

VideoEdge Hardening guide



GPS0017-CE-EN
Version 6.2
Rev A
Revised 01.26.2024

Introduction



Our solution provides peace of mind to our customers with a holistic cyber mind set beginning at initial design concept, continues through product development, and is supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.

The Hardening Guide intends to provide cybersecurity guidance used in planning, deployment, and maintenance periods.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution's functional operation.

This guide provides hardening guidance for configuration and maintenance, including the operating system, user accounts, permissions and roles, backup and restore, redundancy, and patch management.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided "as is", and Johnson Controls makes no representation or warranty, expressed or implied, as to the efficacy of the cybersecurity practices or recommendations described within. Johnson Controls disclaims all liability for any damages that may occur because of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Contents

| | |
|--|----|
| Introduction..... | 2 |
| Legal disclaimer..... | 3 |
| 1 Planning..... | 8 |
| 1.1.0 VideoEdge overview | 8 |
| 1.1.1 Deployment architecture..... | 8 |
| 1.1.2 Components..... | 9 |
| 1.1.3 Supporting components..... | 9 |
| 1.2.0 Security feature set..... | 9 |
| 1.2.1 Easy security configuration..... | 10 |
| 1.2.2 Human user account safeguards..... | 10 |
| 1.2.3 User authentication safeguards | 11 |
| 1.2.4 Camera authentication | 11 |
| 1.2.5 User authorization | 11 |
| 1.2.6 Camera authorization | 11 |
| 1.2.7 Secure communications | 11 |
| 1.2.8 Digital certificate management | 12 |
| 1.2.9 Audit logs | 12 |
| 1.2.10 Availability assurance..... | 12 |
| 1.2.11 Alarms and alerts | 12 |
| 1.2.12 Media encryption..... | 13 |
| 1.2.13 Software updates | 14 |
| 1.2.14 Compliance “ready”..... | 14 |
| 1.2.15 Encryption ciphers..... | 14 |
| 1.3.0 Intended environment | 15 |
| 1.3.1 Internet connectivity | 15 |
| 1.3.2 Integration with IT networks..... | 15 |
| 1.3.3 Integration with external systems | 15 |
| 1.4.0 Hardening methodology | 15 |
| 1.4.1 User management best practices..... | 15 |
| 1.5.0 VideoEdge data flow diagram | 17 |
| 1.5.1 Communication paths table | 19 |
| 1.6.0 Network planning | 22 |
| 1.6.1 Trust boundaries overview | 22 |
| 1.6.2 Network protection | 22 |
| 1.6.3 Endpoint protection support..... | 23 |
| 1.7.0 Anti-virus..... | 23 |
| 1.8.0 Hardware and software requirements | 23 |

| | | |
|-------|---|----|
| 1.8.1 | Required services..... | 23 |
| 1.8.2 | Internet service table | 24 |
| 2 | Deployment | 25 |
| 2.1.0 | Deployment overview..... | 25 |
| 2.1.1 | Getting started..... | 25 |
| 2.1.2 | Physical installation considerations | 25 |
| 2.1.3 | Default security behavior | 25 |
| 2.1.4 | Resetting to factory defaults | 26 |
| 2.1.5 | Considerations for commissioning..... | 26 |
| 2.1.6 | Recommended knowledge level..... | 26 |
| 2.2.0 | Hardening | 26 |
| 2.2.1 | Hardening checklist..... | 27 |
| 2.2.2 | Administration | 29 |
| 2.2.3 | BIOS configuration | 32 |
| 2.2.4 | Set boot sequence | 32 |
| 2.2.5 | User management..... | 32 |
| 2.2.6 | User management overview..... | 48 |
| 2.3.0 | Additional operating system hardening | 49 |
| 2.4.0 | Software updates..... | 54 |
| 2.4.1 | Operating System updates | 54 |
| 2.4.2 | VideoEdge application updates | 54 |
| 2.4.3 | Camera updates..... | 55 |
| 2.5.0 | Communication hardening | 55 |
| 2.5.1 | Communication management best practices..... | 55 |
| 2.5.2 | Communication port and encryption configuration | 55 |
| 2.5.3 | Communication certificate support..... | 60 |
| 2.5.4 | FIPS 140-2 support | 65 |
| 2.6.0 | Configuring security monitoring features | 66 |
| 2.6.1 | Audit logs | 66 |
| 2.6.2 | SIEM integration..... | 66 |
| 2.6.3 | SNMP..... | 66 |
| 2.6.4 | Security alerts | 67 |
| 2.7.0 | Availability hardening | 69 |
| 2.7.1 | Backup/Restore..... | 69 |
| 2.7.2 | Redundant server failover | 72 |
| 2.7.3 | RAID storage..... | 72 |
| 2.7.4 | Network isolation..... | 72 |
| 2.8.0 | Security audits and documentation | 76 |

| | | |
|------------|---|----|
| 2.8.1 | Security documentation | 76 |
| 2.8.2 | Security audit checklist | 76 |
| 3 | Maintain | 77 |
| 3.1.0 | Cybersecurity maintenance checklist | 77 |
| 3.1.1 | Backup runtime data | 78 |
| 3.1.2 | Backup configuration data | 78 |
| 3.1.3 | Test backup data | 78 |
| 3.1.4 | Assure failover solutions are operating | 78 |
| 3.1.5 | Lock accounts on termination of employment | 78 |
| 3.1.6 | Remove inactive user accounts | 79 |
| 3.1.7 | Update user account roles | 79 |
| 3.1.8 | Disable unused features, ports, and services | 79 |
| 3.1.9 | Check for and prioritize advisories | 80 |
| 3.1.10 | Plan and execute advisory recommendations | 80 |
| 3.1.11 | Check and prioritize patches and updates | 80 |
| 3.1.12 | Plan and execute software patches and updates | 80 |
| 3.1.13 | Review organizational policy updates | 81 |
| 3.1.14 | Review updates to regulations | 81 |
| 3.1.15 | Update as-build documentation | 81 |
| 3.1.16 | Conduct security audits | 81 |
| 3.1.17 | Update password policies | 82 |
| 3.1.18 | Update standard operating procedures | 82 |
| 3.1.19 | Update logon banners | 82 |
| 3.1.20 | Renew licensing agreements | 82 |
| 3.1.21 | Renew support contracts | 82 |
| 3.1.22 | Check for end-of-life announcements and plan for replacements | 83 |
| 3.1.23 | Periodically delete sensitive data in accordance with policies or regulations | 83 |
| 3.1.24 | Monitor for cyber attacks | 83 |
| 3.2.0 | Patch policy | 83 |
| | Release schedule | 84 |
| 3.3.0 | Recovery and factory reset | 84 |
| 3.4.0 | VideoEdge testing process | 84 |
| 3.5.0 | Customer specific testing | 84 |
| 3.5.1 | Vulnerability assessment | 85 |
| 3.5.2 | Vulnerability assessment – third party components | 85 |
| 3.5.3 | Vulnerability assessment – third party software | 85 |
| 3.5.4 | VideoEdge vulnerability reporting | 85 |
| Appendix A | Third party attestations and certificates | 87 |

Appendix B Third party security approvals..... 88

- FISMA..... 88
- NERC CIP v5..... 88
- DISA 88

Appendix C.1 Operating system level user accounts (non-interactive)..... 89

Appendix C.2 Operating system level service accounts (non-interactive) 91

Appendix C.3 Operating system level user accounts (interactive)..... 92

ANNEX D - Email Alerts 93

1 Planning

This section is designed to help plan for the deployment of VideoEdge. The contents within this section are useful in several planning stage functions:

- Assuring compliance with the cybersecurity criteria that governs the target environment.
- Designing the deployment architecture
- Providing a reference for settings made during deployment

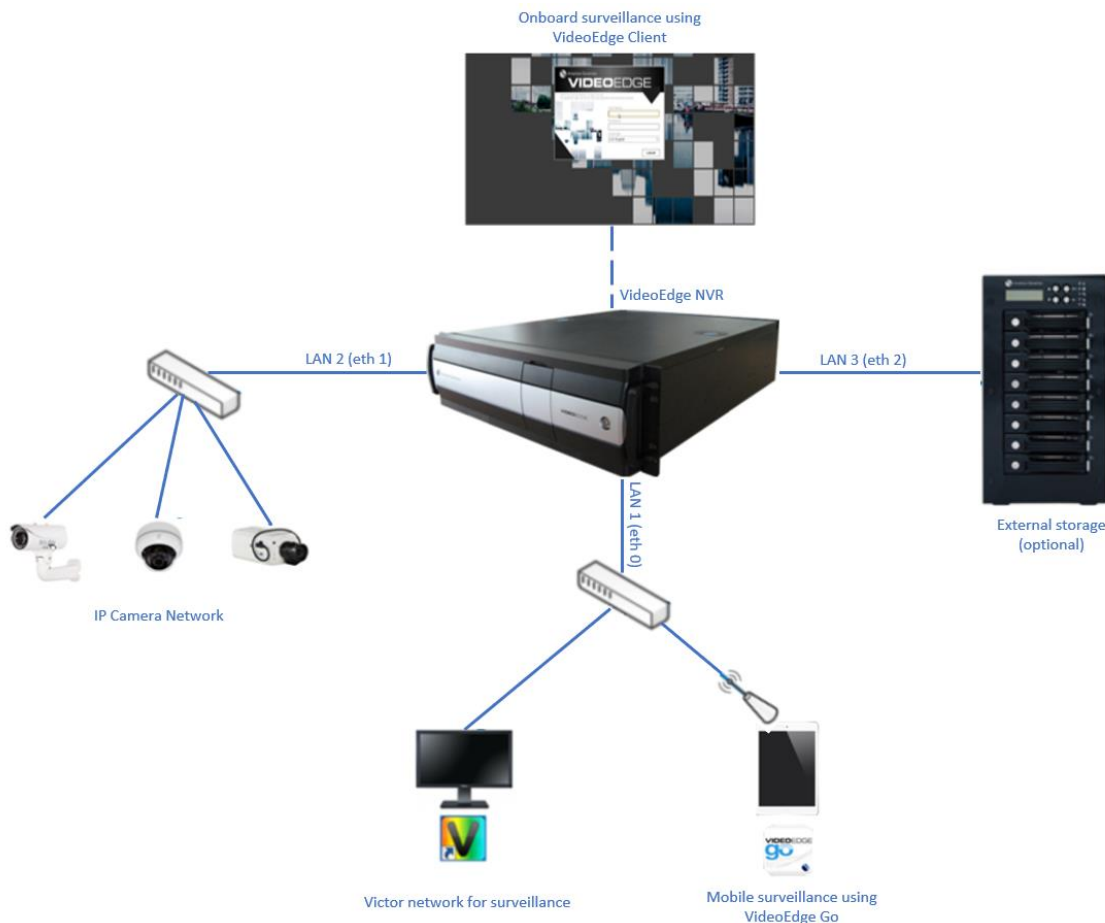
1.1.0 VideoEdge overview

VideoEdge is a network video recorder (NVR), available with a full range of intuitive clients to manage surveillance in very active environments with both onsite and remote accessibility options. VideoEdge is scalable from a single NVR to a large multi-site architecture. Users can easily deploy any number of cameras, adding licenses at any time. You can use built-in intelligence to tailor viewing conditions. Users can receive multiple live, recorded, alarm, and meta-data collection video streams. VideoEdge has optimized video streaming that requires less network bandwidth, CPU, and memory resources than comparable systems. Multicast video streams further reduce the bandwidth required for streaming high-quality video.

When a victor client connects with VideoEdge NVRs, it can leverage high-performance video streaming capabilities, while gaining access to the expansive feature set of VideoEdge, including audio and motion meta-data. Visit the victor web page for more information on the victor solution deployment architecture.

1.1.1 Deployment architecture

Figure 1.1.1.1



1.1.2 Components

VideoEdge is available as several different models that share the same cybersecurity capabilities. This guide covers all variations of VideoEdge models.

VideoEdge NVR - VideoEdge NVR is available in various physical sizes, storage capacities, and camera ports, making it capable of handling a variety of customer needs.

1.1.3 Supporting components

VideoEdge is designed to be compatible with standard IP video and networking components which are often included as part of the deployment architecture:

IP Camera – An IP camera is a surveillance camera that communicates over the Ethernet using IP addressing. While VideoEdge supports third-party IP cameras, Illustra IP cameras offer enhanced functionality when coupled with a VideoEdge NVR. (Refer to Illustra Security Hardening Guide for more details).

IP encoder - An IP encoder converts an analog surveillance camera signal to a digital signal and can stream the resulting digital signal over Ethernet using an IP address.

PoE Camera - An IP enabled surveillance camera that receives its power from the Ethernet cable – Power over Ethernet (PoE).

Network Switch - A VideoEdge system can utilize standard off the shelf networking switches that are rated for the communication speeds of the IP video streams.

PoE Switch - A PoE Camera may be powered by a standard off the shelf PoE Switch rated for the speed and power requirements of the PoE camera.

1.2.0 Security feature set

All VideoEdge models support the following features:

Table 1.2.0.1: Feature summary table

| Section | Type | Feature name | New feature |
|---------|--------------------------------|----------------------------------|-------------|
| 1.2.1 | Easy security configuration | Security Dashboard | - |
| | | Enhanced security mode | v5.3 |
| 1.2.2 | Human user account safeguards | No backdoor passwords | - |
| | | User account password policy | - |
| | | Password policy | - |
| 1.2.3 | User authentication safeguards | Enhanced password validation | - |
| | | Hidden password entry | - |
| | | Maximum login attempts | - |
| | | Local user authentication | - |
| 1.2.4 | Camera authentication | LDAP support | - |
| | | Active Directory support | - |
| | | (As supported by camera) | - |
| | | Role Based Access Control (RBAC) | - |
| 1.2.5 | User authorization | Role based camera access | v5.3 |
| | | Object level permissions | - |
| 1.2.6 | Camera authorization | (As supported by camera) | - |
| 1.2.7 | Secure communications | Configurable network ports | - |

| | | | |
|---------------|--------------------------------|---|--------|
| | | Configurable web server | - |
| | | Remote access controls | v5.1 |
| | | Isolated camera LAN | - |
| | | Firewall | - |
| | | SNMP v2c support | - |
| | | SSH support (disabled by default) | v5.1 |
| | | TLS v1.2 only | v5.7 |
| | | HTTPS support | - |
| | | LPR metadata encryption and key export / import | V6.1.1 |
| 1.2.8 | Digital certificate management | View certificates | - |
| | | Third party certificate support | - |
| 1.2.9 | Audit logs | Audit logs | - |
| | | - enabled by default | - |
| | | - time synchronized | - |
| | | - delete protected | - |
| | | - no removable storage | - |
| 1.2.10 | Availability assurance | Redundancy failover | - |
| | | Backup and restore | - |
| 1.2.11 | Alarms and alerts | Real-time notifications | - |
| | | Tamper detection | - |
| 1.2.12 | Media encryption | Supports media encryption and key export / import | v5.4 |
| 1.2.13 | Software updates | Camera firmware mass update | v5.3 |
| 1.2.14 | Compliance “Ready” | FISMA | - |
| | | NERC CIP v5 | - |
| | | DISA | - |
| 1.2.15 | Encryption ciphers | VideoEdge TLS ciphers are regularly reviewed | V6.1 |

1.2.1 Easy security configuration

Security Dashboard - View, monitor and assess the security of VideoEdge from a common dashboard.

Enhanced security mode – a single setting in the installation wizard can force the replacement of the default user accounts, activate additional password security measures, and disable HTTP and UPnP access.

Upon initial install https-only is set by default, certificate creation is performed in the install wizard.

1.2.2 Human user account safeguards

No backdoor passwords – VideoEdge does not have a backdoor password.

User account password policy – VideoEdge contains rules which govern password formation, expiration, reuse, and other restrictions including password length, history, and complexity.

Enhanced password validation – a mode which enforces restrictions when setting or changing passwords:

- Passwords must be different than the previous three passwords. This setting is configurable within a range of three to ten. Please note that the default value is three. Passwords must differ from the previous password by a minimum of three characters
- Passwords must be a minimum of fifteen characters long and must contain a mixture of upper and lower case letters, numbers, and special characters

Linux user passwords cannot contain the username, permutations of a dictionary word, or be comprised of trivial patterns. These restrictions apply in enhanced and standard security modes. NVR passwords cannot contain the username, and in enhanced security mode are subject to the rules in **Enhanced password validation**, cannot be permutations of a dictionary word, or be comprised of trivial patterns.

All passwords must be changed upon initial install. In enhanced security mode, usernames must also be changed.

1.2.3 User authentication safeguards

Hidden password entry - password entries are hidden from view as the user enters them.

Maximum login attempts - restricts the user to the configured number of consecutive authentication attempts allowed before that account is locked from further authentication retries.

Microsoft Active Directory support - enables centralized authentication using a Microsoft Active Directory server for the management of user accounts and logon authentication by LDAP (see LDAP support).

LDAP support – enables centralized authentication using a Lightweight Directory Access Protocol (LDAP) compliant authentication server for the management of user accounts and logon authentication. VideoEdge implementation of LDAP provides the following functions:

- LDAP & Active Directory authentication and authorization for the VideoEdge admin GUI.
- LDAP & Active Directory authentication and authorization for the VideoEdge API.
- Secure connections using TLS

1.2.4 Camera authentication

As supported by camera - VideoEdge authenticates with a connected camera using a username and password stored in the camera.

1.2.5 User authorization

Role Based Access Control (RBAC) – Authorizations can be assigned to a role which users are members of. The user inherits the authorizations of each role they are a member of.

Role based camera access - Camera permissions to restrict camera access to specific VideoEdge roles: viewer1, viewer2, and viewer3. These camera permissions are enforced for all applicable clients including VideoEdge 'Local' Client, victor Web LT, and VideoEdge GO.

1.2.6 Camera authorization

As supported and configured by each specific camera - Authorizations for a connected camera are restricted to the functions authorized for that camera's user account being used to connect with VideoEdge.

1.2.7 Secure communications

Configurable network ports – Administrators can manage the settings of network ports.

Configurable web server – Administrators can disable HTTP support, change the web server ports, and restrict admin GUI access.

Remote access controls – Administrators can control remote access by enabling/disabling Remote Desktop Protocol (xRDP), which is disabled by default.

Isolated camera LAN – VideoEdge can be deployed so that connected cameras are on an isolated local area network (LAN).

Firewall – VideoEdge includes a firewall that you can configure with security rules to monitor and control incoming and outgoing network traffic.

SNMP v2c support – You can use Simple Network Management Protocol (SNMP) for network management and monitoring of VideoEdge by network monitoring tools. SNMP version 2c provides a level of security not available in SNMP version 1. SNMP v2c is also used on the VideoEdge server to monitor status of optional VideoEdge functions, such as failover and connectivity with victor clients.

SSH - VideoEdge uses Secure Shell (SSH) for remote access to the server and is also used for failover functionality status monitoring. SSH is disabled by default.

TLS v1.2 – VideoEdge uses Transport Layer Security (TLS) for encrypted communication including web-based HTTPS communications. Only TLS version 1.2 is supported.

LPR metadata encryption and key export / import – LPR metadata encryption is enabled by default. The encryption key is included in VideoEdge system backups but can also be exported and imported directly in the event that a media drive needs to be transferred to another recorder.

Note: As of version 5.0, the VNC communication protocol is no longer available.

1.2.8 Digital certificate management

Administrators can view the details of the installed certificate: subject, issuer name, and validity dates.

Administrators can generate a self-signed certificate, or upload a certificate signed by a trusted third party.

Important: It is the customer’s responsibility to deploy a suitable security certificate.

1.2.9 Audit logs

Audit logs - Activity and events from VideoEdge are stored in audit log records that administrators can access to view evidence of the activities that have affected the system and indicate the timestamped operation, procedure, or event. System and boot logs are recorded along with the logs from the VideoEdge application.

- Enabled by default – VideoEdge is preconfigured to record activity and events in an audit log.
- Time synchronized – VideoEdge audit log timestamps are synchronized to a common reference clock for the system.
- Delete protected – VideoEdge audit logs are protected from deletion.
- No removable storage – VideoEdge prevents the storage of audit logs on removable storage.

1.2.10 Availability assurance

Redundancy failover – You can configure a backup VideoEdge server to maintain a real-time copy of the VideoEdge configuration and run-time data whereby its services can continue using an automatic failover process if the primary system is not available.

Backup and Restore – A backup copy of the VideoEdge configuration and run-time data that can restore a VideoEdge server.

1.2.11 Alarms and alerts

Real-time notifications – VideoEdge provides real-time notification of alarms and alerts by email that may indicate a condition that may impact the secure operation of VideoEdge including:

- Analog Handler Reboot
- Archive
- Area Temperature
- Audio Malfunction
- Blur Detection
- Camera Dark Frame
- Camera Media Injection

- Camera Processing Malfunction
- Camera Video Loss
- Centralized License Server
- Clip Storage
- Device Not Recording
- Dry Contact
- Face Detection
- Failover
- License Plate Recognition
- Log Storage Space Low
- Motion Detection
- NIC
- OS Storage Space Low
- Security Alert
- Security Configuration Change
- Sensor Event
- Spot Temperature
- Storage
- Storage Activation
- Storage Configuration Change
- Storage Retention
- System
- System Reboot
- Tamper detection
- Text Stream
- Video Analytics Abandoned / Removed
- Video Analytics Crowd Formation
- Video Analytics Direction
- Video Analytics Dwell
- Video Analytics Enter
- Video Analytics Exit
- Video Analytics Linger
- Video Analytics Object Detection
- Video Analytics Perimeter
- Video Analytics Queue Analysis
- Video Analytics Tripwire

Tamper detection – VideoEdge can provide notification of a detection camera tamper alert received from the camera.

1.2.12 Media encryption

VideoEdge supports media encryption on freshly installed systems. The encryption key is included in VideoEdge system backups but can also be exported and imported directly in the event that a media drive needs to be transferred to another recorder.

A procedure is available for enabling encryption in the RAID card if you have deployed self-encrypting drives.

1.2.13 Software updates

Camera firmware mass update – Using the camera firmware update page, a user can select one or more cameras of the same model (limited to Illustra using iAPI3), upload the desired firmware, and then perform an upgrade. They can cancel an update, this will complete the current update, and remove any queued updates.

1.2.14 Compliance “ready”

The VideoEdge NVR has been deployed in many sites that require accreditation. Here you can find overviews of accreditations and resources that may be used to assist in meeting the requirements of each.

FISMA – You can configure the VideoEdge system to support the controls necessary for overall FISMA compliance. These controls include:

- Authenticated system access
- Account login/log out management
- Role-based separation of capabilities, permissions, and privileges
- System event and configuration change auditing, alerting, and management
- Restriction of ports, protocols, and services to only those ports, protocols and services required
- Encrypted communications

For more information, refer to the VideoEdge FISMA-Ready Compliance Guide available on the Cyber Protection website.

NERC CIP v5 - The VideoEdge NERC-CIP V5 READY Compliance Guide provides an overview of the NERC-CIP standard and describes how VideoEdge may be configured to meet the requirements of the NERC-CIP v5 requirements. When used in conjunction with VideoEdge installation and configuration guides, this information should assist in the installation of a compliant system and provide the necessary information for an audit.

For more information, refer to the VideoEdge NERC-CIP v5 Compliance Guide available on the Cyber Protection website.

Defense Information Systems Agency (DISA) - To assist installations within the Department of Defense in meeting the security hardening requirements of DISA, Tyco Security Products has developed this System Security Requirements guide based on the DISA General Purpose operating Systems STG, Version 1, Release 3 published 22 January 2016, for the sole purposes of meeting said requirements for the VideoEdge Network Video Recorder (NVR) appliance. We have provided the 250 technical control requirements of the General-Purpose Operating System Security Requirements Guide (SRG) and a description of how a VideoEdge device meets the technical controls or if it does not meet the controls, guidance has been provided so the customer can configure VideoEdge to meet the requirements.

For more information, refer to the VideoEdge - DISA Security Requirements available on the Cyber Protection website.

1.2.15 Encryption ciphers

The minimum supported encryption key strength in VideoEdge is 256 bits.

By default, VideoEdge only supports ciphers with perfect forward secrecy and strong encryption algorithms. Specifically:

- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256

1.3.0 Intended environment

The VideoEdge server is installed on premise within a data center equipment rack with restricted access.

1.3.1 Internet connectivity

This product does not require Internet access.

1.3.2 Integration with IT networks

The server components for this system are often deployed on a dedicated and isolated network. VLANs may be used to share infrastructure but maintain isolation. It is typical for clients to be installed on shared IT networks.

1.3.3 Integration with external systems

VideoEdge can be integrated with Microsoft Active Directory and the victor video management system.

1.4.0 Hardening methodology

While VideoEdge provides many onboard security safeguards, including many secure-by-default settings, we recommend that the device is hardened according to the guidance outlined in section 2, deployment.

Generally, a defense-in-depth strategy employing standard IT hardening methods and compensating controls as needed to compliment the base security features of each component.

1.4.1 User management best practices

Following best practices for managing user accounts, their credentials, and authorizations (permissions) can greatly improve the security for the system. Some guidance is presented in this section. For additional guidance NIST standards such as SP 800-63 Digital Identity Guidelines may be consulted.

You can create unique user accounts for each operator of VideoEdge. A role-based access control (RBAC) controls the operator functions in VideoEdge. With RBAC, a user is assigned a role in which they acquire the permissions associated with that role.

The proper configuration of individual user accounts assures that security best practices are followed and that all user actions cannot be repudiated. Best practices for account management include:

1.4.1.1 No shared accounts

Unique accounts should be used during all phases of operation for VideoEdge. Installers, technicians, auditors, and other deployment phase users should never share common user accounts to assure a non-repudiable audit trail of their actions.

When user accounts are shared, it no longer becomes possible to determine which specific operator performed actions on VideoEdge. While VideoEdge still logs a user's actions, the user can repudiate that they used VideoEdge at that time. Furthermore, sharing of user accounts makes the application of least privilege and separation of duties more challenging.

1.4.1.2 Remove or rename default user accounts (as permitted)

By removing or renaming default user accounts, the ability to gain unauthorized access to the system will be reduced as those attempting to do so will need to enter an unpublished username which is much harder to gain knowledge of. When a default user account cannot be removed or renamed, the best practice is to at least change their default passwords (see Change default passwords).

1.4.1.3 Change default passwords

Default passwords should be changed as these published defaults are easily guessed by unauthorized users and automated scripts can use them to gain access.

1.4.1.4 *Least privilege*

When assigning access rights users should only be given access to what they need to access to do their job. The VideoEdge NVR assists with privilege management by using role-based authorization for actions such as operator access, general system configuration, software installation, access to PTZ, and clip export features. This way, users may be assigned only responsibilities required for their function.

1.4.1.5 *Separation of duties*

No single user should have full access rights to perform all administrative actions. By separating duties among multiple operators, the amount of power held by a single person is restricted and aids in preventing fraud. Examples of separation of administrative duties - by site, building, sub-system (Fire, HVAC, security), building owner vs. integrator role, functions (operations vs network management vs. backup). Active Directory groupings can facilitate this. This reduces the risk of insiders successfully committing fraud.

1.4.1.6 *Centralized user account management*

Identity Management Systems (IDMS) offer enhanced security over the local management of users within VideoEdge. An IDMS, such as Microsoft Active Directory or a Lightweight Directory Access Protocol (LDAP) capable IDMS, can provide user account management for multiple devices or systems, including a VideoEdge NVR. By centrally managing user accounts, an administrator can assure consistency throughout the domain the IDMS manages. This assures that when an account is disabled in the domain, access by that user is disabled everywhere in the domain including all connected VideoEdge NVRs. Furthermore, IDMS provides a centralized location to manage password policies which dictates password formation rules including, length, capitalization, reuse, and expiration.

1.4.1.7 *Strong passwords*

Strong passwords should be used to minimize the risk of password guessing. Automated forms of password guessing such as "dictionary attacks" and "rainbow tables" can run through commonly used passwords and can be successful if strong passwords are not used. You can strengthen a password with length and complexity. The length of a password has the biggest impact on making password guessing difficult. VideoEdge provides a configurable password policy which you can use to achieve the desired level of password strength. Password policies are often governed by local policies. VideoEdge is enabled by default with a password policy which may be strengthened as required.

1.4.1.8 *Password aging*

Password aging is a technique used to reduce to possibility of password exploitation. When enabled the user is forced to change their password after a set time-period has elapsed.

1.4.1.9 *Password history*

Password histories are used to mitigate against password reuse.

1.4.1.10 *Password policy*

It is important to have a password policy. Customers often have password policies that all systems must support.

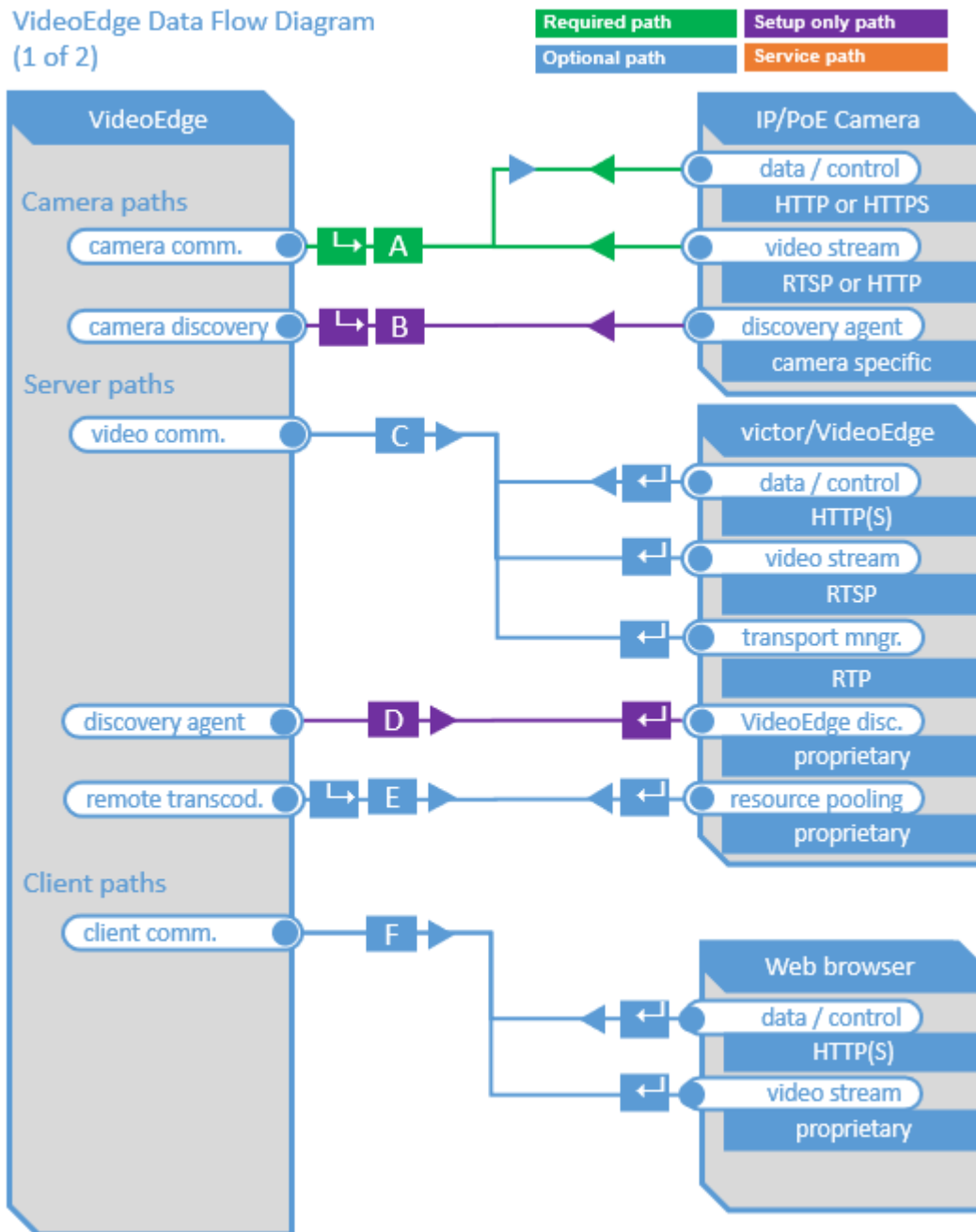
1.4.1.11 *Account expiration*

Automatic account expiration for known temporary usage.

1.5.0 VideoEdge data flow diagram

Figure 1.5.0.1

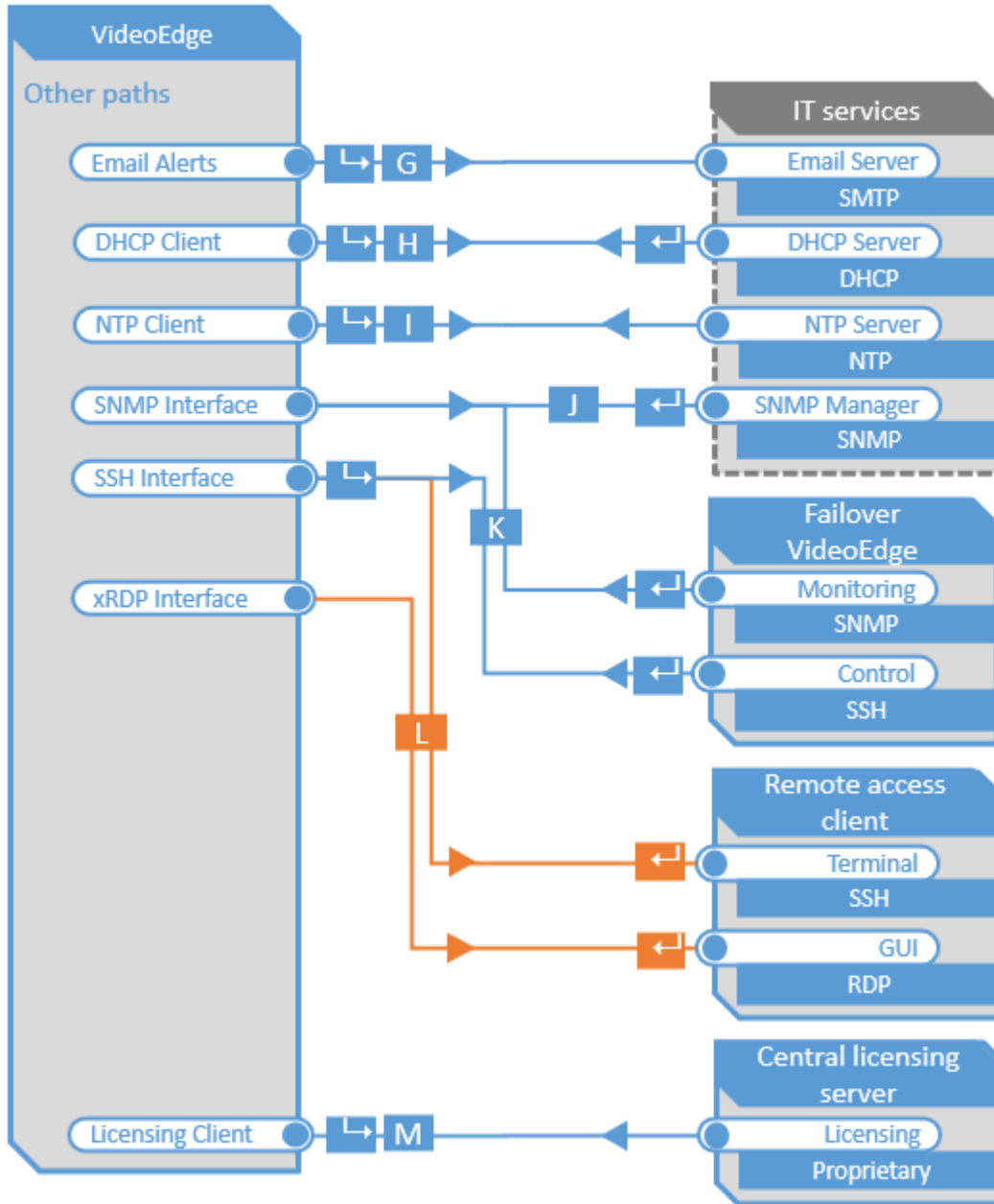
VideoEdge Data Flow Diagram
(1 of 2)



- A** Path identifier used in protocols and ports table
- L** Component can initiate communications
- ▶** Response data can flow in this direction

VideoEdge Data Flow Diagram
(2 of 2)

| | |
|---------------|-----------------|
| Required path | Setup only path |
| Optional path | Service path |



- A** Path identifier used in protocols and ports table
- L** Component can initiate communications
- ▶** Response data can flow in this direction

1.5.1 Communication paths table

Table 1.5.1.1: Communications paths table

| Path | Function | VideoEdge | | | | Direction / use requirement ² | Connecting Component | | | Notes |
|----------|--------------------------------------|------------------|-------------------------|-----------------------------------|----------------------------|--|--|----------|------------------------------|---|
| | | Interface | Default Port Assignment | Default Port State ^{1,2} | Port Activity (if enabled) | | Default Port Assignment ^{1,3} | Protocol | Internet access ⁴ | |
| A | Camera communications | | | | | Required | IP/PoE Camera | | | |
| | <i>data and control (non-secure)</i> | HTTP Client | Dynamic | <i>if standard mode</i> | ∞ | | 80 | TCP | - | <i>select between HTTP or HTTPS^{4,6}</i> |
| | <i>data and control (secure)</i> | HTTPS Client | Dynamic | Enabled | ∞ | | 443 | TCP | - | |
| | <i>video stream</i> | RTSP Client | Dynamic | Enabled | ∞ | | 554 | TCP | - | <i>select between RTSP or HTTP⁶</i> |
| | <i>video stream</i> | HTTP Client | Dynamic | Enabled | ∞ | | 80 | TCP | - | |
| B | camera discovery | | | | | Commissioning only | IP/PoE Camera | | | |
| | <i>veAutoDiscScanPort</i> | camera discovery | 32768-60999 | Enabled | On demand | | 8992 | UDP | - | |
| | <i>veAutoDiscMDNS</i> | camera discovery | 32768-60999 | Enabled | On demand | | 5353 | UDP | - | |
| | <i>veAutoDiscMDNS</i> | camera discovery | 5353 | Enabled | On demand | | Dynamic | UDP | - | |
| | <i>veAutoDiscWSDDiscovery</i> | camera discovery | 32768-60999 | Enabled | On demand | | 3702 | UDP | - | |
| | <i>veAutoDiscWSDDiscovery</i> | camera discovery | 3702 | Enabled | On demand | | Dynamic | UDP | - | |
| | <i>veAutoDiscADPort8848</i> | camera discovery | 8848 | Enabled | On demand | | Dynamic | UDP | - | |
| | <i>veAutoDiscADPort12345</i> | camera discovery | 12345 | Enabled | On demand | | Dynamic | UDP | - | |
| C | victor communications | | | | | Optional | victor | | | |
| | <i>data and control</i> | HTTP(S) Server | 443 | Enabled | ∞ | | Dynamic | TCP | - | <i>Required if connected with victor</i> |
| | <i>video stream</i> | RTSP Server | 554 | Enabled | ∞ | | Dynamic | TCP | - | |
| | <i>transmit manager</i> | RTP | 55555 | Enabled | ∞ | | Dynamic | TCP | - | |
| D | VideoEdge discovery | | | | | Commissioning only | VideoEdge | | | |
| | <i>veAutoDiscSSDP</i> | VE Discovery | 32768-60999 | Enabled | On demand | | 1900 | UDP | - | |
| | <i>veAutoDiscSSDP</i> | VE Discovery | 1900 | Enabled | On demand | | 32768-60999 | UDP | - | |
| | <i>nvrupnpn</i> | VE Discovery | 32768-60999 | Disabled | On demand | | 1900 | UDP | - | |
| E | Resource pooling | | VideoEdge | | | Optional | VideoEdge | | | |
| | <i>Remote transcoding</i> | | 55555 | Disabled | ∞ | | 1900 | UDP | - | - |

- Continued -

| Path | Function | VideoEdge | | | | Direction / use requirement ² | Connecting Component | | | Notes | |
|----------|----------------------------------|--------------|-------------------------|-----------------------------------|----------------------------|--|--|----------|------------------------------|----------|--|
| | | Interface | Default Port Assignment | Default Port State ^{1,2} | Port Activity (if enabled) | | Default Port Assignment ^{1,3} | Protocol | Internet access ⁴ | | |
| F | web browser communication | | | | | Optional | web browser | | | | |
| | <i>data/control non-secure</i> | HTTP Server | 80 | | ∞ | | | Dynamic | TCP | - | ⁷ these services not required for commissioning / admin web |
| | <i>data/control secure</i> | HTTPS Server | 443 | Enabled | ∞ | | | Dynamic | TCP | - | |
| | <i>video stream⁷</i> | HTTPS Server | 443 | Enabled | ∞ | | | Dynamic | TCP | - | |
| G | Email alerts | | | | | Optional | Mail Server | | | | |
| | <i>email</i> | SMTP Client | | Disabled | On demand | | | 25 | TCP | Optional | |
| H | Obtain IP address | | | | | Optional | DHCP Server | | | | |
| | | DHCP Client | 68 | Enabled | ∞ | | | 67 | UDP | | |
| I | Provide IP addresses | | | | | Optional | DHCP Client | | | | |
| | | DHCP Server | 67 | Disabled | ∞ | | | 68 | UDP | | |
| J | Time sync | | | | | Optional | NTP Server | | | | |
| | | NTP Client | 123 | Disabled | ∞ | | | 123 | UDP | Optional | - |
| K | Network Monitoring | | | | | Optional | SNMP manager | | | | |
| | <i>monitor</i> | SNMP Server | 161 | Disabled | ∞ | | | | UDP | - | - |
| L | Redundant server failover | | | | | Optional | VideoEdge (failover server) | | | | |
| | <i>snmpd</i> | SNMP Server | 161 | Disabled | ∞ | | | 161 | UDP | - | - |
| | | SSH Server | 22 | Disabled | ∞ | | | 22 | TCP | - | - |
| | <i>VEAPI</i> | HTTPS | 443 | Disabled | ∞ | | | 443 | TCP | - | - |
| M | Remote access | | | | | Service | Remote client | | | | |
| | <i>terminal</i> | SSH Server | 22 | Disabled | ∞ | | | 22 | TCP | Optional | - |
| | <i>GUI</i> | xRDP | 3389 | Disabled | ∞ | | | Dynamic | TCP | Optional | <i>if client is Windows</i> |
| N | Centralized licensing | VideoEdge | | | | Optional | Licensing Server | | | | |
| | <i>VideoEdge</i> | | | Disabled | ∞ | | | 27000 | TCP | - | <i>Option to local licensing</i> |

1. Yellow fill color denotes that the port number and port state that VideoEdge will use is configurable from within VideoEdge.
2. Application requirements are represented by the following color codes and symbols:

| | |
|--|---|
| | Green = required path |
| | Blue = optional path |
| | Purple = Commissioning-only path |
| | Orange = Service path |
| | These arrows indicate that the component can initiate communication in the direction of the arrow |
| | These arrows indicate that the component can send data in this direction of the arrow |
| | This symbol indicates that the component only consumes data from this path. |

3. Typical default setting for connecting components, VideoEdge settings must match
4. Any Internet access, if used should be indirect and managed through a firewall

5. Data flow if VideoEdge is configuring or controlling camera functions such as PTZ positioning
6. Use depends on protocol supported by camera

Note: VNC is no longer supported by VideoEdge

1.6.0 Network planning

Video surveillance systems transmit, collect, process and, store sensitive data that will disclose sensitive information if accessed by unauthorized users. While several security controls are inherent to the VideoEdge system to limit access to authorized users, it is best practice for the network design to provide additional layers of defense.

When designing a network for a video management system, first determine which components will be included in the full scope of the system required to provide all the planned functions for that system, for example, video cameras, network video recorders, clients, service connections, and remote access points.

With the full scope of components and functions in mind you can build the appropriate level of protection into the network design to protect both the network and endpoints. Keep in mind that some of the system components, while compatible with VideoEdge, may not support the same level of protection as VideoEdge. In those cases, compensating controls may be utilized within the network design to reduce risk.

Important: The network infrastructure security is the customer's responsibility.

1.6.1 Trust boundaries overview

A trust boundary within a system is the boundary in which data is passed between components that do not share an equal level of trust. Products that are not part of the VideoEdge system or do not provide methods to sufficiently authenticate a component or user may be regarded as having a lower level of trust. Networks may also have different levels of trust. For example, an isolated network with only video cameras and NVRs is usually trusted more than a shared use network such as the corporate IT network or a remote network.

When the trust deviation is beyond the risk tolerance, it is best to control the flow of data between trusted and untrusted network using a switch or router with data flow control capabilities, such as a firewall.

1.6.2 Network protection

Isolating the VideoEdge system from networks of lower trust is recommended.

1.6.2.1 *Isolated Camera LAN*

The VideoEdge NVR has dedicated camera LAN ports to isolate the camera network from the network used at the system level.

1.6.2.2 *Demilitarized Zone (DMZ)*

When communications to or from the VideoEdge NVR is required from an untrusted network (from the perspective of VideoEdge), such as a corporate LAN, a demilitarized zone (DMZ) may be established to provide a high degree of data flow control and prevent direct access to resources on the VideoEdge network.

Use of a DMZ is strongly recommended with providing remote connectivity in conjunction with other safeguards such as a VPN and multi-factor authentication.

1.6.2.3 *VLANs*

A Virtual Local Area Network (VLAN) provides the ability to share the networking infrastructure while maintaining separation between trusted and untrusted networks. The use of VLANs reduce deployment costs by removing the need to run dedicated cabling and networking equipment for the VideoEdge system.

If physical access to the cabling used for the VLAN is possible by authorized users, it is recommended that the VLAN switches are configured for to protect eavesdropping by employing encryption technology.

1.6.2.4 *Firewalls*

Routers and switches which are used to bridge trust boundaries should employ firewalls.

1.6.2.5 Remote access

Remote access points should be protected and always treated as access from an untrusted network.

1.6.2.6 VPN

A Virtual Private Network (VPN) should always be used to provide encrypted and authenticated communication for remote access connections. VPN technologies that are enabled for multi-factor authentication are recommended. Victor Web is intended for internal network use and therefore if used over the internet, must be done through a VPN connection.

1.6.3 Endpoint protection support

The operating system of the VideoEdge NVR includes a firewall that you can enable and configure. By default the SUSE firewall is disabled, but VideoEdge applies a number of its own firewall rules. If the customer enables the SUSE firewall they may have to apply these rules themselves. They can see the configured VideoEdge firewall rules using “iptables -L” *before* enabling the SUSE firewall.

1.7.0 Anti-virus

The VideoEdge NVR does not include pre-installed Anti-virus software. As specific Linux compatible anti-virus software is not pre-qualified for use with the VideoEdge NVR, it is recommended that the anti-virus software compatibility is tested in a controlled, non-production environment.

1.8.0 Hardware and software requirements

Most VideoEdge NVR models are sold as a pre-configured appliance which meets all the hardware and software requirements for the VideoEdge application.

VideoEdge is an embedded video server appliance built upon the openSUSE Linux distribution Leap.



The Operating System VideoEdge OS is built on an openSUSE Linux distribution which has been customized to contain only the components and services needed for the operation of VideoEdge. The number of vulnerabilities is reduced as unnecessary components are removed.

You can perform administration of the operating system by logging on to the NVR either through a terminal window on the NVR or through SSH, and then elevating your privileges to root. You can perform administration through the GUI using YAST or by opening a terminal and then running the “su” command and entering the root password.

For convenience, some of the Linux settings are available within the VideoEdge System Configuration menu. The **VideoEdge Software Only NVR** is the exception as this model requires that computer hardware to be sourced separately. The computer hardware must meet the requirements outlined in the VideoEdge NVR Engineering Specifications.

1.8.1 Required services

Required services for VideoEdge operations are set up by default with the correct settings. These services must stay enabled for continuous operations.

1.8.2 Internet service table

The VideoEdge application does not utilize Internet services.

2 Deployment

This section is designed to help execute the deployment of VideoEdge. The contents within this section address how to initiate secure deployment for new installations, how to harden VideoEdge and additional steps after commissioning required before the VideoEdge is turned over to runtime operations.

2.1.0 Deployment overview

Security hardening of VideoEdge begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review that section prior to deployment to fully understand the security feature set of VideoEdge, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Resetting to factory defaults
- Considerations for commissioning
- Recommended knowledge level

2.1.1 Getting started

Before you install VideoEdge and power it on, consider the guidance in the following sections.

2.1.2 Physical installation considerations

Install the VideoEdge hardware using the instructions provided in the installation guide. Keep in mind that the physical access to the device and physical installation of the device can impact cybersecurity.

Physical access to this device enables actions that cannot be authenticated and logged electronically through the capabilities of this product. To prevent unauthorized access, be sure to place the device in a room, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control). The device is equipped with an optical tamper switch that you can use to send and log electronic alerts regarding physical tampering of the installation. Consider using protective electric wire conduits for communication wires with paths through areas of lower trust.

2.1.3 Default security behavior

On the initial startup of VideoEdge, the following functions will be enabled to facilitate the most common commissioning tasks including camera discovery:

- Configuration webpage
- Camera discovery

There are built-in user accounts and passwords that may be used to initially login to VideoEdge. On first startup of the VideoEdge hardware, the installation wizard will require passwords and optionally usernames to be changed.

- Section 2.2.5.1 discusses user accounts
- Section 2.2.6 discusses user management overview

During your first logon as the administrator, you will be prompted to select standard or enhanced password validation.

When Enhanced Password Validation is enabled the following configurable policy is applied by default:

- Password must consist of a minimum of eight characters
- Password must not be a duplicate of the previous three passwords associated with that credential
- Password must differ by a minimum of three characters from the previously assigned password
- Password must obey at least three of the following rules -
 - Must contain an uppercase letter
 - Must contain a lowercase letter
 - Must contain a number
 - Must contain one of the following special characters [] { } () ^ \$ # + _ - ~ ! * %

2.1.4 Resetting to factory defaults

If the device was previously used as part of another installation or test environment, the unit should be reset to factory defaults before being put into service in a new deployment.

See section 3.4.0 for details on how to reset to factory defaults.

2.1.5 Considerations for commissioning

In some applications the default settings may not be sufficient to fully commission the system. Functions that will not be used during the commissioning process should be disabled.

In the commissioning phase, a less secure configuration may be used before the full infrastructure is available to speed up the deployment process (for example, using wireless). Once the commissioning phase is complete, be sure to remove the temporary infrastructure and harden the system further before turning over to full runtime operations.

2.1.6 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in VideoEdge administration and networking technologies. Completion of the VideoEdge basic and advanced installation courses is recommended.

2.2.0 Hardening

While VideoEdge has several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment.

In this section configuration settings labelled as “minimum baseline protection” are provided as general guidance; However, the minimum baseline protection may not be sufficient for the target application. It is important to apply to the correct level of protection as warranted by policies and regulations that may govern the application security settings for a deployment instance of VideoEdge.

2.2.1 Hardening checklist

| | | |
|--------------------------|--|----|
| <input type="checkbox"/> | Hardening step 1: Configure BIOS | 32 |
| | Hardening step 1.1: Enable BIOS password | 32 |
| | Hardening step 1.2: Prevent USB boot | 32 |
| <input type="checkbox"/> | Hardening step 2: Configure operating system user accounts | 33 |
| | Security Mode | 33 |
| | Hardening step 2.1: Set the Security Mode to Enhanced | 33 |
| | Hardening step 2.2: Enabling media encryption..... | 34 |
| | Hardening step 2.3: Change System user account passwords | 34 |
| | Hardening step 2.4: Set invalid attempt user lockout policy | 36 |
| | Hardening step 2.5: Set the inactivity log out policy | 37 |
| | Hardening Step 2.6: Set the password complexity policy..... | 38 |
| <input type="checkbox"/> | Hardening step 3: Configure roles..... | 41 |
| | Hardening step 3.1: Set account lockout policy..... | 41 |
| | Hardening step 3.2: Set the inactivity log out policy | 41 |
| | Hardening step 3.3: Set the Enhanced Password Validation | 42 |
| | Hardening step 3.4: Set the Password History policy | 42 |
| | Hardening step 3.5: Set role-based camera access permissions | 42 |
| <input type="checkbox"/> | Hardening step 4: Configure VideoEdge user accounts | 45 |
| | Hardening step 4.1: Create unique user accounts for each user..... | 45 |
| | Hardening step 4.2: Assign roles..... | 45 |
| | Hardening step 4.3: Lock built-in accounts..... | 45 |
| | Hardening step 4.4: Change passwords of built-in accounts..... | 45 |
| <input type="checkbox"/> | Hardening step 5: Configure LDAP and LDAP roles..... | 46 |
| | Hardening step 5.1: Configure LDAP..... | 47 |
| | Hardening step 5.2: Configure LDAP Roles | 48 |
| <input type="checkbox"/> | Hardening step 6: Configure the system use banner | 49 |
| <input type="checkbox"/> | Hardening step 7: Security center and hardening configuration | 50 |
| | Hardening step 7.1: Select a predefined or custom security configuration | 50 |
| | Hardening step 7.2: Set boot permissions | 53 |

| | | |
|--------------------------|---|-------------------------------------|
| <input type="checkbox"/> | Hardening step 8: Modify Windows TLS version..... | 54 |
| <input type="checkbox"/> | Hardening step 9: Update software | 54 |
| | Hardening step 9.1: Update operating system software..... | 54 |
| | Hardening step 9.2: Update VideoEdge software..... | 54 |
| | Hardening step 9.3: Update camera firmware | 55 |
| <input type="checkbox"/> | Hardening Step 10: Configure communication ports and encryption | 56 |
| | Hardening step 10.1: Configure ports using the network, general page..... | 56 |
| | Hardening step 10.2: Configure ports using the network, WAN Settings page..... | 58 |
| | Hardening step 10.3: Configure remote access using the system page, remote access tab | 59 |
| <input type="checkbox"/> | Hardening step 11: Configure Communication Certificate | 61 |
| <input type="checkbox"/> | Hardening step 12: Assure cameras are connected to the protected LAN..... | 62 |
| <input type="checkbox"/> | Hardening step 13: Configure camera security settings | 62 |
| <input type="checkbox"/> | Hardening step 14: Enable FIPS..... | 65 |
| <input type="checkbox"/> | Hardening step 15: Configure SNMP..... | 67 |
| <input type="checkbox"/> | Hardening step 16: Configure alerts..... | 67 |
| | Hardening step 16.1: Configure image tamper detection | 67 |
| | Hardening step 16.2 – Configure email alerts..... | 68 |
| <input type="checkbox"/> | Hardening step 17: Backup VideoEdge configuration and data..... | 70 |
| <input type="checkbox"/> | Hardening step 18: Configure the Log FTP server | 71 |
| <input type="checkbox"/> | Hardening step 19: Configure VideoEdge with a failover server | 72 |
| <input type="checkbox"/> | Hardening step 20: Configure VideoEdge firewall | 72 |
| <input type="checkbox"/> | Hardening step 21: Disable victorWebLT | Error! Bookmark not defined. |
| <input type="checkbox"/> | Hardening step 22: Security documentation | 76 |
| <input type="checkbox"/> | Hardening step 23: Perform a security configuration audit..... | 76 |

2.2.2 Administration

As VideoEdge has been designed as an appliance, users do not need to login to VideoEdge operating system directly for most operations. You can conduct software access to VideoEdge from a remote application or webpage. Some administrators may choose to login to the Operating system directly to deploy operating system level updates. In such cases, unique operating system level accounts are recommended.

2.2.2.1 BIOS administration

BIOS administrator requires direct access to the VideoEdge NVR.

To enter the BIOS configuration, complete the following steps:

1. Turn on the computer.
2. Within 10 seconds of startup press the F2 button on the keyboard.
3. Enter **Advanced mode**.

Note: each hardware platform may have a slight deviation.

2.2.2.2 Operating System administration

You can access Operating System administration locally or remotely. For remote access additional services are required to be enabled as indicated by each interface type.

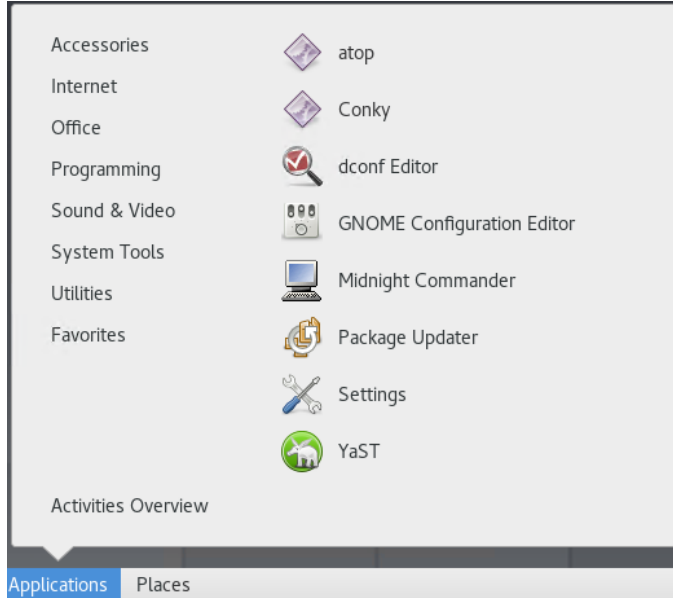
YaST Graphical User Interface

The VideoEdge operating system comes with the Yet another Setup Tool (YaST) to aid with configuration.

To use YaST remotely, RDP must be enabled. See [2.5.2 Communication port and encryption configuration](#)

You can find YaST from the operating system level under applications, system tools:

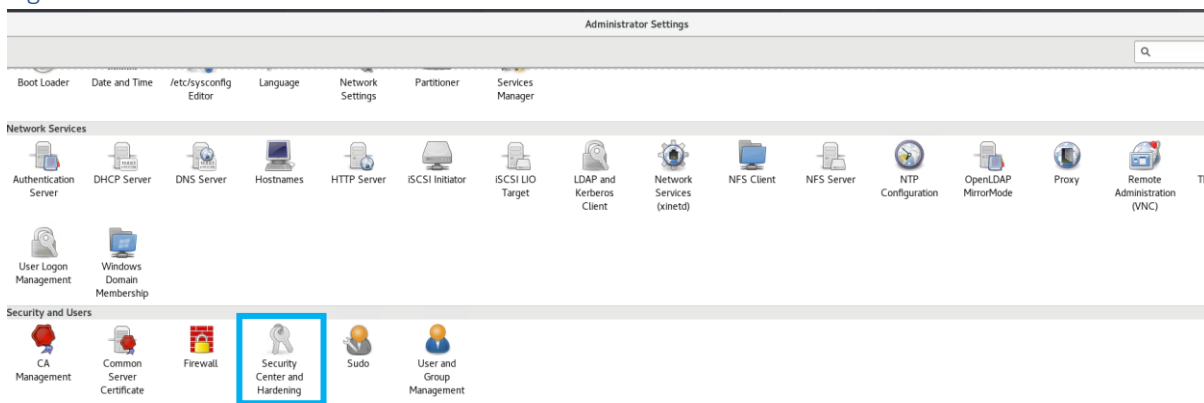
Figure 2.2.2.2.1



Once opened, YaST provides access to the operating system configuration settings. The Security Center and Hardening tool within YaST provides administrative functions to configure predefined security configurations, password settings, boot settings, and login settings among other settings.

You can access the Security Center and Hardening tool from the YaST administrator settings, Security User section:

Figure 2.2.2.2.2



Command Line User Interface

Some administrators prefer to a command line user interface for configuring the operating system security settings.

To use the command line remotely, SSH must be enabled. (See Communication hardening)

Locally the command line may be accessed as follows:

1. To open a terminal, click Application > Utilities.
2. In the terminal window type `su -` enter root password.

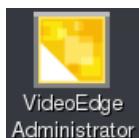
2.2.2.3 VideoEdge administration

The following administration tools are available for the VideoEdge application:

VideoEdge Administrator

You can complete administration for VideoEdge through the VideoEdge administrator a web-based application accessible on the NVR itself or by simply entering the IP address of the NVR into any browser.

Local access - Locally launch the VideoEdge Administrator by selecting the VideoEdge Administrator desktop icon. This will launch Mozilla Firefox ESR with the VideoEdge Administration Interface login page loaded.



Remote access (preferred interface) - From the web browser of a Windows PC with network connectivity to the VideoEdge. Enter the IP address of the VideoEdge in the address bar of your web browser. Supported browsers are Microsoft Edge (latest version), Google Chrome (latest version) and Mozilla Firefox (latest version).

First-time access - VideoEdge Setup Wizard - The first time accessing the Administration Interface after installation you will be automatically directed to the Setup Wizard. The Setup Wizard will present some of the security settings available to the administrator. Once the Setup Wizard completes, VideoEdge security settings the normal VideoEdge Administrator user interface will display.

VideoEdge Administrator - System menu – Using the System menu within the administrator you can configure the NVR’s basic system settings; Users and Roles, Licensing, Template files, Backup/Restore, software updates, Serial Protocols, and the NVR’s Security Configuration.

VideoEdge Administrator – Security Audit page - The Security Audit page contains a dashboard showing a read-only status of several key security settings.

The Security Audit page contains a read-only status summary for the following NVR settings:

- Role Settings
- User Settings
- Camera Restrictions
- Linux user Settings
- Web Server Ports and protocols
- Remote Access
- Certificate settings
- Certificate Authority settings
- SNMP Settings
- System Robustness

You can find the Security Audit page in VideoEdge under System, Security Configuration:

Figure 2.2.2.3.1

The screenshot shows the Security Audit page in VideoEdge. The left sidebar contains navigation options: Live Video, Devices, Storage, Archive, System (expanded), General, Users and Roles, Licensing, Templates, Backup/Restore, Serial Protocols, Security Configuration (selected), Network, Advanced, and Logout. The main content area has tabs for General, Certificate, Remote Access, System Passwords, System Use Banner, SNMP, LDAP, Media Encryption, and Security Audit. Under Role Settings, a table lists roles with columns for Role, Num Users, Auto Logout Interval (Minutes), Failed Login Lockout, Max Login Attempts, Inactivity Lockout Interval (Days), and Enhanced Password Validation. Under User Settings (UTC), a table lists usernames with columns for Username, Password Last Changed, Days Since Password Last Changed, Uses Default Password, and Uses Latest Security Mechanism. A link 'Click to show all users' is present next to the User Settings table.

| ROLE | NUM USERS | AUTO LOGOUT INTERVAL (MINUTES) | FAILED LOGIN LOCKOUT | MAX LOGIN ATTEMPTS | INACTIVITY LOCKOUT INTERVAL (DAYS) | ENHANCED PASSWORD VALIDATION |
|-----------------|-----------|--------------------------------|----------------------|--------------------|------------------------------------|------------------------------|
| admin | 2 | 10 | Disabled | N/A | Disabled | Enabled |
| axisbws | 0 | 10 | Disabled | N/A | Disabled | Enabled |
| cloudnvrlogin | 0 | 10 | Disabled | N/A | Disabled | Enabled |
| nvrgroupadmin | 1 | N/A | Disabled | N/A | Disabled | Enabled |
| nvrserviceuser | 2 | N/A | Disabled | N/A | Disabled | Enabled |
| operator | 0 | 10 | Disabled | N/A | Disabled | Enabled |
| softwareadmin | 1 | 10 | Disabled | N/A | Disabled | Enabled |
| support | 1 | 10 | Disabled | N/A | Disabled | Enabled |
| tycooiaipclient | 0 | N/A | Disabled | N/A | Disabled | Enabled |
| viewer1 | 0 | N/A | Disabled | N/A | Disabled | Enabled |
| viewer2 | 0 | N/A | Disabled | N/A | Disabled | Enabled |
| viewer3 | 0 | N/A | Disabled | N/A | Disabled | Enabled |

| USERNAME | PASSWORD LAST CHANGED | DAYS SINCE PASSWORD LAST CHANGED | USES DEFAULT PASSWORD | USES LATEST SECURITY MECHANISM |
|-------------------|-----------------------|----------------------------------|-----------------------|--------------------------------|
| admin | Fri Jul 21 2023 | 54 | No | Yes |
| axisbwserviceuser | Never | N/A | No | Yes |
| nvrgroupadmin | Fri Jul 21 2023 | 54 | No | Yes |
| nvrserviceuser | Never | N/A | No | Yes |
| softwareadmin | Fri Jul 21 2023 | 54 | No | Yes |
| support | Fri Jul 21 2023 | 54 | No | Yes |

In addition, the NVR settings that are shown on the Security Audit page are color-coded. The color assigned indicates if recommendation for changing the setting is required.

- Black - The setting does not require assessment.
- Red - The setting is not secure. It is strongly recommended that you change this setting.
- Amber - The setting is partially secure. It is strongly recommended that you change this setting.

Note: You should review the Security Audit page every time you change your VideoEdge security settings.

2.2.3 BIOS configuration

Hardening step 1: Configure BIOS

It is important to protect the BIOS configuration from being modified by unauthorized users.

Note: BIOS menus can vary between versions and models of VideoEdge. The following steps are based on the BIOS menus available when this guide was created.

Hardening step 1.1: Enable BIOS password

Enable password protection of the VideoEdge BIOS and set the password. This password should only be known to administrators that have been authorized.

How to set a BIOS password:

1. Turn on the computer.
2. Within 10 seconds of startup press the F2 button on the keyboard.
3. Enter **Advanced mode**.
4. Click the **Security** tab.
5. Set a new Administrator password.

Note: You need the administrator password when any BIOS changes are made

2.2.4 Set boot sequence

The boot sequence should prevent boot up by USB devices as it is a possible for USB devices to inject malicious code without warning.

Hardening step 1.2: Prevent USB boot

How to disable USB ports:

1. Turn on the computer.
2. Within 10 seconds of startup press the F2 button on the keyboard.
3. Enter **Advanced mode**.
4. In the **Advanced** tab click **USB Configuration**.
5. Click on **USB Single Port Control**.
6. Notice all the USB ports are listed as "Enabled".
7. Change all the ports that are not required to "Disabled".
8. Save and restart the machine.

Note: Take note to know which ports are being used prior to disabling. This would be done by using the `lsusb -v` command in a terminal.

An end user should have the ability to restrict ability to interact with physical interfaces. The USB port is an important physical interface that would allow for a malicious user to upload corrupted files or download information.

2.2.5 User management

In this section you can find information on user management.

2.2.5.1 Operating system level user accounts (interactive)

You can access VideoEdge NVR operating system using one of the following accounts.

Table 2.2.5.1.1

| User | Description |
|-----------|---|
| root | root (Administrator) account for the Linux operating system. Full administrative access to the VideoEdge NVR's operating system |
| VideoEdge | VideoEdge is the default account to access the Linux OS. |
| support | Used for remote technical support. |

The support account

The support user on the VideoEdge NVR operating system is intended for the use by American Dynamics Technical Support, as the account has full sudo access. The password for this account is unique to each NVR device and can only be derived by American Dynamics Technical Support when provided with the unique support ID. You can disable the support account on the “System Passwords” page of the admin GUI.

[Hardening step 2: Configure operating system user accounts](#)

Changing default system root and VideoEdge user account passwords and making them unique enhances the security of the product.

Note: the root System and VideoEdge user account password must be changed before you can enable the remote access services (SSH and RDP).

Security Mode

In Standard Security Mode, you must change the passwords for the Linux users and the required NVR accounts. All other changes on the User Accounts page are optional in Standard Security Mode.

In Standard Security Mode, UPnP is enabled by default.

In Enhanced Security Mode, you must create new user accounts and passwords for the Linux users and the required NVR accounts.

In Enhanced Security Mode, UPnP is disabled by default.

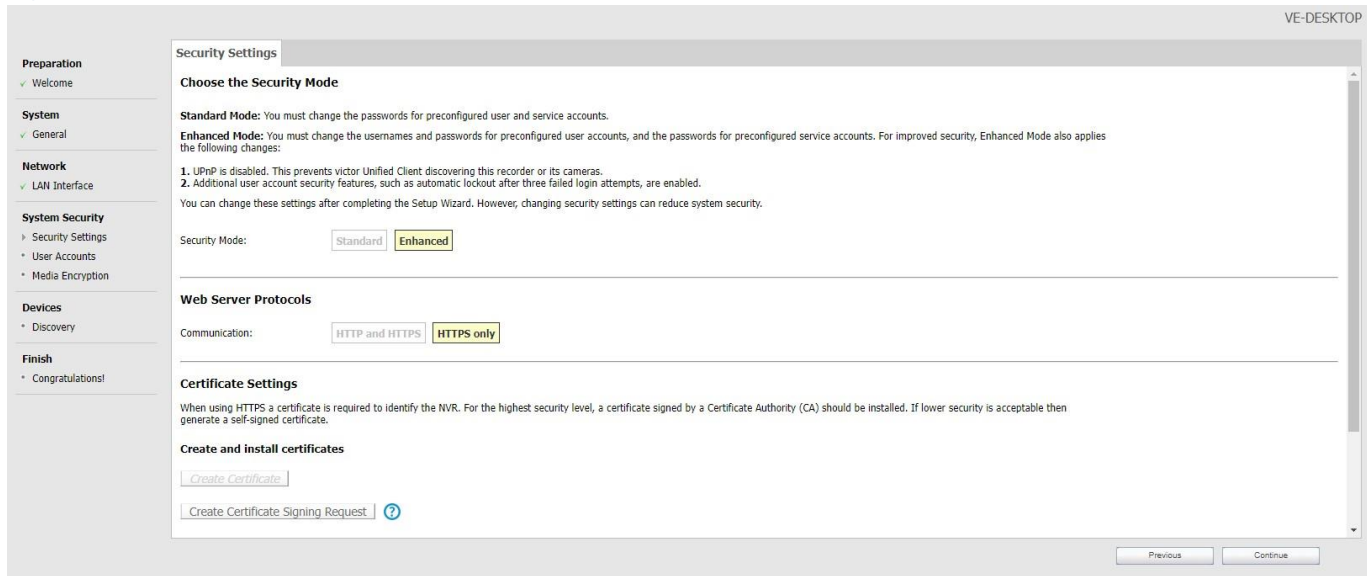
Access for the Linux support user account is enabled by default in Standard Security mode and disabled by default in Enhanced Security Mode. After completing the wizard, you can enable or disable access for the Linux support user account on the System Passwords page.

[Hardening step 2.1: Set the Security Mode to Enhanced](#)

Caution: Upon completing the Setup Wizard, the selected Security Mode is final. Ensure that you have selected the appropriate mode. If Security Mode is set to standard, it is still possible to manually configure the VideoEdge with the same settings as Enhanced Mode.

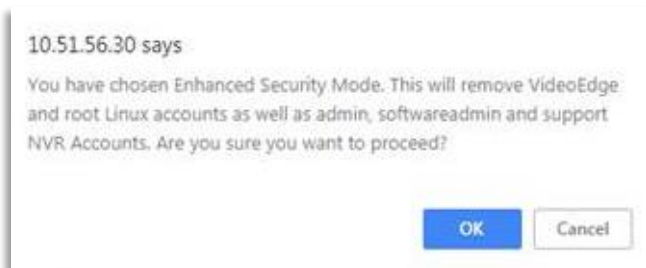
VideoEdge Setup Wizard. On the Security Mode page, select **Enhanced**.

Figure 2.2.5.1.1



Note: When **Enhanced Security** is selected, in the last step of the Setup Wizard remove the default Linux accounts or the system will revert to Standard Security mode. Select **OK** to finalize the Enhanced Security mode process:

Figure 2.2.5.1.2



Hardening step 2.2: Enabling media encryption

To enable media encryption, tick the Encrypt Media check box in the installation wizard.

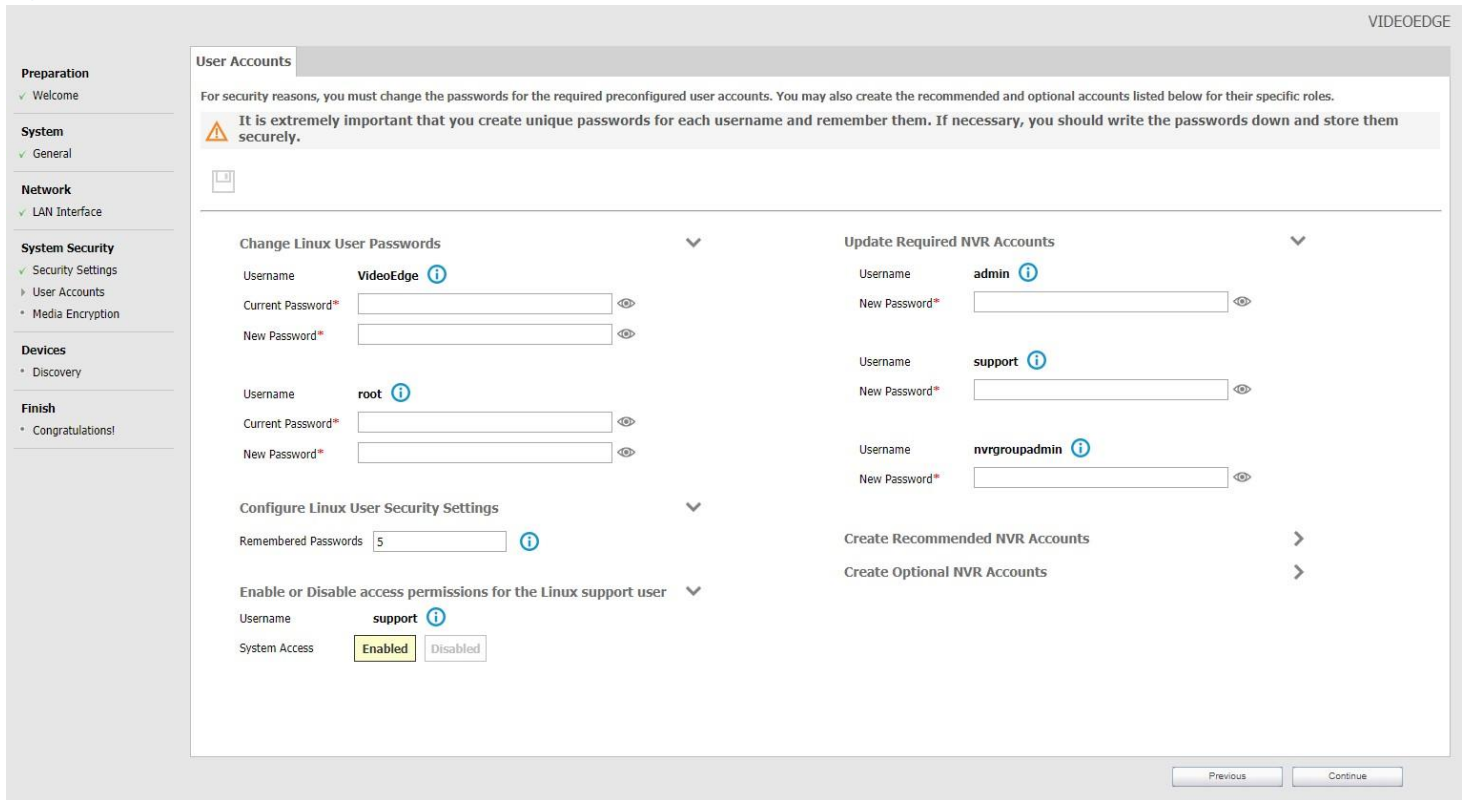
Hardening step 2.3: Change System user account passwords

Change user account passwords using the VideoEdge Setup Wizard

The VideoEdge Setup Wizard includes the ability to change or replace the System VideoEdge and System root passwords. These passwords must conform to the active password policy of the operating system.

The User Accounts page will display after the Security Settings page within the Setup Wizard. You can change or replace the user accounts according to the previously selected security mode.

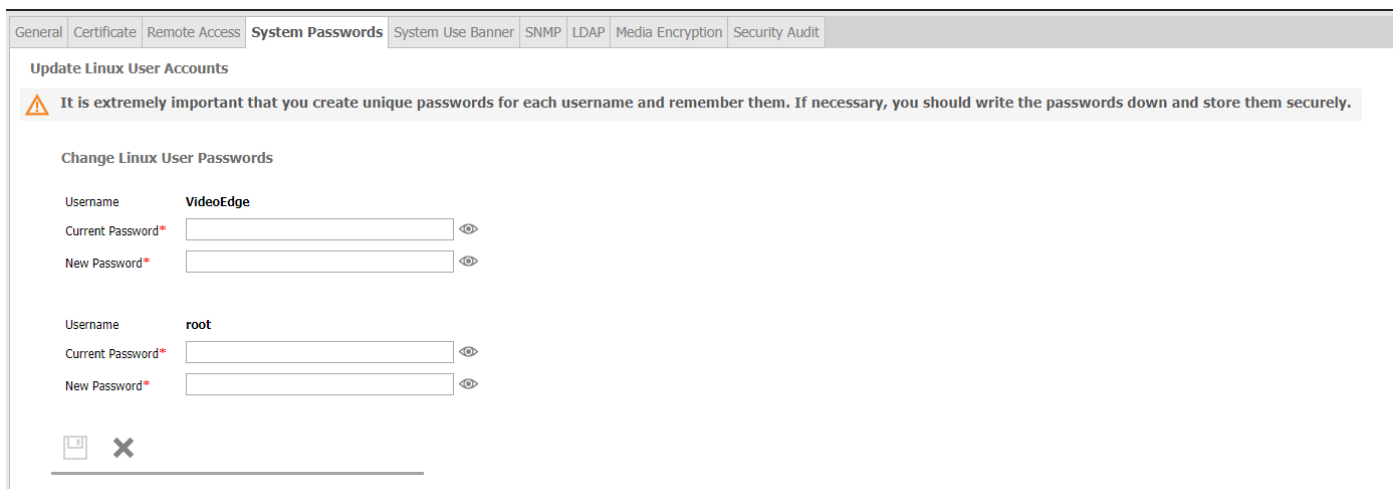
Figure 2.2.5.1.3



Change user account passwords using VideoEdge Administrator

To change the system password from the normal VideoEdge Administrator, access the System Password tab within the System Configuration menu:

Figure 2.2.5.1.4



Note: It is critical that the new password be recorded and kept secure as it cannot be recovered. The web UI has a warning to this effect.

With both methods, enter the current password for the system root user account, and provide the new password. Use the password reveal icon to check you have typed the password correctly, then press save.

Note: From VideoEdge Administrator, the Security Audit page *Linux User Settings* section displays the Operating System accounts and when the passwords were last changed and whether they are still using the default password.

Figure 2.2.5.1.5

Linux User Settings (UTC)

| USERNAME | PASSWORD LAST CHANGED | DAYS SINCE PASSWORD LAST CHANGED | REMEMBERED PASSWORDS | USES DEFAULT PASSWORD | USES LATEST SECURITY MECHANISM |
|-----------|-----------------------|----------------------------------|----------------------|-----------------------|--------------------------------|
| root | Fri Jul 21 2023 | 54 | 5 | No | No |
| VideoEdge | Fri Jul 21 2023 | 54 | 5 | No | No |

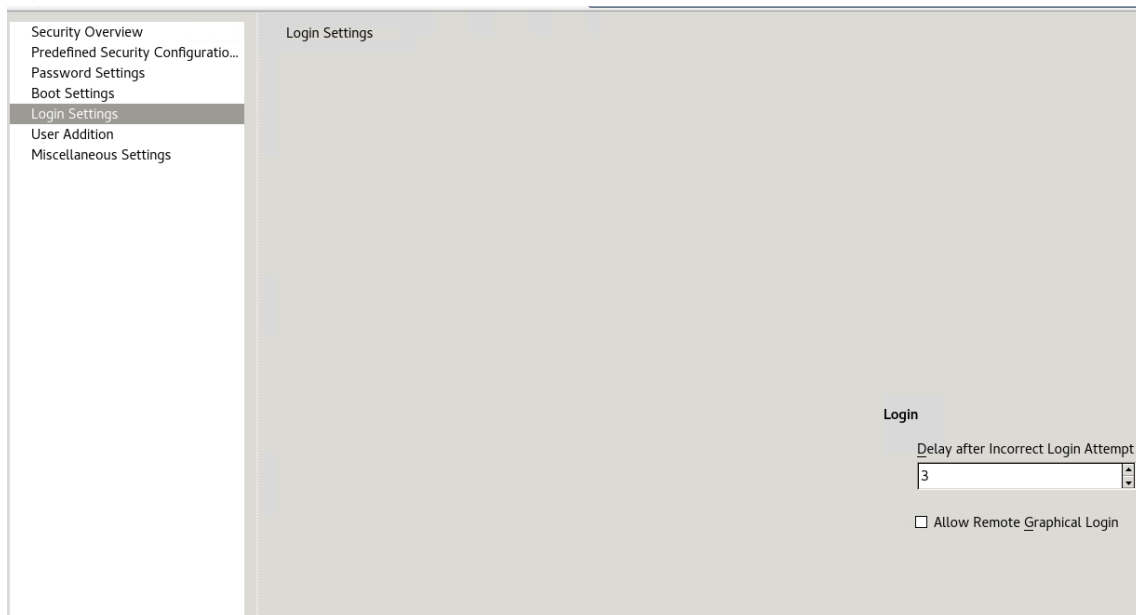
Hardening step 2.4: Set invalid attempt user lockout policy

Configure invalid attempt lockout policy to prevent the use of a user account when the lockout is engaged to protect against brute force attacks. The operating system supports invalid attempt lockout. When the invalid attempt lockout is engaged when a configurable number of invalid operating system login attempts are attempted. This rule may be configured as a temporary lockout (automatically reset after a configurable time-period).

Set invalid attempt user lockout policy using the YaST Graphical User Interface

In **Login settings** there is the capability to set the delay after incorrect login attempts.

Figure 2.2.5.1.6



Set invalid attempt user lockout policy using the command Line User Interface

- **Modify the /etc/pam.d/login file to the following:**

```
auth required pam_tally2.so onerr=fail no_magic_root
account required pam_tally2.so per_user deny=3 no_magic_root reset
```

- The first line counts failed login and failed su attempts for each user. The default location for attempted accesses is recorded in /var/log/faillog.
- The second line specifies to lock accounts automatically after 5 failed logins or su attempts (deny=5). The counter will be reset to 0 (reset) on successful entry if deny=n was not exceeded. But you don't want system or shared accounts to be locked after too many login failures (denial of service attack).
- It is also possible to add the lock_time=n parameter, and then optionally the unlock_time=n parameter. For example, setting the lock_time=60 would deny access for 60 seconds after a failed attempt. The unlock_time=n option would then allow access after n seconds after an account has been locked. If this option is used the user will be locked out for the specified amount of time after he exceeded his maximum allowed attempts. Otherwise, the account is locked until the system administrator removes the lock manually. Refer to the pam_tally man page for more information.
- To exempt system and shared accounts from the deny=n parameter, the per_user parameter was added to the module. The per_user parameter instructs the module *not* to use the deny=n limit for accounts where the maximum number of login failures is set explicitly. For example:

```
jupiter:~ # faillog -u oracle -m -1
Username  Failures  Maximum  Latest
oracle    0         -1       Fri Dec 10 23:57:55 -0600 2005 on unknown
```

- The faillog command with the option -m -1 has the effect of not placing a limit on the number of failed logins—effectively disabling the option. To instruct the module to activate the deny=n limit for this account again, run:

```
faillog -u oracle -m 0
```

- By default, the maximum number of login failures for each account is set to zero (0) which instructs pam_tally to leverage the deny=n parameter. To see failed login attempts, run:

```
faillog
```

- To unlock a locked account (after too many login failures), use the -r option:

```
faillog -u user -r
```

- Make sure to test these changes (and *any* changes – for that matter) thoroughly on your system using ssh and su, and make sure the root id does not get locked! To lock/unlock accounts manually, you can run one of the following commands:

Locking

```
passwd -l user
usermod -L user
```

Unlocking

```
passwd -u user
usermod -U user
```

[Hardening step 2.5: Set the inactivity log out policy](#)

Inactive sessions should be configured to with an auto-log out disconnection to minimize the risk of unauthorized access.

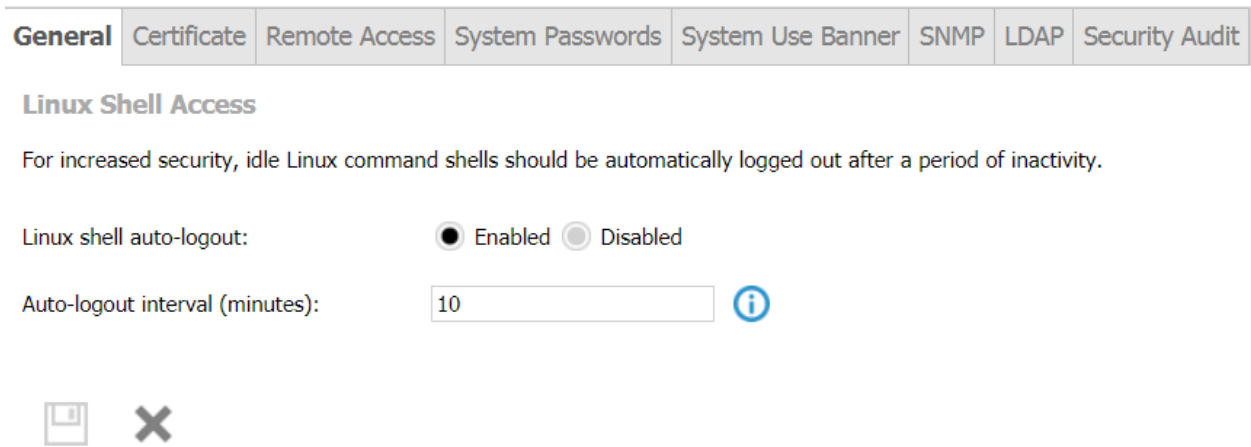
Configure remote access timeout

Table 2.2.5.1.2

| | minimum baseline protection | to strengthen protection |
|---|-----------------------------|---|
| Linux shell auto-log out: | ■ (selected) | ■ (selected) is the strongest setting |
| Auto-log out interval (minutes): | 10 | <i>Lower the interval to strengthen</i> |

You can configure this setting from the VideoEdge Administrator System Configuration General tab.

Figure 2.2.5.1.7



Hardening Step 2.6: Set the password complexity policy

Configure the Operating Systems password length, number of passwords to remember, password encryption method, minimum and maximum password age, and number of days before to give a warning for when a password is about to expire.

Set the password complexity policy using the YaST Graphical User Interface

From Security Center and Hardening tool, select "Password Settings":

Figure 2.2.5.1.8

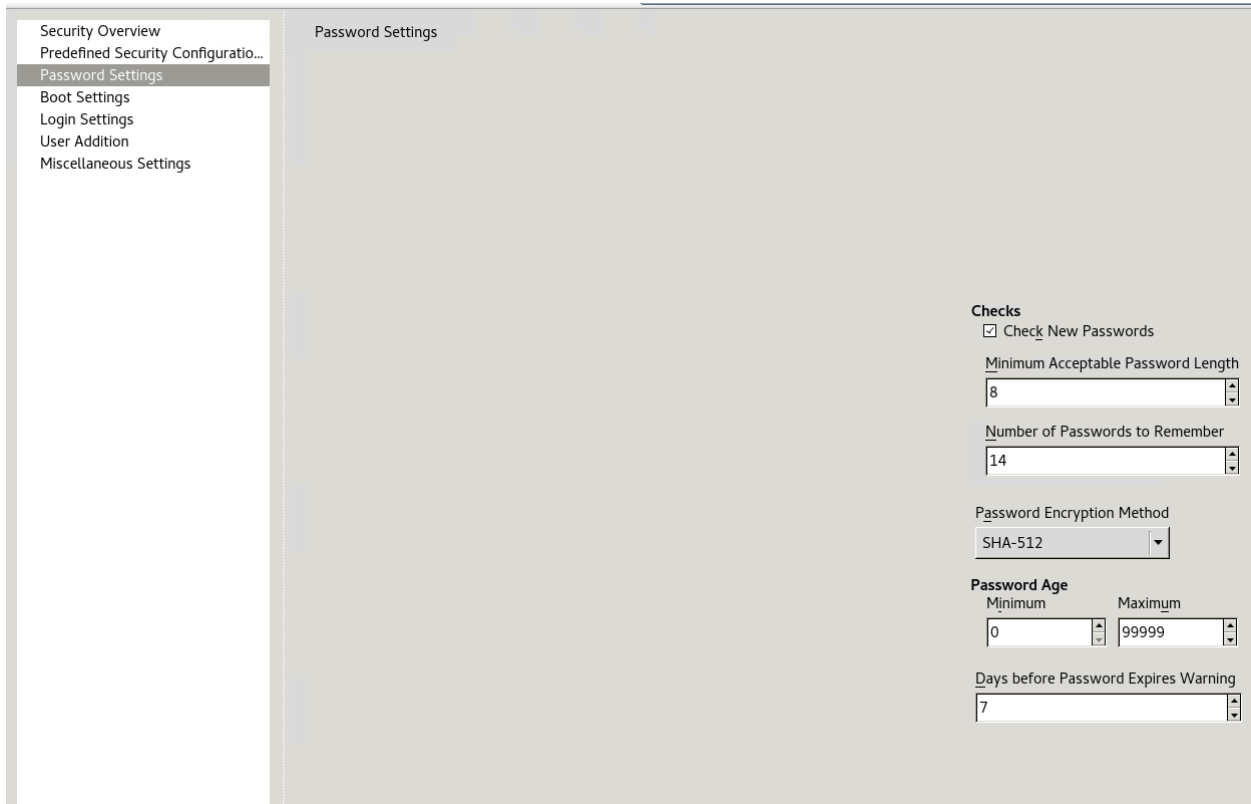


Table 2.2.5.1.3

| | minimum baseline protection | to strengthen protection |
|---|--|--|
| Check New Passwords | <input checked="" type="checkbox"/> (checked) | <input checked="" type="checkbox"/> (checked) is the strongest setting |
| Minimum Acceptable Password Length | 14 | <i>increase length</i> |
| Password Encryption Method | SHA-512 | SHA-512 is the strongest setting |
| Password age minimum | no guidance - consult with local policy / preference | |
| Password age maximum | 90 | <i>shorten length</i> |
| Days before Password Expires Warning | no guidance - consult with local policy / preference | |

Set the password complexity using the Command Line User Interface

Input the following commands into the command line interface:

```
pam-config -a --cracklib --cracklib-minlen=8 --cracklib-lcredit=-1 --cracklib-ucredit=-1 --cracklib-dcredit=-1 --cracklib-ocredit=-1
```

Once set using either method, the use of simple passwords will not be allowed. The system will only accept passwords which satisfy these parameters.

2.2.5.2 VideoEdge roles

Each role must be configured to assure the desired account lockout, inactivity log out and enhanced password validation policies are applied because they can be configured independently.

The Role configuration tab within the Video Administrator System User and Roles provides access to configure the roles local to VideoEdge.

System menu - Role configuration

Figure 2.2.5.2.1

| <input type="checkbox"/> | ROLENAME | INACTIVITY LOCKOUT INTERVAL (DAYS) | FAILED LOGIN LOCKOUT POLICY | FAILED LOGIN RETRY LIMIT | FAILED LOGIN RETRY DELAY (MINUTES) | AUTO LOGOUT | AUTO LOGOUT INTERVAL (MINUTES) | ENHANCED PASSWORD VALIDATION | |
|--------------------------|----------------|------------------------------------|-----------------------------|--------------------------|------------------------------------|-----------------------|--------------------------------|------------------------------|--|
| <input type="checkbox"/> | admin | | None | | | <input type="radio"/> | | Disabled | |
| <input type="checkbox"/> | nvrgroupadmin | | None | | | <input type="radio"/> | | Disabled | |
| <input type="checkbox"/> | operator | | None | | | <input type="radio"/> | | Disabled | |
| <input type="checkbox"/> | snmpuser | | None | | | <input type="radio"/> | | Disabled | |
| <input type="checkbox"/> | softwaresadmin | | None | | | <input type="radio"/> | | Disabled | |
| <input type="checkbox"/> | support | | None | | | <input type="radio"/> | | Disabled | |
| <input type="checkbox"/> | viewer1 | | None | | | <input type="radio"/> | | Disabled | |
| <input type="checkbox"/> | viewer2 | | None | | | <input type="radio"/> | | Disabled | |
| <input type="checkbox"/> | viewer3 | | None | | | <input type="radio"/> | | Disabled | |

Figure 2.2.5.2.2

Rolename: admin

Lockout Policy: Lockout

Retry Limit: 3 (1-50)

Enable Auto Logout:

Auto Logout Interval (minutes): 10 (5-60)

Enhanced Password Validation: Enabled

Remembered Passwords: 3

Note 1: Changing any of the lockout policy settings will unlock all user accounts for this role.

Note 2: The Inactivity Lockout Interval will not apply to admin, support, SoftwareAdmin, nvrGroupAdmin or snmpUser roles.

Note 3: Reducing the number of remembered passwords may cause currently-remembered passwords to be discarded.

Hardening step 3: Configure roles

Hardening step 3.1: Set account lockout policy

Configure the account lockout policy to prevent the use of a user account when the lockout is engaged. VideoEdge supports two types of account lockout:

Invalid attempt lockout – is engaged when a configurable number of invalid login attempts are attempted within a VideoEdge client interface (included VideoEdge Administrator and VideoEdge Client). This rule may be configured as permanent (requiring administrator to reset) or temporary (automatically reset after a configurable time-period).

Hardening guidance for invalid attempt lockout is as follows:

Table 2.2.5.2.1

| role settings | minimum baseline protection | to strengthen protection |
|------------------------------|--|--|
| Lockout Policy | Delay <i>automatically resets lockout</i> | Lockout <i>forces manual reset by administrator</i> |
| Retry Limit | 3 | <i>lower retry limit</i> |
| Retry Delay (minutes) | 10 | <i>increase retry delay</i> |

Inactive account lockout - Accounts may be set to automatically lock if not used within a set time-period, to ensure ex-employee accounts are disabled (Example: 30, 60 or 90 days). When login is attempted after this time-period, the account is locked and may only be unlocked by an administrator.

Table 2.2.5.2.2

| role settings | minimum baseline protection | to strengthen protection |
|--------------------------------|-----------------------------|--------------------------------------|
| Lockout interval (days) | 90 days | <i>lower lockout interval period</i> |

Note 1: Permanent and temporary account lockouts are capable of generating an email alert.

Note 2: Changing any of the lockout policy settings will unlock all user accounts for this role that were previously locked. Therefore, it is important to configure this setting when the system is initialized.

Hardening step 3.2: Set the inactivity log out policy

Configure the session inactivity log out policy to reduce risk of unattended user sessions.

Table 2.2.5.2.3

| | minimum baseline protection | to strengthen protection |
|--|---|--|
| Enabled Auto Log out | <input checked="" type="checkbox"/> (checked) | <input checked="" type="checkbox"/> (checked) is the strongest setting |
| Auto Log out Interval (minutes) | 10 | <i>lower auto log out interval</i> |

Note 1: The Inactivity lockout interval cannot be enabled for admin, support, Softwareadmin, nvrGroupAdmin or snmpUser roles.

Hardening step 3.3: Set the Enhanced Password Validation

Enabling the Enhanced Password Validation assures that the password policy is enabled for the role.

Table 2.2.5.2.4

| | minimum baseline protection | to strengthen protection |
|-------------------------------------|-----------------------------|---|
| Enhanced Password Validation | Enabled | <i>Enabled is the strongest setting</i> |

Hardening step 3.4: Set the Password History policy

The password history setting prevents a user from changing their password to a recently used password.

Table 2.2.5.2.5

| | minimum baseline protection | to strengthen protection |
|-----------------------------|-----------------------------|---|
| Remembered Passwords | 3 | increase the number of remembered passwords |

Note 1: Reducing the value of the Remembered Passwords setting may cause the password history to be cleared from memory.

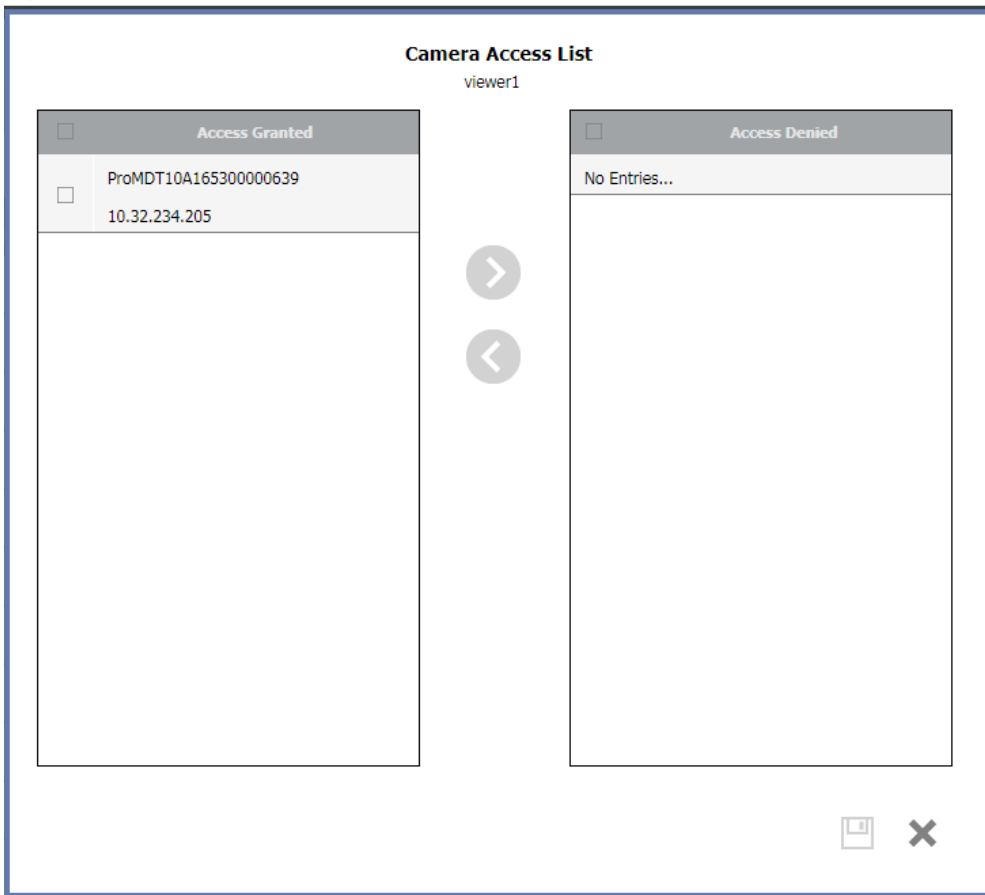
Hardening step 3.5: Set role-based camera access permissions

Use the **Roles** page to configure camera access for the viewer1, viewer2, and viewer3 roles. Filter camera permissions using the **Camera Access** list window. The **Access Granted** list features cameras that the role currently has access to, and the **Access Denied** list features cameras currently hidden from the role.

Select a role to open its **Camera Access** list window and select the checkboxes of the cameras you want to grant or deny access to.

Click the right arrow to move the camera to the **Access Denied** list or click the left arrow to move the camera to the **Access Granted** list.

Figure 2.2.5.2.3



2.2.5.3 VideoEdge user accounts

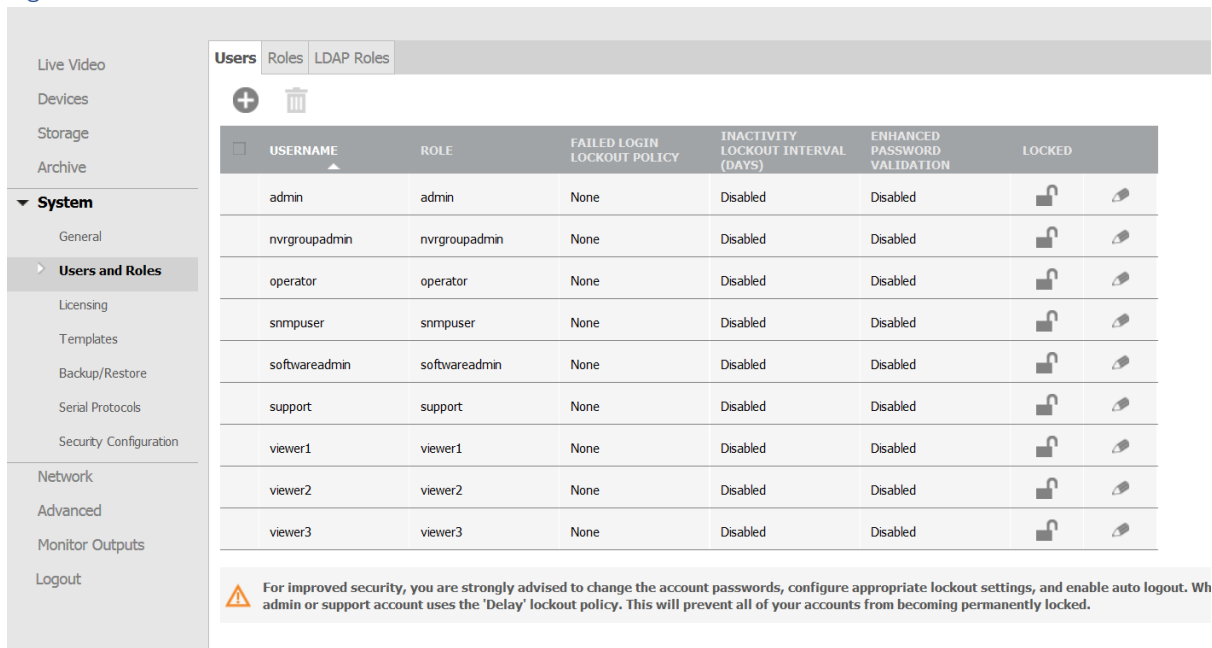
From the VideoEdge administrator you can create new user accounts, edit existing accounts, apply lockout policies and auto log out (lockout and log out policies are ON by default if enhanced security mode is enabled). You can also designate role types for LDAP groups. You can also configure role permissions for LDAP groups which have been configured on your LDAP server.

The user configuration tab within the System User and Roles provides access to configure the user account local to VideoEdge

System menu - User configuration

By default, the VideoEdge NVR comes with the following interactive administrator accounts for use with the VideoEdge Administration Interface.

Figure 2.2.5.3.1



| USERNAME | ROLE | FAILED LOGIN LOCKOUT POLICY | INACTIVITY LOCKOUT INTERVAL (DAYS) | ENHANCED PASSWORD VALIDATION | LOCKED |
|---------------|---------------|-----------------------------|------------------------------------|------------------------------|--------|
| admin | admin | None | Disabled | Disabled | |
| nvrgroupadmin | nvrgroupadmin | None | Disabled | Disabled | |
| operator | operator | None | Disabled | Disabled | |
| snmpuser | snmpuser | None | Disabled | Disabled | |
| softwareadmin | softwareadmin | None | Disabled | Disabled | |
| support | support | None | Disabled | Disabled | |
| viewer1 | viewer1 | None | Disabled | Disabled | |
| viewer2 | viewer2 | None | Disabled | Disabled | |
| viewer3 | viewer3 | None | Disabled | Disabled | |

For improved security, you are strongly advised to change the account passwords, configure appropriate lockout settings, and enable auto logout. Wh admin or support account uses the 'Delay' lockout policy. This will prevent all of your accounts from becoming permanently locked.

Table 2.2.5.3.1

| User and Roles | Description |
|----------------|--|
| Admin | Using this account, you can view and edit the VideoEdge Administration Interface and full functionality of the VideoEdge Client. |
| Operator | Using this account, you can view the VideoEdge Administration Interface and full functionality of the VideoEdge Client. |
| Softwareadmin | Using this account, you can access software updates including camera handler packs. |
| Support | This account is intended for the use by American Dynamics Technical Support, this account password may be changed, and the role is bound by the same access control mechanisms available in the user's page. |
| Nvrgroupadmin | This account is used for communication between NVRs in a group. |
| Snmpuser | This account is used for SNMP communication between NVRs in a group. |

The default interactive viewer accounts are only allowed login into the VideoEdge Client and unable to view or edit the VideoEdge Administration Interface.

Table 2.2.5.3.2

| USER | DESCRIPTION |
|---------|---|
| VIEWER1 | With this account you have full functionality of the VideoEdge Client. |
| VIEWER2 | With this account you have full functionality of the VideoEdge Client with exception of Analog (Real) PTZ. |
| VIEWER3 | With this account you have full functionality of the VideoEdge Client with exception of Analog (Real) and Digital PTZ, Still Image Capture and Clip Export. |

Hardening step 4: Configure VideoEdge user accounts

In this section you can find information on configuring user accounts.

Hardening step 4.1: Create unique user accounts for each user

Each VideoEdge user should have their own dedicated account. An operator must not use built-in accounts.

Note: If an LDAP server is handling VideoEdge authentication this step is not recommended because providing multiple accounts (one for LDAP and one local account) will introduce a security risk.

Hardening step 4.2: Assign roles

Roles should be assigned to users to assure the best practices for user management are followed. The assignment of the role to users sets their authorizations. Therefore, role assignment should consider what a user “needs to have access to” following the principles of least privilege and separate of duties. The definition of roles will be configured in hardening step 2, Configure Roles.

The **Security Audit** page **Role Settings** displays which roles have features such as Auto Log out and **Failed Login Lockout** enabled and the number of users within that role.

Figure 2.2.5.3.2

Role Settings

| ROLE | NUM USERS | AUTO LOGOUT INTERVAL (MINUTES) | FAILED LOGIN LOCKOUT | MAX LOGIN ATTEMPTS | INACTIVITY LOCKOUT INTERVAL (DAYS) | ENHANCED PASSWORD VALIDATION |
|---------------|-----------|--------------------------------|----------------------|--------------------|------------------------------------|------------------------------|
| nvrgroupadmin | 1 | N/A | Disabled | N/A | Disabled | Disabled |
| softwareadmin | 1 | Disabled | Disabled | N/A | Disabled | Disabled |
| admin | 1 | Disabled | Disabled | N/A | Disabled | Disabled |
| support | 1 | Disabled | Disabled | N/A | Disabled | Disabled |
| snmpuser | 1 | N/A | Disabled | N/A | Disabled | Disabled |
| operator | 1 | Disabled | Disabled | N/A | Disabled | Disabled |
| viewer1 | 1 | Disabled | Disabled | N/A | Disabled | Disabled |
| viewer3 | 1 | Disabled | Disabled | N/A | Disabled | Disabled |
| viewer2 | 1 | Disabled | Disabled | N/A | Disabled | Disabled |

Hardening step 4.3: Lock built-in accounts

Built-in accounts should be set to “locked” after they are replaced with unique accounts for each user. It is important that there is a user assigned to each of the required roles before disabling the built-in user accounts.

Hardening step 4.4: Change passwords of built-in accounts

All default passwords should be changed even if an account is locked. This will assure that even if the account is inadvertently enabled, access will not be granted if a default password is entered on logon.

TIP: The Security Audit page **User Settings** displays the status of default passwords in use by comparing the default hash against the stored hash. If there is a match, the test will be red indicating the default password is still being used.

Figure 2.2.5.3.3

User Settings

| USERNAME | DEFAULT PASSWORD |
|---------------|------------------|
| admin | Yes |
| nvrgroupadmin | Yes |
| operator | Yes |
| snmpuser | Yes |
| softwareadmin | Yes |
| support | Yes |
| viewer1 | Yes |
| viewer2 | Yes |
| viewer3 | Yes |

2.2.5.4 VideoEdge LDAP Authentication

Hardening step 5: Configure LDAP and LDAP roles

The configuration and use of a Lightweight Directory Access Protocol (LDAP) server to authenticate users of both the VideoEdge Administration Interface and VideoEdge Client is recommended. This minimizes configuration of users on VideoEdge and enables multiple NVRs to share one centralized server for user management.

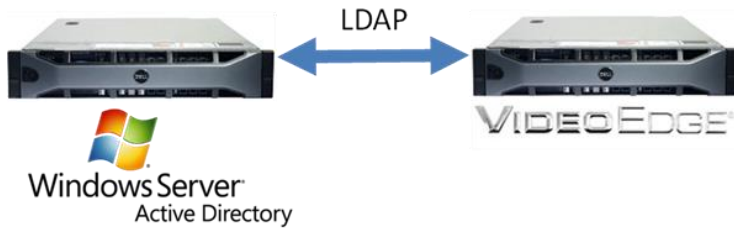
When integrating with Microsoft Active Directory, a secure connection using a Certificate Authority certificate for the LDAP server is recommended.

It is recommended that you establish a secure connection before you perform the following actions:

- Logging on to the VideoEdge as an LDAP user.
- Retrieving a list of LDAP groups on the LDAP Roles page.

VideoEdge integrates with LDAP servers as shown in the following Microsoft Windows Server Active Directory example:

Figure 2.2.5.4.1



To enable LDAP authentication, including configurations for Active Directory, in VideoEdge access the Security configuration, LDAP tab of the VideoEdge system menu and complete the configuration form.

- From the **System menu**, click **Security configuration**, then click the **LDAP** tab.

System menu – Security configuration – LDAP tab

Figure 2.2.5.4.2

The screenshot shows the 'LDAP' tab selected in the 'Security configuration' menu. The interface includes a navigation bar with tabs: Certificate, Remote Access, System Password, System Use Banner, SNMP, LDAP (selected), and Security Audit. Below the navigation bar, the 'User Authentication Method' section has a question mark icon and an unchecked checkbox labeled 'Use LDAP for VideoEdge administrator and VE Client authentication'. The 'LDAP Client Configuration' section contains a 'Server Address' text field, 'Use Active Directory' and 'Secure Connection' checkboxes. The 'LDAP User Query Configuration' section has a 'User Query DN' text field. The 'LDAP Group Query Configuration' section includes 'Base DN', 'Administrator DN', and 'Search Filter' text fields, a 'Fetch DN' button, and a question mark icon next to the 'Search Filter' field.

Hardening step 5.1: Configure LDAP

LDAP may be enabled for VideoEdge administrator and VideoEdge Client authentication. It is recommended that the LDAP communication utilize the secure connection setting which validates the presence of a Certificate Authority signed certificate.

Table 2.2.5.4.1

| | minimum baseline protection | to strengthen protection |
|--|---|--|
| Use LDAP for VideoEdge administrator and VE client authentication | <input checked="" type="checkbox"/> (checked) | <input checked="" type="checkbox"/> (checked) is the strongest setting |
| Secure connection | <input checked="" type="checkbox"/> (checked) | <input checked="" type="checkbox"/> (checked) is the strongest setting |

Note: If the LDAP server is offline, access to the VideoEdge Administration Interface/VideoEdge Client can only be achieved using the local on-board credentials.

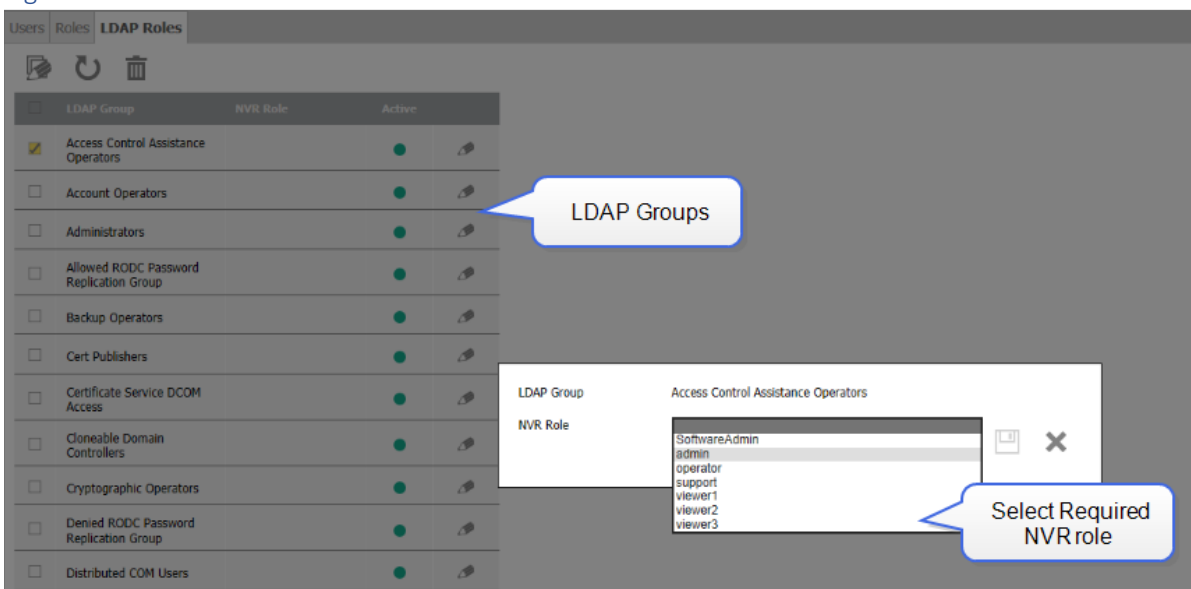
System menu - LDAP Role configuration

Once an LDAP server has been configured on VideoEdge, you can link LDAP Groups to VideoEdge Roles. This means that all users in the LDAP Group will be assigned the linked role on VideoEdge.

Hardening step 5.2: Configure LDAP Roles

Map each role within VideoEdge that will support LDAP users to the respective LDAP group.

Figure 2.2.5.4.3



2.2.6 User management overview

As VideoEdge has been designed as an appliance, users do not need to login to VideoEdge operating system directly. Software access to VideoEdge is conducted from a remote application or webpage. Some administrators may choose to login to the Operating system directly to deploy operating system level updates. In such cases, unique operating system level accounts are recommended.

You can create unique user accounts for each operator of the VideoEdge application or webpage. These interfaces support either local accounts or accounts managed by an LDAP compliant server, such as Active Directory.

Operator functions in VideoEdge are controlled by a role-based access control (RBAC) feature set. With RBAC, a user is assigned a role in which they acquire the permissions associated with that role.

The proper configuration of individual user accounts assures that security best practices are followed and that all user actions cannot be repudiated.

2.2.6.1 Password policy configuration

The built-in VideoEdge password policy is non-configurable. In Enhanced Security Mode, you are required to create new user accounts and passwords to replace the default root and VideoEdge accounts.

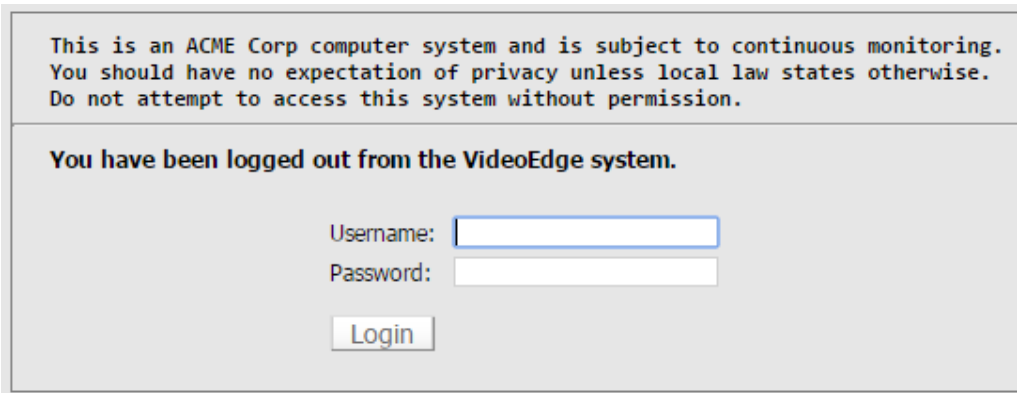
2.2.6.2 System use banner

A System Use Banner provides the operator with details on the system use policy they must comply with in order to use the system. The banner message text needs to be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance that governs the system use.

This message is displayed prior to the user login. By logging on to the system the user is acknowledging their acceptance of the policy outlined in the banner

Example:

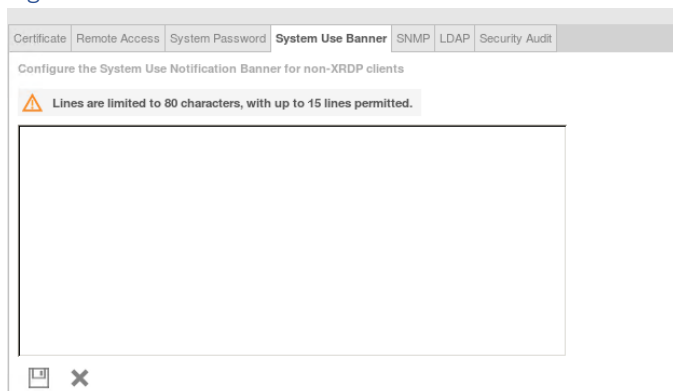
Figure 2.2.6.2.1



Hardening step 6: Configure the system use banner

You can configure the system use banner from the System Configuration menu, System Use Banner tab. Entry of the message can utilize text or an image.

Figure 2.2.6.2.2



2.3.0 Additional operating system hardening

You can perform additional operating system hardening using YaST.

When the Security Center and Hardening tool is opened, it displays a security overview by default showing the status of the security features as either enabled or disabled:

Figure 2.3.0.1

| Security Setting | Status | Security Status |
|---|---------------------------|------------------------|
| Use magic SysRq keys | Configure | ✓ Help |
| Use secure file permissions | Configure | ✗ Help |
| Remote access to the display manager | Disabled | ✓ Help |
| Write back system time to the hardware clock | Enabled | ✓ Help |
| Always generate syslog message for cron scripts | Disabled | ✗ Help |
| Run the DHCP daemon in a chroot | Unknown | ✗ Help |
| Run the DHCP daemon as dhcp user | Unknown | ✗ Help |
| Remote root login in the display manager | Disabled | ✓ Help |
| Remote access to the X server | Disabled | ✓ Help |
| Remote access to the email delivery subsystem | Unknown | ✗ Help |
| Restart services on update | Disabled | ✓ Help |
| Stop services on removal | Disabled | ✓ Help |
| Enable TCP syncookies | Enabled | ✓ Help |
| IPv4 forwarding | Disabled | ✓ Help |
| IPv6 forwarding | Disabled | ✓ Help |
| Enable basic system services | Configure | ✗ Help |
| Disable extra services | Configure | ✗ Help |

To refresh the status, the security center and hardening tool will need to be closed and re-launched.

Hardening step 7: Security center and hardening configuration

In this section you can find information on the security center and hardening configuration

Hardening step 7.1: Select a predefined or custom security configuration

There are four predefined security configurations to choose from: **Workstation**, **Roaming Device**, **Network Server**, or **Custom Settings**.

1. From Security Center and Hardening tool, select **Predefined Security Configuration**.

Figure 2.3.0.2



2. Configure your workstation and network to the following settings:

Figure 2.3.0.3

| Security Setting | Status | Security Status |
|---|---------------------------|------------------------|
| Use magic SysRq keys | Configure | ✓ Help |
| Use secure file permissions | Configure | ✗ Help |
| Remote access to the display manager | Disabled | ✓ Help |
| Write back system time to the hardware clock | Enabled | ✓ Help |
| Always generate syslog message for cron scripts | Enabled | ✓ Help |
| Run the DHCP daemon in a chroot | Unknown | ✗ Help |
| Run the DHCP daemon as dhcp user | Unknown | ✗ Help |
| Remote root login in the display manager | Disabled | ✓ Help |
| Remote access to the X server | Disabled | ✓ Help |
| Remote access to the email delivery subsystem | Disabled | ✓ Help |
| Restart services on update | Disabled | ✓ Help |
| Stop services on removal | Disabled | ✓ Help |
| Enable TCP synccookies | Enabled | ✓ Help |
| IPv4 forwarding | Disabled | ✓ Help |
| IPv6 forwarding | Disabled | ✓ Help |
| Enable basic system services | Configure | ✗ Help |
| Disable extra services | Configure | ✗ Help |

Table 2.3.0.1

| | minimum baseline protection | to strengthen protection |
|----------------------------|--|--|
| Check New Passwords | <input checked="" type="checkbox"/> Network Server | <input checked="" type="checkbox"/> Custom Settings select Network Server + additional protection |

The network configuration adds in use of secure file permissions of the workstation profile. A custom profile provides the flexibility to configure specific settings tailored for the target environment. The **Roaming Device** profile is not suitable because the VideoEdge hardware is stationary.

Hardening step 7.2: Set boot permissions

In the security center and hardening you can set boot permissions. The administrator can set what the system will do when a user executes Ctrl+Alt+Delete. You can restrict shutdown to root only and set the system to require authentication to hibernate the NVR.

Figure 2.3.0.4

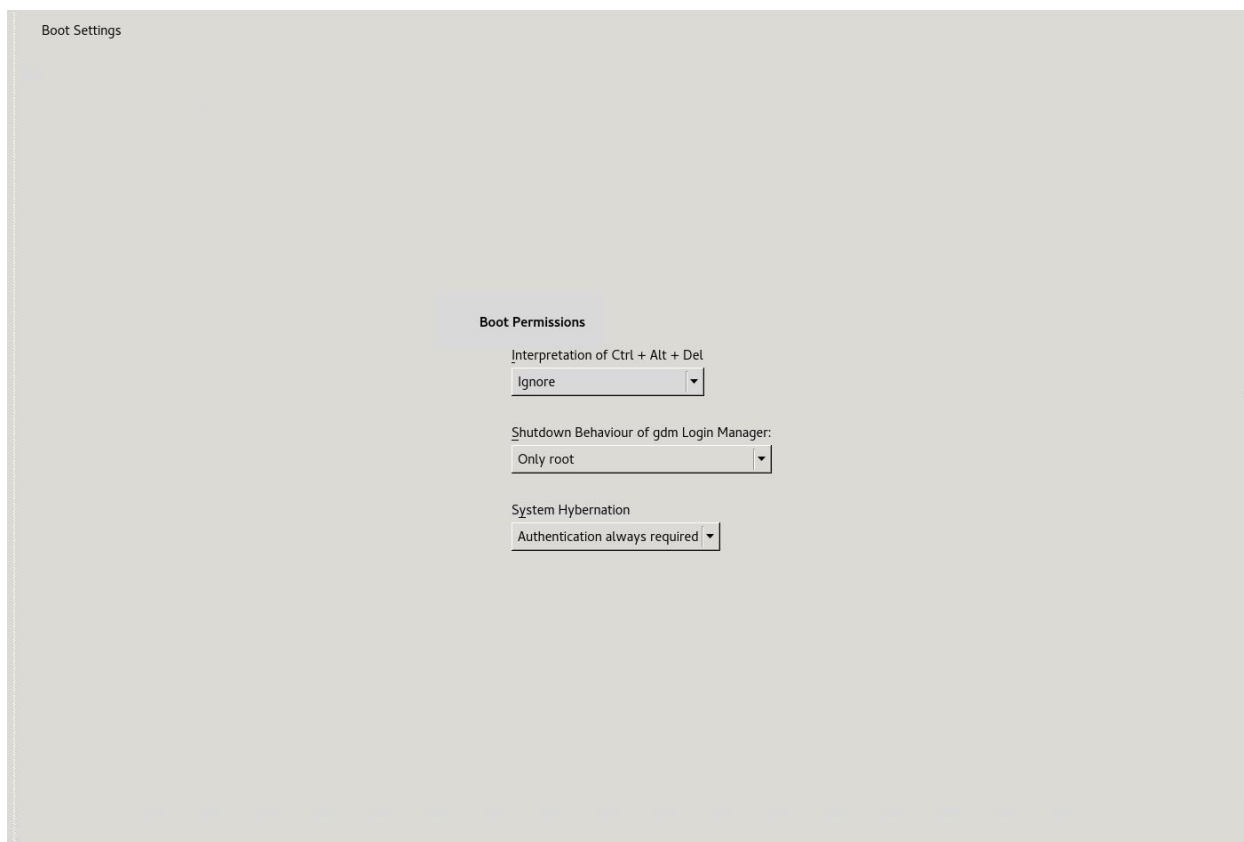


Table 2.3.0.2

| | minimum baseline protection | to strengthen protection |
|---|-----------------------------|------------------------------------|
| Interpretation of Ctrl + Alt + Del | Reboot | Ignore |
| Shutdown behavior of GDM | Only root | Only root is the strongest setting |
| System Hibernation | User on console | Authentication always required |

Hardening step 8: Modify Windows TLS version

Integrated Driver Service only supports TLS 1.2 and above. To modify the TLS version in Windows, complete the following steps:

1. In Windows open the **Control Panel**.
2. Click **Control Panel > Internet Options**.
3. Click **Advanced**.
4. Enable the appropriate TLS version for VideoEdge and any other applications.
5. Click **Apply**.
6. Click **OK**.

2.4.0 Software updates

Here you can find information on software updates including operating system updates, VideoEdge application updates, and camera updates.

2.4.1 Operating System updates

Hardening step 9: Update software

VideoEdge should be updated to the current released version with all applicable patches applied during and after the commissioning process. Applying security patches assists in mitigating known vulnerabilities. It is important that any known issue is addressed, even during the commissioning process.

Hardening step 9.1: Update operating system software

Operating system updates are distributed with each release of VideoEdge. To update the operating system, run the most current update of VideoEdge. Refer to Hardening step 8.2, Update VideoEdge software, to update the operating system to latest supported version.

2.4.2 VideoEdge application updates

You can apply VideoEdge software updates or patches using the **Softwareadmin** user credential.

The current version of the installed software is displayed. To update the software, you must upload a new software package and then install the update.

Caution: NVR Services cease during a software update; this results in a pause in recording until the operation is completed and the system reboots. You will be prompted to reboot the VideoEdge when the update completes.

Hardening step 9.2: Update VideoEdge software

1. Login using the **Softwareadmin** user credential.
2. Enter **softwareadmin** in the **username** field.
3. Enter your password.

Note: The default password for the **Softwareadmin** user credential is **Softwareadmin**. This password is changed with successful completion of hardening step 4.4

The Update Software page opens.

4. Click **Browse**.
5. Select the update or patch file and click **Open**.
6. The name and file path of the patch file appears in the **Upload New Package** field.
7. Click **Upload**.
8. The uploaded package is displayed in the **Uploaded Packages** list.
9. Select the new package from the list and click **Install**.

Note: The software upgrade process will interrupt recording and the recorder will automatically reboot, as necessary.

1. Once the NVR reboots, select the uploaded package, and click **Delete**.
2. Select **Logout**.
3. A dialog box opens asking 'Are you sure you want to logout?'
4. Click **OK**.

2.4.3 Camera updates

Hardening step 9.3: Update camera firmware

To apply firmware updates, navigate to the **Video Edge Administrator Update Camera Firmware** page, and enter the **softwareadmin** user credential. The **Update Camera Firmware** page lists the cameras currently added to the VideoEdge whose firmware can be updated. To update camera firmware, upload a new camera firmware package and install the update. A progress status displays to the right of the camera table.

Note: Firmware uploaded for a camera model is deleted and replaced with any firmware subsequently uploaded for that same model.

2.5.0 Communication hardening

Communication hardening limits an attacker's ability to gain access to VideoEdge. Attackers look for weakness in communication protocols, and communications that is left on encrypted and unauthenticated include the risk that the attacker will be successful in their efforts. Employ techniques to harden the communication interfaces and the transmission of data within this section.

2.5.1 Communication management best practices

Communication to and from the VideoEdge NVR should be configured according to the principle of least functionality.

Least functionality is a security measure designed to limit functions only to those required for the target application and communication sessions used at a given time. In configuring components in this manner, the attack surface is reduced and with it the risk of a cybersecurity breach is minimized.

2.5.2 Communication port and encryption configuration

The communication ports settings for VideoEdge are available within the System and Network pages of VideoEdge administrator.

Note: The Security Audit page, Ports and Protocols section displays of summary of which ports and protocols are enabled.

Figure 2.5.2.1

Web Server Ports and Protocols

| HTTP ENABLED | HTTP USES DEFAULT PORT | HTTPS USES DEFAULT PORT | UPnP | TLSV1 ENABLED |
|--------------|------------------------|-------------------------|------|---------------|
| Yes | Yes | Yes | Yes | No |

Hardening Step 10: Configure communication ports and encryption

In this section you can find information on configuring communication ports and encryption.

Hardening step 10.1: Configure ports using the network, general page

From the Network General page, it is possible to configure the RTSP port, SNMP, UPnP, Multicast, NTP ports:

Figure 2.5.2.2

The screenshot shows the 'Network General' configuration page. The settings are as follows:

- Domain Name: [Empty text box]
- Domain Name Servers: [Green plus icon]
- Default Gateway: [Empty text box]
- RTSP Port: [554]
- RTSP Encryption: Enabled Disabled
- SNMP Port: [161]
- UPnP: Enabled Disabled [Information icon]
- Multicast: Enabled Disabled
- Multicast Start Port: [9000]
- Multicast End Port: [9511]
- NTP Status: Enabled Disabled
- WAN Bitrate Cap: [Max] [Dropdown arrow]
- LAN Bitrate Cap: [Max] [Dropdown arrow]

At the bottom left, there are two icons: a document with a checkmark and a close (X) button.

RTSP Port – This port is required for communications with cameras that are configured to stream video over RTSP. The default port value of 554 is configurable.

RTSP Encryption – Using the RTSP Encryption feature victor and VideoEdge NVR can transmit RTSP credentials and RTSP commands (Describe, Options, Setup, Play, Teardown, and Announce) over a secure, encrypted TLS tunnel.

SNMP Port – This is the port that the Simple Network Management Protocol (SNMP) is sent over. The NVR uses SNMP for communication purposes when using the NVR Groups functionality. If required, you can modify the default SNMP port for your NVR to conform to your network rules. The default port value of 161 is configurable.

UPnP – Should only be used during commissioning to aid with the discovery process. Once your devices are discovered, UPnP should be disabled. By default, the NVR sends UPnP advertisements to allow victor unified client to discover it on a network.

Multicast – Is used to provide streams to connected clients. However, its use can utilize more network resources and can impact system availability. Use of multicast is generally discouraged from a hardening perspective because it can impact system availability. When multicast is enabled the port range is defined by the configurable start and end port fields.

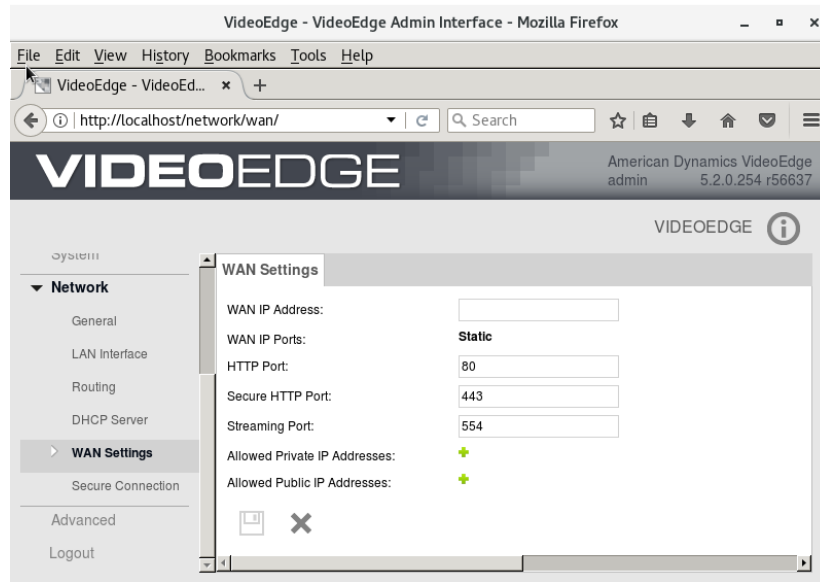
NTP – Is used to synchronize time throughout the network to an external NTP server. Its use is encouraged for system hardening because it assures that all logs are referencing the same time. When enable NTP will use port 123.

Table 2.5.2.1

| | minimum baseline protection | to strengthen protection |
|------------------------|---------------------------------------|--------------------------------------|
| RTSP Encryption | ▪ (Enabled) | ▪ (Enabled) is the strongest setting |
| UPnP | ▪ (Enabled) during commissioning only | ▪ (Disabled) after commissioning |
| Multicast | Use if required | ▪ (Disabled) |
| NTP Status | ▪ (Enabled) | ▪ (Enabled) is the strongest setting |

WAN and LAN Bitrate Caps - To assist network balancing you can assign both a WAN and LAN bitrate cap. A bitrate cap limits the amount of streaming data (video) leaving the NVR to remote clients or clients connected using VPN. You can set the WAN and LAN bitrate caps to either a predefined value from the dropdown menus or alternatively you can enter a custom value in the field.

Figure 2.5.2.3



HTTP Port – This port is used for all non-secure web communications. The default value of 80 is configurable.

Secure HTTP Port – This port is used for all secure web communications. The default value of 443 is configurable.

Streaming Port – This is the port number used for the real time streaming protocol (RTSP) connection. The default value of 554 is configurable.

If more than one NVR is behind the NAT firewall, they will need to be allocated different external ports on the NAT firewall. This page is used to let external client know what ports to use to contact VideoEdge. For example, when video is being streamed to a client programmatically by RTSP, port 554 is the default port for RTSP connection. However, if two NVRs are behind the same NAT firewall, they are both exposed as the same public address, so the only way to distinguish between them is to set up port forwarding rules at the firewall level. This means that both NVRs listen on port 554 for HTTPS requests but that publicly NVR1 might be contactable as `https://70.30.22.81:554`, while NVR2 is contactable as `https://70.30.22.81:100554`. The firewall is configured to accept NVR2 requests at `https://70.30.22.81:100554` and forward them to `https://<NVR2 private IP>:554`.

The HTTP, HTTPS, and RTSP port fields must be set in scenarios where multiple NVRs are situated behind the same NAT firewall. In this example, the RTSP field on NVR2 must be set to 10554.

Allowed Private IP - These are the private IP addresses that are permitted for use with the VideoEdge:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

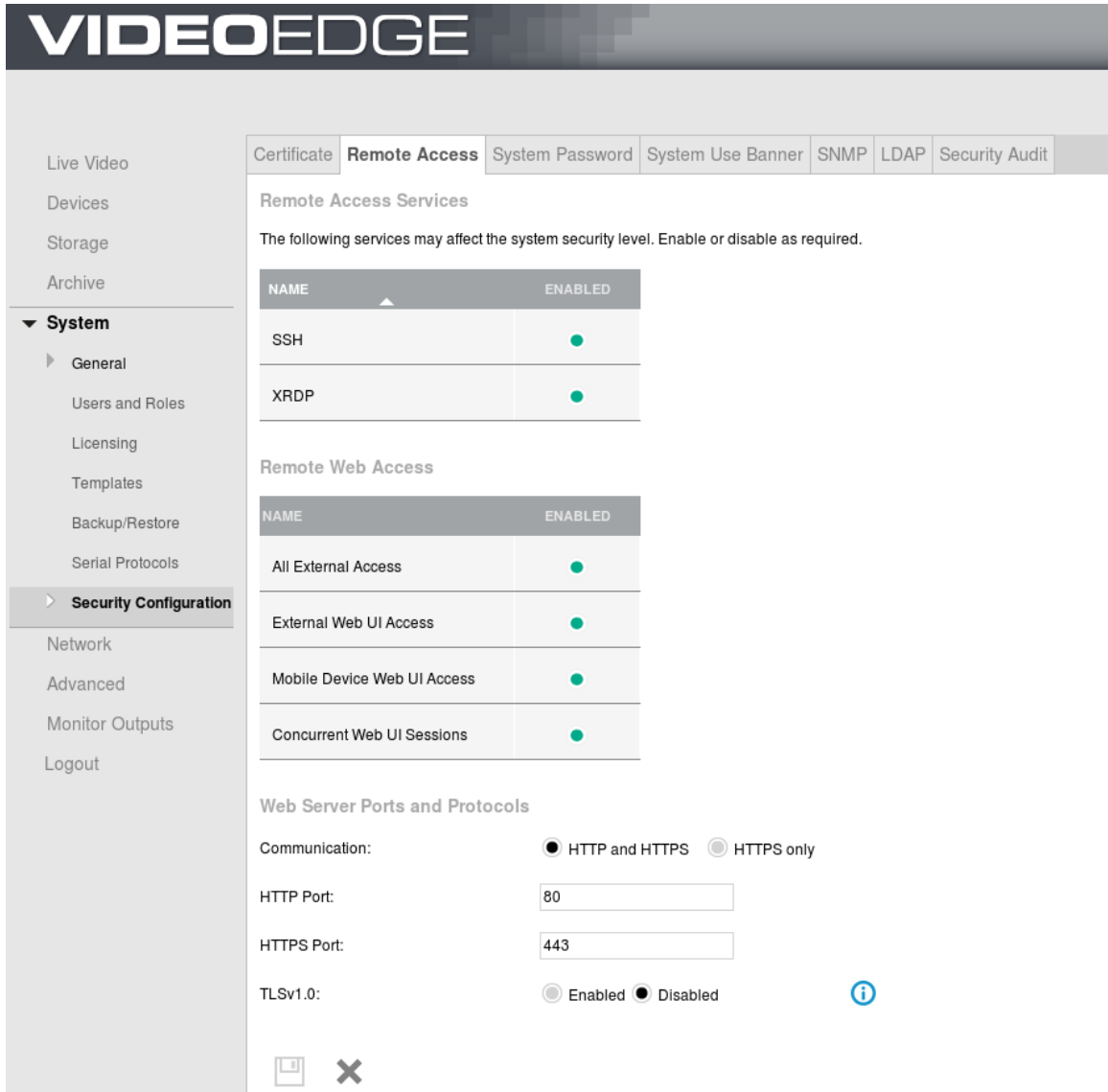
You can add a maximum of 20 Allowed IP Addresses to the VideoEdge.

Public IP Addresses - A public IP address is one that is not within the Private IP ranges

Hardening step 10.3: Configure remote access using the system page, remote access tab

Using the remote access tab, the administrator can enable or disable remote access services, restrict, or disable web and mobile access, and change ports used for HTTP and HTTPS communications.

Figure 2.5.2.4



Remote Access Services

The remote access services VideoEdge supports are SSH and RDP

SSH (Secure Shell) - is an encrypted network protocol for text-based sessions on remote machines (for example, VideoEdge) from another machine that has network access. 'PuTTY' is a common piece of software used to access remote machines by SSH.

To avoid having to logon to the VideoEdge server directly, the SSH interface can provide remote administrative access for those familiar with command line interfaces.

RDP (Remote Desktop Protocol) - is a graphical desktop sharing protocol developed by Microsoft. It allows control of remote machines (for example, VideoEdge) from another machine that has network access. Using

the 'Remote Desktop Connection' available in Windows you can access remote VideoEdge recorders using the VideoEdge's XRDP server.

To avoid having to logon to the VideoEdge server directly, the XRDP can provide remote administrative access.

Remote Web Access

Remote web access can be restricted in the following ways.

All External Access: Disabling all external access is the most restrictive configuration. Disabling external access prevents the external administration of VideoEdge. It will also disable access from victor Client (possibly including the ability to play video), although recording will not be affected. You will need to physically connect to the NVR to re-enable external access.

External Web UI Access: Disabling external web UI access prevents external administration of VideoEdge. To enable external web UI access, you must physically connect to the NVR.

Mobile Device Web UI Access: Disabling Mobile Device Web UI access prevents external administration of VideoEdge from a mobile device. You will need to physically connect to the NVR or use a non-mobile device to re-enable mobile device web UI access.

Concurrent Web UI Sessions: Disabling concurrent web UI sessions means that only one login for each web UI account is allowed at a time. It is the system owner's responsibility to assign every person accessing the VideoEdge system a unique user account and prevent multiple users from sharing the same account. Disable concurrent web UI sessions to highlight to a user that someone may be logged into the web UI using their account. Always terminate a web UI session when you finish your work. When concurrent web UI sessions are disabled, to increase security and avoid false alarms, use the **Logout** button to terminate a web UI session rather than just closing the browser tab.

Web Server Ports and Protocols

HTTPS is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. It is recommended that you use HTTPS only. It is also recommended that you change default ports to help defend against non-targeted attacks.

Tip: The Security Audit tab, *Remote Access* section displays which remote access protocols are enabled, what the current certificate setting are. It also displays if a certificate Authority is installed, SNMP settings and system robustness.

SSH: Secure Shell is a cryptographic network protocol for secure data communication. Using the SSH protocol on the VideoEdge NVR you can get remote access to the server and is also used for failover functionality. (Default port 22 – not configurable, disabled by default)
xRDP: Using Microsoft Remote Desktop Protocol you can get remote desktop access to the VideoEdge NVR. (Default port 3389- not configurable, disabled by default)
TLS: Transport Layer Security is a protocol used for encrypted communication such as HTTPS. (Default port 443 – configurable, VideoEdge uses TLS 1.2)

2.5.3 Communication certificate support

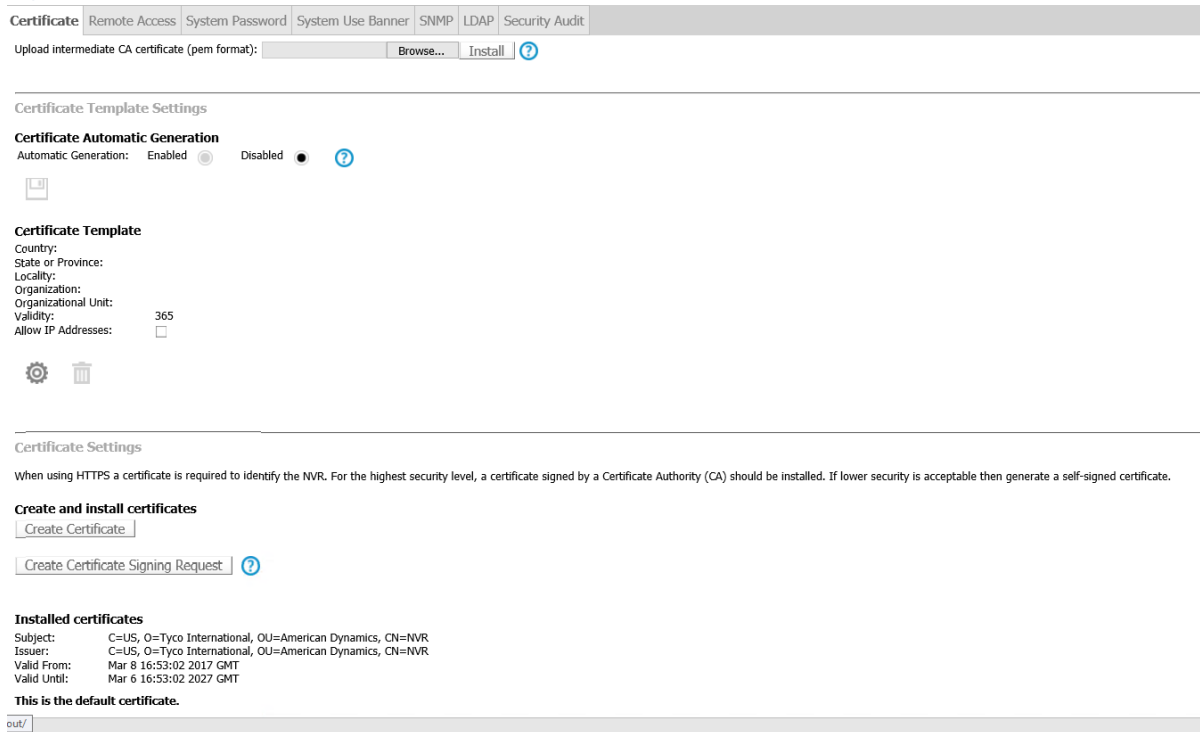
HTTPS encrypts web traffic but does not verify the identity of the remote host without a properly configured digital certificate. VideoEdge NVRs allow you to create a certificate that is unique to the individual NVR so your

web browser or victor client can verify its identity. The certificate can be self-signed, or for more security-conscious customers, a trusted certificate authority can sign it. VideoEdge certificates use 2048-bit keys.

Victor Client can use the digital certificate feature in VideoEdge NVRs to ensure that communications between the two are secure and to verify the identity of recorders added to victor Client. To get instructions on how to install Device Authentication and certificates refer to VideoEdge *NVR Installation and User Guide*.

Hardening step 11: Configure Communication Certificate

Figure 2.5.3.1



1. Select the type of certificate to use; automatically generated or from a trusted certificate authority (CA). If using CA generated certificate disable automatic generation and install the CA generated certificate.

Table 2.5.3.1

| | minimum baseline protection | to strengthen protection |
|-----------------------------|-----------------------------|---|
| Automatic Generation | Enabled ■ | Disabled ■ <i>(must install signed certificate from trusted certificate authority if disabled)</i> |

2. To verify that the certificate is successfully installed view the Installed certificates details. The valid date range should encompass the current date.

Network protection

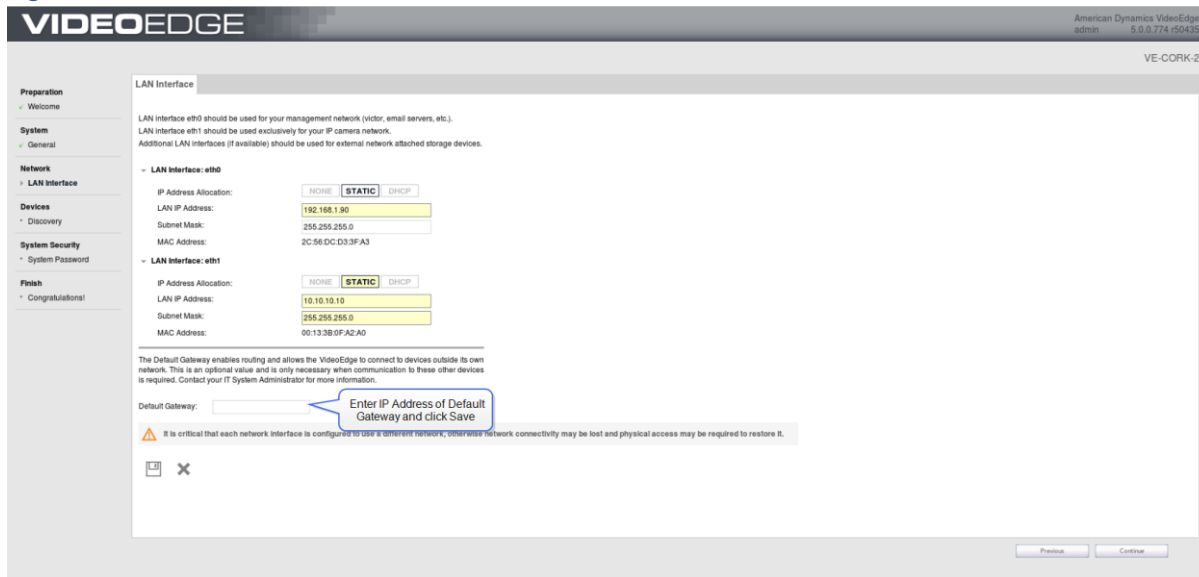
A VideoEdge NVR has multiple network interface controllers (NICs). The NICs are both physically and logically separated by default and can only be bridged by a Linux administrator allowing the NVR to act as a barrier between the camera network and the management network.

Potentially vulnerable cameras are protected from an attack initiated on the production network. Also, if a camera is located where a physical attack is possible, this separation prevents an attacker from gaining access to the production network if the camera port is compromised.

Hardening step 12: Assure cameras are connected to the protected LAN

The protected LAN port is labeled as “eth1.” This port is configured using the VideoEdge Administrator. On first startup the **VideoEdge Setup Wizard** is present this setting:

Figure 2.5.3.2



Camera security settings

When an IP camera is added to an NVR, the server uses the manufacturer’s default communication and security settings to communicate with the camera.

Administrators can change the default settings of the connected cameras. However, when these are changed the NVR will lose communications with the camera as the NVR will utilize default passwords and non-encrypted communications unless configured manually to match the camera settings.

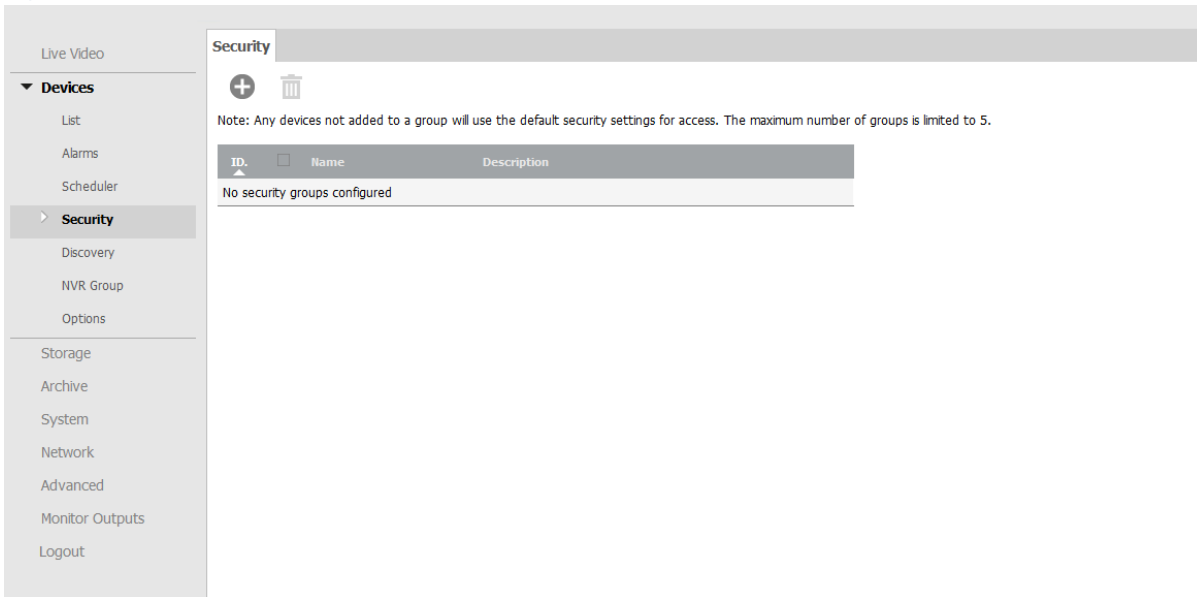
Hardening step 13: Configure camera security settings

To harden camera communications, change the default passwords on all cameras. If a camera supports an encrypted communications method that VideoEdge also supports, such as HTTPS using TLS 1.2, encryption should also be enabled on those cameras.

Once the camera configuration has been changed, through web interfaces, you need to configure VideoEdge with matching settings.

In VideoEdge, a security group is used to simplify the connection of multiple cameras with the same settings and is required to change the communication settings used to connect cameras that are not used default settings. The security group is added from the VideoEdge Administrator Devices Security page.

Figure 2.5.3.3



Once a security group is created, the new password and communication method (labeled as “Security Level” with settings of HTTP/Basic, HTTP/Digest or HTTPS) may be assigned and cameras with the same settings added to that group.

Note: The camera security groups feature is applicable to IP cameras and encoders only. Analog cameras connected directly to the NVR do not have password capabilities.

Figure 2.5.3.4

Security Group

Group Name:

Description:

Leave the following blank for camera default.

Username:

Password:

Advanced Settings

Security Level:

Port:

ONVIF RTSP Authentication:

Cameras

Available Cameras

Cameras In This Group

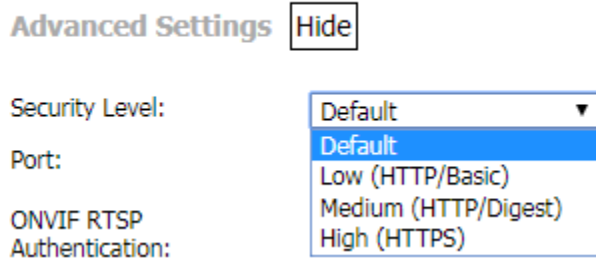
>

<

Save

Close

Figure 2.5.3.5



2.5.4 FIPS 140-2 support

Enabling FIPS on 5.6

The 5.0 VideoEdge release includes FIPS packages to allow the OS to run in a FIPS enabled mode. The VideoEdge product is not classified as FIPS compliant and has NOT been through a certification/validation process.

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules. The title is Security Requirements for Cryptographic Modules.

A FIPS module is a cryptographic module which may be comprised of hardware, firmware or software that implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques and random number generation.

[Hardening step 14: Enable FIPS](#)

When FIPS is enabled, both the Linux kernel and some libraries perform extra integrity checks to ensure they have not been tampered with. Additionally, only FIPS compliant crypto algorithms will be allowed. For example, OpenSSL will not allow the use of the deprecated MD5 hash.

FIPS packages are included beginning in VideoEdge NVR version 5.1. However additional command line steps are needed to enable FIPS.

1. Login to VideoEdge
2. Open a terminal type su – then enter root password
3. Query the current status: `/opt/americandynamics/venvr/bin/fipsmode`
4. Enable FIPS mode `/opt/americandynamics/venvr/bin/fipsmode 1`
5. Disable FIPS mode `/opt/americandynamics/venvr/bin/fipsmode 0`

Changes will take effect upon the next reboot.

2.6.0 Configuring security monitoring features

In this section you can find information on configuring security monitoring features.

2.6.1 Audit logs

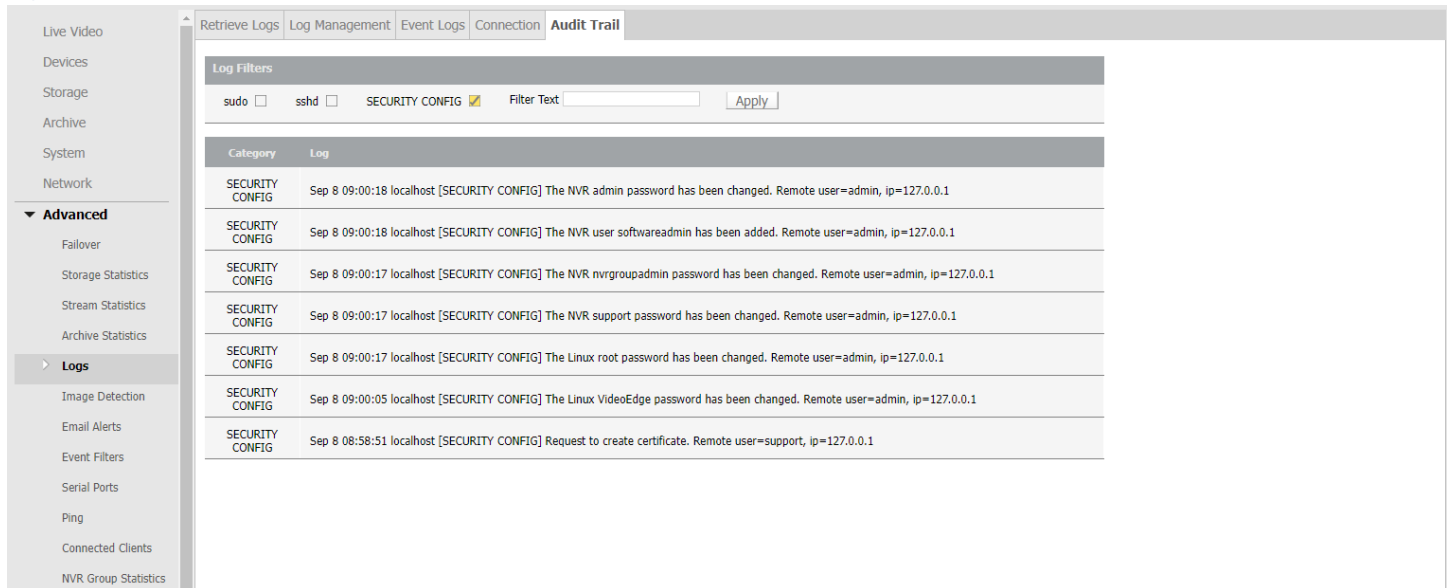
The NVR tracks important types of system events and system operation and stores the data in logs which are useful for troubleshooting and incident investigation. You can view logs data containing administrative changes, camera alerts, changes to cameras, and system events.

The Linux operating system of the NVR generates several different log files specific to each function such as general system operation, web server operation, web server errors, and Network time Protocol (NTP) operation.

The VideoEdge server also generates several application-specific log files to aid in diagnosing areas such as camera communication and video playback events.

These audit trails keep track of system configuration operations including the configuration of information security controls. An audit log interrogation tool is provided as part of the VideoEdge Administrator Interface. Using the audit log interrogation tool, you can audit events to be queried by severity and searched using a text filter.

Figure 2.6.1.1



| Category | Log |
|-----------------|---|
| SECURITY CONFIG | Sep 8 09:00:18 localhost [SECURITY CONFIG] The NVR admin password has been changed. Remote user=admin, ip=127.0.0.1 |
| SECURITY CONFIG | Sep 8 09:00:18 localhost [SECURITY CONFIG] The NVR user softwareadmin has been added. Remote user=admin, ip=127.0.0.1 |
| SECURITY CONFIG | Sep 8 09:00:17 localhost [SECURITY CONFIG] The NVR nvrgroupadmin password has been changed. Remote user=admin, ip=127.0.0.1 |
| SECURITY CONFIG | Sep 8 09:00:17 localhost [SECURITY CONFIG] The NVR support password has been changed. Remote user=admin, ip=127.0.0.1 |
| SECURITY CONFIG | Sep 8 09:00:17 localhost [SECURITY CONFIG] The Linux root password has been changed. Remote user=admin, ip=127.0.0.1 |
| SECURITY CONFIG | Sep 8 09:00:05 localhost [SECURITY CONFIG] The Linux VideoEdge password has been changed. Remote user=admin, ip=127.0.0.1 |
| SECURITY CONFIG | Sep 8 08:58:51 localhost [SECURITY CONFIG] Request to create certificate. Remote user=support, ip=127.0.0.1 |

2.6.2 SIEM integration

Using a third-party System Information and Event Monitoring (SIEM) tool, it is possible to collect syslog data from VideoEdge.

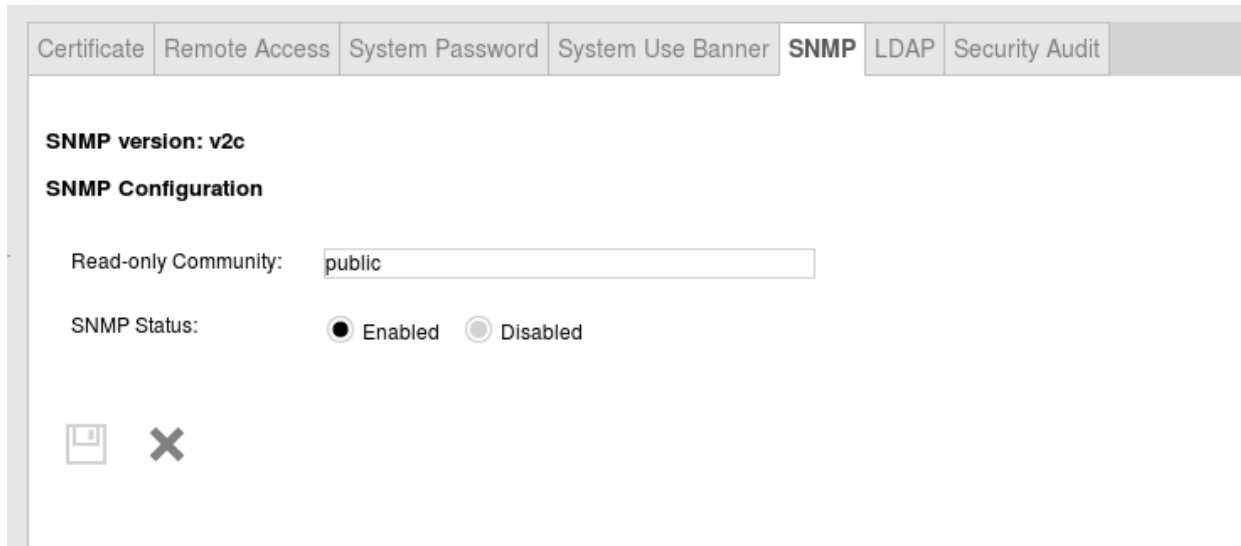
2.6.3 SNMP

Simple Network Management Protocol (SNMP) governs network management and monitors network devices. It is used on the VideoEdge NVR to monitor the NVR's status for victor Client health monitoring and failover

functionality. VideoEdge uses SNMP v2c for NVR groups, failover, and the various dashboards. It is highly recommended that the community string is changed from public.

[Hardening step 15: Configure SNMP](#)

Figure 2.6.3.1



2.6.4 Security alerts

You can generate security alerts by email under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using TLS. You can configure these alerts to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

[Hardening step 16: Configure alerts](#)

[Hardening step 16.1: Configure image tamper detection](#)

To help determine when a camera is being tampered with, the VideoEdge NVR automatically performs an image detection test on every camera to determine if a camera has lost network connection or is broadcasting black video. If this occurs the NVR can send alerts.

This feature should be used in areas where IP cameras are used and at high risk of physical attack. If an IP camera is removed, an attacker can gain access to the network cable connecting the camera. However, when this occurs, VideoEdge can trigger an alarm.

Figure 2.6.4.1

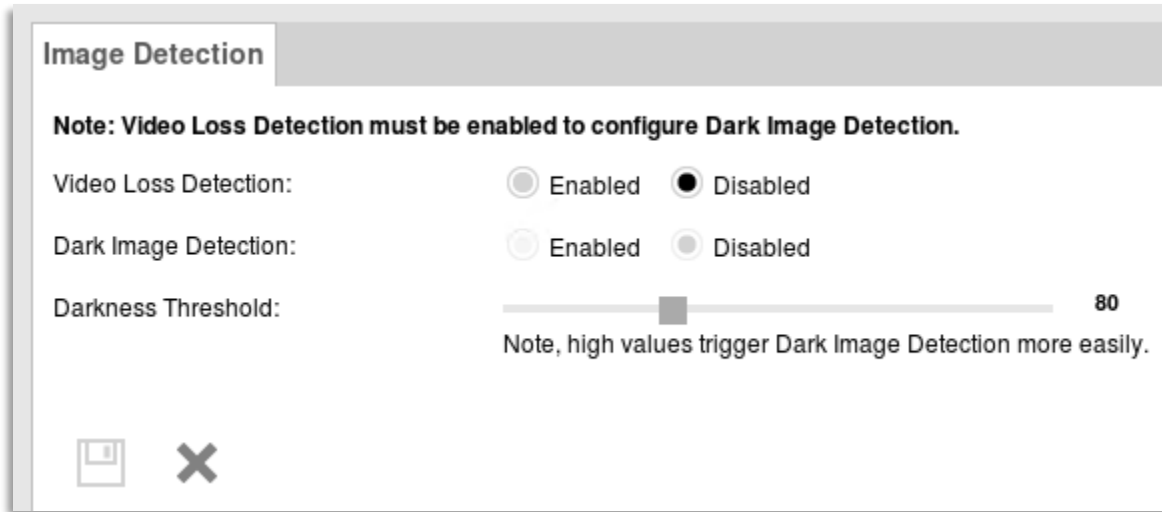


Table 2.6.4.1

| | minimum baseline protection | to strengthen protection |
|-----------------------------|---|--|
| Video Loss Detection | Enabled | Enabled <i>is the strongest setting</i> |
| Dark Image Detection | Enabled | Enabled <i>is the strongest setting</i> |
| Darkness Threshold | Configure to maximize detection but minimize false positives. This setting will vary based on camera and lighting conditions. | |

Hardening step 16.2 – Configure email alerts

The **Email Alerts** page consists of the **Email Alerts** tab, the **Email Blocks** tab, and the **Alert Logs** tab. You can set up **Email Alerts** in the NVR to send notifications to selected email addresses regarding several different categories.

The **Email Blocks** tab is used to block specified email alerts being sent from specified devices.

Email alerts are configured using the advanced **Email Alerts** tab within VideoEdge Administrator.

Figure 2.6.4.2

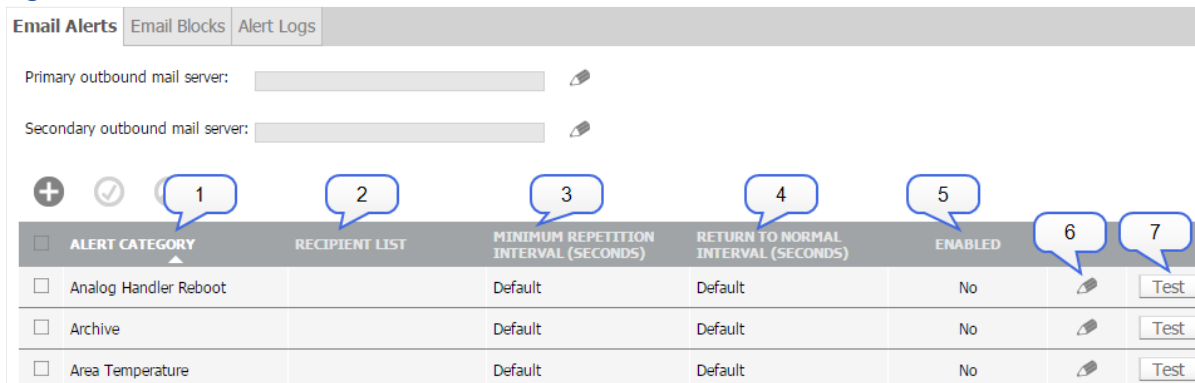


Table 2.6.4.2: Email alerts list summary table

| Field | Description |
|---------------------------------------|--|
| 1. Alert Category | Displays the name of the alert type. |
| 2. Recipient | List Displays any recipient email addresses associated with the alert. |
| 3. Minimum Repetition Interval | The minimum time (in seconds) between sending repeat alert emails |
| 4. Return To Normal Interval | The time to wait before sending out the “return to normal” email. The alert itself may already have cleared. |
| 5. Enabled | Displays “Yes” if the alert is enabled. |
| 6. Edit | Select the edit icon to edit the alert settings. |
| 7. Test | Select the “Test” button to send a test alert email to the assigned recipients |

The Alert Logs tab displays all the email alerts that have been transmitted. To setup email alerts, refer to VideoEdge *User Guide*. For a full list of available alerts, see

Appendix C.3 Operating system level user accounts (interactive)

| User | Description |
|------------------|---|
| support | Used by JCI technical support to perform maintenance tasks using sudo. This account has a per-nvr password that must be generated from the NVR's support id, so it is not active unless the system operator gives JCI the support id. |
| VideoEdge | This is the desktop user account for the default Linux user on VideoEdge. This is used for running VE local client and the admin UI. This user account can be replaced during setup. |
| Tyco | This is the desktop user account for the default Linux user on the Tyco appliances. This is used for running admin UI. This user account can be replaced during setup. |
| root | This is the Linux administrator account. This user account can be disabled, and a replacement created during setup. |

2.7.0 Availability hardening

VideoEdge provides a critical function, and its continuous operation may be essential for the safety of the building occupants and the contents of the facility. Therefore, it is important that VideoEdge is continuously available for operation.

The backup and restore, and failover server features of VideoEdge help to assure that the system is continuously available.

2.7.1 Backup/Restore

Making frequent backups of the VideoEdge configuration during the commissioning phase can be beneficial if an error is made or lost due to a hardware failure. Once the system is made operational, being able to restore from a good backup minimizes the downtime of the system.

VideoEdge configuration

VideoEdge has a built-in utility to backup and restore the NVR server configuration data. In the event of a system failure, the NVR may be restored to the saved configuration.

Operating system configuration

While Operating System (OS) settings cannot be stored in the configuration backup file, the system will automatically export a text file containing the OS settings once you click the back button. You can use the text file as reference for manually configuring the OS settings.

Video data

Video data, which is not backed up through the built-in utility, should be backed up using archiving (refer to VideoEdge Installation and User Manual page 182).

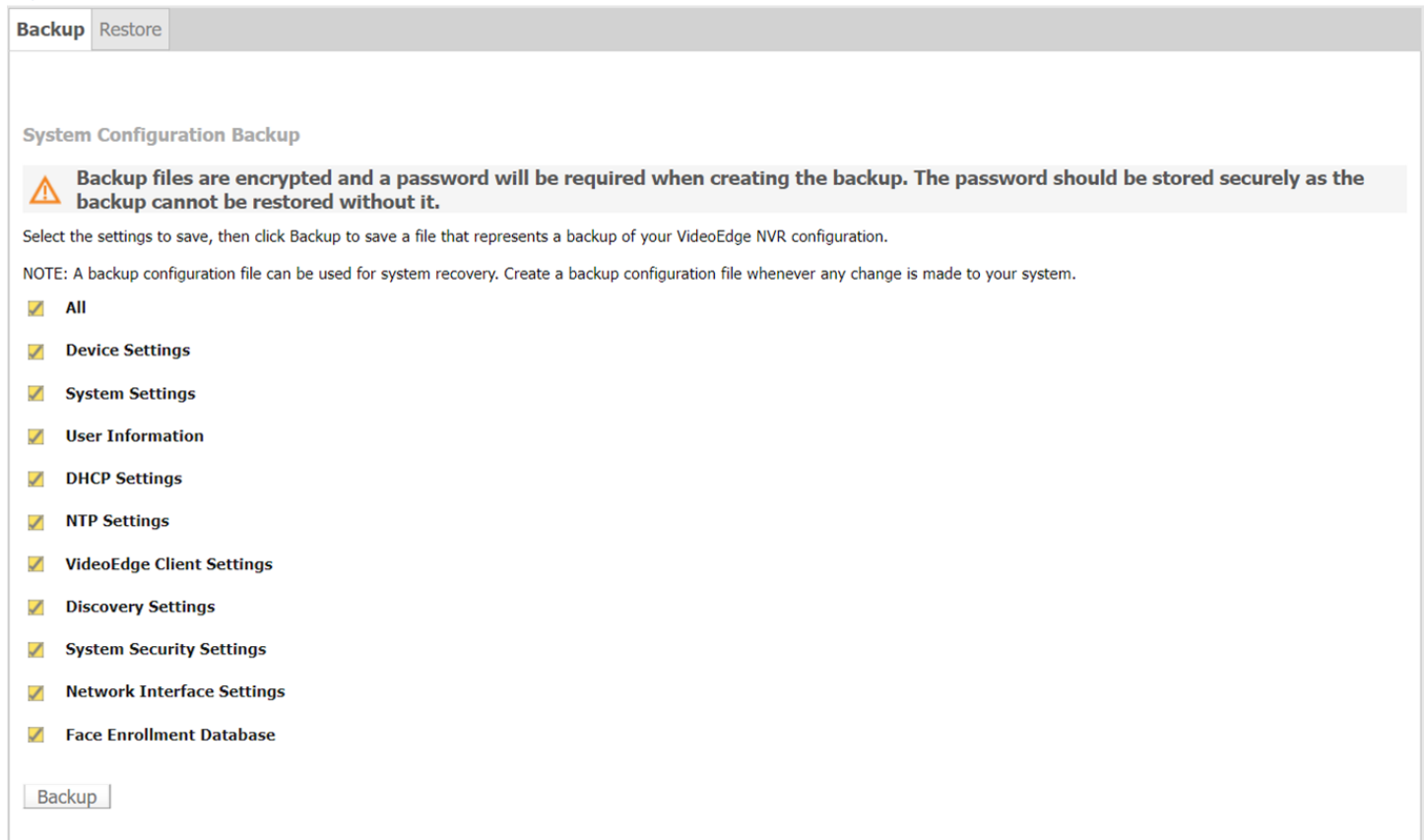
Best practices for backup storage

Copies for the backup files should be stored externally from the server and ideally in a remote location to assure all the necessary backup files will still be available if there is a hardware failure or disaster at the site. Backup should be protected from unauthorized access using encryption.

[Hardening step 17: Backup VideoEdge configuration and data](#)

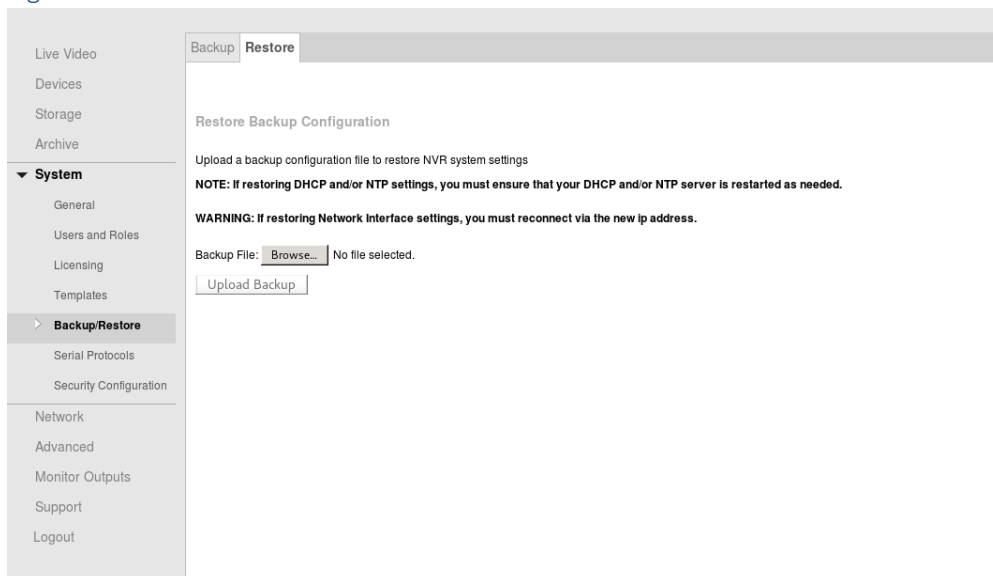
- To access the built-in VideoEdge Backup utility click the **Backup** tab.

Figure 2.7.1.1



- To access the built-in VideoEdge Restore utility click the **Restore** tab.

Figure 2.7.1.2



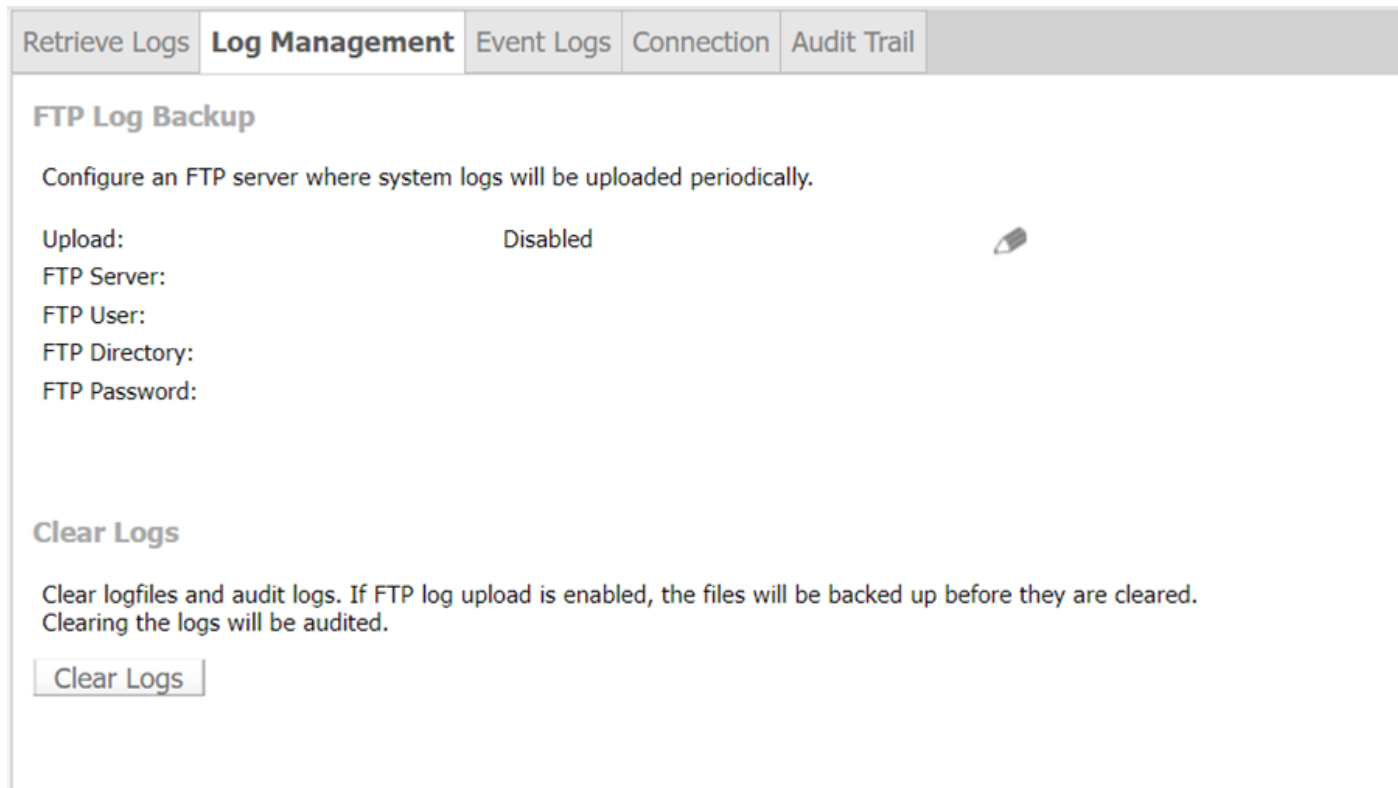
FTP Log backup

Using the **Log Management** page, you can configure FTP server settings where system logs will be uploaded periodically. The **Event Log** is rotated (all entries are cleared) when it is full. To preserve the **Event Log** this function should be configured and enabled.

Note: Only syslog files are uploaded when using this feature.

Using the Log Management page, you can input the FTP server IP Address, FTP Username, remote FTP Directory and FTP Password.

Figure 2.7.1.3



The screenshot shows a web interface with a navigation bar at the top containing tabs: Retrieve Logs, **Log Management**, Event Logs, Connection, and Audit Trail. The main content area is titled "FTP Log Backup" and includes the following elements:

- A heading "FTP Log Backup" followed by the instruction: "Configure an FTP server where system logs will be uploaded periodically."
- A label "Upload:" with a value of "Disabled" and a pencil icon to its right.
- Labels for "FTP Server:", "FTP User:", "FTP Directory:", and "FTP Password:" followed by empty input fields.
- A section titled "Clear Logs" with the text: "Clear logfiles and audit logs. If FTP log upload is enabled, the files will be backed up before they are cleared. Clearing the logs will be audited."
- A "Clear Logs" button.

Hardening step 18: Configure the Log FTP server

1. Click **Advanced**.
2. Click **Logs**.
3. Click the **Log Management** tab.

The **Log Management** page opens.

4. Select the Enabled option button to enable Event Log upload to the FTP Server.
5. Enter the IP Address in the FTP Server field.
6. Enter the username in the FTP User field.
7. Enter the directory in the FTP Directory field.
8. Enter the password in the FTP Password field.
9. Enter the password again in the Confirm Password field.

Note: When FTP Log upload is enabled, a **Test Upload** button displays. Use this button to verify the FTP server settings. A successful upload test will create a test file on the specified location of the FTP Server.

2.7.2 Redundant server failover

When configured as a secondary NVR, VideoEdge will monitor other VideoEdge NVRs that have been added to its server monitoring list. If a primary NVR fails, the secondary NVR will detect the failure after approximately 60 seconds and will assume the role of the primary NVR.

During this failover period, the NVR will not be receiving video from cameras and video loss will occur. However, Illustra cameras and Axis cameras have a video backfill feature which provides the capability for the VideoEdge NVR to fill in the gaps in recorded video.

[Hardening step 19: Configure VideoEdge with a failover server](#)

For NVR failover please refer to the **NVR Group** section in the [VideoEdge NVR Installation and User Guide](#)

2.7.3 RAID storage

While there is no hardening step associated with RAID storage, we encourage you to review details how to configure RAID Drives, manage RAID drives, and other storage options that may harden your installation. (Refer to Storage section of VideoEdge Installation and User Manual).

2.7.4 Network isolation

VideoEdge firewall

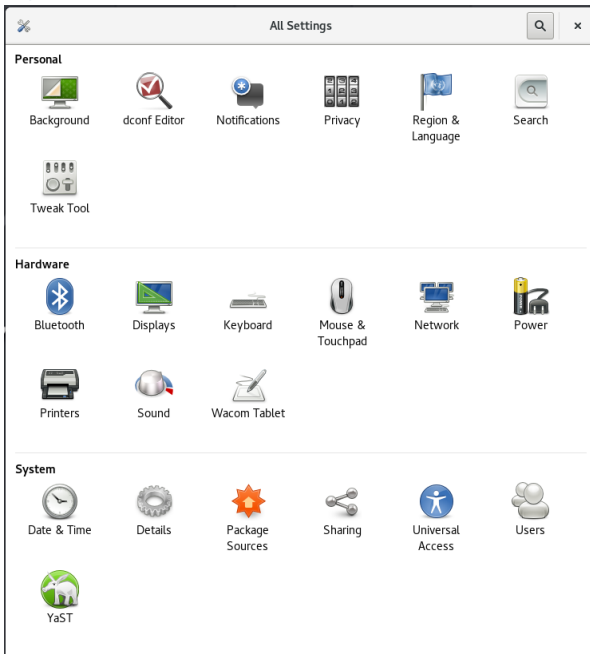
A firewall is an important feature that should be utilized. A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Using a predefined set of rules, it can disallow malicious activity from intruding into the system.

[Hardening step 20: Configure VideoEdge firewall](#)

To enable the VideoEdge firewall, complete the following steps:

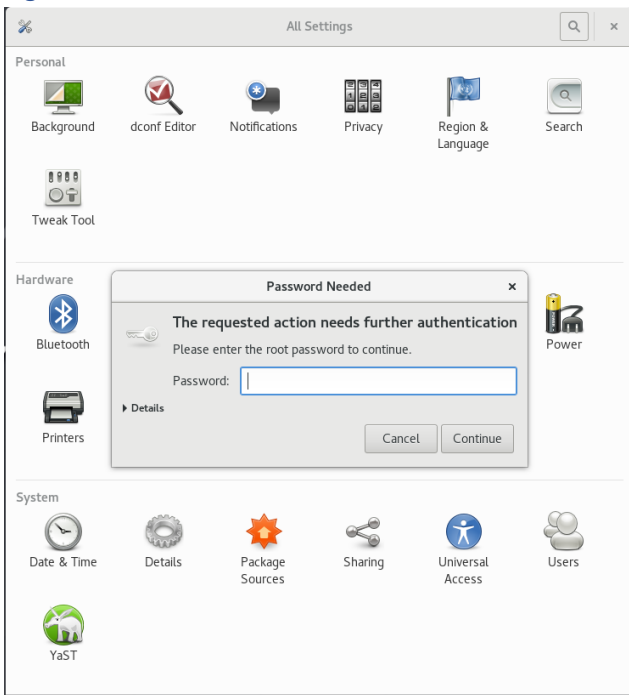
1. Connect to the local desktop.
2. Press the power button. This brings up the menu in figure 2.6.4.2.

Figure 2.7.4.1



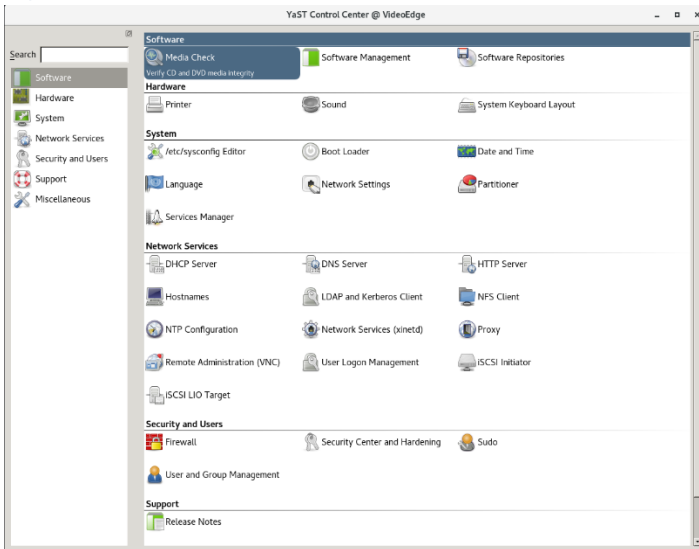
3. Enter the root user password.

Figure 2.7.4.2



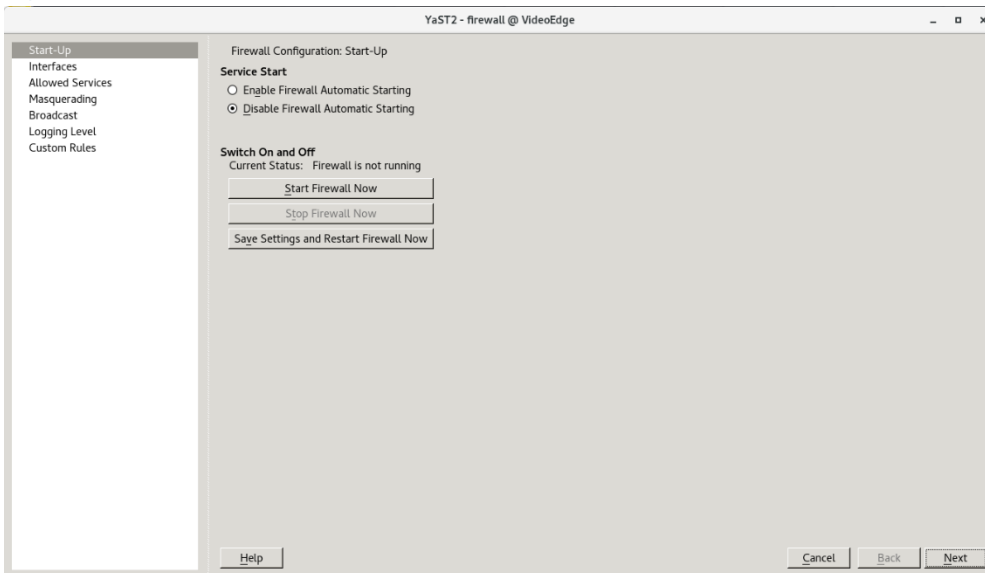
4. Click **Firewall**.

Figure 2.7.4.3



5. Enable or disable the firewall.

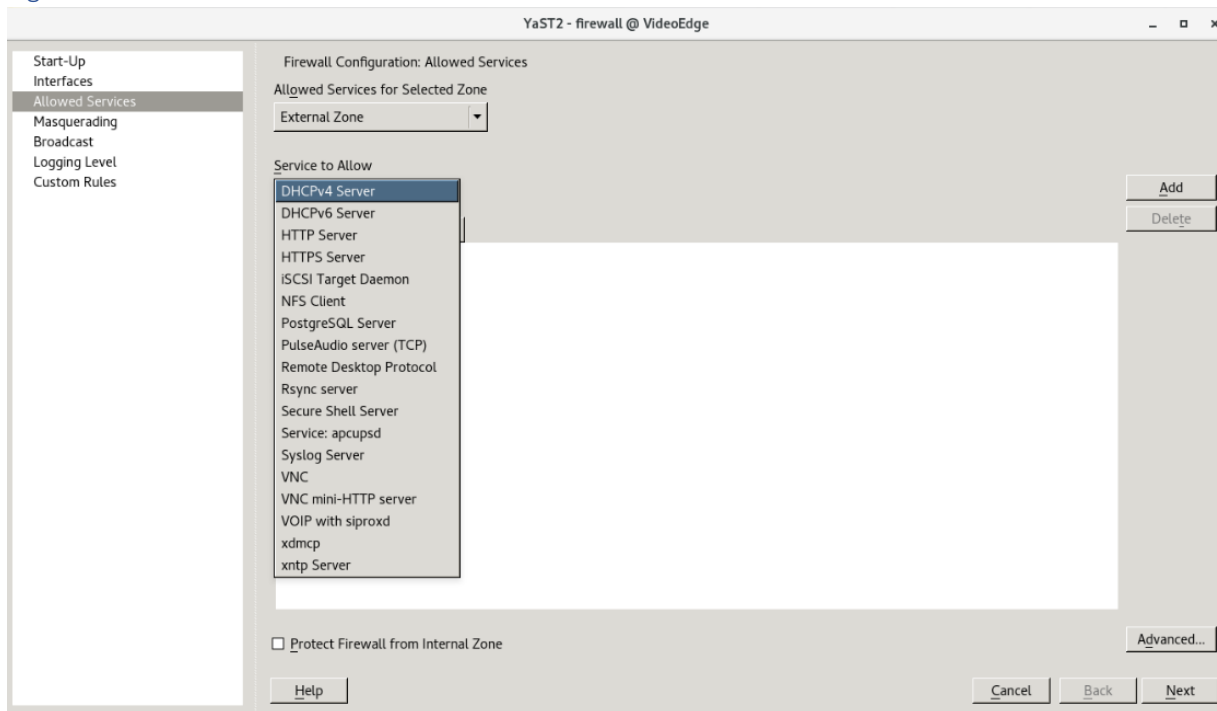
Figure 2.7.4.4



6. On the side bar click on **Allowed Services**.

Note: You can add default services for External/Internal/DMZ Zones.

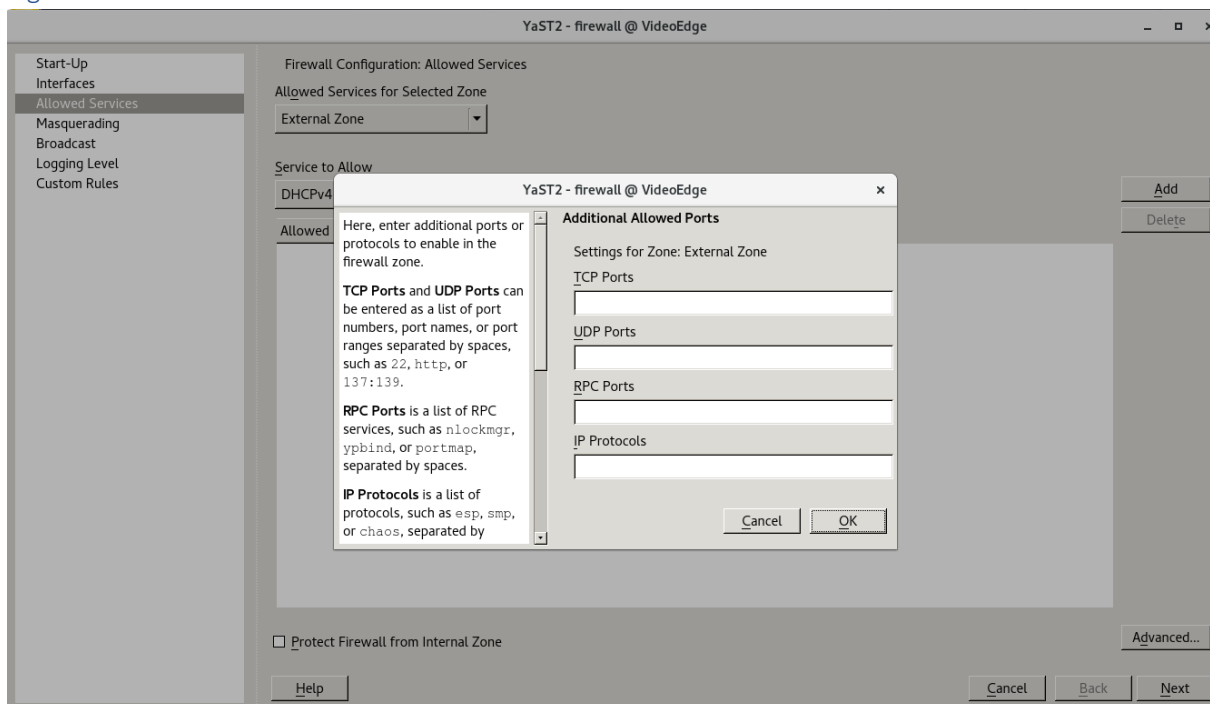
Figure 2.7.4.5



7. To add ports that do not show in the default list, click **Advanced**.

Note: Refer to the VideoEdge port document for specific port number and protocols.

Figure 2.7.4.6



2.8.0 Security audits and documentation

A well-documented deployment of VideoEdge will be useful in security audits, and a security audit can expose errors in the system documentation and identifying gaps in protection. Each task feeds the other and it may be necessary to repeat hardening step 19, after an audit is complete and the gaps are addressed.

2.8.1 Security documentation

Document deployment once hardening is sufficient for run-time operations. When updates are released, or security advisories are published this documentation will be useful. The documentation will allow for quick assessment to determine if the deployment is impacted by the issues described in a security advisory and requires a configuration change, software update or patch.

[Hardening step 22: Security documentation](#)

Include the following details in creating as-built security documentation:

- As-built architecture drawing of system
- For all system components (NVRs, clients, and cameras) record:
 - Component identification
 - Name
 - Description
 - Device Type
 - Location
 - Vendor
 - Model
 - IP address
 - MAC address
 - Support details
 - Software version
 - Hardware version
 - Licenses
 - Installation date
 - Communication configuration details
 - Enabled Ports and protocols
 - Encryption settings

2.8.2 Security audit checklist

An audit of the security configuration will help reveal any missed steps and will allow for further hardening of the system. This will be particularly important if a less secure configuration was utilized to facilitate efficient deployment before the full infrastructure was available. Use the security gaps identified with the audit to tighten security to the appropriate levels of protection for the target environment before turning over the system to run-time operations.

[Hardening step 23: Perform a security configuration audit](#)

The security audit must be conducted by someone who was not involved with the initial hardening of the system. An independent reviewer is more likely to find the security gaps the audit is intended to reveal.

The Hardening checklist outlined in this section must be used as the basis for the security audit checklist. (Section 2.2.1 Hardening checklist).

3 Maintain

The contents within this section address how to monitor for potential cybersecurity issues and maintain protection levels because conditions change.

An audit that produces a report indicating low cybersecurity risk is a very positive result and suggests that the deployment was conducted with a high degree of care and consideration. However, new attack vectors combined with enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

The impacted technologies and their implementation may have been previously well regarded by cybersecurity experts. The discovery of vulnerabilities post the final deployment audit may not reflect the quality of that audit. You may require a higher degree of protection for the environment that VideoEdge is serving because policies, regulations and guidance may change over time.

3.1.0 Cybersecurity maintenance checklist

Continuously or periodically practice the following cybersecurity maintenance items. The frequency of their execution will depend on the policies and regulations which govern the site. The typical maintenance periods provided are a starting point and adjusted to best suit the target conditions of the deployed environment:

| Item | Description | Immediate | Base on Priority | Daily | Weekly | Monthly | Quarterly | Annual |
|------|---|-----------|------------------|-------|--------|---------|-----------|--------|
| 1 | Backup runtime data | | | ✓ | | | | |
| 2 | Backup configuration data | | | | ✓ | | | |
| 3 | Test backup data | | | | | | ✓ | |
| 4 | Assure failover solutions are operating | | | | | | ✓ | |
| 5 | Lock user accounts of terminated employees | ✓ | | | | | | |
| 6 | Remove inactive user accounts | | | | | ✓ | | |
| 7 | Update user account roles | | | | | | ✓ | |
| 8 | Disable unused features, ports, and services | | | | | | ✓ | |
| 9 | Check for and prioritize advisories | | | | ✓ | | | |
| 10 | Plan and execute advisory recommendations | | ✓ | | | | | |
| 11 | Check and prioritize software patches and updates | | | | ✓ | | | |
| 12 | Plan and execute software patches and updates | | ✓ | | | | | |
| 13 | Review updates to organizational policies | | | | | | | ✓ |
| 14 | Review updates to regulations | | | | | | | ✓ |
| 15 | Update as build documentation | ✓ | | | | | | ✓ |
| 16 | Conduct security audits | | | | | | | ✓ |
| 17 | Update password policies | | | | | | | ✓ |
| 18 | Update standard operating procedures | | | | | | | ✓ |
| 19 | Update logon banners | | | | | | | ✓ |
| 20 | Renew licensing agreements | | | | | | | ✓ |
| 21 | Renew support contracts | | | | | | | ✓ |
| 22 | Check for end-of-life announcements and plan for replacements | | | | | | ✓ | |

| | | | | | | | | |
|-----------|--|--|---|---|--|--|--|--|
| 23 | <i>Periodically delete sensitive data in accordance with policies or regulations</i> | | ✓ | | | | | |
| 24 | <i>Monitor for cyber attacks</i> | | | ✓ | | | | |

3.1.1 Backup runtime data

Runtime data, including video recordings and logs, can be the most valuable assets within the VideoEdge system. You can replace or reconstruct everything else. Confirm that the following backup steps are being executed:

Table 3.1.1.1

| Action | Details | Suggested frequency |
|------------------------|---|---------------------|
| Video archiving | See Backup/Restore and the VideoEdge Installation and refer to the User Manual v5.4 | Daily |
| FTP log backup | See Backup/Restore | Daily |

3.1.2 Backup configuration data

If you need to restore or replace a component it is important to have a backup of its configuration data to minimize the time required to restore its functions. If you need to restore or replace a component it is important to have a backup of its configuration data to minimize the time required to restore its functions. Please note that a manual record of the encryption configuration will help assure that the system can be reconstituted should a self-encrypting drive need to be restored.

Table 3.1.2.1

| Action | Details | Suggested frequency |
|----------------------------------|--------------------|---------------------|
| Backup configuration data | See Backup/Restore | Weekly |

3.1.3 Test backup data

Test backups to provide assurance that the data backups contain the expected data and integrity.

Table 3.1.3.1

| Action | Details | Suggested frequency |
|-------------------------|---|---------------------|
| Test Backup data | Load data from backup media into a non-production VideoEdge NVR | Quarterly |

3.1.4 Assure failover solutions are operating

Backup solutions that provide continuity of operations through a hardware failure, such as redundant server failover and RAID, should be inspected to assure that they are operating properly.

Table 3.1.4.1

| Action | Details | Suggested frequency |
|----------------------------------|--|---------------------|
| Redundant server failover | See Section 2.6.7 Redundant server failure | Quarterly |
| RAID storage | See Section 2.6.8 RAID storage | Quarterly |

3.1.5 Lock accounts on termination of employment

Disable user accounts of personnel who voluntarily or non-voluntarily are terminated from employment immediately.

Table 3.1.5.1

| Action | Details | Suggested frequency |
|----------------------|---|---------------------|
| Lock accounts | See 2.2.5.3 VideoEdge user accounts, refer to VideoEdge Installation and User manual Procedure 168 Locking accounts from the Users table p. 214 | Immediate |

3.1.6 Remove inactive user accounts

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may not have utilized it for a long period. This suggests that independent of being authorized to use the system, they do not have a need to use the system and you should remove their user account. This is sometimes referred to as a use it or lose it policy. This best practice reduced the amount of active user accounts in the system and therefore lowers the potential attack footprint.

Table 3.1.6.1

| Action | Details | Suggested frequency |
|---------------------------------|--|---------------------|
| Remove inactive accounts | See 2.2.5.3 VideoEdge user accounts. Refer to VideoEdge Installation and User Manual, Procedure 171 Removing a User, p.215 | Monthly |

3.1.7 Update user account roles

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may have changed roles or have increased or decrease their need to utilize the system. When adding a role or a permission to a user's account when that user has been granted new authorizations due to an organizational role change, be sure to remove the VideoEdge roles and permissions no longer required or utilized in their new role.

Table 3.1.7.1

| Action | Details | Suggested frequency |
|----------------------------------|---|---------------------|
| Update user account roles | See 2.2.5.2 VideoEdge roles. Refer to VideoEdge Installation and User Manual, Procedure 172 Configuring additional security on roles, p.217 | Quarterly |

3.1.8 Disable unused features, ports, and services

Reassess the need for optional features, ports, and services that are not required, and disable them. This practice will lower the attack surface of VideoEdge resulting in a higher level of protection.

Table 3.1.8.1

| Action | Details | Suggested frequency |
|---------------------------------|--|---------------------|
| Disabled unused features | See 2.2.4 Set boot sequence, 2.5.2 Communication port and encryption configuration | Quarterly |

3.1.9 Check for and prioritize advisories

You can find security advisories for VideoEdge on the Cyber Protection website. Access is provided once you have registered a user account with that site. User account registration is open to JCI customers and authorized representatives. Determine if VideoEdge is impacted by the conditions outlined in the advisories. Based on how the VideoEdge system is deployed, configured, and used, the advisory may not be of concern. Referring to as-built documentation of the VideoEdge system will help with this assessment. A good set of as-built documentation will help you identify the number of components impacted and where they are located. While advisories call attention to a cybersecurity issue, it is not always possible to take immediate action or execute the full recommendation described in the advisories. If so, prioritization will aid in your planning to ensure that any issue impacting your system is fully and appropriately addressed in order of priority. Check for advisories from third party components such as networking equipment and operating systems by consulting with the respective vendor.

Table 3.1.9.1

| Action | Details | Suggested frequency |
|--|--|---------------------|
| Check for and prioritize advisories | Refer to https://tycosecurityproducts.com/CyberProtection/SecurityAdvisories.aspx | Weekly |

3.1.10 Plan and execute advisory recommendations

Follow the plan determined in maintenance step 9.

Table 3.1.10.1

| Action | Details | Suggested frequency |
|--|---|---------------------|
| Plan and execute advisory recommendations | Plan and execute advisory recommendations | Based on priority |

3.1.11 Check and prioritize patches and updates

While a VideoEdge patch or update may or may not relate to a security advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements also fixes to known issues. Review the release notes and prioritize the benefits of the patch or update. The overall benefit should include the improved protection that will aid in lowering the cybersecurity risk. Be sure also to check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor.

Table 3.1.11.1

| Action | Details | Suggested frequency |
|--|--|---------------------|
| Check for and prioritize advisories | Refer to http://www.americandynamics.net/Products/VideoEdge_NVR.aspx | Weekly |

3.1.12 Plan and execute software patches and updates

Follow the plan determined in maintenance step 9.

Table 3.1.12.1

| Action | Details | Suggested frequency |
|--|---|---------------------|
| Plan and execute software patches and updates | As determined in maintenance step 9. Follow update process as outlined in Section 2.4.1 Operating System updates, Section 2.4.2 VideoEdge application updates and Section 2.4.3 for camera firmware updates | Base on priority |

3.1.13 Review organizational policy updates

Organizations may update their policies which include cybersecurity requirements. Changes to these policies can impact systems which complied prior to the change. Periodically check to see if policy changes were made and re-assess compliance with those policies.

Table 3.1.13.1

| Action | Details | Suggested frequency |
|---|---|---------------------|
| Review organizational policy updates | Collect most recent security policies for your organization | Annual |

3.1.14 Review updates to regulations

If VideoEdge is deployed in a location that is governed by regulation, it is important to check to see if there are any updates to those regulations. In some cases, new regulations are introduced. Whether it is a review of an updated regulation to maintain compliance and a new regulation, an assessment of the changes should be conducted periodically.

Table 3.1.14.1

| Action | Details | Suggested frequency |
|--------------------------------------|---|---------------------|
| Review updates to regulations | Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration. | Annual |

3.1.15 Update as-build documentation

Update as-build documentation if the deployment architecture or component configuration changes. Some configuration changes happen without a formal project or plan and if such cases it may be common to negate updating the as-built documentation. Schedule a full update of the as-built documentation on a regular basis to ensure that all changes are documented.

Table 3.1.15.1

| Action | Details | Suggested frequency |
|--------------------------------------|--|-------------------------------|
| Update as-build documentation | See section 2.7.1 Security documentation | As changes are made or annual |

3.1.16 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use, and configuration and threats have likely changed since the last audit. By conducting periodic security audits, the latest knowledge and conditions can be applied revealing gaps in protection previously undetected or created by changes in system use of configuration.

Table 3.1.16.1

| Action | Details | Suggested frequency |
|--------------------------------|--|---------------------|
| Conduct security audits | See section 2.7.2 Security audit checklist | Annual |

3.1.17 Update password policies

Guidance on password policies has been evolving. Password policies should be re-assessed periodically to make sure the right policy is in place for the target environment based on current organizational policies, regulations, and guidance from standards organizations such as NIST.

Table 3.1.17.1

| Action | Details | Suggested frequency |
|---------------------------------|--|---------------------|
| Update password policies | See section 2.2.5.1 Operating system level user accounts (interactive) and 2.2.5.2 VideoEdge roles | Annual |

3.1.18 Update standard operating procedures

Including best practices for cybersecurity within standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses, a gap in protection can be created, prevented, or closed. Therefore, it is important to update standard operating procedures periodically.

Table 3.1.18.1

| Action | Details | Suggested frequency |
|---|--|---------------------|
| Update standard operating procedures | Collect standard operating procedures for use of VideoEdge within the organization | Annual |

3.1.19 Update logon banners

The system use policy details included on logon banners can change over time. Review and update as required.

Table 3.1.19.1

| Action | Details | Suggested frequency |
|-----------------------------|-------------------------------|---------------------|
| Update logon banners | See section System use banner | Annual |

3.1.20 Renew licensing agreements

Assure that your VideoEdge software license supports the necessary functions

Table 3.1.20.1

| Action | Details | Suggested frequency |
|-----------------------------------|-----------------------------------|---------------------|
| Renew licensing agreements | Collect active licensing details. | Annual |

3.1.21 Renew support contracts

Assure that your VideoEdge software support agreement (SSA) is up to date.

Table 3.1.21.1

| Action | Details | Suggested frequency |
|--------------------------------|---------------------|---------------------|
| Renew support contracts | Collect SSA details | Annual |

3.1.22 Check for end-of-life announcements and plan for replacements

Review product announcements to determine if any of the components of VideoEdge have a planned end-of-life announcement, including cameras.

Table 3.1.22.1

| Action | Details | Suggested frequency |
|--|-----------------------------|---------------------|
| Check for end-of-life announcements and plan for replacements | Collect end-of-life details | Quarterly |

3.1.23 Periodically delete sensitive data in accordance with policies or regulations

Table 3.1.23.1

| Action | Details | Suggested frequency |
|--|---|---------------------|
| PERIODICALLY DELETE SENSITIVE DATA IN ACCORDANCE WITH POLICIES OR REGULATIONS | Collect details on policies and regulations that apply to your VideoEdge location | As required |

3.1.24 Monitor for cyber attacks

Monitoring site perimeters, networks and endpoints for cyber-attacks is a part of good cybersecurity operation. Many tools are available to assist with real-time analytics-based detection.

Table 3.1.24.1

| Action | Details | Suggested frequency |
|----------------------------------|---|-----------------------------------|
| Monitor for cyber attacks | Determine which security monitoring tools and services to implement | Run continuously once implemented |

There are many rootkit and malware detection tools available for Linux, however some place significant load upon the system and may interfere with recording and playback. Lynis, Chkrootkit, and Rkhunter provide useful output while placing little additional load upon the system. ClamAV places significant load upon the system for an extended period and is not suitable for VideoEdge.

Note: It is your responsibility to verify that VideoEdge continues to operate properly after you have installed any security monitoring tools.

3.2.0 Patch policy

The policy documented here sets forth the current internal operating guidelines and process regarding VideoEdge, which may change from time to time at the sole discretion of Johnson Controls. Johnson Controls employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Johnson Controls at its discretion. Regardless, Johnson Controls endeavors to address issues that arise within VideoEdge with the severity that they warrant.

When CRITICAL security vulnerabilities are discovered within VideoEdge, Johnson Controls will use commercially reasonable efforts to issue a Critical Service Pack for the current version of VideoEdge as soon as is reasonably practicable.

When non-CRITICAL vulnerabilities are discovered within VideoEdge, Johnson Controls will use commercially reasonable efforts to:

- Apply fixes for HIGH severity vulnerabilities in the next immediate release of VideoEdge
- Apply fixes for LOW and MEDIUM vulnerabilities within one of the next two available releases of VideoEdge

Note: The VideoEdge does not have a back-port policy. Updates are only applied to latest version of the released product.

When CRITICAL security vulnerabilities are discovered within VideoEdge, American Dynamics will use commercially reasonable efforts to issue a Critical Service Pack for the current version of VideoEdge as soon as is reasonably practicable.

When non-CRITICAL vulnerabilities are discovered within VideoEdge, American Dynamics will use commercially reasonable efforts to:

- Apply fixes for HIGH severity vulnerabilities in the next immediate release of VideoEdge
- Apply fixes for LOW and MEDIUM vulnerabilities within one of the next two available releases of VideoEdge

Note: The VideoEdge NVR does not have a backport policy. Updates are only applied to latest version of the released product.

Release schedule

An update to VideoEdge including new features and security fixes is released approximately every 6-8 months.

An interim update that will include only updates for the operating system will be released approximately three months after each release unless there is VideoEdge release within this timeframe.

No VideoEdge update will be released without undergoing extensive quality assurance testing.

An update to the VideoEdge NVR including new features and security fixes is released approximately every 6-8 months.

3.3.0 Recovery and factory reset

If a recovery is necessary, see section [2.1.4 Resetting to factory defaults](#)

3.4.0 VideoEdge testing process

As part of the requirements of the Product Security Program, the VideoEdge NVR receives regular vulnerability and penetration testing from our internal product security engineers. The VideoEdge NVR is also subjected to third party penetration testing annually and at milestone releases.

See ANNEX F for letters of attestation from the vendors.

3.5.0 Customer specific testing

If a customer requires specific testing (for example, deployed architecture and configuration) on a VideoEdge NVR, the Cyber Protection Team is available to provide consultation and response directly to the testing team. For assistance, contact TSPCyberProtection@jci.com

The VideoEdge NVR regularly undergoes repeated security tests during the development process including network vulnerability scans. Web application scans are done on a regular maintenance schedule. Web

applications are also tested during development to identify flaws such as cross-site injection points and missing security flags. Proprietary code is analyzed during the development cycle for items such as buffer overflow points, null dereference points and memory leaks. Third party and open-source code is continuously scanned to identify released security flaws.

3.5.1 Vulnerability assessment

Vulnerabilities discovered in VideoEdge proprietary software are assessed on the CVSS v3 score.

CVSS v3 Score, Assessment

≥ 9, Critical

≥ 7, High

< 7, Medium

3.5.2 Vulnerability assessment – third party components

Vulnerabilities discovered in VideoEdge proprietary software are assessed on the CVSS v3 score.

| CVSS v3 Score | Assessment |
|---------------|------------|
| ≥ 9 | Critical |
| ≥ 7 | High |
| < 7 | Medium |

3.5.3 Vulnerability assessment – third party software

American Dynamics must use commercially reasonable efforts to monitor third party and open-source software included within the VideoEdge NVR for disclosed vulnerabilities from the product vendors and open-source communities. Vulnerabilities that are discovered and disclosed will be assessed first on its assigned CVSS v3 score from the product vendor or the National Vulnerability Database and then on the ability to be exploited within the VideoEdge NVR.

| CVSS v3 Score | Exploitability | Assessment |
|---------------|-----------------|------------|
| ≥ 9 | Exploitable | Critical |
| ≥ 9 | Not Exploitable | High |
| ≥ 7 | Exploitable | High |
| ≥ 7 | Not Exploitable | Medium |
| < 7 | Exploitable | Medium |
| < 7 | Not Exploitable | Low |

If a patch is not available to correct the vulnerability, American Dynamics will use commercially reasonable efforts to mitigate the vulnerability within its capabilities.

3.5.4 VideoEdge vulnerability reporting

To better protect our customers and honor the trust they put in us, we are firm believers in responsible coordinated disclosure. Security Researchers, consultants and others who believe they may have found a potential security vulnerability in a Security Product can make immediate notice to our Cyber Protection Team through email to TSPCyberProtection@jci.com or by the [Building Products Vulnerability Reporting](#) webpage to make immediate notice to our Product Security Incident Response Team (PSIRT).

Those working directly on behalf of a Security Products customer should also notify their local Security

Products representative. Thank you for your partnership with us in creating a smarter, safer more sustainable world.

Additionally, American Dynamics Technical Support staff have direct access to the Cyber Protection team to help assess and resolve any issues.

Appendix A Third party attestations and certificates

VideoEdge has undergone review by third party organizations resulting in the following certifications:



DHS SAFETY Act Designation – The VideoEdge technology was included in a certificate of SAFETY Act Designation issued on March 19, 2018, by the United States Department of Homeland Security. This designation is described as follows:

March 19, 2018 – Johnson Controls International plc, Sensormatic Electronics, LLC, and Tyco International Management Company, provide VideoEdge, victor, and Illustra (the “Technology”). The Technology is a scalable video management system consisting of video recorder hardware and management software supporting the integration of cameras and third-party devices, enabling management through a single interface. This Designation will expire on April 30, 2023.

Appendix B Third party security approvals

The VideoEdge NVR has been installed in many installations that require accreditation. Here you can find an overview of accreditations and resources that may be used to assist in meeting the requirements of each.

FISMA

You can configure the VideoEdge system to support the controls necessary for overall FISMA compliance. These controls include:

- Authenticated system access
- Account login/log out management
- Role-based separation of capabilities, permissions, and privileges
- System event and configuration change auditing, alerting, and management
- Restriction of ports, protocols, and services to only those required
- Encrypted communications

For more information, refer to the *VideoEdge FISMA-Ready Compliance Guide available on the Cyber Protection website.*

NERC CIP v5

The *VideoEdge NERC-CIP V5 READY Compliance Guide* provides an overview of the NERC-CIP standard and describes how VideoEdge may be configured to meet the requirements of the NERC-CIP v5 requirements. When used in conjunction with VideoEdge installation and configuration guides, this information should assist in the installation of a compliant system and provide the necessary information for an audit.

For more information, refer to the *VideoEdge NERC-CIP v5 Compliance Guide available on the Cyber Protection website.*

DISA

To assist installations within the Department of Defense in meeting the security hardening requirements of the Defense Information Systems Agency (DISA), Tyco Security Products has developed this System Security Requirements guide based on the DISA General Purpose operating Systems STG, Version 1, Release 3 published 22 January 2016, for the sole purposes of meeting said requirements for the VideoEdge Network Video Recorder (NVR) appliance. We have provided the 250 technical control requirements of the General-Purpose Operating System Security Requirements Guide (SRG) and a description of how a VideoEdge device meets the technical controls or if it does not meet the controls, guidance has been provided so the customer can configure VideoEdge to meet the requirements.

For more information, refer to the *VideoEdge - DISA Security Requirements available on the Cyber Protection website.*

Appendix C.1 Operating system level user accounts (non-interactive)

The following built-in operating system level user accounts are used for non-interactive processes:

Known Limitation: The VideoEdge NVR has Linux built-in accounts present on the operating system. These accounts are non-interactive and there is no login to these accounts. *bin, lp, mail, news, uucp, games, nobody, epmd, polkitd, rtkit*

| User | Description |
|-------------------|---|
| bin | Standard subdirectory of the root directory in Unix-like operating systems that contains the executable (ready to run) applications that must be available to attain minimal functionality for the purposes of booting (starting) and repairing a system. |
| daemon | Is used to run as a process in the background. |
| lp | This account is used for printer systems. |
| mail | Handles aspects of electronic mail. Used by sendmail and postfix daemons. |
| news | Used for Usenet news. |
| uucp | Controls ownership of the Unix serial ports. |
| games | This account allows some games to run as user "game" under the principle of least privilege. |
| man | This account is used to run the man page. |
| ftp | This account is intended to run ftp server software. |
| nobody | Owens no files and is used as a default user for unprivileged operations. |
| messagebus | This account is a combination of a common data model, a common command set, and a messaging infrastructure to allow different systems to communicate through a shared set of interfaces. |
| rpc | This account is used to route requests between clients and servers. |
| statd | It is used by the NFS file locking service, rpc.lockd, to implement lock recovery when the NFS server machine crashes and reboots. |
| epmd | This account maps symbolic node names to machine addresses. |
| ntp | Account is used by the operating system which sets and maintains the system time of day. |
| sshd | Performs unprivileged operations for the OpenSSH Secure Shell daemon. |
| scard | Account is for integrated support for smart card readers. |
| dhcpcd | Account is used by the dhcp server daemon. |
| hacluster | Account is used for the nvr groups feature. It controls the virtual ip address. |
| oprofile | A system-wide statistical profiling tool for Linux. |
| polkitd | This account provides the org.freedesktop.PolicyKit1 D-Bus service on the system message bus. |
| rtkit | Realtime Policy and Watchdog Daemon. RealtimeKit is a D-Bus system service that changes the scheduling policy of user processes/threads to SCHED_RR (real-time scheduling mode) on request. |

| | |
|-------------------------|---|
| pulse | Account is for the pulse audio daemon. It is used for the push-to-talk audio feature. |
| gdm | Account is used for the display manager |
| systemd-network | systemd Network Management |
| systemd-timesync | systemd Time Synchronization |
| dhcpd | DHCP server daemon |
| scard | Smart Card Reader |
| vnc | user for VNC |
| srvGeoClue | User for GeoClue D-Bus service. This is used for geographical information and is not used by VideoEdge. |
| systemd-coredump | systemd Core Dumper |
| lightdm | LightDM daemon (display manager). |

Appendix C.2 Operating system level service accounts (non-interactive)

The following accounts are non-interactive and only used to run VideoEdge services on the operating system.

| User | Description |
|-----------------------|--|
| postgres | Used to run the database server. |
| wwwrun | This account is used to run Apache and all NVR application services. |
| nvr | The NVR service account. Most services run as this (or wwwrun, which is synonymous). |
| pgbouncer | Used for database connection pooling. A connection pool is a cache of database connections maintained so that the connections can be reused when future requests to the database are required. |
| couchdb | Used for the victorWeb database. |
| stunnel | This is automatically created by the stunnel service and is the service account for RTSP TLS. |
| AudioSpeakerDn | Service user for adnvr_SpeakerAudioDemon |
| redis | User for redis key-value store. |
| teamd | Teamd daemon user. Used for administering teamed NICs. |
| at | Batch jobs daemon. Used by the illustra camera handler. |

Appendix C.3 Operating system level user accounts (interactive)

| User | Description |
|------------------|---|
| support | Used by JCI technical support to perform maintenance tasks using sudo. This account has a per-nvr password that must be generated from the NVR's support id, so it is not active unless the system operator gives JCI the support id. |
| VideoEdge | This is the desktop user account for the default Linux user on VideoEdge. This is used for running VE local client and the admin UI. This user account can be replaced during setup. |
| Tyco | This is the desktop user account for the default Linux user on the Tyco appliances. This is used for running admin UI. This user account can be replaced during setup. |
| root | This is the Linux administrator account. This user account can be disabled, and a replacement created during setup. |

ANNEX D - Email Alerts

To setup email alerts, refer to *VideoEdge User Guide*.

| Alert Category | Description |
|--------------------------------------|---|
| Analog Handler Reboot | Sent when any device controller stops responding. The device handler will be automatically restarted to re-establish communication with the camera. |
| Archive | Sent when the archive is unhealthy, the archive is falling behind, data deleted before being archived and when archive is nearing full |
| Audio Malfunction | Sent when audio malfunctions occur. |
| Blur Detection | Generated when a configured camera becomes out of focus. |
| Camera Dark Frame | Sent when the camera images cross a configured threshold of darkness. This alert indicates that the camera may be obscured. |
| Camera Processing Malfunction | Sent when a camera refuses to respond. |
| Camera Video Loss | Sent when the record pipeline detects that there is no video coming from the camera. |
| Device Not Recording | Generated when recording does not occur on one or more cameras. |
| Dry Contact | Sent when a dry contact is triggered. |
| Face Detection | Generated when a face is present in a camera's configured view. |
| Failover | Sent when a failover is detected. The IP address of the NVR which has failed will be included. |
| Log Storage Space Low | Sent when less than 5% of the log storage area is available. |
| Motion Detection | Generated by motion detection alerts. Does not include image attachments. |
| Security Alert | Sent when a user is temporarily and permanently locked out of their account. |
| Security Config Change | Sent if any security settings on the system are changed. |
| Storage | Transmitted when storage is not healthy. |
| Storage Activation | Generated when no storage can be activated. |
| Storage Config | Sent when storage configuration errors occur. |
| Storage Retention | Transmitted when storage capacity is almost reached. |
| System | All general system alerts not included in other categories. |
| System Reboot | Sent when the system is rebooted. |
| Text Stream | Sent when user defined Text Stream exception rules are met. |
| Video Intelligence | Generated by video intelligence alerts. |