/UEFI password to restrict people from booting alternative operating systems.
- In order to prevent data transfer to the client, the USB ports and the CD/DVD drive shall be disabled. In addition the unused NIC ports shall be disabled.

18.2 Windows Workstation Hardening

- Workstation shall be part of a Windows Domain. Integration of the workstation to a Windows domain allows security relevant settings to be managed centrally.
- **Windows updates:** Stay up to date with Windows operating software patches and updates.
- **Installation of Antivirus software:** Install Antivirus and antispyware software and keep it up to date.

18.3 CIS Benchmark Reference

For comprehensive Windows workstation hardening, apply the **CIS Microsoft Windows Desktop Benchmark** (available at https://www.cisecurity.org/benchmark/microsoft_windows_desktop). The CIS Benchmark provides detailed, consensus-based security configuration guidelines covering:

- User Account Control (UAC) settings
- AutoPlay policies
- External device restrictions
- User rights assignment
- Screen saver and lockout policies
- Password policies
- Non-essential Windows services

Apply CIS Benchmark Level 1 as a baseline. For IQSIGHT BVMS workstations, note the following deviations:

- BVMS Operator Client and Configuration Client require specific Windows services to remain enabled — refer to the BVMS documentation for the list of required services.
- BVMS uses specific network ports that must remain open in the Windows Firewall (see Workstation Firewall Configuration).

Additional workstation-specific recommendations:

- Disable unused Windows Operating system accounts.
- Disable Remote Desktop Access to the client workstation.
- Run workstation with non-administrative rights to avoid that standard users change system settings.

18.4 Windows User Accounts and Lockout

The Windows Operating System user accounts have to be protected with complex passwords. Ensure that strong passwords are used for the administrator accounts.

Passwords must contain characters from three of the following categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: `~!@#$%^&*_-+=\` |(){}[]:;"'<>,.?/`
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase (includes Unicode characters from Asian languages)

Use of Windows Account Lockout to make it harder for password-guessing attacks to succeed. Windows 8.1 Security Baselines recommendation is 10/15/15:

Setting	Value
Account lockout duration	15 minutes
Account lockout threshold	10 failed logon attempts
Reset account lockout counter after	15 minutes

Ensure that all default passwords of the server and the Windows Operating system are replaced with new strong passwords.

18.5 Workstation Firewall Configuration

Enable communication of BVMS standard ports according to BVMS ports.

> **NOTICE**
>
> Refer to the BVMS documentation for relevant port settings and usage. Be sure to re-check settings on upgrades of firmware or software.

CHAPTER 19 — BVMS AND CONFIGURATION MANAGER

BVMS and Configuration Manager are the primary tools for managing IQSIGHT IP video systems. Securing these components protects the entire video infrastructure.

19.1 Password Management via Configuration Manager

Utilizing IQSIGHT Configuration Manager, passwords can be easily applied to individual or multiple devices simultaneously.

1. In the Configuration Manager, select one or more devices.
2. Select the **General** tab, then select **Unit Access**.
3. In the **Password** menu, enter and confirm the desired password for each of the three accounts (**Password 'service'**, **Password 'user'** and **Password 'live'**).
4. Click the save icon to push and save changes.

In larger installations that are managed by either BVMS, or Video Recording Manager installed on a recording appliance, global passwords can be applied to all IP video devices that are added to the system. This allows easy management and ensures a standard level of security across the entire network video system.

19.2 Password Management via VRM

The Video Recording Manager provides user management to enhance flexibility and security. By default, there are no passwords assigned to any of the user accounts. Password assignment is a critical step in protecting any network device. It is strongly advised to assign passwords to all installed network video devices.

The same is valid for the users of Video Recording Manager.

Additionally, members of a user group can be assigned to have access to certain cameras and privileges. Thus, a detailed user-based right-management can be achieved.

19.3 Password Management via BVMS

Device password protection

Cameras and encoders, managed by BVMS can be protected against unauthorized access with a password protection. Passwords for the built-in user accounts of encoders/cameras can be configured with the BVMS Configuration Client.

To set a password for the built-in user accounts in the BVMS Configuration Client:

1. In the Device tree, select the desired encoder.
2. Right-click the encoder and click **Change password...**.
3. Enter a password for the three built-in user accounts live, user and service.

Default password protection

BVMS versions 5.0 and higher provide the ability to implement global passwords on all devices in a video system of up to 2000 IP cameras. This feature can be accessed either via the BVMS Configuration Wizard when working with DIVAR IP 3000 or DIVAR IP 7000 recording appliances, or through BVMS Configuration Client on any system.

To access the global passwords menu in BVMS Configuration Client:

1. On the **Hardware** menu, click **Protect Devices with Default Password...**.
2. In the **Global default password** field, enter a password and select **Enforce password protection on activation**.

After saving and activating system changes, the entered password will be applied to the live, user, and service accounts of all devices, including the administrator account of Video Recording Manager.

> **NOTICE**
>
> If the devices already have existing passwords set in any of the accounts, they will not be overwritten. For example, if password is set for service but not for live and user, global password will only be configured for live and user accounts.

BVMS configuration and VRM settings

By default, the BVMS uses the built-in administration account **srvadmin** to connect to Video Recording Manager with a password protection. To avoid unauthorized access to Video Recording Manager, the admin account **srvadmin** shall be protected with a complex password.

To change the password of the srvadmin account in BVMS Configuration Client:

1. In the Device tree, select the VRM device.
2. Right-click the VRM device and click **Change VRM Password**.
3. Enter a new password for the **srvadmin** account and click **OK**.

19.4 Encrypted Communication with BVMS

Since BVMS version 7.0, live video data and control communication between the camera and the BVMS Operator Client, Configuration Client, Management Server and Video Recording Manager can be encrypted.

After enabling the secure connection in the **Edit Encoder** dialog box, the BVMS Server, Operator Client and Video Recording Manager will use a secure HTTPS connection in order to connect to a camera or encoder.

The BVMS internally used connection string will change from `rcpp://a.b.c.d` (plain RCP+ connection on port 1756) to `https://a.b.c.d` (HTTPS connection on port 443) instead. For legacy devices that do not support HTTPS the connection string remains unchanged (RCP+).

If selecting the HTTPS communication, the communication will utilize HTTPS (TLS) to encrypt all control communication and video payload via the encryption engine in the device. When utilizing TLS, all HTTPS control communication and video payload is encrypted with an AES encryption key up to 256 bits in length.

To enable the encrypted communication in BVMS Configuration Client:

1. In the Device tree, select the desired encoder/camera.
2. Right-click the encoder/camera and click **Edit Encoder**.
3. In the **Edit Encoder** dialog box, enable **Secure connection**.
4. Save and activate the configuration.

After enabling the secure connection to the encoder, other protocols can be disabled (see Feature Descriptions and Recommendations in Chapter 12).

> **NOTICE**
>
> BVMS only supports the default HTTPS port 443. Usage of different ports is not supported.

19.5 SSH Tunneling for Remote Access

For a remote device access with BVMS Operator Client via public networks, BVMS provides Secure Shell (SSH) tunneling to ensure secure (encrypted) communication.

SSH tunnelling constructs an encrypted tunnel established by an SSH protocol/socket connection. This encrypted tunnel can provide transport to both, encrypted and un-encrypted traffic. The IQSIGHT SSH implementation also utilizes Omni-Path protocol, which is a high performance low latency communications protocol developed by Intel.

For more information on how to configure the SSH service in BVMS, refer to the BVMS documentation.

For more information on how to configure DIVAR IP systems for a secure remote access with BVMS Operator Client, refer to the DIVAR IP documentation.

APPENDICES

APPENDIX A – HARDENING CHECKLIST

Use this checklist during deployment or audit of IQSIGHT IP video systems.

IP Cameras and Encoders

- ☐ Passwords assigned to all user accounts (service, user, live)
- ☐ SNMPv3 enabled if monitoring required
- ☐ Password reset mechanism disabled (if not needed)
- ☐ HSTS enabled
- ☐ 802.1x enabled (if network infrastructure supports it)
- ☐ Syslog configured (TCP or TLS)
- ☐ IPv4 filter configured to restrict access
- ☐ Time synchronization configured (SNTP or TLS Date)
- ☐ Software sealing enabled
- ☐ Firmware updated to latest version

Servers (BVMS, VRM)

- ☐ Installed in physically secured area with access control
- ☐ BIOS/UEFI password set
- ☐ USB ports and CD/DVD drives disabled
- ☐ Unused NIC ports disabled
- ☐ Management ports (ILO) disabled or password-protected
- ☐ Server joined to Windows Domain
- ☐ Windows updates current
- ☐ Anti-virus software installed and up to date
- ☐ CIS Windows Server Benchmark Level 1 applied
- ☐ All default passwords replaced with strong passwords
- ☐ Account lockout configured (10/15/15)
- ☐ Windows Firewall enabled with BVMS port exceptions
- ☐ BVMS srvadmin password changed from default

Storage (iSCSI)

- ☐ CHAP password configured on all iSCSI targets
- ☐ Default usernames and passwords removed
- ☐ Telnet disabled; SSH used for administrative access
- ☐ Console access protected with strong password
- ☐ Unused network interfaces disabled

Workstations (Operator Client, Configuration Client)

- ☐ BIOS/UEFI password set
- ☐ USB ports and CD/DVD drives disabled
- ☐ Workstation joined to Windows Domain
- ☐ Windows updates current
- ☐ Anti-virus software installed and up to date
- ☐ CIS Windows Desktop Benchmark Level 1 applied
- ☐ All default passwords replaced with strong passwords
- ☐ Account lockout configured (10/15/15)
- ☐ Remote Desktop Access disabled
- ☐ Non-administrative user accounts used for daily operation
- ☐ Windows Firewall enabled with BVMS port exceptions

APPENDIX B — COMPLIANCE MAPPING

The following tables map this guidebook's chapters to NIST Cybersecurity Framework (CSF) functions and IEC 62443 requirements.

NIST CSF Mapping

NIST CSF Function	Guidebook Chapter
Identify (ID)	Ch 1 Threat Landscape, Ch 2 Security Frameworks
Protect (PR) — Access Control	Ch 5 Identity and Authentication, Ch 11 Camera Passwords, Ch 19 BVMS Password Management
Protect (PR) — Data Security	Ch 6 Cryptography and PKI, Ch 13 Camera Certificates
Protect (PR) — Information Protection	Ch 4 Network Security, Ch 12 Camera Hardening, Ch 16–18 Server/Storage/Workstation Hardening
Protect (PR) — Maintenance	Ch 9 Lifecycle Management
Protect (PR) — Protective Technology	Ch 3 Zero Trust, Ch 7 Supply Chain Security
Detect (DE)	Ch 8 Monitoring and Incident Response
Respond (RS)	Ch 8.3 Vulnerability Management, Ch 8.4 Incident Response
Recover (RC)	Ch 9 Lifecycle Management

IEC 62443 Mapping

IEC 62443 Requirement	Guidebook Chapter
Zones and conduits	Ch 4 Network Security (VLANs, VPNs, segmentation)
User identification and authentication	Ch 4.2 Network Access Control (802.1x), Ch 5 Identity and Authentication, Ch 11 Camera Passwords
Use control / least privilege	Ch 11.1.2 Access Rights Groups
Data integrity and confidentiality	Ch 6 Cryptography and PKI, Ch 13.3 Video Authentication
Restricted data flow	Ch 4.1 Network Segmentation, Ch 12.5 IPv4 Filtering
Timely response to events	Ch 8 Monitoring and Incident Response
Resource availability	Ch 16–18 Server/Storage/Workstation Hardening
Component security (SL-C)	Ch 10 Camera Architecture, Ch 7 Supply Chain Security

APPENDIX C — ADDITIONAL RESOURCES

For more information, software downloads, and documentation, go to the respective product page in the product catalog: http://www.iqsight.com

GLOSSARY

802.1x — The IEEE 802.1x standard provides a general method for authentication and authorization in IEEE-802 networks. Authentication is carried out via the authenticator, which checks the transmitted authentication information using an authentication server (see RADIUS server) and approves or denies access to the offered services (LAN, VLAN or WLAN) accordingly.

Authentication — Process of verifying the identity of a user, device, or service before granting access.

CHAP — Challenge-Handshake Authentication Protocol: an authentication scheme used to verify the identity of a client connecting to an iSCSI target.

CIS Benchmark — A set of best-practice security configuration guidelines published by the Center for Internet Security for hardening operating systems and applications.

CVSS — Common Vulnerability Scoring System: a free and open industry standard for assessing the severity of computer system security vulnerabilities, with scores ranging from 0 to 10.

Device — Hardware component such as camera, encoder/decoder, NVR, DiBos, analog matrix, ATM/POS bridge.

DHCP — Dynamic Host Configuration Protocol: uses an appropriate server to enable dynamic assignment of an IP address and other configuration parameters to computers on a network (Internet or LAN).

Hardening — Process of increasing the security of a system by only using dedicated software that is necessary for systems operation, applying specific protective settings, and removing software that is not mandatory.

HTTP — Hypertext Transfer Protocol: protocol for transmitting data over a network.

HTTPS — Hypertext Transfer Protocol Secure: encrypts and authenticates communication between Web server and browser.

IEC 62443 — An international series of standards addressing cybersecurity for industrial automation and control systems, including physical security systems.

IPv4 address — A 4-byte number uniquely defining each unit on the Internet. It is usually written in dotted decimal notation, for example `209.130.2.193`.

LAN — Local Area Network. This is a network that connects devices within a confined geographical area.

Multicast — Communication between a single transceiver and multiple receivers on a network by distribution of a single data stream on the network to a number of receivers in a defined group. Requirement for multicast operation is a multicast compliant network with implementation of the UDP protocol and the IGMP protocol.

Net mask — A mask that explains which part of an IP address is the network address and which part is the host address. It is usually written in dotted decimal notation, for example `255.255.255.192`.

NIST CSF — National Institute of Standards and Technology Cybersecurity Framework: a voluntary framework of standards, guidelines, and best practices to manage cybersecurity risk.

ONVIF — Open Network Video Interface Forum. Global standard for network video products. ONVIF conformant devices are able to exchange live video, audio, metadata, and control information and ensure that they are automatically discovered and connected to network applications such as video management systems.

PKI — Public Key Infrastructure: the systems needed to generate, distribute, and manage digital certificates.

PSIRT — Product Security Incident Response Team: a team responsible for coordinating the response to security vulnerabilities in a vendor's products.

RADIUS server — Remote Authentication Dial-In User Service: a client/server protocol for the authentication, authorization and accounting of users with dial-up connections on a computer network. RADIUS is the de-facto standard for central authentication of dial-up connections via Modem, ISDN, VPN, Wireless LAN (see 802.1x) and DSL.

RCP+ — Remote Control Protocol: a proprietary IQSIGHT protocol which uses specific static ports to detect and communicate with IQSIGHT IP video devices.

RTSP — Real Time Streaming Protocol. A network protocol which allows to control the continuous transmission of audio-visual data or software over IP-based networks.

SIEM — Security Information and Event Management: a system that collects, correlates, and analyzes log data from multiple sources to detect security threats.

SNMP — Simple Network Management Protocol; a protocol for network management, for managing and monitoring network components.

SSL — Secure Sockets Layer; an outdated encryption protocol for data transmission in IP-based networks (see TLS).

TCP — Transmission Control Protocol. Connection-oriented communication protocol used to transmit data over an IP network. Offers a reliable and ordered data transmission.

Telnet — Login protocol with which users can access a remote computer (Host) on the Internet.

TLS — Transport Layer Security. TLS 1.0 and 1.1 are the standard advanced developments of SSL 3.0 (see SSL). Modern devices use TLS 1.2 or 1.3.

TPM — Trusted Platform Module: a hardware chip that provides secure storage for cryptographic keys and certificates.

TTL — Time-To-Live; life cycle of a data packet in station transfers.

UDP — User Datagram Protocol. A connectionless protocol used to exchange data over an IP network. UDP is more efficient than TCP for video transmission because of lower overhead.

User group — User groups are used to define common user attributes, such as permissions, privileges and PTZ priority. By becoming a member of a group, a user automatically inherits all the attributes of the group.

VPN — A virtual private network (VPN) implements a private network within a public network, such as the Internet. Network traffic within the VPN is encrypted and so protected from espionage.

Wide Area Network — A long distance link used to extend or connect remotely located local area networks.

Zero Trust — A security model that requires strict identity verification for every person and device attempting to access resources, regardless of whether they are inside or outside the network perimeter.