tyco

security

VideoEdge

Cybersecurity Overview

Whitepaper

Version 1.0
VideoEdge v5.2
Date: 2-May-2018

Introduction

The Tyco security, Cyber Protection Product Security Program provides peace of mind to our customers with a holistic cyber mindset beginning at initial design concept, continues through product development, and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

The VideoEdge Cybersecurity Overview Whitepaper is intended to provide cybersecurity guidance used in planning, deployment and maintenance periods.

As cybersecurity threats have become a risk impacting all connected devices, it is important to assure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a product'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.

Table of Contents

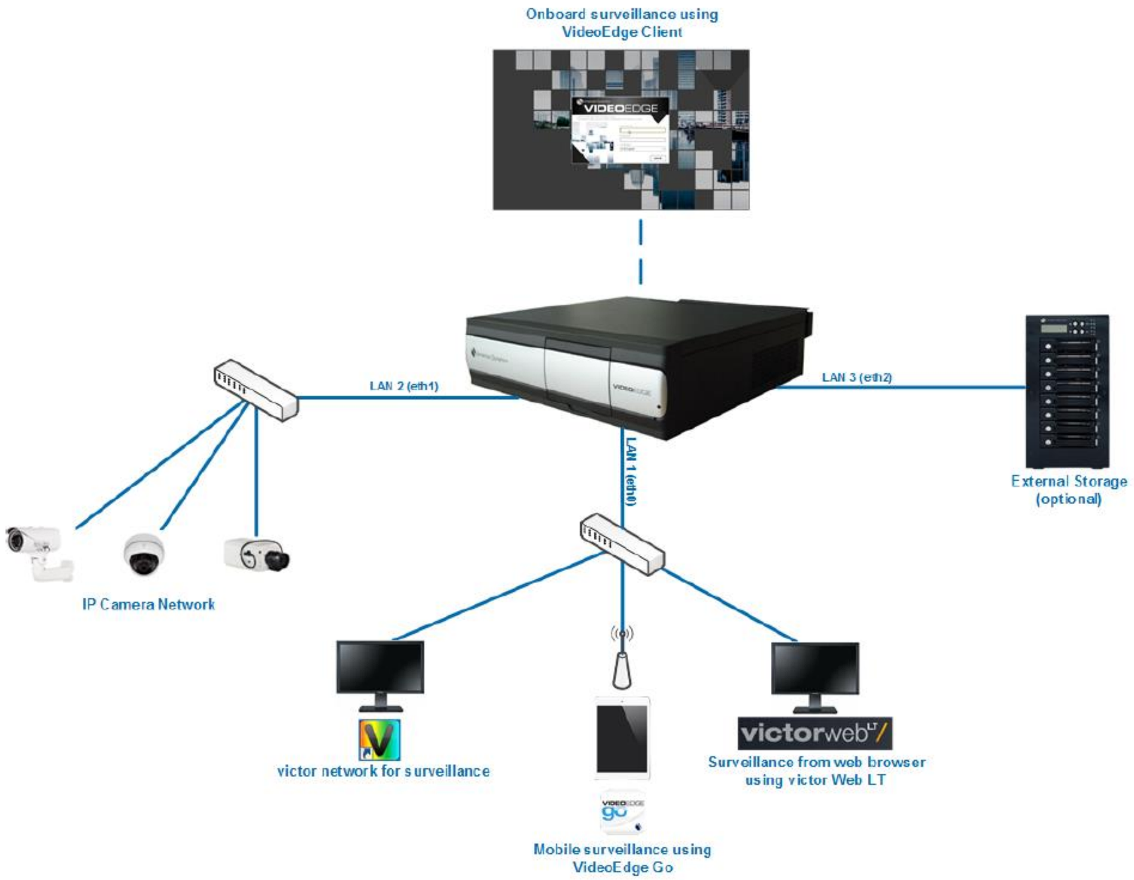
VideoEdge Network Video Recorders (NVRs)

Introduction

One of the fastest and most powerful NVRs in the industry, VideoEdge is available with a full range of intuitive clients to manage surveillance in very active environments, on-site and remotely. Scalable from a single NVR to a large, multi-site architecture, users can easily deploy any number of cameras, adding licenses at any time. Built-in intelligence allows for tailored viewing conditions which allow users to receive multiple live, recorded, alarm, and meta-data collection video streams. The end result is superior video performance with significantly reduced network bandwidth, CPU resources, and memory usage. Multicast video streams further reduce the bandwidth required for streaming high-quality video.

Using the victor client with VideoEdge NVRs allows the operator to leverage high-performance video streaming, audio, motion meta-data and an expansive feature set. Visit the victor web page for more information on the power of the victor solution.

Network Architecture



The VideoEdge Administrator

Administrating the VideoEdge application can be done 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.

The VideoEdge Operating System

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

The distribution used in VideoEdge NVRs is 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.

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

The operating system can received and harden directly from openSUSE distribution.

VideoEdge System menu

The System menu allows you to 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.

Users and Roles

Unique user accounts can be created for each operator of VideoEdge. 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. Best practices for account management include:

No shared accounts – Operators should not share user accounts. When user accounts are shared, it no longer becomes possible to determine which specific operator performed actions on VideoEdge. While VideoEdge still logs 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.

Least privilege – When assigning access rights users should only be given access to what they need to do their job. The VideoEdge NVR assist with least 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.

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.

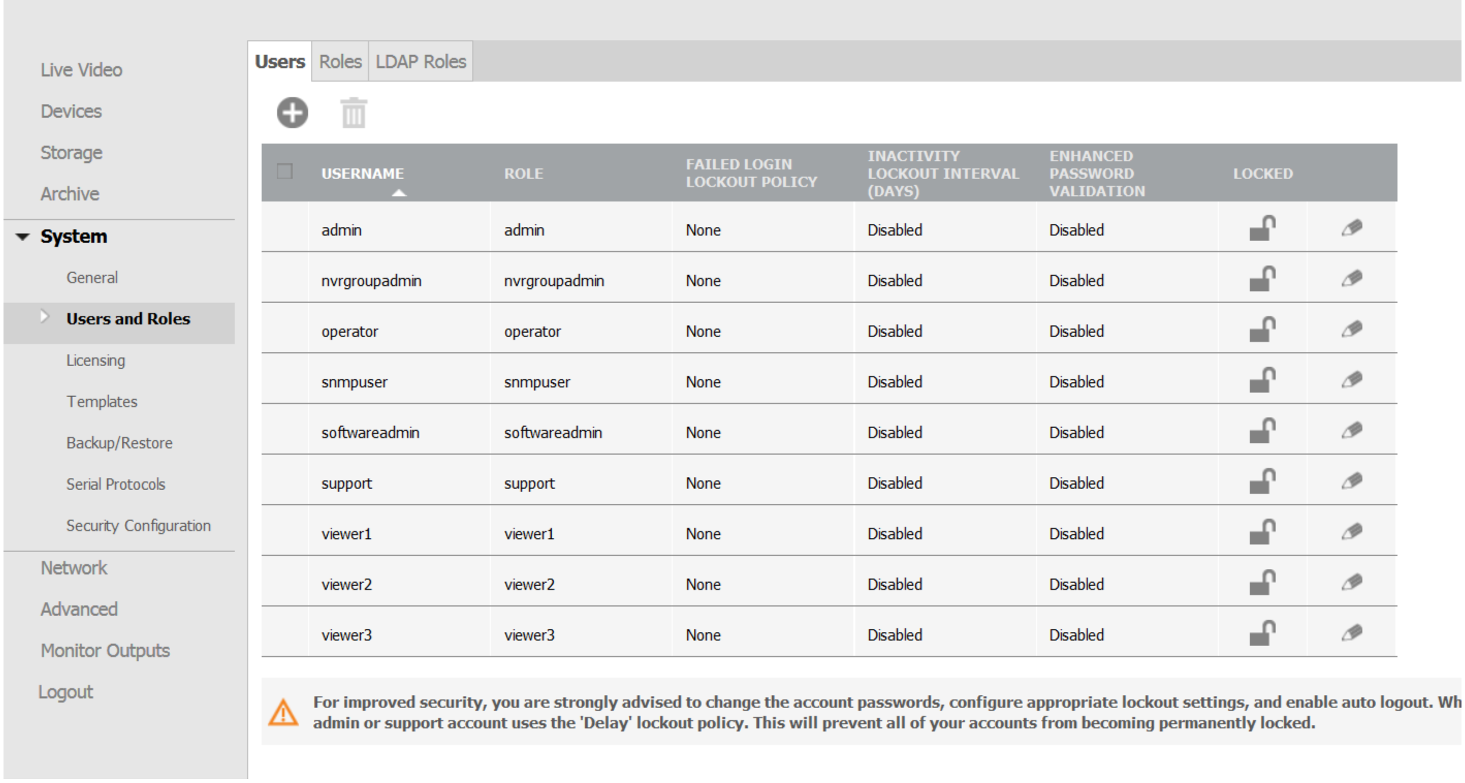
Centralized user account management – Identity Management Systems (IDMS) offer enhanced security over the local management of users within VideoEdge. An IDMS, such as Microsoft Active Directory or a Lightweight Directory Access Protocol (LDAP) capable IDMS, can provide user account management for multiple 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, expiration, etc.

Users and Roles

From here you can create new user accounts, edit existing accounts, apply lockout polices and auto logout (lockout and logout polices are OFF by default).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.

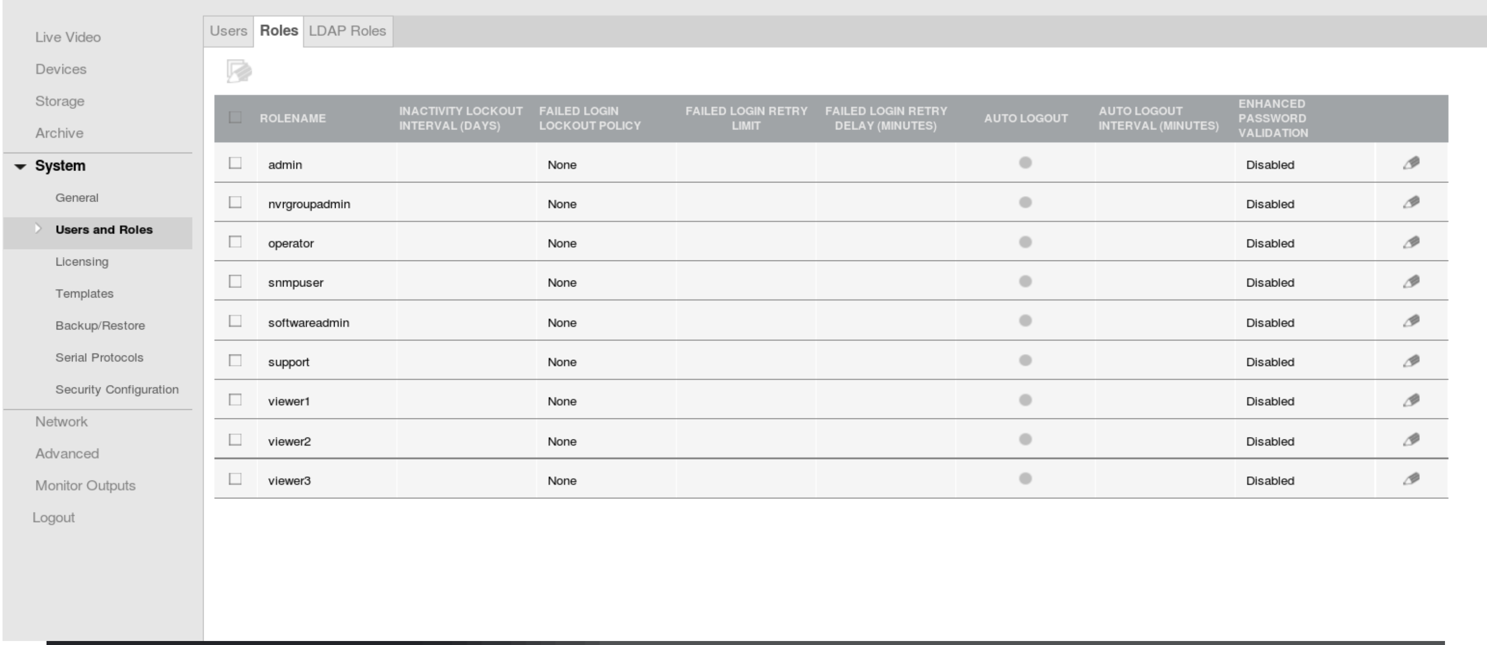
LDAP Roles

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.

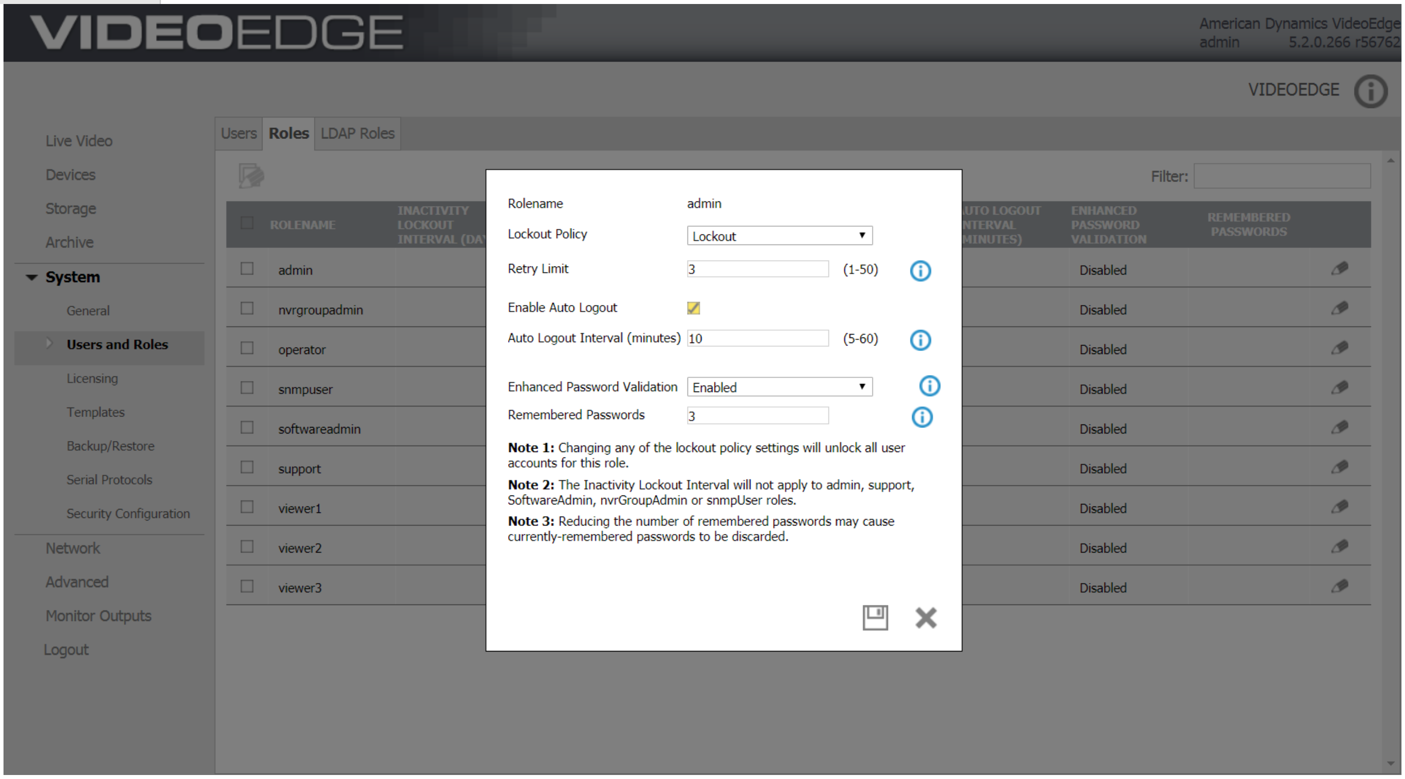


□	USERNAME	ROLE	FAILED LOGIN LOCKOUT POLICY	INACTIVITY LOCKOUT INTERVAL (DAYS)	ENHANCED PASSWORD VALIDATION	LOCKED	
	admin	admin	None	Disabled	Disabled	🔓	✎
	nvrgroupadmin	nvrgroupadmin	None	Disabled	Disabled	🔓	✎
	operator	operator	None	Disabled	Disabled	🔓	✎
	snmpuser	snmpuser	None	Disabled	Disabled	🔓	✎
	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.



□	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	
□	admin		None			●		Disabled	
□	nvrgroupadmin		None			●		Disabled	
□	operator		None			●		Disabled	
□	snmpuser		None			●		Disabled	
□	softwareadmin		None			●		Disabled	
□	support		None			●		Disabled	
□	viewer1		None			●		Disabled	
□	viewer2		None			●		Disabled	
□	viewer3		None			●		Disabled	



□	ROLENAME	INACTIVITY LOCKOUT INTERVAL (DA	UTO LOGOUT NTERVAL MINUTES)	ENHANCED PASSWORD VALIDATION	REMEMBERED PASSWORDS
□	admin			Disabled	
□	nvrgroupadmin			Disabled	
□	operator			Disabled	
□	snmpuser			Disabled	
□	softwareadmin			Disabled	
□	support			Disabled	
□	viewer1			Disabled	
□	viewer2			Disabled	
□	viewer3			Disabled	

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.

VideoEdge Administrator Users and Roles

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

User and Roles	Usability	Description
Admin	Interactive	This account allows viewing and editing of the VideoEdge Administration Interface and full functionality of the VideoEdge Client.
Operator	Interactive	This account allows viewing of the VideoEdge Administration Interface and full functionality of the VideoEdge Client.
Softwareadmin	Interactive	This account only access software updates including camera handler packs.
Support	Interactive	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	Interactive	This account is used for communication between NVRs in a group which is done using CGIs.
Snmpuser	Interactive	This account is used for SNMP communication between NVRs in a group.

VideoEdge User Roles

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

User	Usability	Description
viewer1	Interactive	Allows full functionality of the VideoEdge Client.
viewer2	Interactive	Allows full functionality of the VideoEdge Client with exception of Analog (Real) PTZ.
viewer3	Interactive	Allows full functionality of the VideoEdge Client with exception of Analog (Real) and Digital PTZ, Still Image Capture and Clip Export.

Operating System User Accounts

The VideoEdge NVR operating system may be accessed by one of the following accounts.

User	Usability	Description
root	Interactive	Root (Administrator) account for the Linux operating system.
VideoEdge	Interactive	VideoEdge is the default account to access the Linux OS.
support	Interactive	Used for remote technical support. (See note below)

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. Further, remote access can be prevented by disabling the SSH remote access.

Operating System Service Accounts

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

User	Usability	Description
postgres	Non-Interactive	Used to run the database server.
wwwrun	Non-Interactive	This account is used to run Apache and all NVR application services.
pgbouncer	Non-Interactive	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	Non-Interactive	Used for the victorWeb database.
stunnel	Non-Interactive	This is automatically created by the stunnel service and is the service account for RTSP TLS.

For a full list of Linux accounts on the VideoEdge NVR, see Annex A

Passwords

Enhanced Password Validation

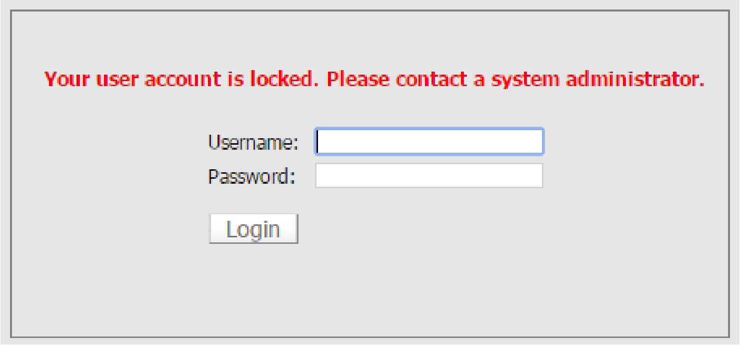
VideoEdge NVRs ship with preset passwords on all accounts. When first activated, the VideoEdge Administrator Interface advises users that these passwords should be changed. The enhanced password validation feature enforces restrictions when setting or changing passwords:

Enhanced Password Validation Requirements

- Passwords must be different than the previous three passwords
- Passwords must differ from the previous password by a minimum of three characters
- Passwords must be a minimum of eight characters long and must contain a mixture of upper and lower case letters, numbers, and special characters

VideoEdge Access Control

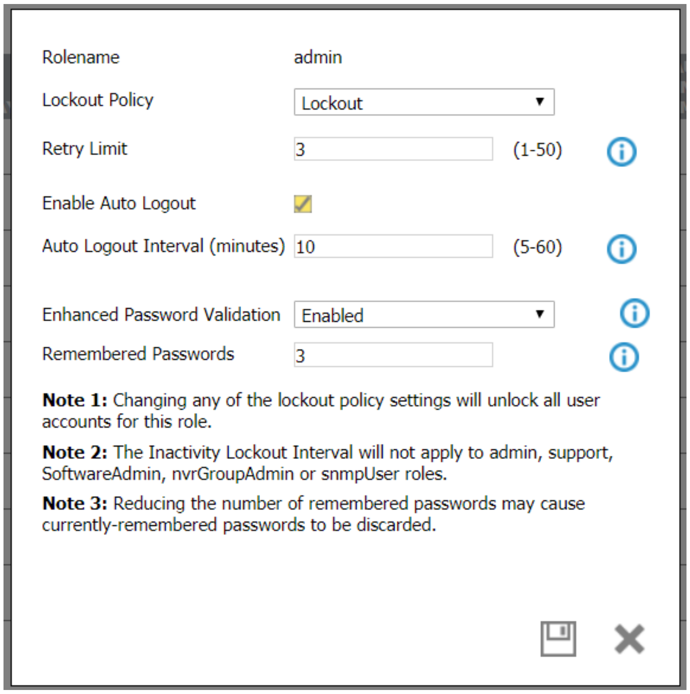
Locking User Accounts



Your user account is locked. Please contact a system administrator.

Username:
Password:

User accounts for VideoEdge Administrator Interface and VideoEdge Client may be set to permanently or temporarily lock (delay) after a configurable number of invalid login attempts. Accounts may also be set to automatically lock if not used within a set period of time 30, 60 or 90 days, e.g., to ensure ex-employee accounts are disabled. When login is attempted after this time period, the account is locked and may only be unlocked by an administrator. Permanent and temporary account lockouts are capable of generating an email alerts. You can also set enhanced password validation.



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	

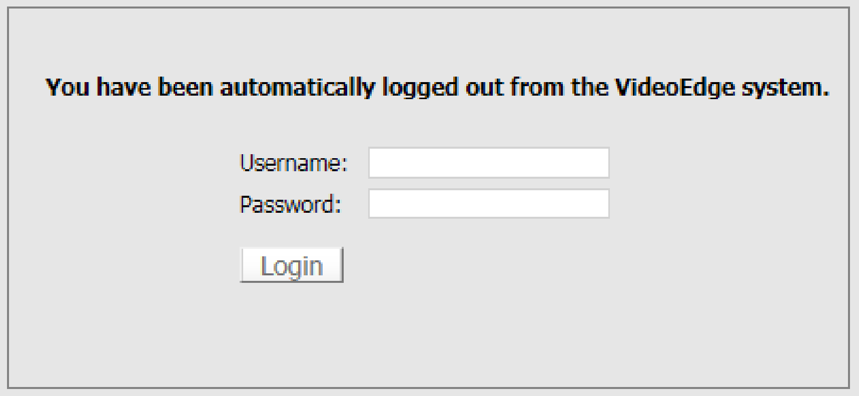
Note 1: Changing any of the lockout policy settings will unlock all user accounts for this role.

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.

Auto Logout

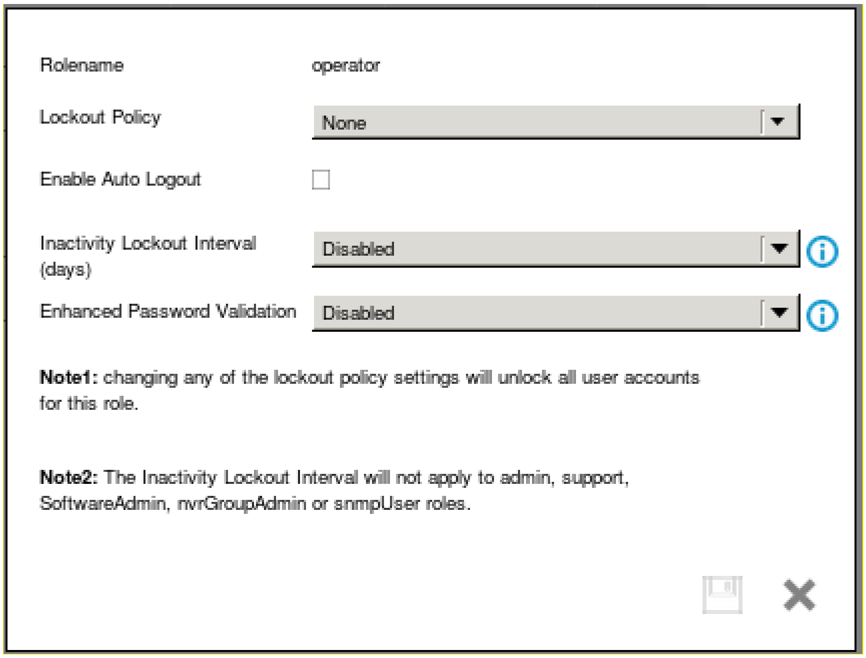
VideoEdge Administrator Interface user accounts can be configured to automatically log out the user after a configurable period of inactivity (between 5 and 60 minutes). Follow same instructions from above to set automatic logout.



You have been automatically logged out from the VideoEdge system.

Username:

Password:



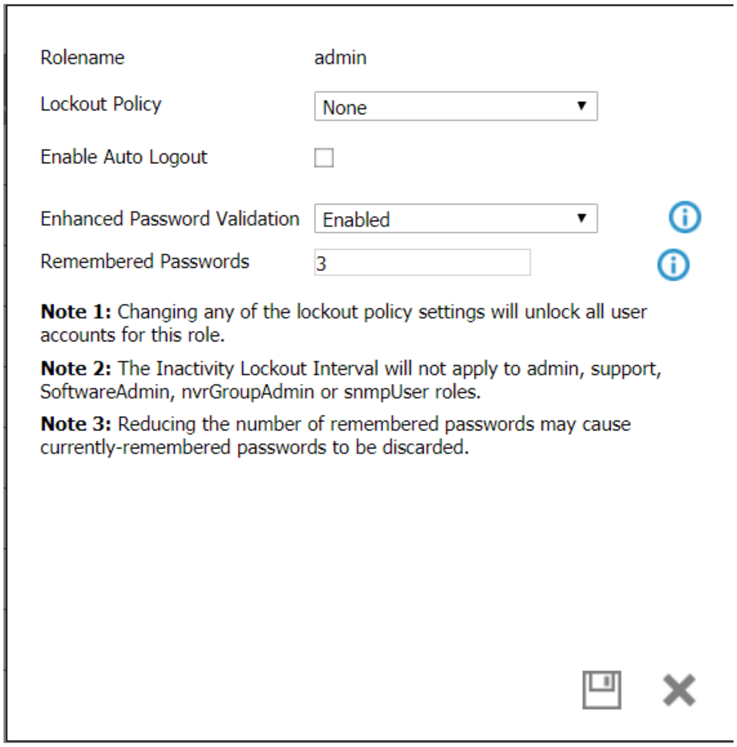
Rolename	operator
Lockout Policy	None
Enable Auto Logout	□
Inactivity Lockout Interval (days)	Disabled
Enhanced Password Validation	Disabled

Note1: changing any of the lockout policy settings will unlock all user accounts for this role.

Note2: The Inactivity Lockout Interval will not apply to admin, support, SoftwareAdmin, nvrGroupAdmin or snmpUser roles.

Password History

The VideoEdge Administrator Interface user accounts can be configured to have a password history requirement (between 3 and 10).



Rolename	admin
Lockout Policy	None
Enable Auto Logout	□
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.

Operating System User Lockout

In order to restrict unauthorized attempts to log into the local machine operating system.

Modify the /etc/pam.d/login file to reflect:

```
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 added 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 added line specifies to lock accounts automatically after 5 failed login 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 lock is removed by a manual intervention of the system administrator. See 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

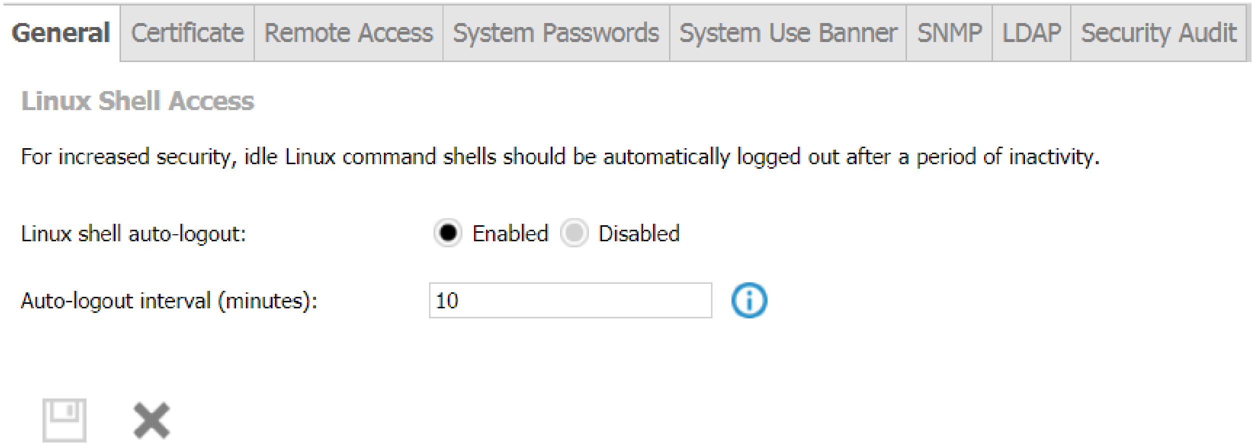
```
passwd -l user

      usermod -L user
```

Unlocking

```
passwd -u user

usermod -U user
```

Operating System remote access timeout

Local and remote terminal sessions should be configured to disconnect after a period of inactivity (default is 10 minutes).



Linux Shell Access

For increased security, idle Linux command shells should be automatically logged out after a period of inactivity.

Linux shell auto-logout: ● Enabled ○ Disabled

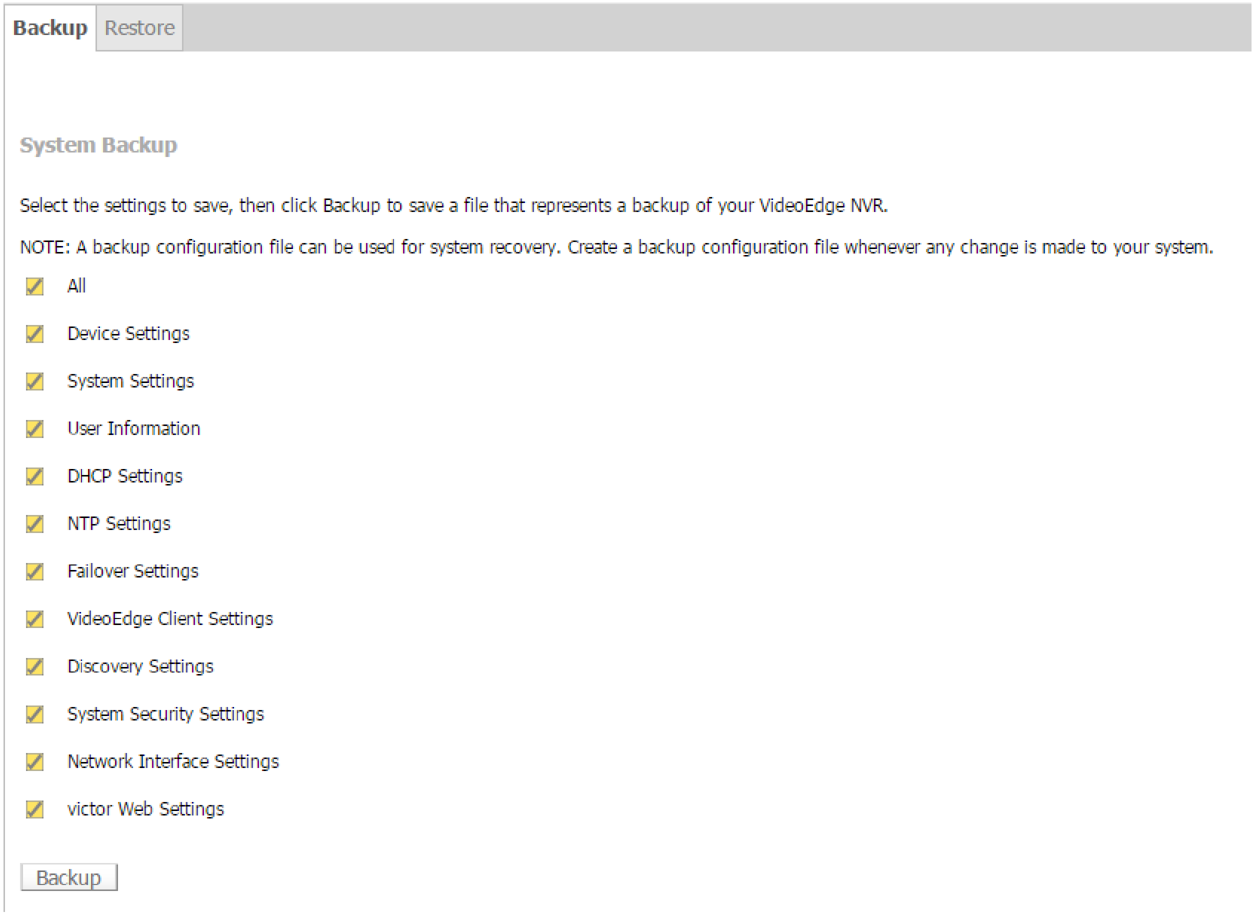
Auto-logout interval (minutes): 10

Robustness

Having redundancy is a security best practice, and it is vital for your system to have it. Having a robust system will help to limit down time and enable you to recover if your system had an attack e.g. ransomware.

Backup / Restore

In the event of a system failure, recovery of the NVR server's configuration data is possible via a system backup file stored to a USB or local disk. The backup file can be imported to the NVR to restore the saved configuration.



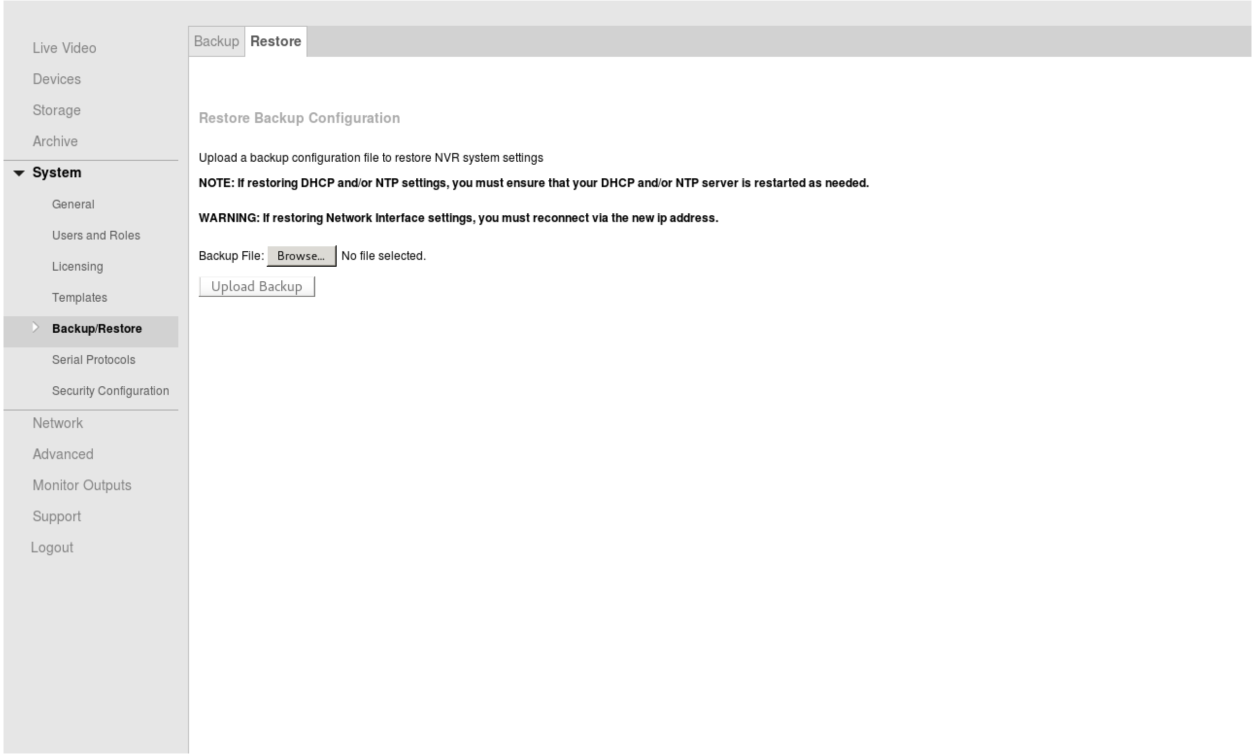
System Backup

Select the settings to save, then click Backup to save a file that represents a backup of your VideoEdge NVR.

NOTE: A backup configuration file can be used for system recovery. Create a backup configuration file whenever any change is made to your system.

- ☑ All
- ☑ Device Settings
- ☑ System Settings
- ☑ User Information
- ☑ DHCP Settings
- ☑ NTP Settings
- ☑ Failover Settings
- ☑ VideoEdge Client Settings
- ☑ Discovery Settings
- ☑ System Security Settings
- ☑ Network Interface Settings
- ☑ victor Web Settings

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. The text file can be used as reference for manually configuring the OS settings.



Restore Backup Configuration

Upload a backup configuration file to restore NVR system settings

NOTE: If restoring DHCP and/or NTP settings, you must ensure that your DHCP and/or NTP server is restarted as needed.

WARNING: If restoring Network Interface settings, you must reconnect via the new ip address.

Backup File: Browse... No file selected.

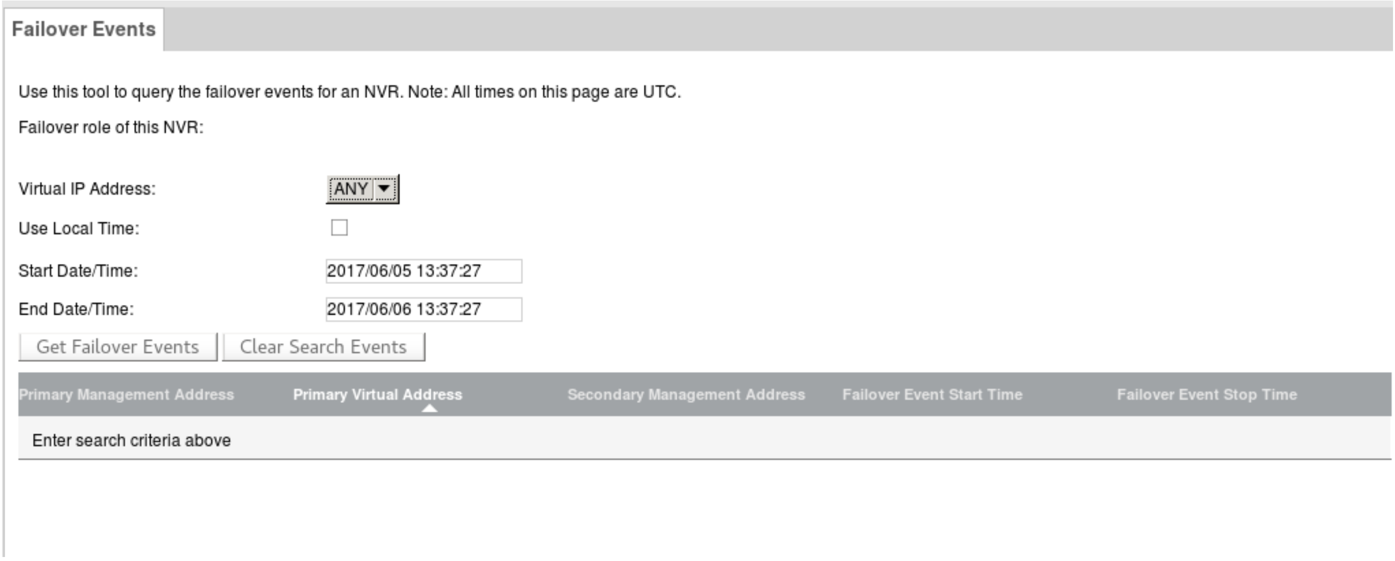
Upload Backup

Failover

When configured as a secondary NVR, VideoEdge will monitor other VideoEdge NVRs that have been added to its server monitoring list. In the event that a primary NVR fails, the secondary NVR will detect the failure after approximately 30 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 have a video backfill feature which provides the capability for the VideoEdge NVR to fill in the gaps in recorded video.

Known limitation: SNMP and SSH are required for VideoEdge NVRs to be configured for failover. It is recommended that the SNMP Read-only community string to something unique and change the SSH password.



Use this tool to query the failover events for an NVR. Note: All times on this page are UTC.

Failover role of this NVR:

Virtual IP Address: ANY

Use Local Time: □

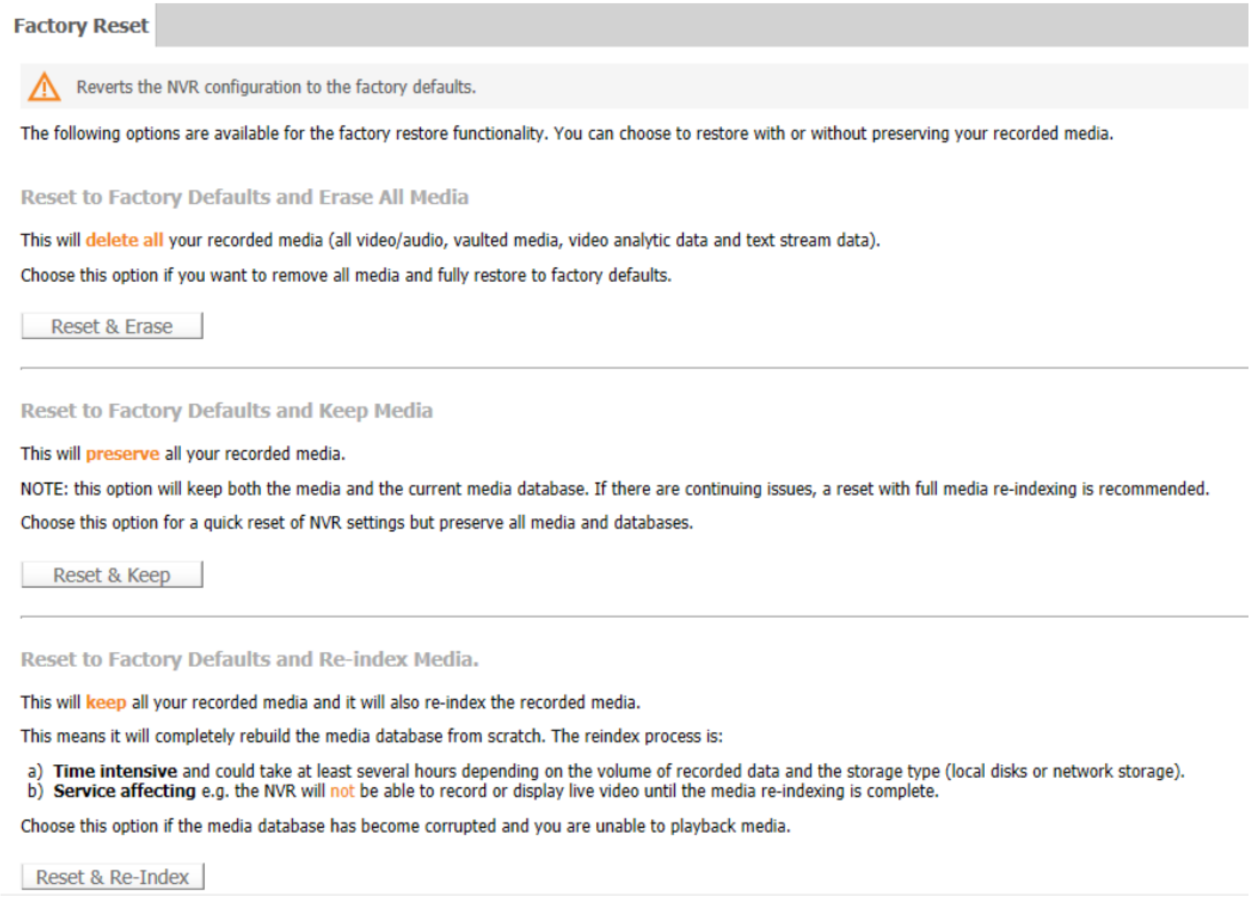
Start Date/Time: 2017/06/05 13:37:27

End Date/Time: 2017/06/06 13:37:27

Primary Management Address	Primary Virtual Address	Secondary Management Address	Failover Event Start Time	Failover Event Stop Time
Enter search criteria above				

Recovery / Factory Reset

VideoEdge provides multiple options for resetting the NVR and OS to its initial factory conditions; some while preserving recorded media. Carrying out a Reset to Factory Defaults will have no effect on the NVR's Linux based operating system.



Factory Reset

⚠ Reverts the NVR configuration to the factory defaults.

The following options are available for the factory restore functionality. You can choose to restore with or without preserving your recorded media.

Reset to Factory Defaults and Erase All Media

This will delete all your recorded media (all video/audio, vaulted media, video analytic data and text stream data).

Choose this option if you want to remove all media and fully restore to factory defaults.

Reset to Factory Defaults and Keep Media

This will preserve all your recorded media.

NOTE: this option will keep both the media and the current media database. If there are continuing issues, a reset with full media re-indexing is recommended.

Choose this option for a quick reset of NVR settings but preserve all media and databases.

Reset to Factory Defaults and Re-index Media.

This will keep all your recorded media and it will also re-index the recorded media.

This means it will completely rebuild the media database from scratch. The reindex process is:

a) **Time intensive** and could take at least several hours depending on the volume of recorded data and the storage type (local disks or network storage).
b) **Service affecting** e.g. the NVR will not be able to record or display live video until the media re-indexing is complete.

Choose this option if the media database has become corrupted and you are unable to playback media.

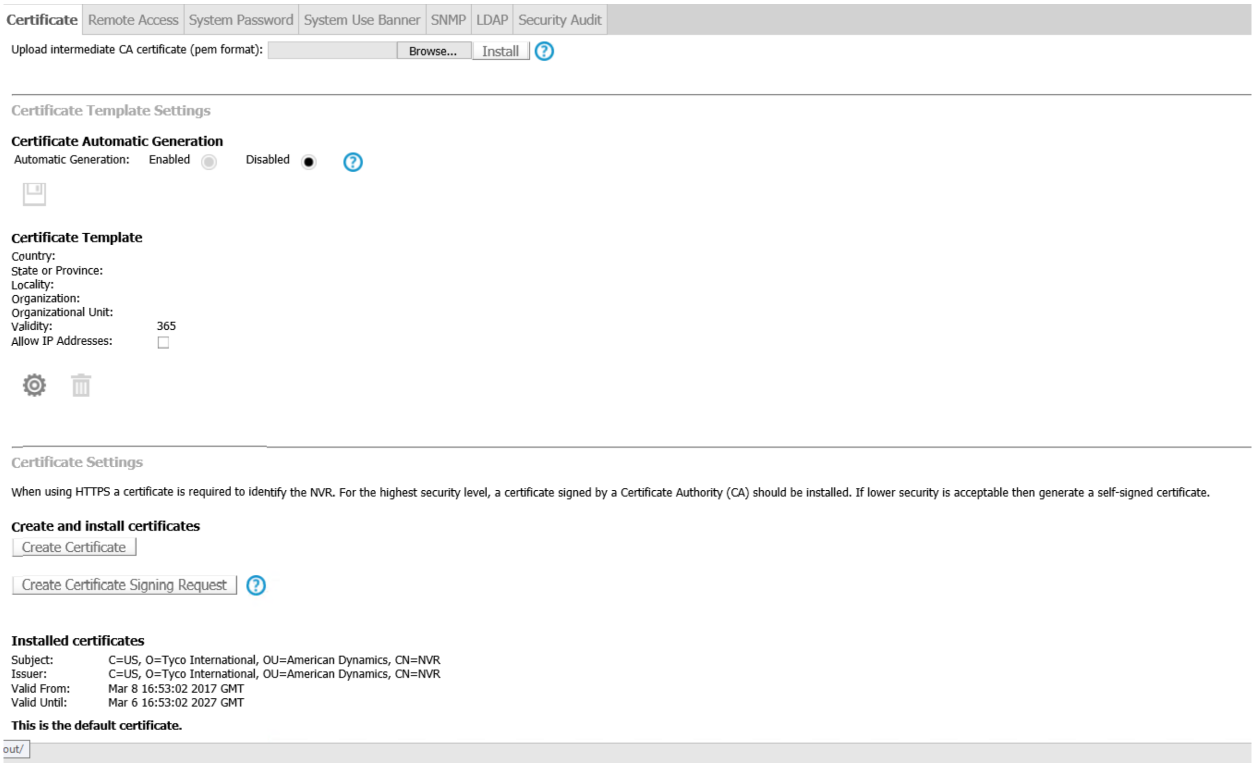
Security Configuration

The VideoEdge administration has several features to help monitor and assess the security of the NVR. For convenience, many of these features are located in the Security Configuration section located under System.

Certificate

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 that its identity can be verified by your web browser or victor Client. The certificate can be self-signed, or for more security-conscious customers, it can be signed by a trusted certificate authority. 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 please see *VideoEdge NVR Installation and User Guide.*



Upload intermediate CA certificate (pem format):

Certificate Template Settings

Certificate Automatic Generation

Automatic Generation: Enabled ○ Disabled ●

Certificate Template

Country:
State or Province:
Locality:
Organization:
Organizational Unit:
Validity: 365
Allow IP Addresses: □

Certificate Settings

When using HTTPS a certificate is required to identify the NVR. For the highest security level, a certificate signed by a Certificate Authority (CA) should be installed. If lower security is acceptable then generate a self-signed certificate.

Create and install certificates

Installed certificates

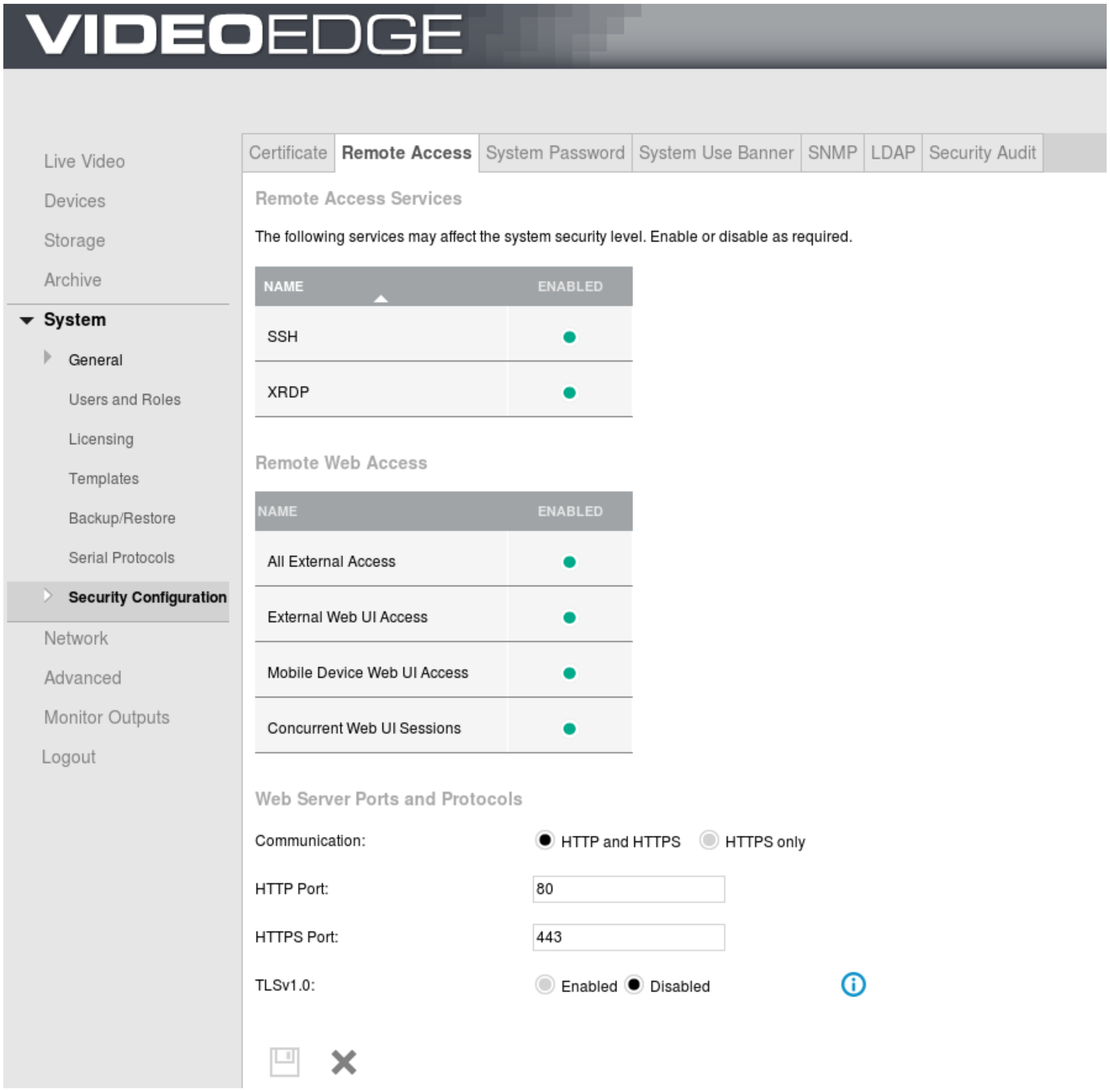
Subject:	C=US, O=Tyco International, OU=American Dynamics, CN=NVR
Issuer:	C=US, O=Tyco International, OU=American Dynamics, CN=NVR
Valid From:	Mar 8 16:53:02 2017 GMT
Valid Until:	Mar 6 16:53:02 2027 GMT

This is the default certificate.

Remote Access

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

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 recommend that you use HTTPS only. It is also recommended that you change default ports to help defend against non-targeted attacks.



Remote Access Services

The following services may affect the system security level. Enable or disable as required.

NAME	ENABLED
SSH	●
XRDP	●

Remote Web Access

NAME	ENABLED
All External Access	●
External Web UI Access	●
Mobile Device Web UI Access	●
Concurrent Web UI Sessions	●

Web Server Ports and Protocols

Communication:	● HTTP and HTTPS ○ HTTPS only
HTTP Port:	80
HTTPS Port:	443
TLSv1.0:	○ Enabled ● Disabled

SSH: Secure Shell is a cryptographic network protocol for secure data communication. The SSH protocol on the VideoEdge NVR allows remote access to the server, and is also used for failover functionality. (default port 22 – not configurable, disabled by default)

xRDP: Microsoft Remote Desktop Protocol allows 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. It replaces the SSL (Secure Socket Layer) protocol now obsolete. (default port 443 – configurable, TLS 1.2 enabled by default, TLS 1.0 disabled by default)

New in 5.0: Starting with version 5.0, VNC will no longer be available.

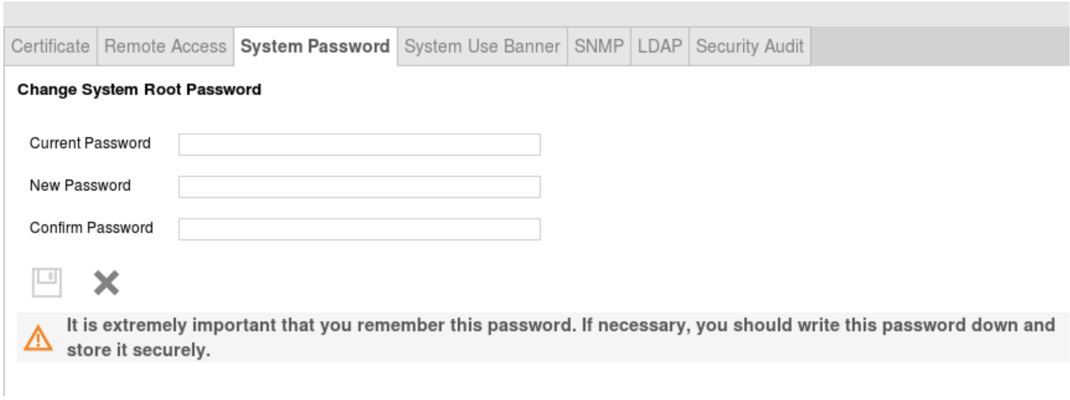
New in 5.1: Starting with version 5.1, new installations of VideoEdge will have SSH and xRDP disabled by default. However, upgrades will maintain the existing status

New in 5.1: To enable SSH, the default credentials cannot be utilized.

New in 5.1: Starting with version 5.1, the VideoEdge NVR will support TLS version 1.2 only by default. TLS version 1.0 may be enabled through the VideoEdge Administratorfor installations needing to add recorders securely to versions of victor prior to 4.9.1 TLSv1 can then be disabled after the recorder has been added.

System Password

VideoEdge NVR provides the ability to change the local root account password. This is highly recommend, as the default password prioritises ease of installation above security. The root account provides full administrative access to the VideoEdge NVR's operating system. Changing the system password and making it unique enhances the security of the product. See instructions below.



Change System Root Password

Current Password

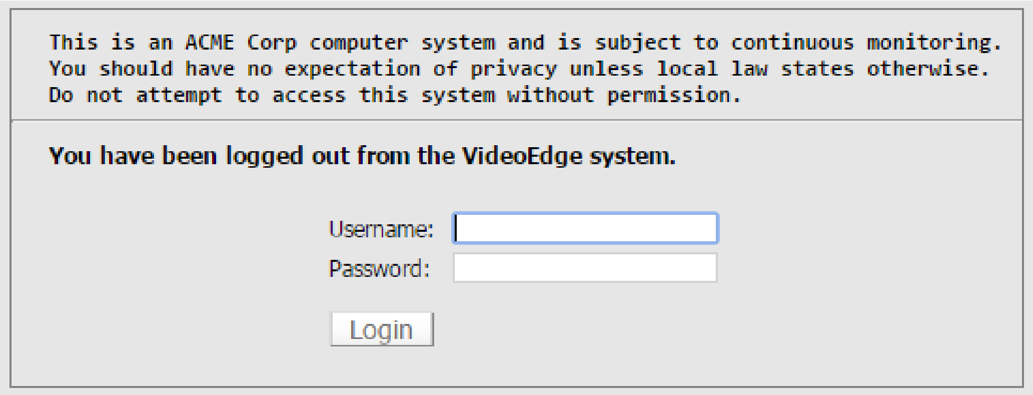
New Password

Confirm Password

It is extremely important that you remember this password. If necessary, you should write this password down and store it securely.

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.

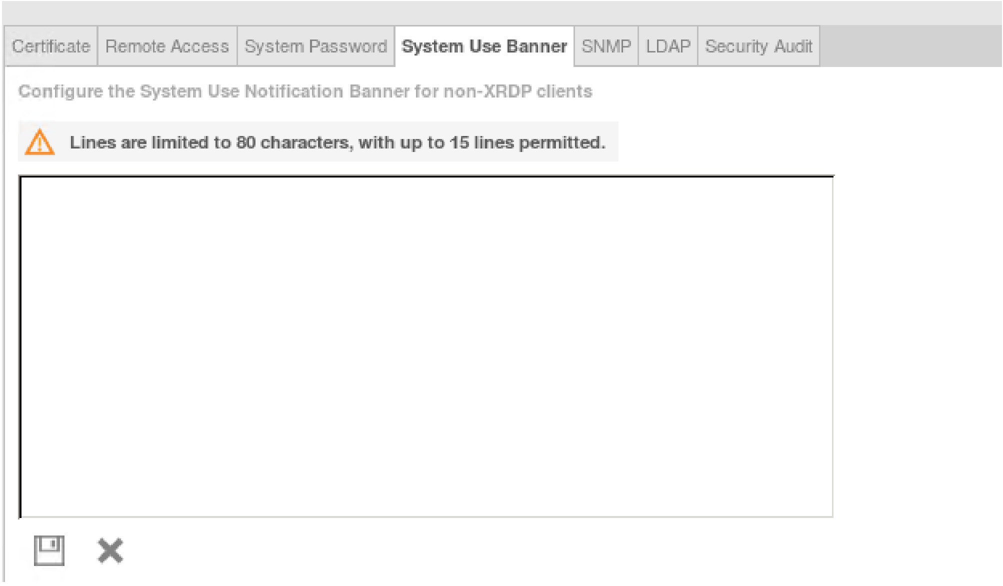
System Use Banner



```
This is an ACME Corp computer system and is subject to continuous monitoring.
You should have no expectation of privacy unless local law states otherwise.
Do not attempt to access this system without permission.
```

You have been logged out from the VideoEdge system.

The System Use Banner can be configured to display a notification message or image before the user logs on to the system either locally or remotely. It can be used to provide privacy and security notices consistent with applicable laws, executive orders, directives, polices, regulations, standards, and guidance.

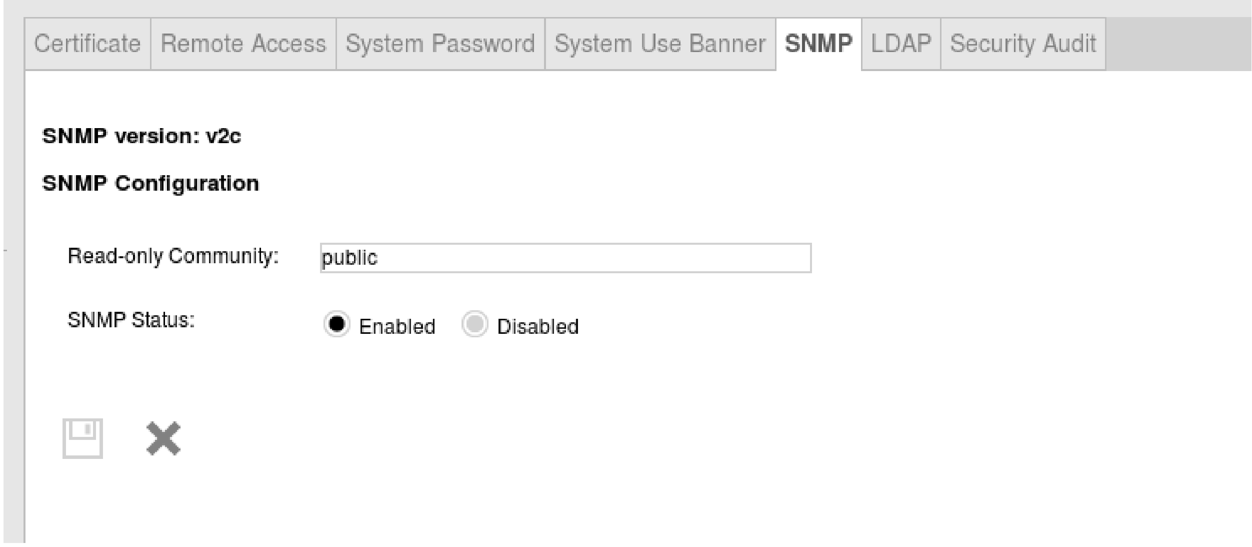


Configure the System Use Notification Banner for non-XRDP clients

Lines are limited to 80 characters, with up to 15 lines permitted.

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.



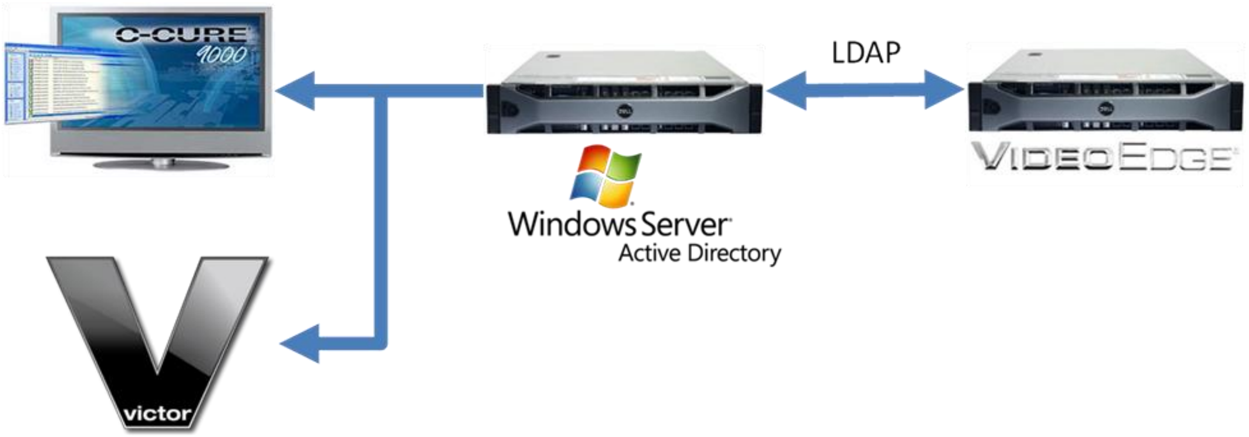
SNMP version: v2c

SNMP Configuration

Read-only Community: public

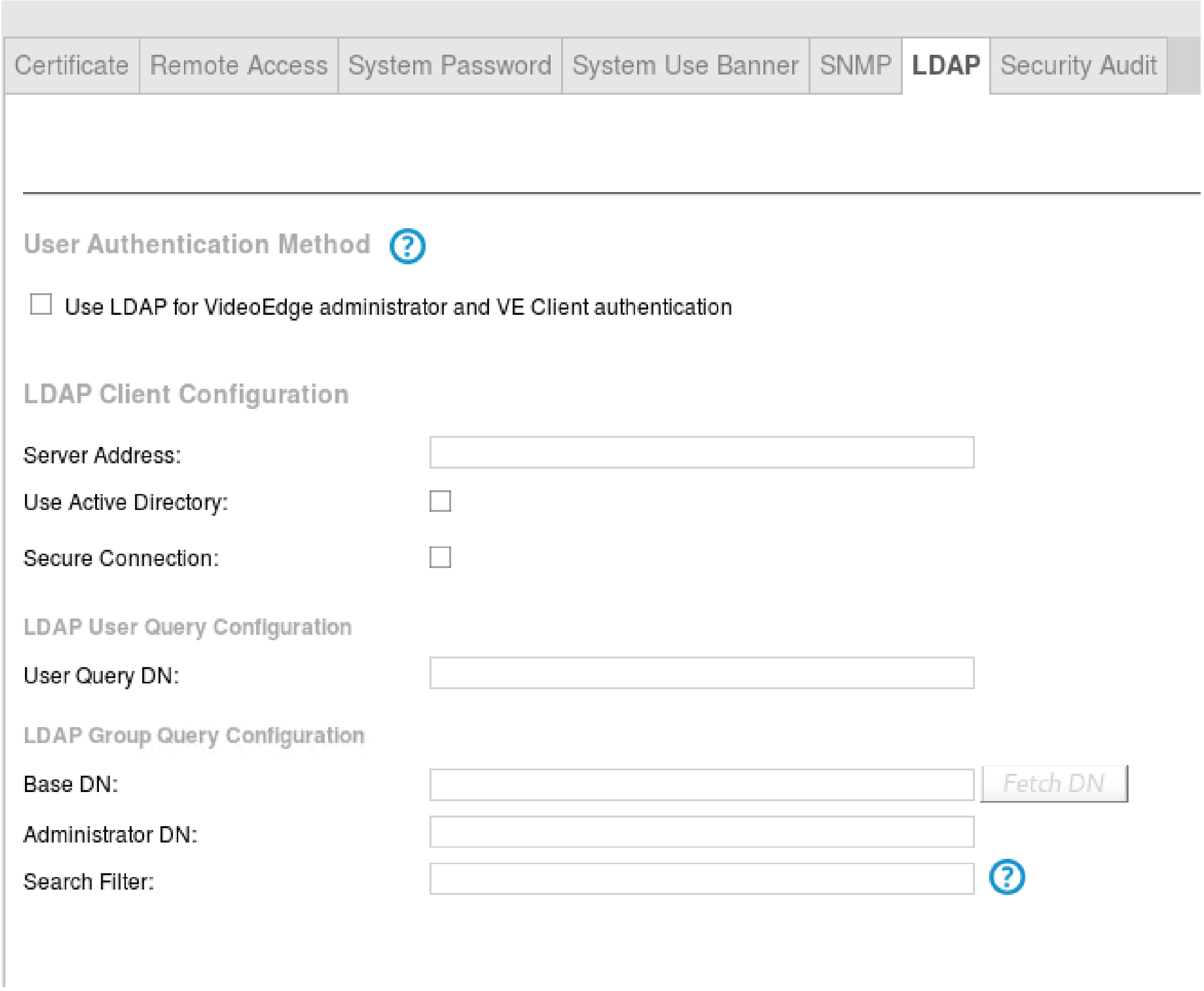
SNMP Status: ● Enabled ○ Disabled

LDAP



LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.

- LDAP authentication and authorization for admin GUI
- OpenLDAP and Microsoft Active Directory
- Secure connections using TLS



User Authentication Method

□ Use LDAP for VideoEdge administrator and VE Client authentication

LDAP Client Configuration

Server Address:

Use Active Directory: □

Secure Connection: □

LDAP User Query Configuration

User Query DN:

LDAP Group Query Configuration

Base DN:

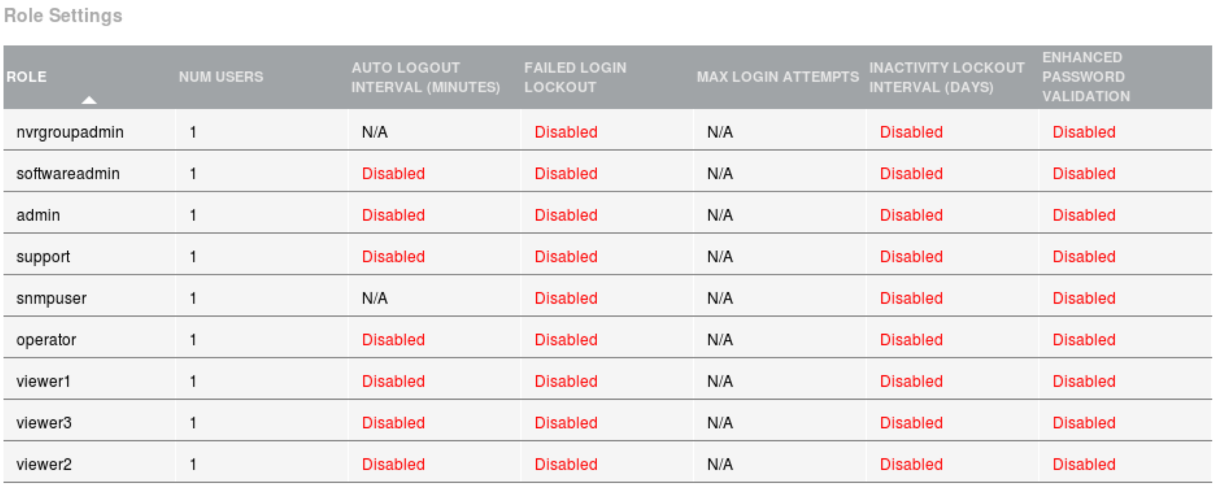
Administrator DN:

Search Filter:

Security Audit Dashboard

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

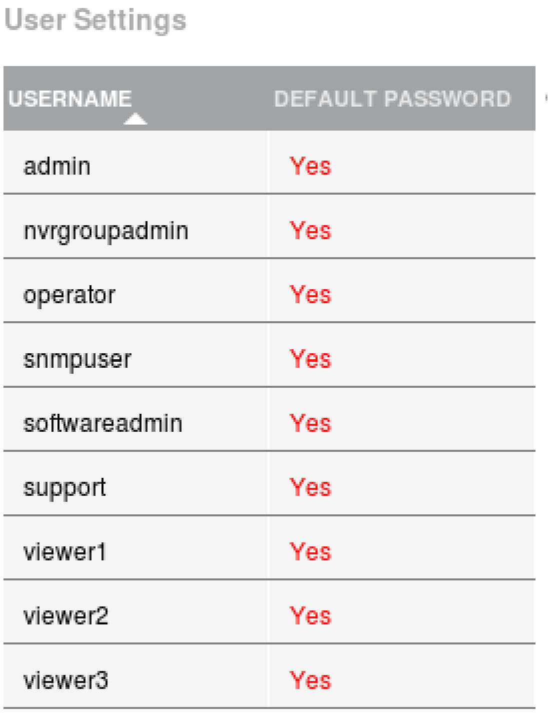
Role Settings displays which roles have features such as Auto Logout and Failed Login Lockout enabled as well as the number of users within that role.



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

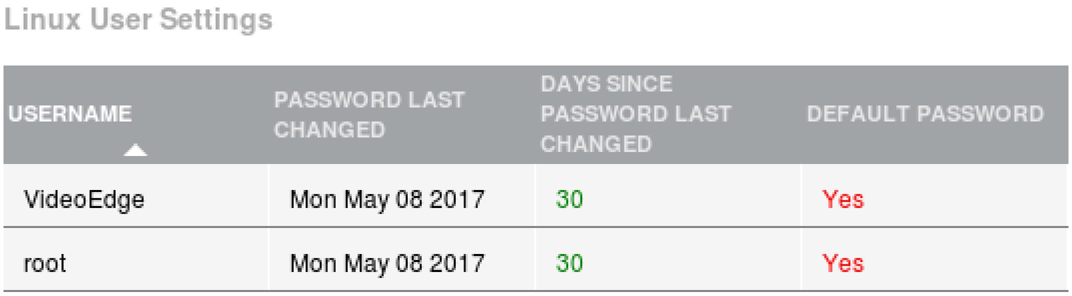
User Settings displays the status of default passwords in use by comparing the default hash against the stored hash. If there is a match, the test will be red indicating the default password is still being used.



User Settings

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

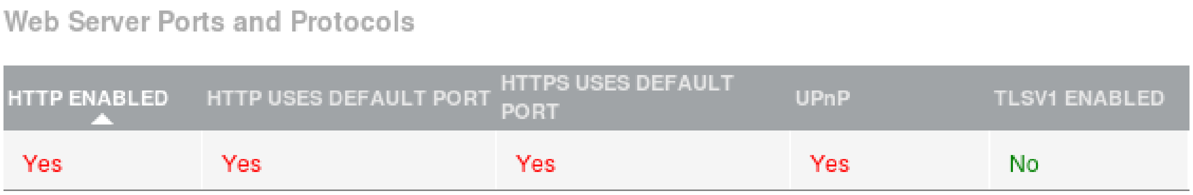
Linux User Settings displays the Operating System accounts and when the passwords were last changed and whether they are still using the default password.



Linux User Settings

USERNAME	PASSWORD LAST CHANGED	DAYS SINCE PASSWORD LAST CHANGED	DEFAULT PASSWORD
VideoEdge	Mon May 08 2017	30	Yes
root	Mon May 08 2017	30	Yes

The Web Server Ports and Protocols displays which web server ports and protocols are enabled.

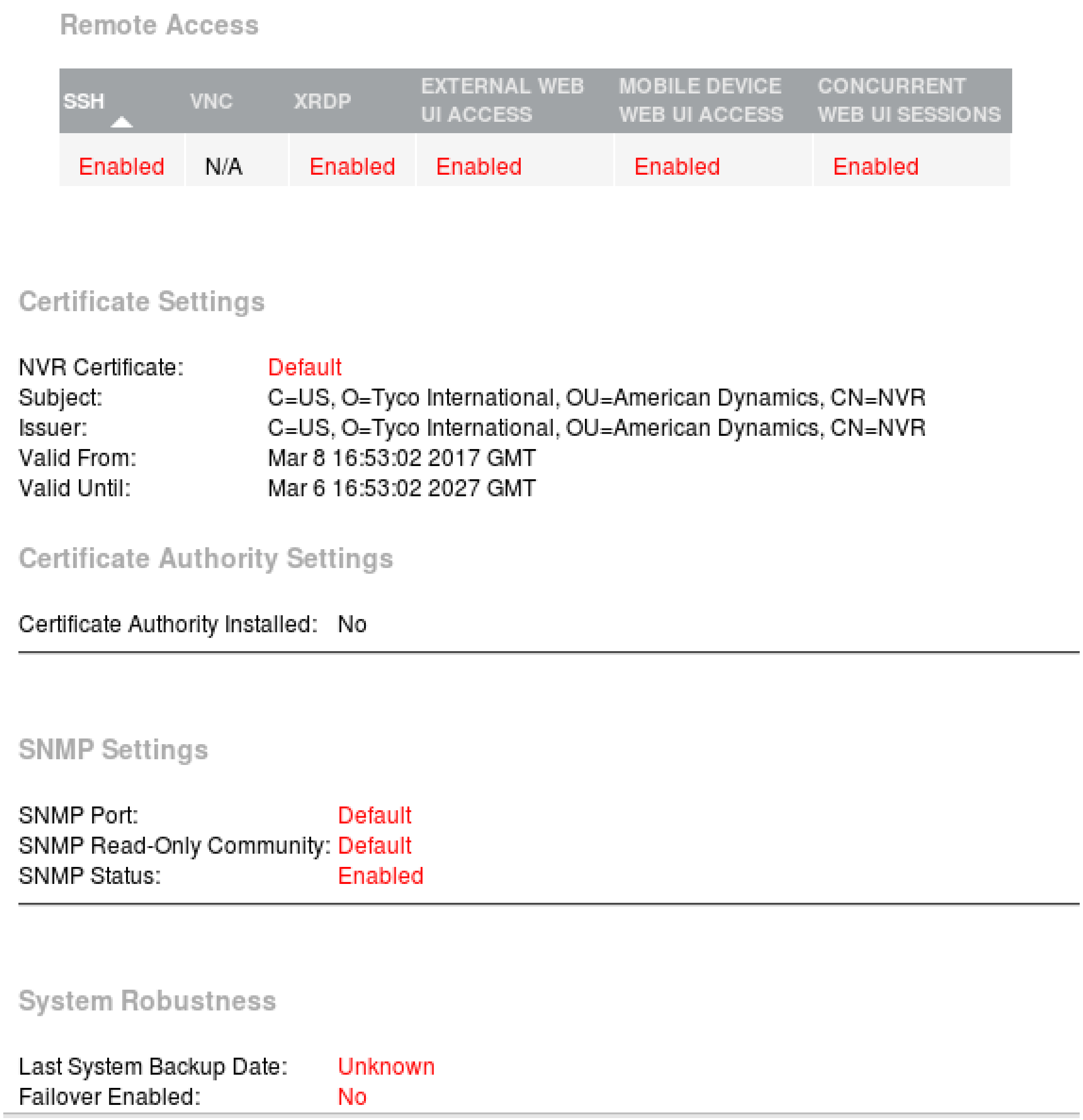


Web Server Ports and Protocols

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

Remote Access 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.

SNMP Read-only community string - enables a remote device to retrieve "read-only" information from a device.



Remote Access

SSH	VNC	XRDP	EXTERNAL WEB UI ACCESS	MOBILE DEVICE WEB UI ACCESS	CONCURRENT WEB UI SESSIONS
Enabled	N/A	Enabled	Enabled	Enabled	Enabled

Certificate Settings

NVR Certificate:	Default
Subject:	C=US, O=Tyco International, OU=American Dynamics, CN=NVR
Issuer:	C=US, O=Tyco International, OU=American Dynamics, CN=NVR
Valid From:	Mar 8 16:53:02 2017 GMT
Valid Until:	Mar 6 16:53:02 2027 GMT

Certificate Authority Settings

Certificate Authority Installed: No

SNMP Settings

SNMP Port:	Default
SNMP Read-Only Community:	Default
SNMP Status:	Enabled

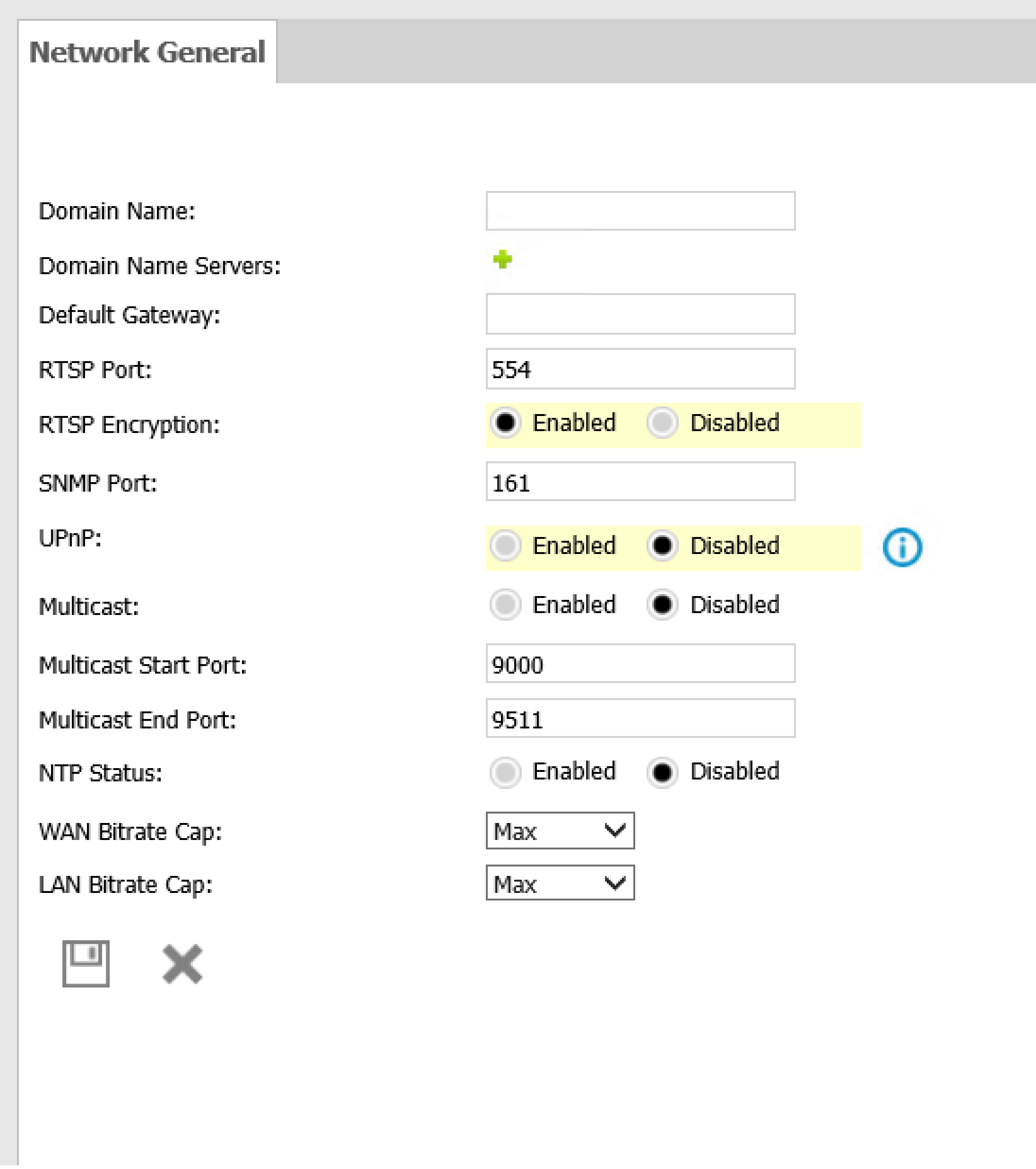
System Robustness

Last System Backup Date:	Unknown
Failover Enabled:	No

Securing Network General

TLS Tunneling of RTSP Credentials

The RTSP Encryption feature allows victor and VideoEdge NVR to transmit RTSP credentials and RTSP commands (i.e Describe, Options, Setup, Play, Teardown, Announce, etc.) over a secure, encrypted TLS tunnel. Additionally, authentication is done through TLS certificates.



Network General

Domain Name:	
Domain Name Servers:	
Default Gateway:	
RTSP Port:	554
RTSP Encryption:	● Enabled ○ Disabled
SNMP Port:	161
UPnP:	○ Enabled ● Disabled
Multicast:	○ Enabled ● Disabled
Multicast Start Port:	9000
Multicast End Port:	9511
NTP Status:	○ Enabled ● Disabled
WAN Bitrate Cap:	Max
LAN Bitrate Cap:	Max

System and Communication Protection

OpenSSL

The VideoEdge operating system uses the industry-standard OpenSSL platform to provide secure connections for communications such as SSH, HTTPS, and TLS LDAP sessions.

For a list of ciphers supported by VideoEdge NVR, see ANNEX C

Enabling FIPS on 5.2

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.

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.

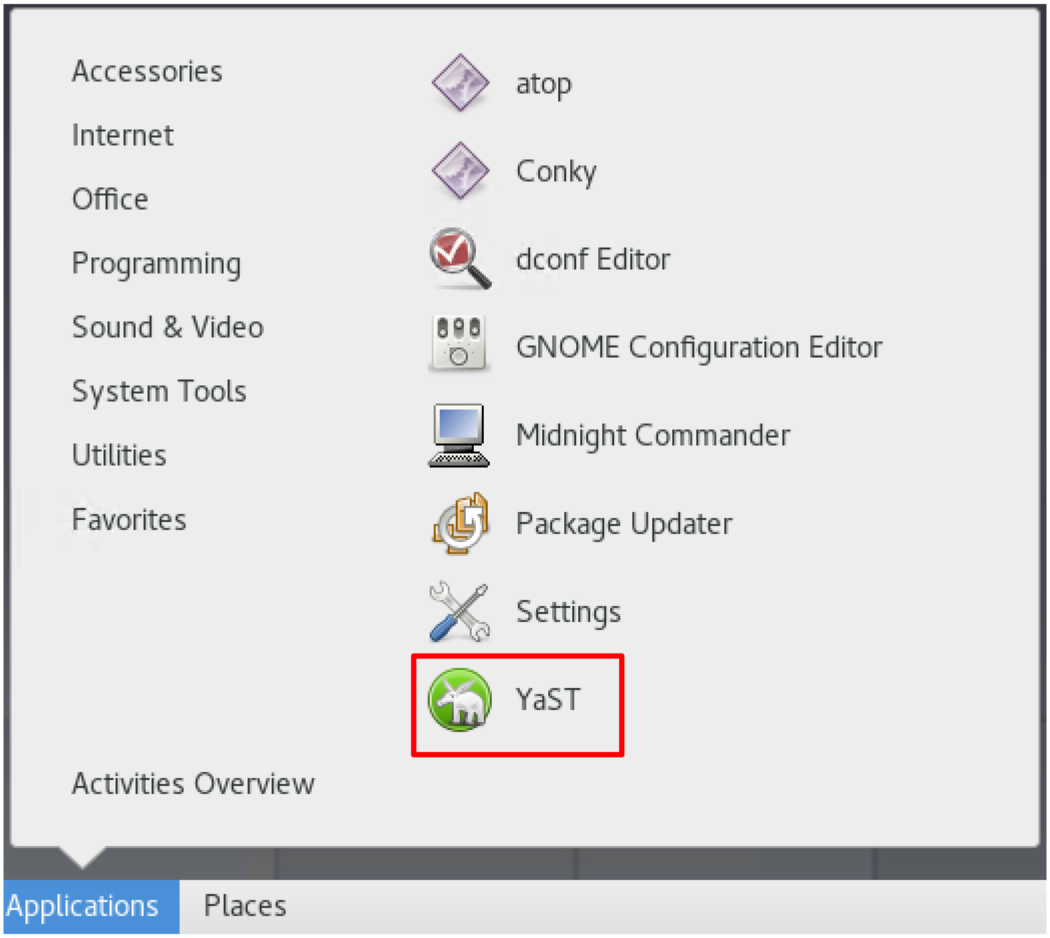
FIPS packages are included beginning in VideoEdge NVR version 5.1. However additional command line steps are needed to enable FIPS.

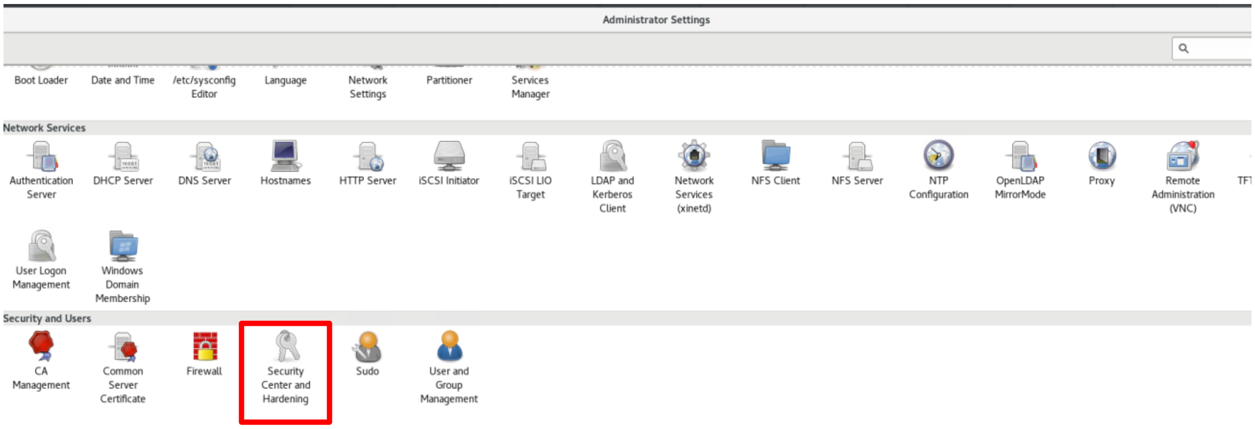
1. Login into the VideoEdge
2. Open a terminal type su – then enter root password
3. Query the current status: /opt/americandynamics/venvr/bin/fipsmode
4. Enable FIPS mode /opt/americandynamics/venvr/bin/fipsmode 1
5. Disable FIPS mode /opt/americandynamics/venvr/bin/fipsmode 0

Changes will take effect upon the next reboot.

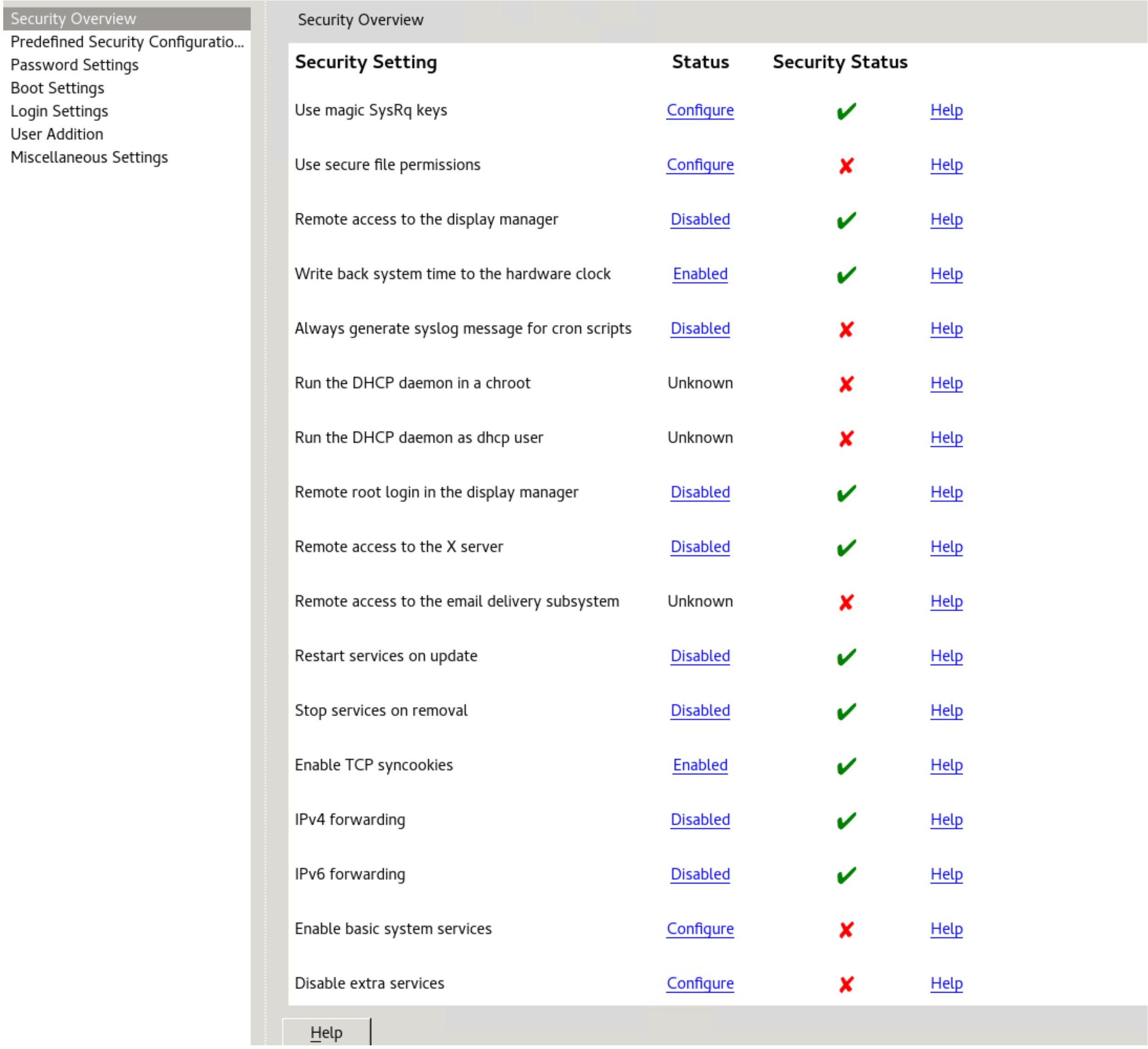
Security Center and Hardening

The SLES Operating System comes with built-in Security Center and Hardening to configure predefined security configurations, password settings, boot settings, login settings among other settings. Setting the hardening through YaST only hardens the Operating System and does not harden the VideoEdge. To get to the SecurityCenter and Hardening go to applications, system tools, and then click on YaST. Security Center and Hardening is located under security and users.



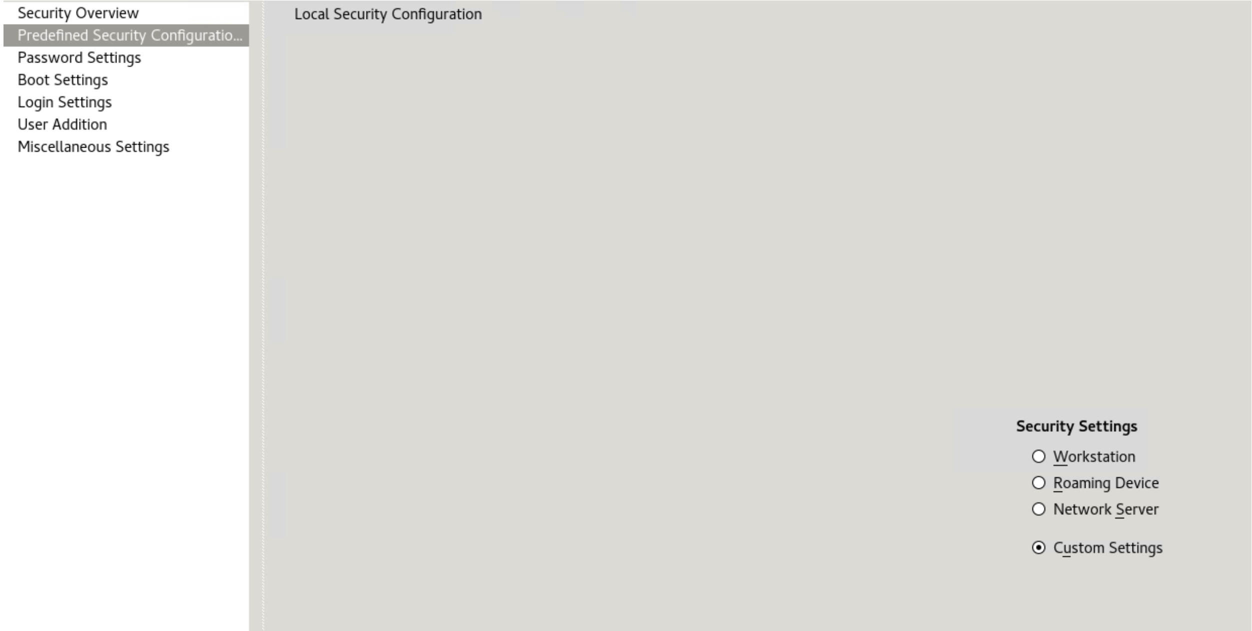


Below shows the page that opens when you open Security Center and Hardening. The security overview shows the status of what security feature is enabled or disabled.



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

There are four predefined security configurations to choose from, they are listed below. Once you click one of the security settings it will close out the page, once the administrator re-opens security center and hardening, notice that the security overview has been changed. Below are two examples, one being the workstation configuration and the other the Network Server configuration.



- Security Overview
- Predefined Security Configuratio...
- Password Settings
- Boot Settings
- Login Settings
- User Addition
- Miscellaneous Settings

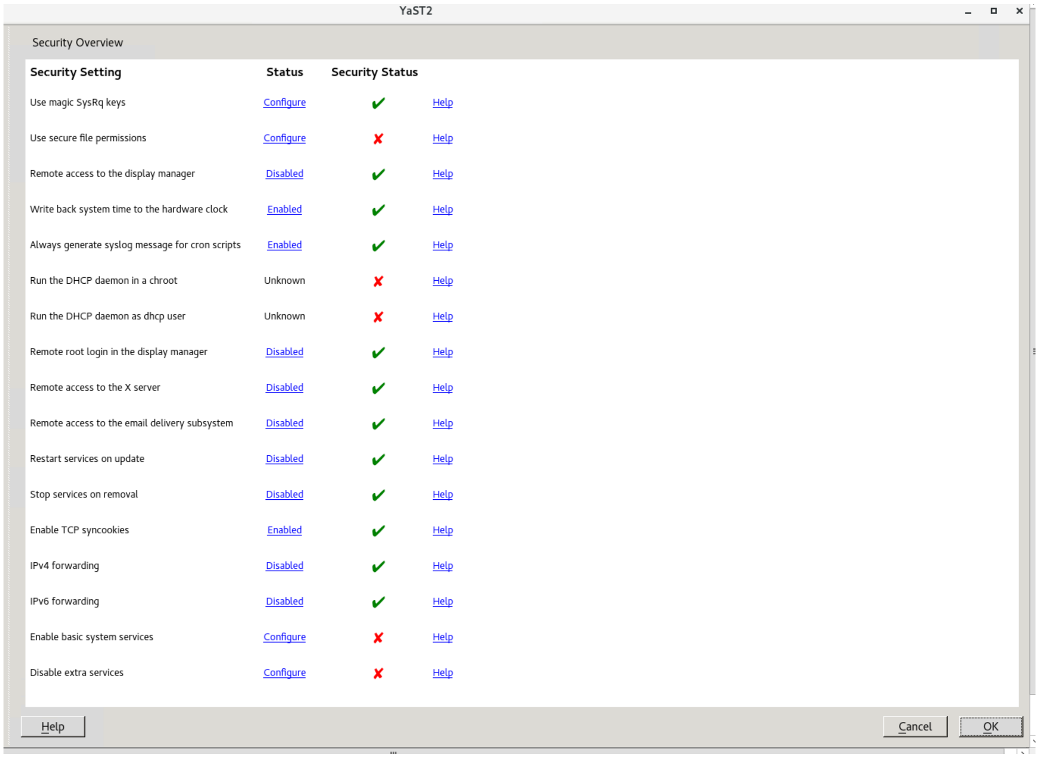
Local Security Configuration

Security Settings

○ Workstation
○ Roaming Device
○ Network Server

● Custom Settings

Workstation Configuration

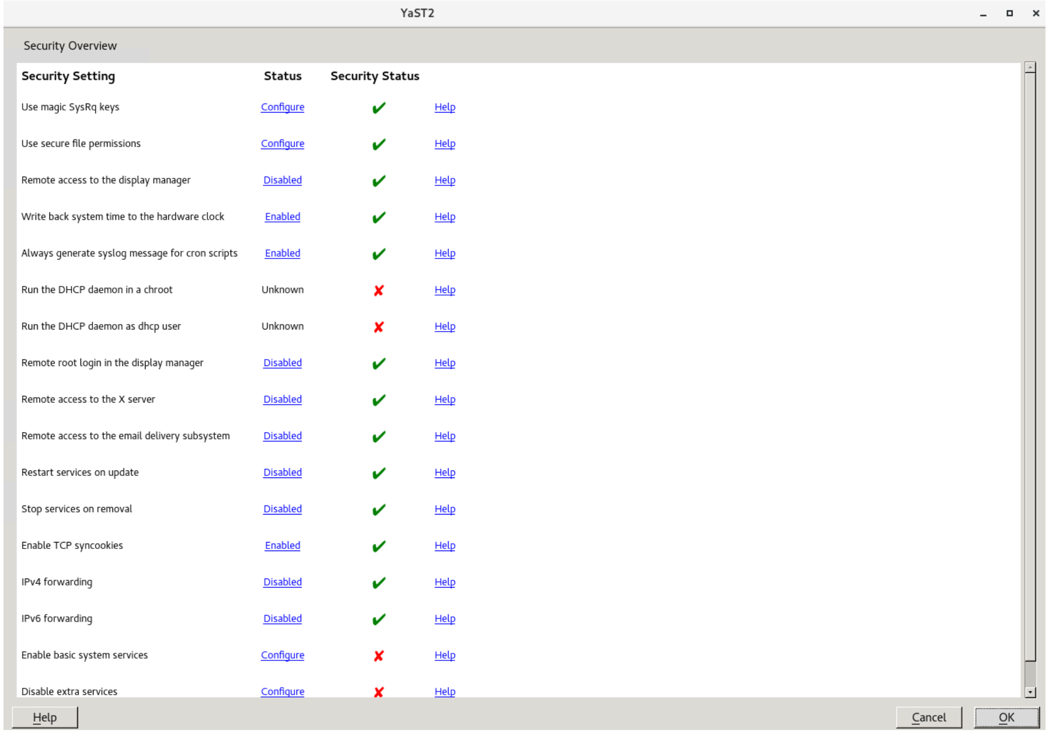


YaST2

Security Overview

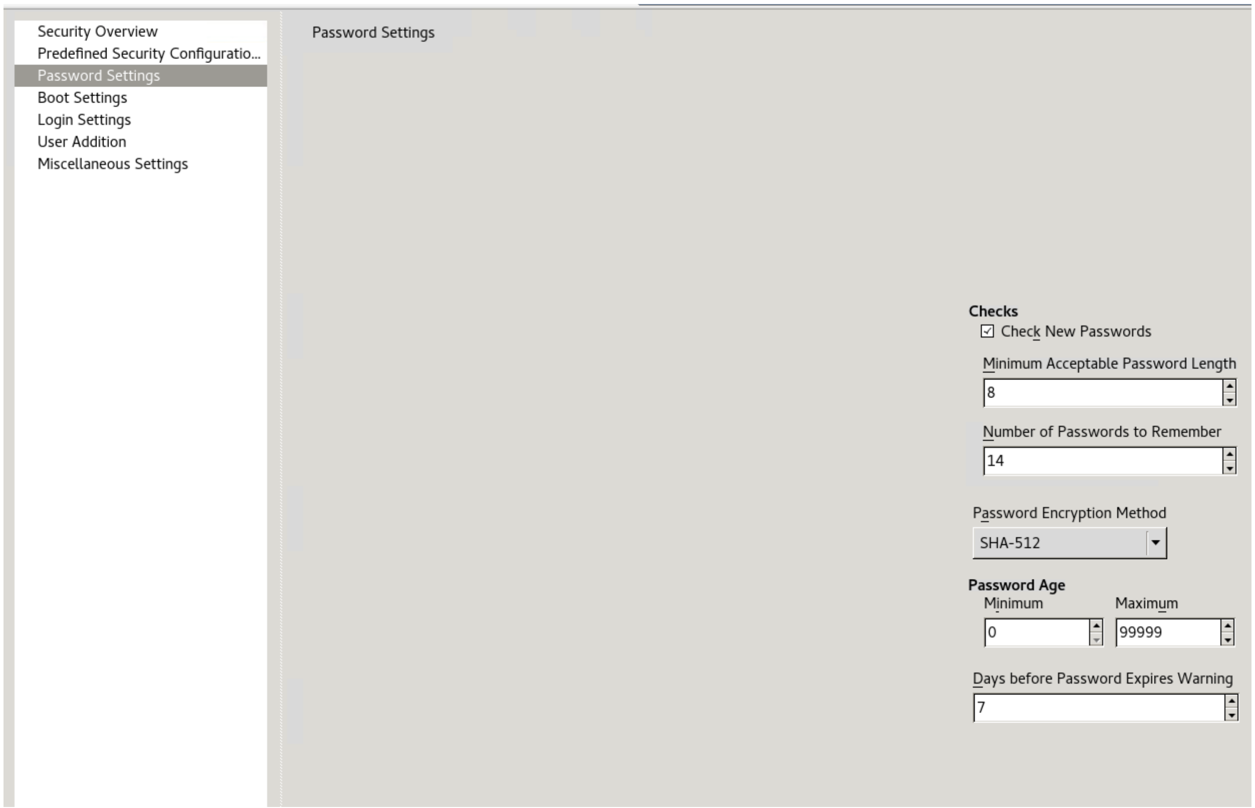
Security Setting	Status	Security Status	
Use magic SysRq keys	Configure	✓	Help
Use secure file permissions	Configure	✗	Help
Remote access to the display manager	Disabled	✓	Help
Write back system time to the hardware clock	Enabled	✓	Help
Always generate syslog message for cron scripts	Enabled	✓	Help
Run 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 syncookies	Enabled	✓	Help
IPv4 forwarding	Disabled	✓	Help
IPv6 forwarding	Disabled	✓	Help
Enable basic system services	Configure	✗	Help
Disable extra services	Configure	✗	Help

Network Configuration



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 syncookies	Enabled	✔	Help
IPv4 forwarding	Disabled	✔	Help
IPv6 forwarding	Disabled	✔	Help
Enable basic system services	Configure	✘	Help
Disable extra services	Configure	✘	Help

You can 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.



Password Settings

Checks

☑ Check New Passwords

Minimum Acceptable Password Length: 8

Number of Passwords to Remember: 14

Password Encryption Method: SHA-512

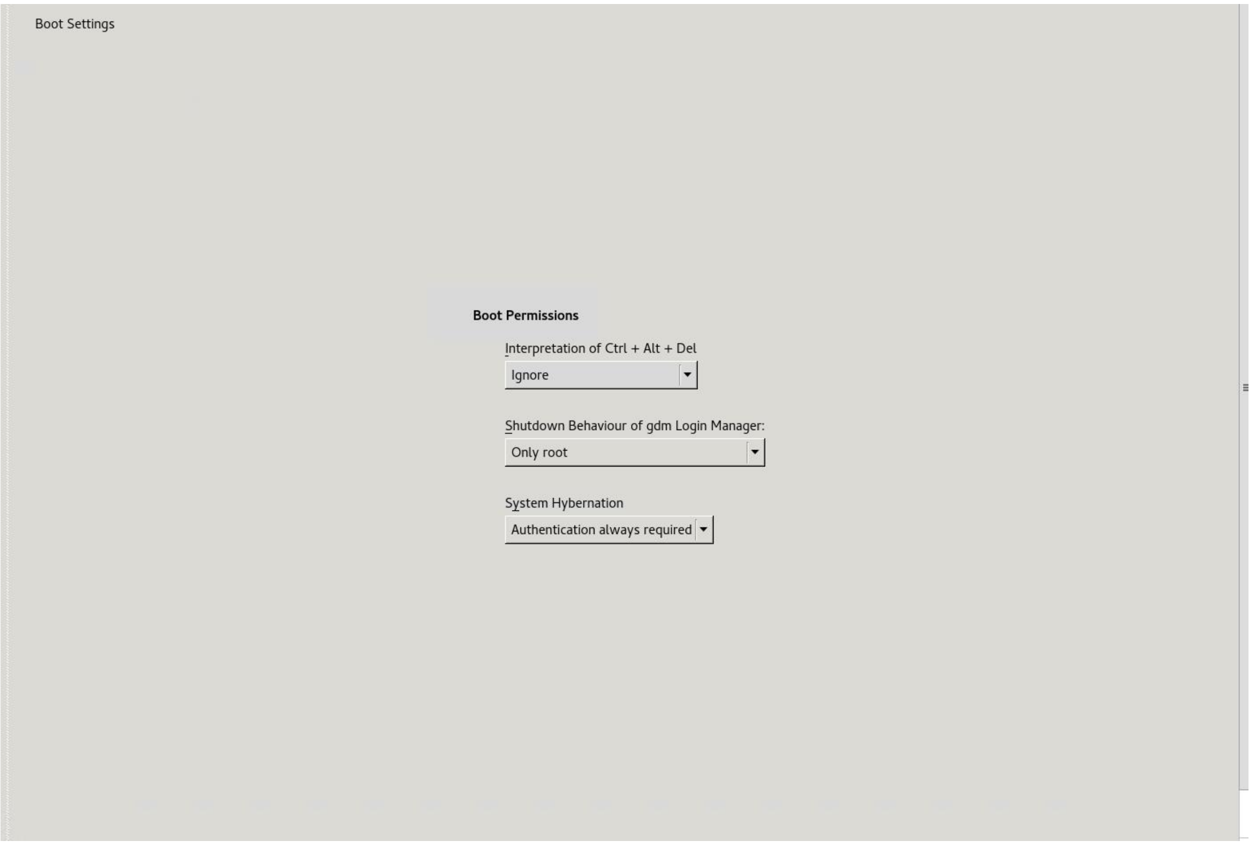
Password Age

Minimum: 0

Maximum: 99999

Days before Password Expires Warning: 7

In the security center and hardening, it allows for the capability to set boot permissions. The administrator is able to set what the system will do when Ctrl + Alt + Delete are executed. You can restrict shutdown to root only and set the system to require authentication to be able to hibernate the NVR.



Boot Settings

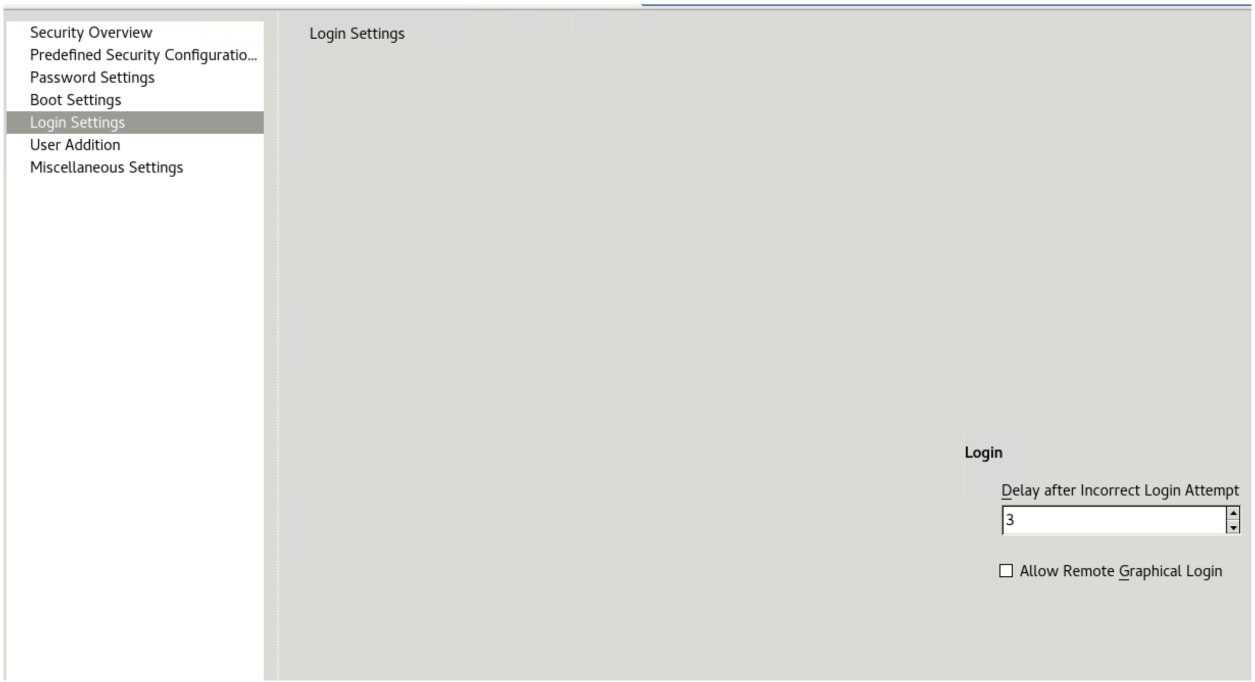
Boot Permissions

Interpretation of Ctrl + Alt + Del: Ignore

Shutdown Behaviour of gdm Login Manager: Only root

System Hybernation: Authentication always required

In login settings there is the capability to set the delay after incorrect login attempts, which help prevent brute force attacks.



Login Settings

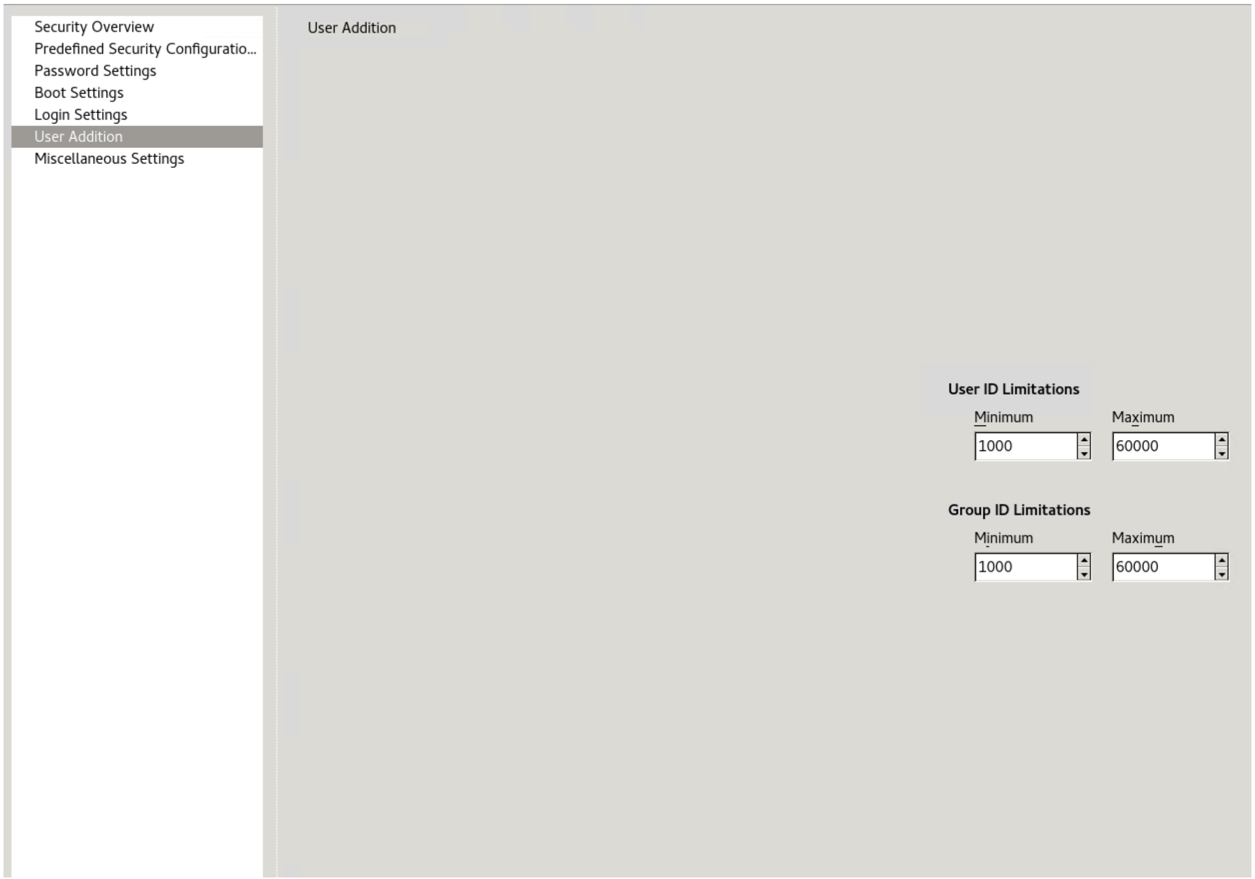
Login

Delay after Incorrect Login Attempt: 3

☐ Allow Remote Graphical Login

In User addition the administrator can set the user id and group id minimum and maximum limitations.

User and group identification in the context of both Linux and Window machines determine the amount of access control that a user or group can have. It will restrict which system resources a user can access in relation to operating system processes. These values should not be addressed unless the administrator is fully aware of impact to access control within a Linux environment.



User ID Limitations

Minimum 1000

Maximum 60000

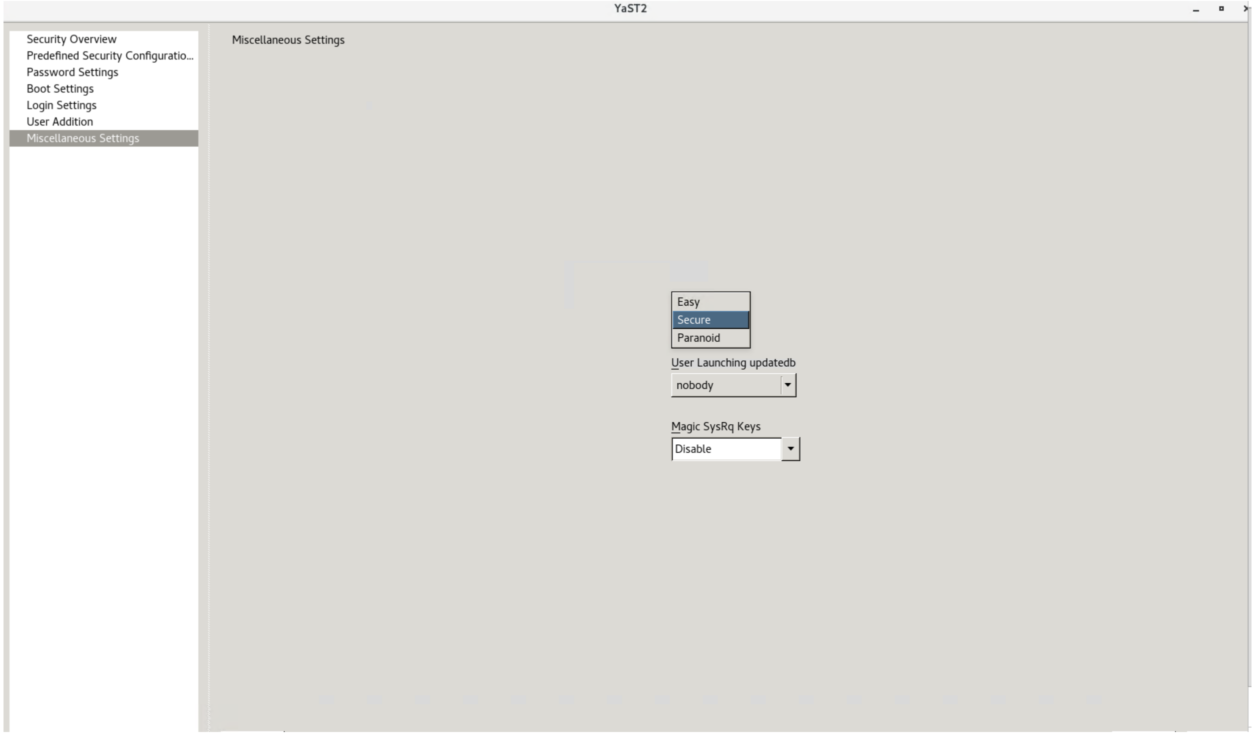
Group ID Limitations

Minimum 1000

Maximum 60000

The last configuration in security center and hardening is miscellaneous settings. The administrator can set file permissions, to easy, secure or paranoid. The administrator can configure who can launch updated either nobody or root. The administrator can disable Magic SysRq Keys.

Magic SysRq Key allows the user to perform various low-level commands regardless of the systems state, it is generally used to recover from freezes or to reboot a computer without corrupting the filesystem



Miscellaneous Settings

User Launching updatedb: nobody

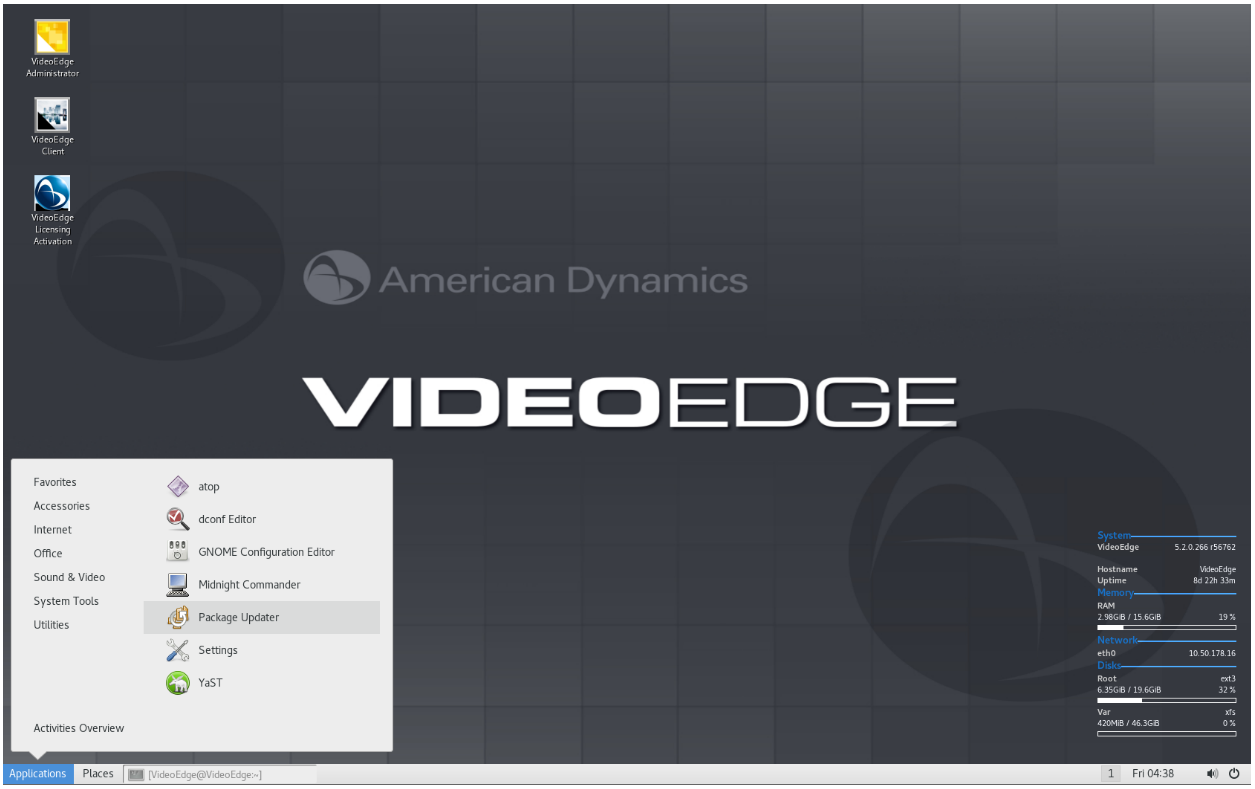
Magic SysRq Keys: Disable

Operating System Patch Updater

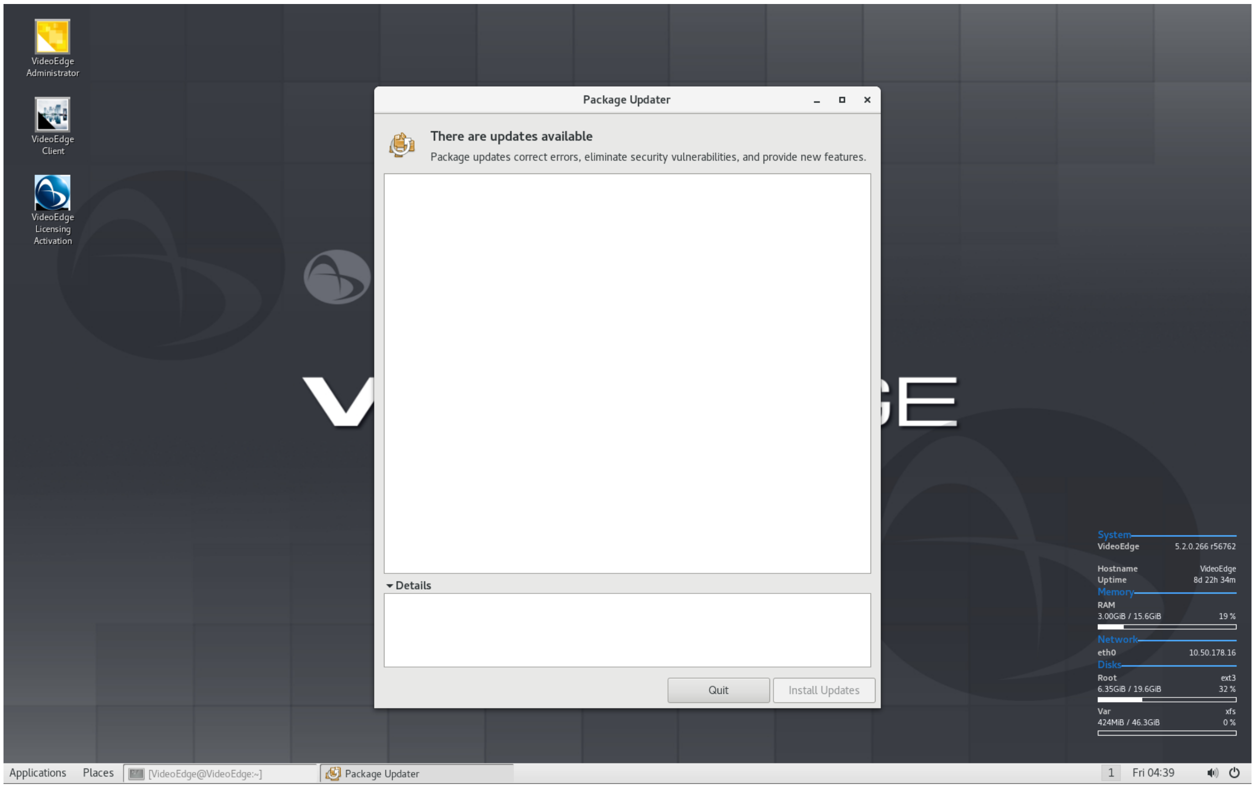
The end user has the ability to apply security patches. Applying security patches assists in mitigating known vulnerabilities.

Security patches are sourced directly from openSUSE.

Under applications, locate Package Updater



```
System
VideoEdge          5.2.0.266 r56762

Hostname                  VideoEdge
Uptime                  8d 22h 33m
Memory
RAM
2.98GiB / 15.6GiB              19 %
Network
eth0                   10.50.178.16
Disks
Root                           ext3
6.35GiB / 19.6GiB              32 %
Var                             xfs
420MiB / 46.3GiB                0 %
```



Package Updater

There are updates available

Package updates correct errors, eliminate security vulnerabilities, and provide new features.

Details

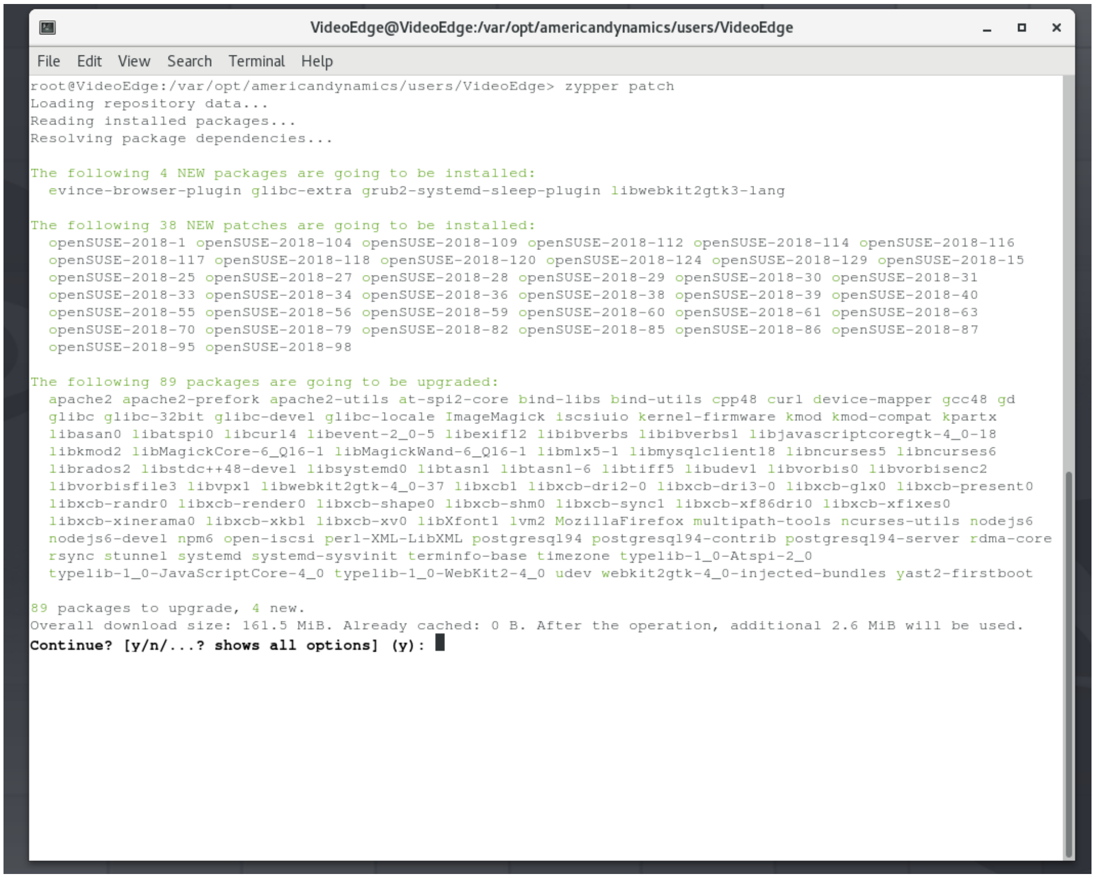
```
System
VideoEdge          5.2.0.266 r56762

Hostname                  VideoEdge
Uptime                  8d 22h 34m
Memory
RAM
3.00GiB / 15.6GiB              19 %
Network
eth0                   10.50.178.16
Disks
Root                           ext3
6.35GiB / 19.6GiB              32 %
Var                             xfs
424MiB / 46.3GiB                0 %
```

Further information can be located on the openSUSE documentation site:

https://doc.opensuse.org/documentation/leap/startup/html/book.opensuse.startup/cha.onlineupdate.you.html

Alternatively patches can be identified and applied through a terminal window.

Open a terminal window and type “zypper patch”. This must be run at root level


VideoEdge@VideoEdge:/var/opt/americandynamics/users/VideoEdge
File Edit View Search Terminal Help

```
root@VideoEdge:/var/opt/americandynamics/users/VideoEdge> zypper patch
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following 4 NEW packages are going to be installed:
  evince-browser-plugin glibc-extra grub2-systemd-sleep-plugin libwebkit2gtk3-lang

The following 38 NEW patches are going to be installed:
  openSUSE-2018-1 openSUSE-2018-104 openSUSE-2018-109 openSUSE-2018-112 openSUSE-2018-114 openSUSE-2018-116
  openSUSE-2018-117 openSUSE-2018-118 openSUSE-2018-120 openSUSE-2018-124 openSUSE-2018-129 openSUSE-2018-15
  openSUSE-2018-25 openSUSE-2018-27 openSUSE-2018-28 openSUSE-2018-29 openSUSE-2018-30 openSUSE-2018-31
  openSUSE-2018-33 openSUSE-2018-34 openSUSE-2018-36 openSUSE-2018-38 openSUSE-2018-39 openSUSE-2018-40
  openSUSE-2018-55 openSUSE-2018-56 openSUSE-2018-59 openSUSE-2018-60 openSUSE-2018-61 openSUSE-2018-63
  openSUSE-2018-70 openSUSE-2018-79 openSUSE-2018-82 openSUSE-2018-85 openSUSE-2018-86 openSUSE-2018-87
  openSUSE-2018-95 openSUSE-2018-98

The following 89 packages are going to be upgraded:
  apache2 apache2-prefork apache2-utils at-spi2-core bind-libs bind-utils cpp48 curl device-mapper gcc48 gd
  glibc glibc-32bit glibc-devel glibc-locale ImageMagick iscsiuio kernel-firmware kmod kmod-compat kpartx
  libasan0 libatspi0 libcurl4 libevent-2_0-5 libexif12 libibverbs libibverbs1 libjavascriptcoregtk-4_0-18
  libkmod2 libMagickCore-6_Q16-1 libMagickWand-6_Q16-1 libmlx5-1 libmysqlclient18 libncurses5 libncurses6
  librados2 libstdc++48-devel libsystemd0 libtasn1 libtasn1-6 libtiff5 libudev1 libvorbis0 libvorbisenc2
  libvorbisfile3 libvpx1 libwebkit2gtk-4_0-37 libxcb1 libxcb-dri2-0 libxcb-dri3-0 libxcb-glx0 libxcb-present0
  libxcb-randr0 libxcb-render0 libxcb-shape0 libxcb-shm0 libxcb-sync1 libxcb-xf86dri0 libxcb-xfixes0
  libxcb-xinerama0 libxcb-xkb1 libxcb-xv0 libXfont1 lvm2 MozillaFirefox multipath-tools ncurses-utils nodejs6
  nodejs6-devel npm6 open-iscsi perl-XML-LibXML postgresql94 postgresql94-contrib postgresql94-server rdma-core
  rsync stunnel systemd systemd-sysvinit terminfo-base timezone typelib-1_0-Atspi-2_0
  typelib-1_0-JavaScriptCore-4_0 typelib-1_0-WebKit2-4_0 udev webkit2gtk-4_0-injected-bundles yast2-firstboot

89 packages to upgrade, 4 new.
Overall download size: 161.5 MiB. Already cached: 0 B. After the operation, additional 2.6 MiB will be used.
Continue? [y/n/...? shows all options] (y):
```

With the adoption of openSUSE the end user has the ability to apply patches. With this ability consideration needs to be taken as to when to apply.

Patches should be applied at a regular cadence with special attention brought on highly visible vulnerabilities.

The cyber protection issuance of advisories indicating systems should be patched shall be adhered to for maintaining a strong security posture.

Prior to any release of security patches the system should be tested in a sandbox to ensure the system maintains normal operation.

For details on how to create a regular patch schedule, refer to the documentation provided by SUSE.

https://doc.opensuse.org/documentation/leap/reference/html/book.opensuse.reference/cha.sw_cl.html

https://www.suse.com/documentation/suse-best-practices/susemanager/data/susemanager.html

BIOS Password

A BIOS password should be configured to ensure that a system configuration is maintained. By having a set bootup sequence this will disallow the ability to boot from a malicious USB device.

How to set a BIOS password:

1. Boot the machine
2. Within 10 seconds of startup press the F2 button on the keyboard
3. You will be entered into the BIOS screen
4. Note that each hardware platform may have a slight deviation.
5. Enter into Advanced mode
6. Locate the Security tab
7. Set a new Administrator password and a user password.
8. The user password will be prompted when the machine is started.
9. The administrator password will be required when any BIOS changes are made

Machine Physical Port Restriction

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

How to disable USB ports:

1. Boot the machine
2. Within 10 seconds of startup press the F2 button on the keyboard
3. You will be entered into the BIOS screen
4. Note that each hardware platform may have a slight deviation.
5. Enter into Advanced mode
6. Under Advanced tab locate USB Configuration
7. Click on USB Single Port Control
8. Notice all the USB ports are listed as “Enabled”
9. Change all the ports that are not required to “Disabled”
10. Save and restart the machine.
11. Please 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.

VideoEdge Firewall

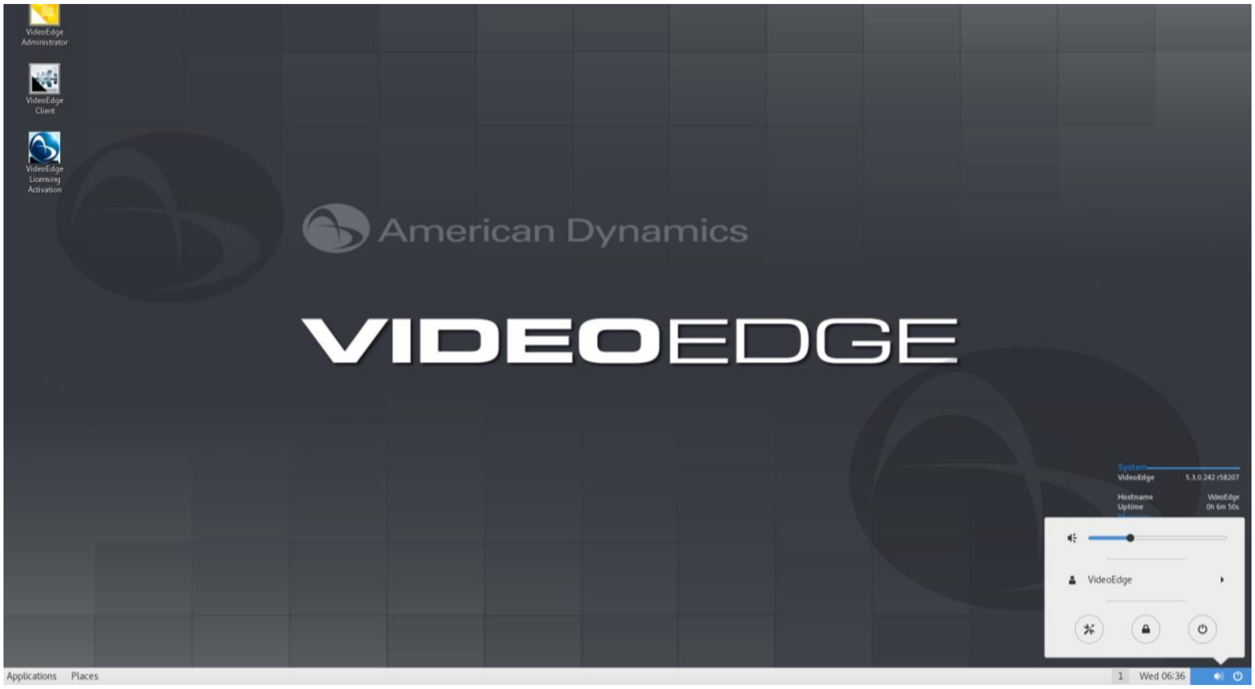
A firewall is an important feature that should be utilized. A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. By having a predefined set of rules it can disallow malicious activity from intruding into the system.

How to enable the VideoEdge firewall:

Connect to the local desktop.

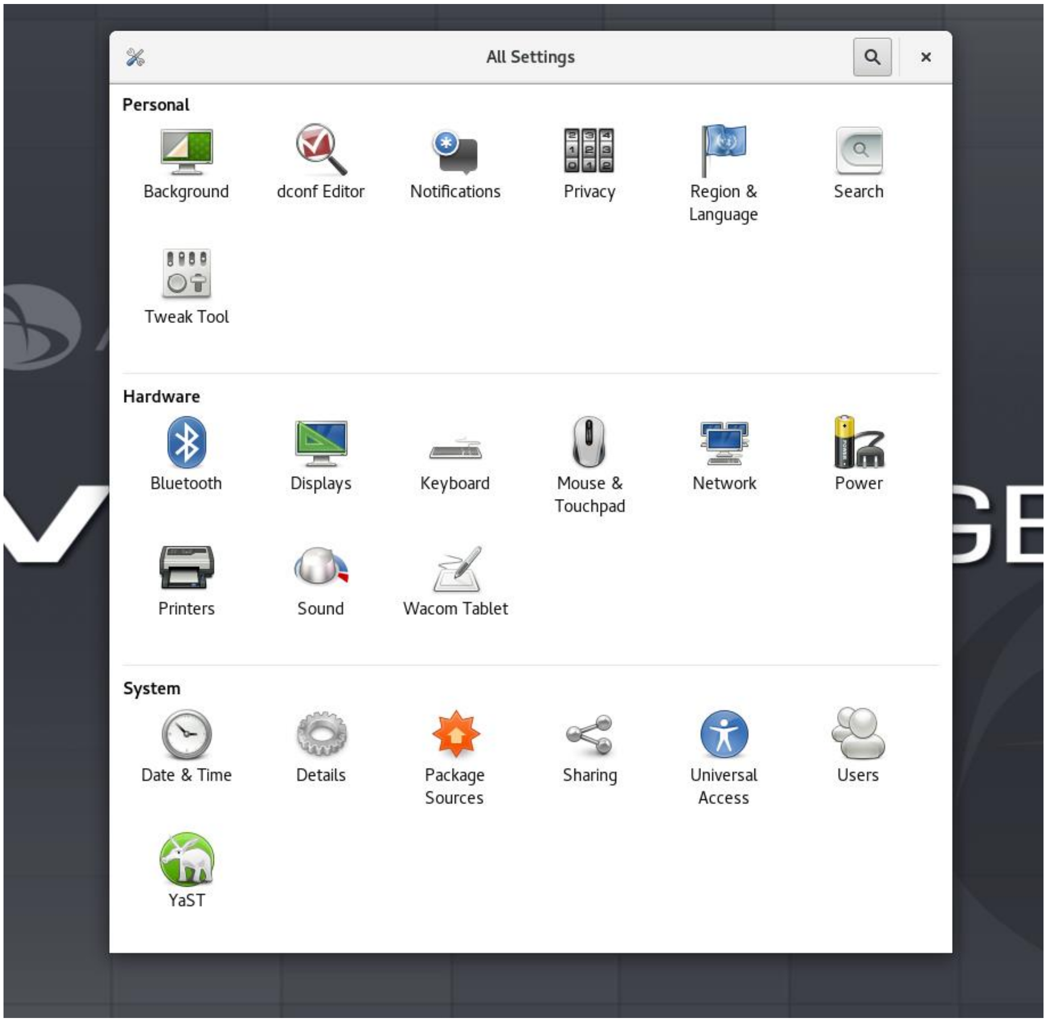
Press the power button to bring up the menu located below.

Click on the Settings button (screwdriver and wrench)

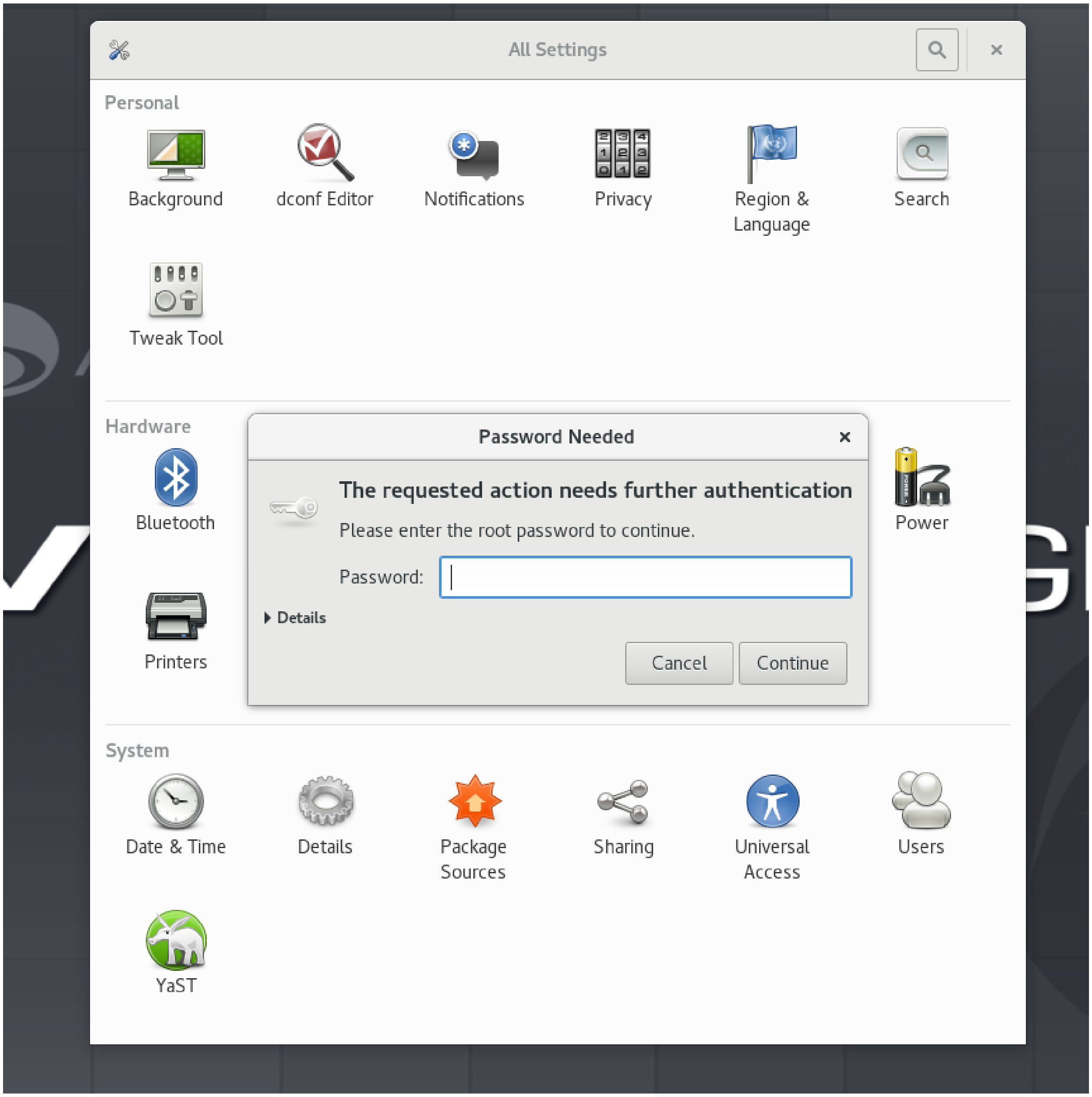


You will be presented with the Settings screen.

Click on the YaST button



You will have to enter the root user password.

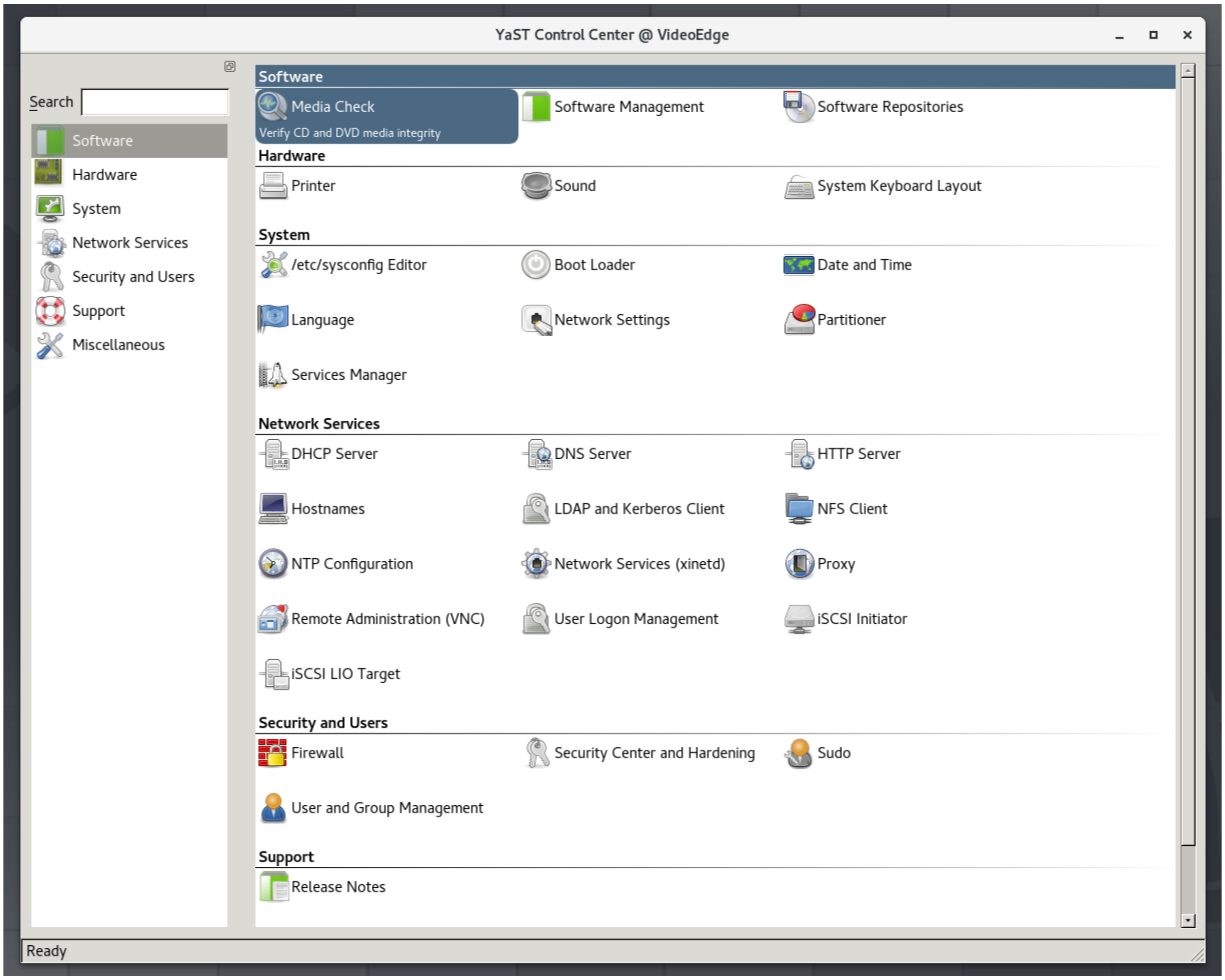


The requested action needs further authentication

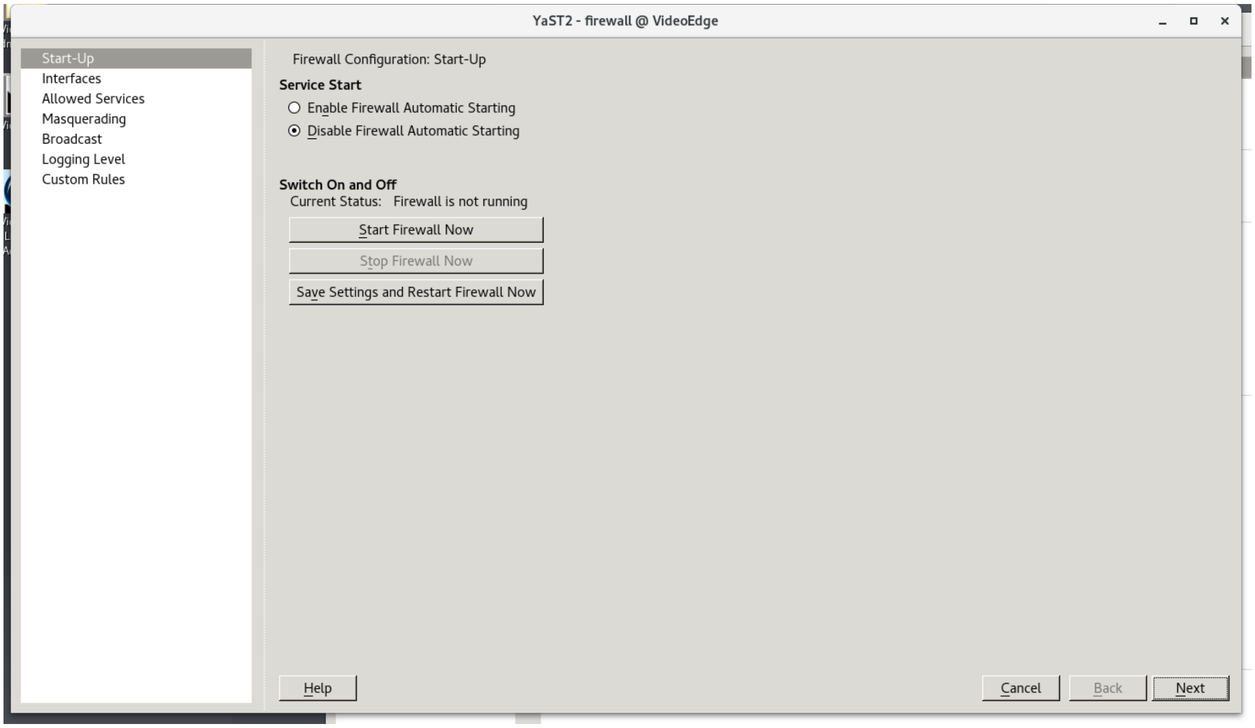
Please enter the root password to continue.

Now you will be presented with the YaST Control Center.

Locate and press the Firewall button.



This is the location to enable or disable the firewall.



YaST2 - firewall @ VideoEdge

Firewall Configuration: Start-Up

Service Start

○ Enable Firewall Automatic Starting

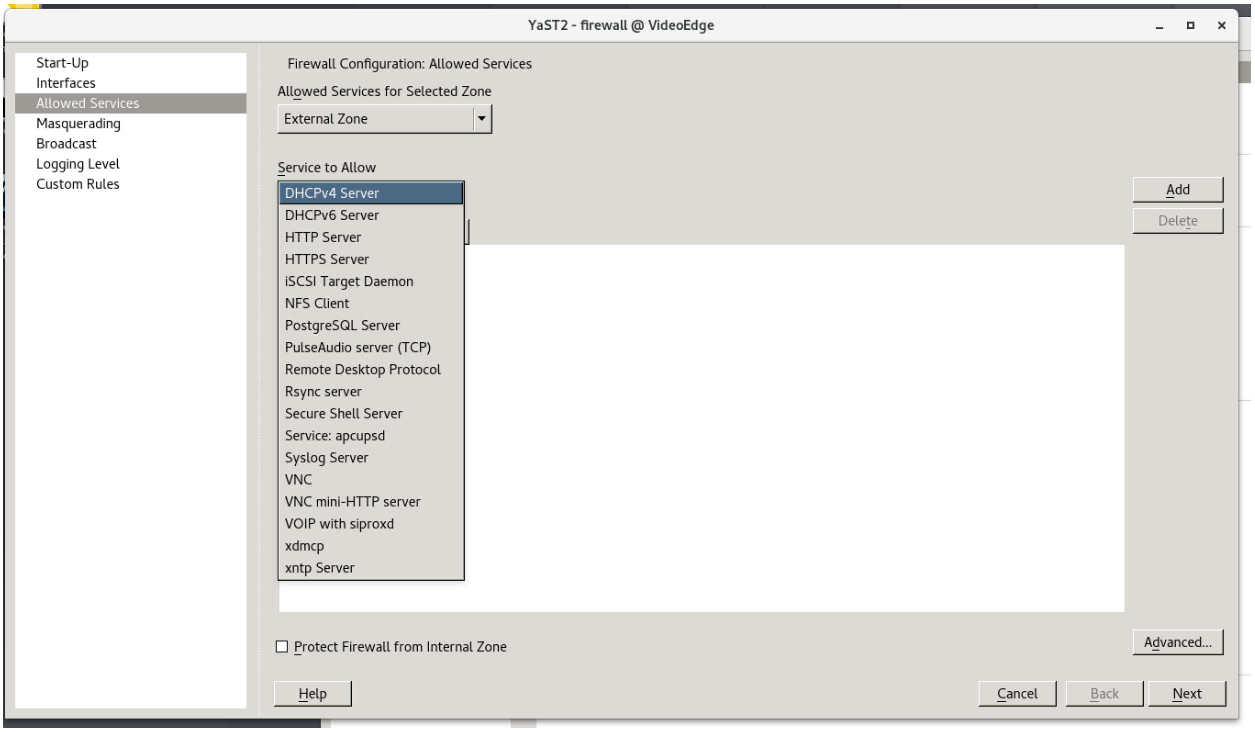
● Disable Firewall Automatic Starting

Switch On and Off

Current Status: Firewall is not running

On the side bar click on Allowed Services

Default services are allowed to be added for External/Internal/DMZ Zones.



YaST2 - firewall @ VideoEdge

Firewall Configuration: Allowed Services

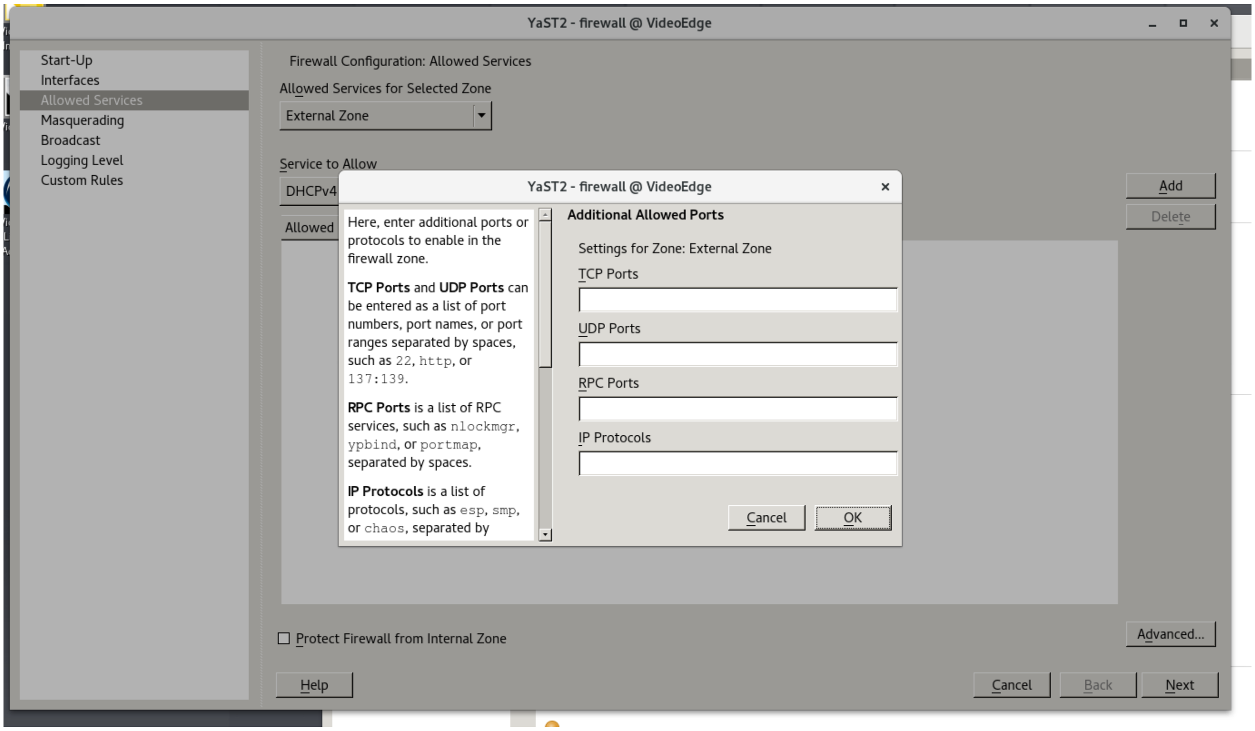
Allowed Services for Selected Zone: External Zone

Service to Allow: DHCPv4 Server

□ Protect Firewall from Internal Zone

By clicking the Advanced button in the lower right hand corner specific ports that do not show up in the default list may be added manually.

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



Allowed Services for Selected Zone: External Zone

☐ Protect Firewall from Internal Zone

Settings for Zone: External Zone

Here, enter additional ports or protocols to enable in the firewall zone.

TCP Ports and **UDP Ports** can be entered as a list of port numbers, port names, or port ranges separated by spaces, such as `22`, `http`, or `137:139`.

RPC Ports is a list of RPC services, such as `nlockmgr`, `ypbind`, or `portmap`, separated by spaces.

IP Protocols is a list of protocols, such as `esp`, `smp`, or `chaos`, separated by

Cameras

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.

This protection was validate through third party penetration testing (see ANNEX F).

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.

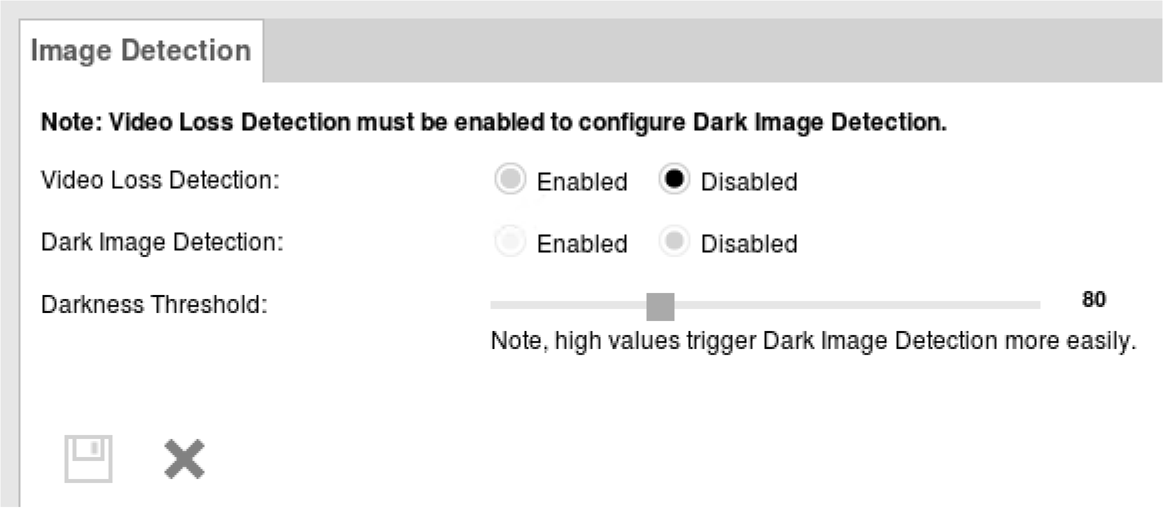


Image Detection

Note: Video Loss Detection must be enabled to configure Dark Image Detection.

Video Loss Detection: ○ Enabled ● Disabled

Dark Image Detection: ○ Enabled ○ Disabled

Darkness Threshold: 80

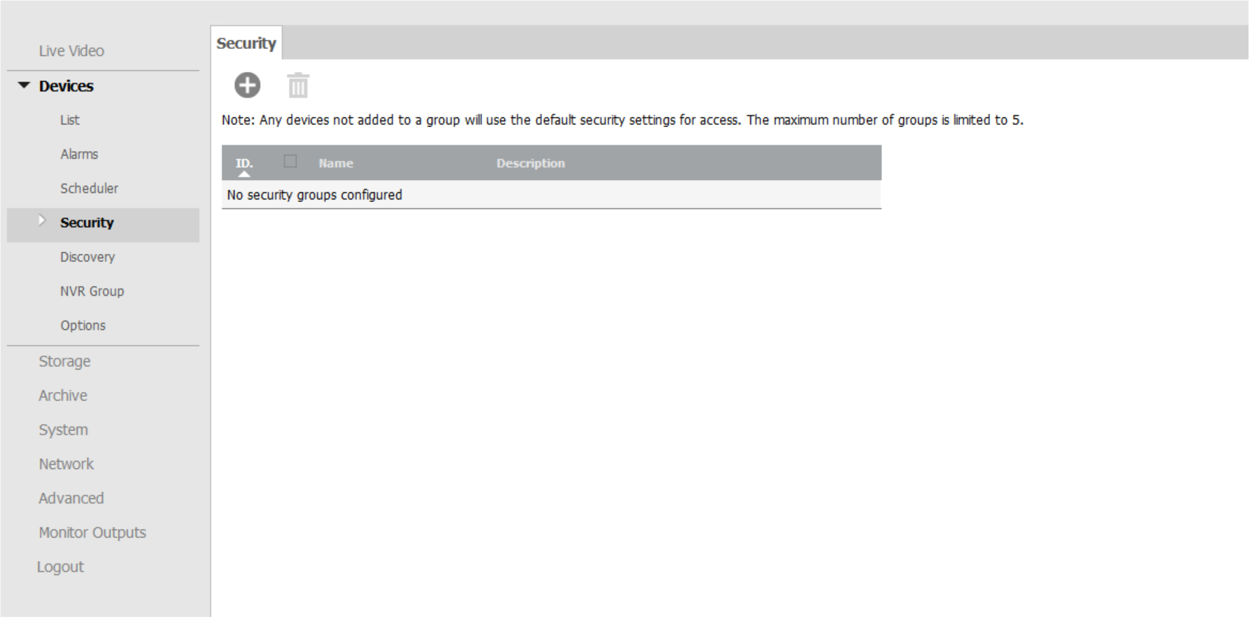
Note, high values trigger Dark Image Detection more easily.

Camera Security Groups

When an IP camera is added to a NVR, the server uses the manufacturer's default communication and security settings to communicate with the camera. Administrators can change the default settings. However, when these are changed the NVR can no longer communicate with the camera using the default settings. If you change the security settings for a camera or a number of cameras, usually through web interfaces, you need to create a Security Group for those cameras and assign it the same password. 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.

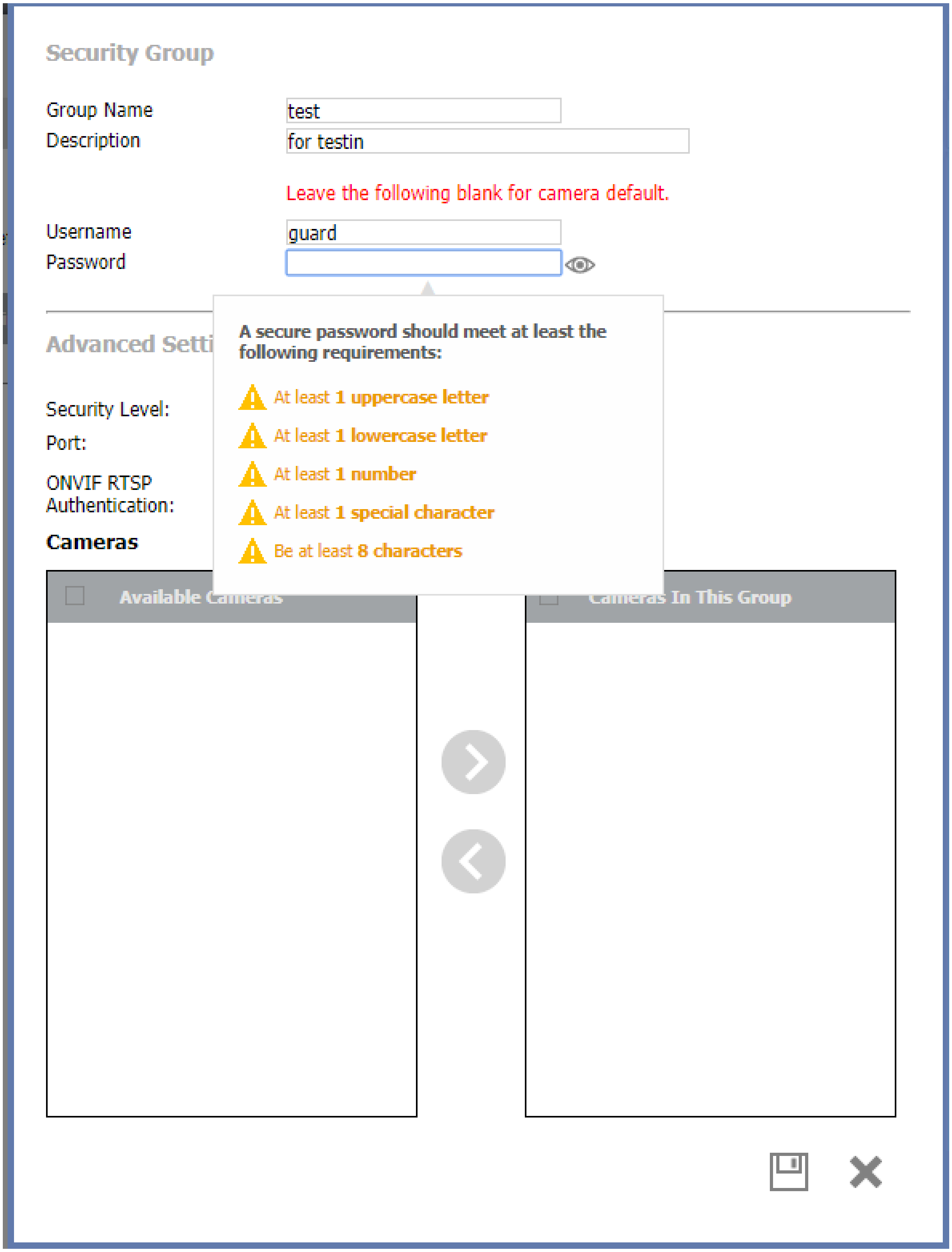
The security group is also used to configure if the communication is performed via HTTP or HTTPS.

The Security Group will be set to default. VideoEdge will use the manufacturer's default password to connect to the camera. However, if you have changed the password for this camera, you need to assign the camera to the appropriate password group, or create a new password group.



Note: Any devices not added to a group will use the default security settings for access. The maximum number of groups is limited to 5.

ID.	□	Name	Description
No security groups configured			



Security Group

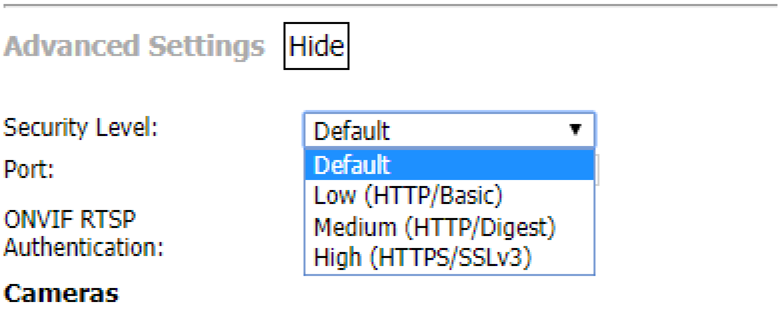
Group Name	test
Description	for testin

Leave the following blank for camera default.

Username	guard
Password	

A secure password should meet at least the following requirements:

- ⚠ At least 1 uppercase letter
- ⚠ At least 1 lowercase letter
- ⚠ At least 1 number
- ⚠ At least 1 special character
- ⚠ Be at least 8 characters



Advanced Settings Hide

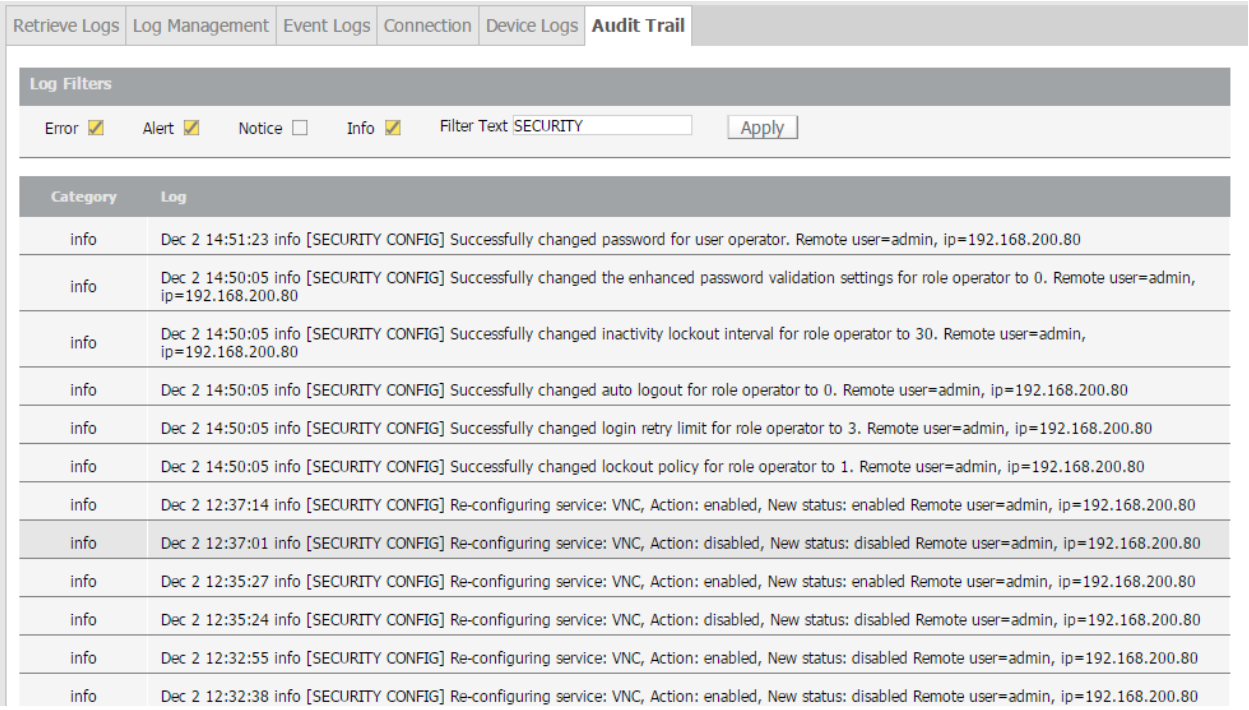
Security Level: Default

Auditing and Alerts

Enhanced Security Logging, Audit Trail, and Email Alerts

Logs track general system operation and are useful for troubleshooting and incident investigation. The VideoEdge NVR generates a number of different log files to track areas such as general system operation, web server operation, web server errors, and Network time Protocol (NTP) operation. These logs are useful in monitoring the general operation of the Linux system. The VideoEdge system also generates a number of application-specific log files to aid in diagnosing areas such as camera communication and video playback events. Log backup for VideoEdge to an external server is supported via FTP.

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. This allows audit events to be queried by severity and searched using a text filter.



Log Filters

Error ☑ Alert ☑ Notice ☐ Info ☑ Filter Text SECURITY

Category	Log
info	Dec 2 14:51:23 info [SECURITY CONFIG] Successfully changed password for user operator. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed the enhanced password validation settings for role operator to 0. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed inactivity lockout interval for role operator to 30. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed auto logout for role operator to 0. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed login retry limit for role operator to 3. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed lockout policy for role operator to 1. Remote user=admin, ip=192.168.200.80
info	Dec 2 12:37:14 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: enabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:37:01 info [SECURITY CONFIG] Re-configuring service: VNC, Action: disabled, New status: disabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:35:27 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: enabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:35:24 info [SECURITY CONFIG] Re-configuring service: VNC, Action: disabled, New status: disabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:32:55 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: disabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:32:38 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: disabled Remote user=admin, ip=192.168.200.80

Alerts

Alerts can be generated via email under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using TLS. These alerts can be configured to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

For a full lists of available alerts, see ANNEX D

Vulnerability Management and Updates

The policy documented here sets forth the current internal operating guidelines and process for American Dynamics in regards to the VideoEdge NVR, which may change from time to time at the sole discretion of American Dynamics. American Dynamics 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 American Dynamics at its discretion. Regardless, American Dynamics endeavors to address issues that arise within the VideoEdge NVR with the severity that they warrant.

Patch Policy

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 the VideoEdge NVR 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 a VideoEdge NVR release within this timeframe.

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

Vulnerability Assessment – VideoEdge NVR

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

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

Vulnerability Assessment – Third Party Software

American Dynamics shall 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.

Reporting a Vulnerability

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@tycoint.com** or via 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.

Certifications

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

UL 2900-2-3 (Level 3) – VideoEdge was certified March22, 2018 by Underwriter Laboratories (UL), Cybersecurity Assurance Program (CAP) as compliant with UL 2900-2-3. This cybersecurity standard is specific to life safety and physical security. The level 3 assessment that was conducted by UL evaluated the business practices of Johnson Controls as well as the security capabilities of the product with knowledge of internal security controls.

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.

Security Approvals

The VideoEdge NVR has been installed in many installations that require accreditation. Below are overview of accreditations and resources that may be used to assist in meeting the requirements of each.

FISMA

The VideoEdge system can be configured to support the controls necessary for overall FISMA compliance. These controls include:

- Authenticated system access
- Account login/logout 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, see 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, see 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) as well as a description of how a VideoEdge device meets the technical controls or if it is does not meet the controls, guidance has been provided so the customer can configure VideoEdge to meet the requirements.

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

Penetration Testing

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.

Customer Specific Testing

If a customer requires specific testing (e.g. 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@tycoint.com

Product Security Testing

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.

Table: Product Security Testing[1]

Development Cycle	
Test	**Tool**
Vulnerability scanning	Nexpose, Nessus
Web application scanning	Rapid7 AppSpider, BurpSuite professional, OWASP ZAP
Static code analysis – proprietary source code	SonarQube, HP Fortify
Static code analysis – open source code	Comparison against National Vulnerability Database (NVD), BlackDuck knowledge database

Release Cycle		
Test	**Tool / Method**	**Frequency**
Vulnerability scanning	Nexpose, Nessus	Weekly
Web application scanning	Rapid7 AppSpider, BurpSuite professional, OWASP ZAP	Monthly
Static code analysis – open source code	Comparison against National Vulnerability Database (NVD), BlackDuck knowledge database	Continuous

[1] A regular testing schedule for VideoEdge will apply during the actively supported period of the product’s lifecycle. The frequency, tools and methods used are subject to change to accommodate the current best practices for cybersecurity, market conditions and tools available for a given period.

VideoEdge Hardening Steps

As seen in this document, there are several options and features available to secure the VideoEdge NVR. Many of these must be customized to meet the needs and requirements of each organization. However, the following items are recommended to achieve a more secure version of the VideoEdge NVR.

- Enable RTSP encryption over TLS
    - Transmit RTSP command and control traffic over a secure, encrypted TLS tunnel.
    - Change TLS port from default 443
- Disable SSH, RDP
    - Disables remote connection to the VideoEdge
- Change all default passwords
    - Initial password change is mostly used to prevent the "default password" problem.
- Implement Camera Security groups.
    - When an IP camera is added to a NVR, the server uses the manufacturer’s default communication and security settings to communicate with the camera.
- Disable UPnP

  UPnP is a security risk. It allows applications with network access on computers to create publicly accessible service on your network.
- Enable enhanced password validation
    - Force users to comply with enhanced password requirements.
    - Enable a strong password history requirement to prevent reuse.
- Enable lockout policy

    - Protects against brute force password attacks, account will lockout after too many failed attempts.
- Enable auto logout
    - This will log out a session if it is idle longer than a specified time.
- Enable inactivity lockout interval (30,60,90 days)
    - Allows the system to automatically disable inactive users, which is a security best practice.
- Enable HTTPS only
    - Without HTTPS, any data passed is insecure.
- Configure security setting in Security Center and Hardening
    - This will allow you to lock down your operating system and provide a more secure platform.
- Use LDAP integrations when a site contains multiple units
    - Using an Active Directory integration allows for more control over the roles a user can have while that user goes from machine to machine
- Apply operating system issued patches on a regular occurrence
    - Leveraging the open distribution of security patches from openSUSE will keep the system continually up to date from known system vulnerabilities.

ANNEX A - Linux built-in accounts

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. *lp, mail, news, uucp, games, nobody, epmd, polkitd, rtkit*

User	Description
bin	a standard subdirectory of the root directory in Unix-like operating systems that contains the executable (i.e., ready to run) applications that must be available in order to attain minimal functionality for the purposes of booting (i.e., starting) and repairing a system.
daemon	Is used to run as a processes 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	Owns 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.
usbmux	This account is used for multiplexing connections over USB to an iOS device.

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.
dhcpd	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 (i.e. realtime 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
nvr	The NVR service account. Most services run as this (or wwwrun, which is synonymous).

ANNEX B - VideoEdge Port Assignments

For port assignments see victor and VideoEdge Port Assignments document.

ANNEX C - Encryption Ciphers

- The minimum supported encryption key strength in VideoEdge NVRs is 128 bits.
- Export ciphers are disabled by default.
- RC4 cipher is disabled by default.

Supported ciphers

ECDHE-RSA-AES256-GCM-SHA384

ECDHE-RSA-AES256-SHA384

DHE-RSA-AES256-GCM-SHA384

AES256-GCM-SHA384

AES256-SHA256

When enabled TLSv1.0

ECDHE-RSA-AES256-SHA

ANNEX D - Email Alerts

To setup email alerts, see *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.

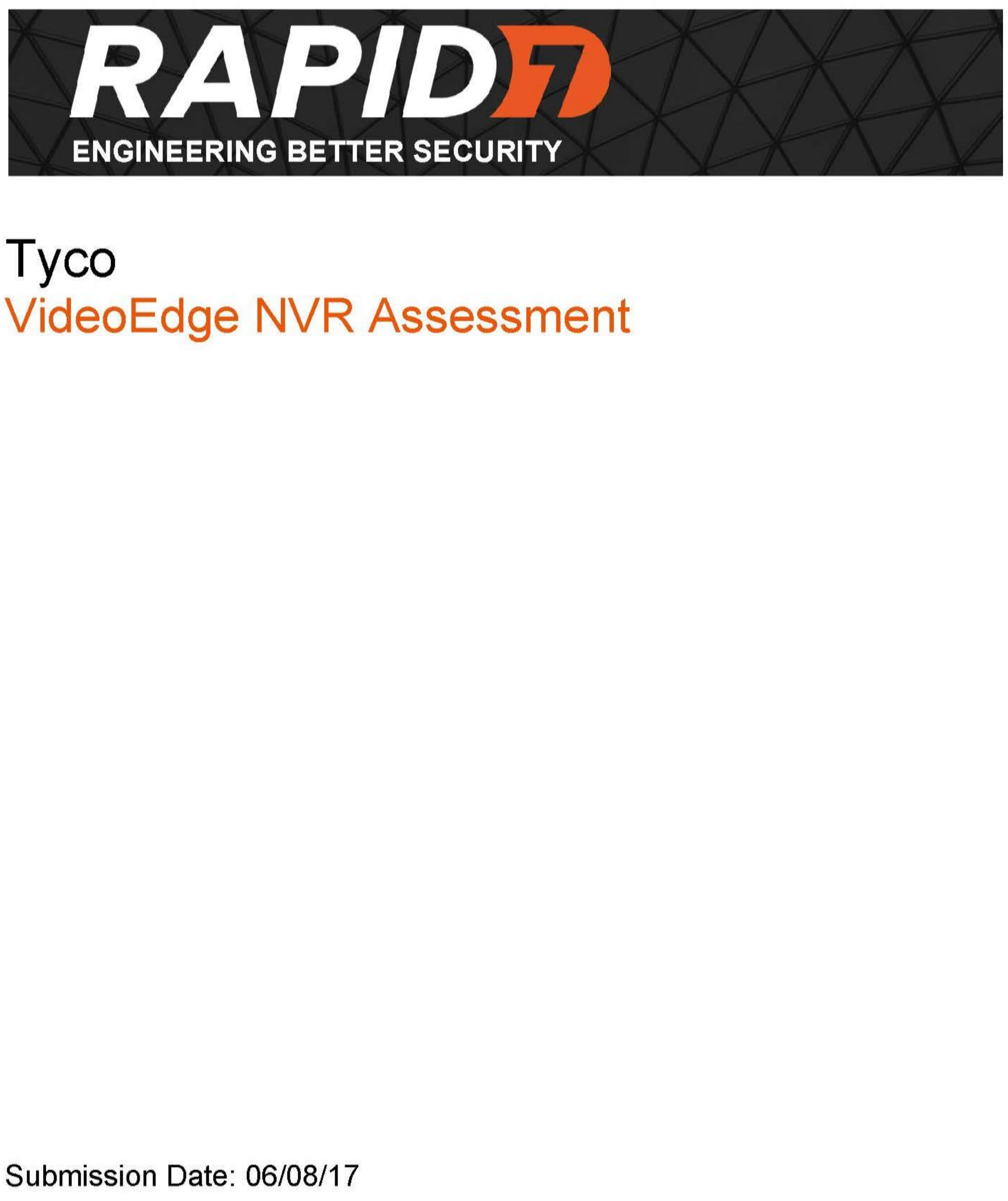
ANNEX E - Enabling Password Complexity for Linux Accounts

1. From the VideoEdge desktop, open a terminal.
2. Open a terminal by clicking on Applications at the bottom left cornerclick on Utilities in the terminal window type su – enter root password.
3. Run the following command:

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

Now going forward, the use of simple passwords will not be allowed. The system will only accept passwords which satisfy the above parameters.

ANNEX F – Third Party Penetration Testing Attestation



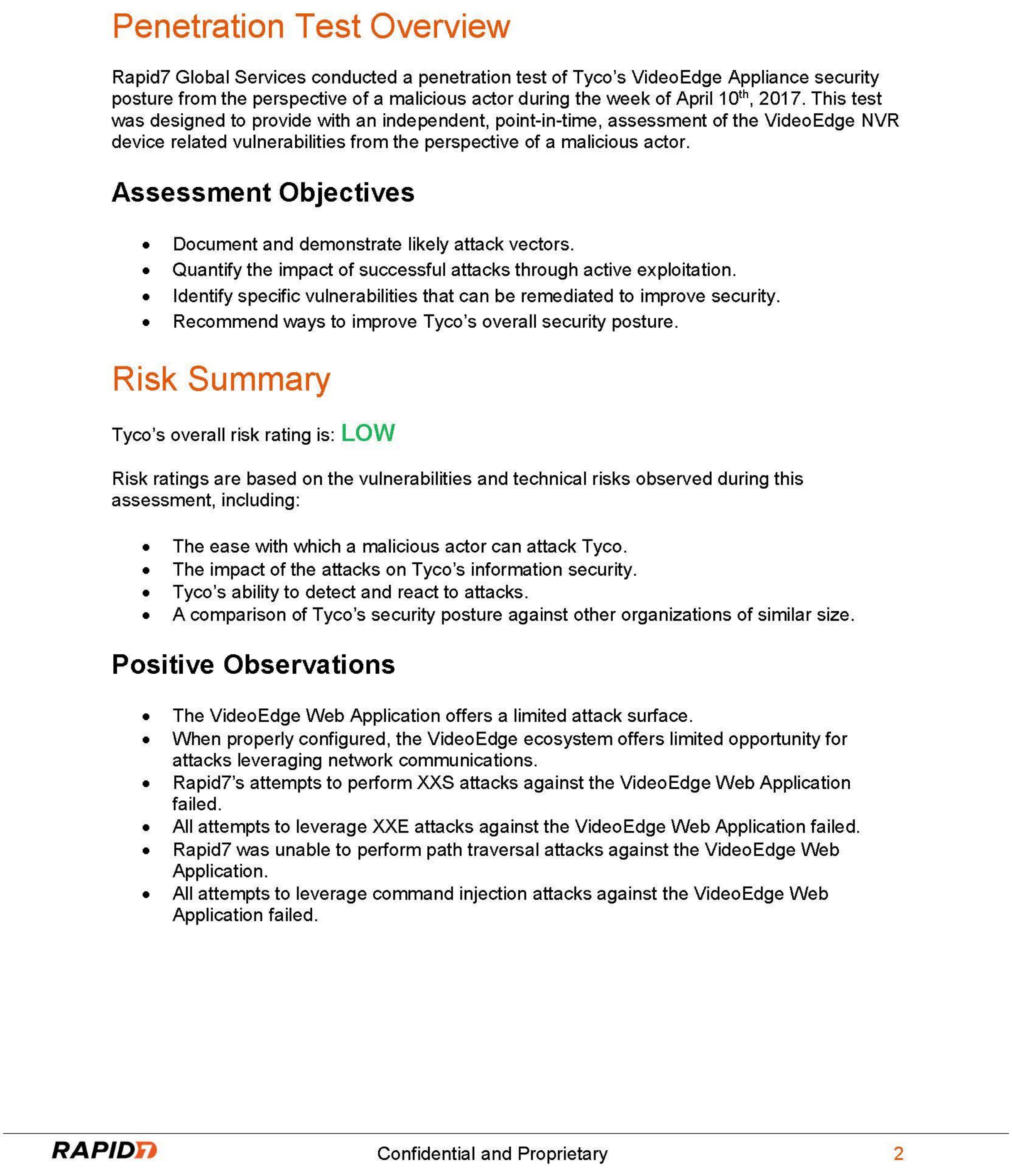
RAPID7

ENGINEERING BETTER SECURITY

Tyco

VideoEdge NVR Assessment

Submission Date: 06/08/17



Penetration Test Overview

Rapid7 Global Services conducted a penetration test of Tyco's VideoEdge Appliance security posture from the perspective of a malicious actor during the week of April 10th, 2017. This test was designed to provide with an independent, point-in-time, assessment of the VideoEdge NVR device related vulnerabilities from the perspective of a malicious actor.

Assessment Objectives

- Document and demonstrate likely attack vectors.
- Quantify the impact of successful attacks through active exploitation.
- Identify specific vulnerabilities that can be remediated to improve security.
- Recommend ways to improve Tyco's overall security posture.

Risk Summary

Tyco's overall risk rating is: LOW

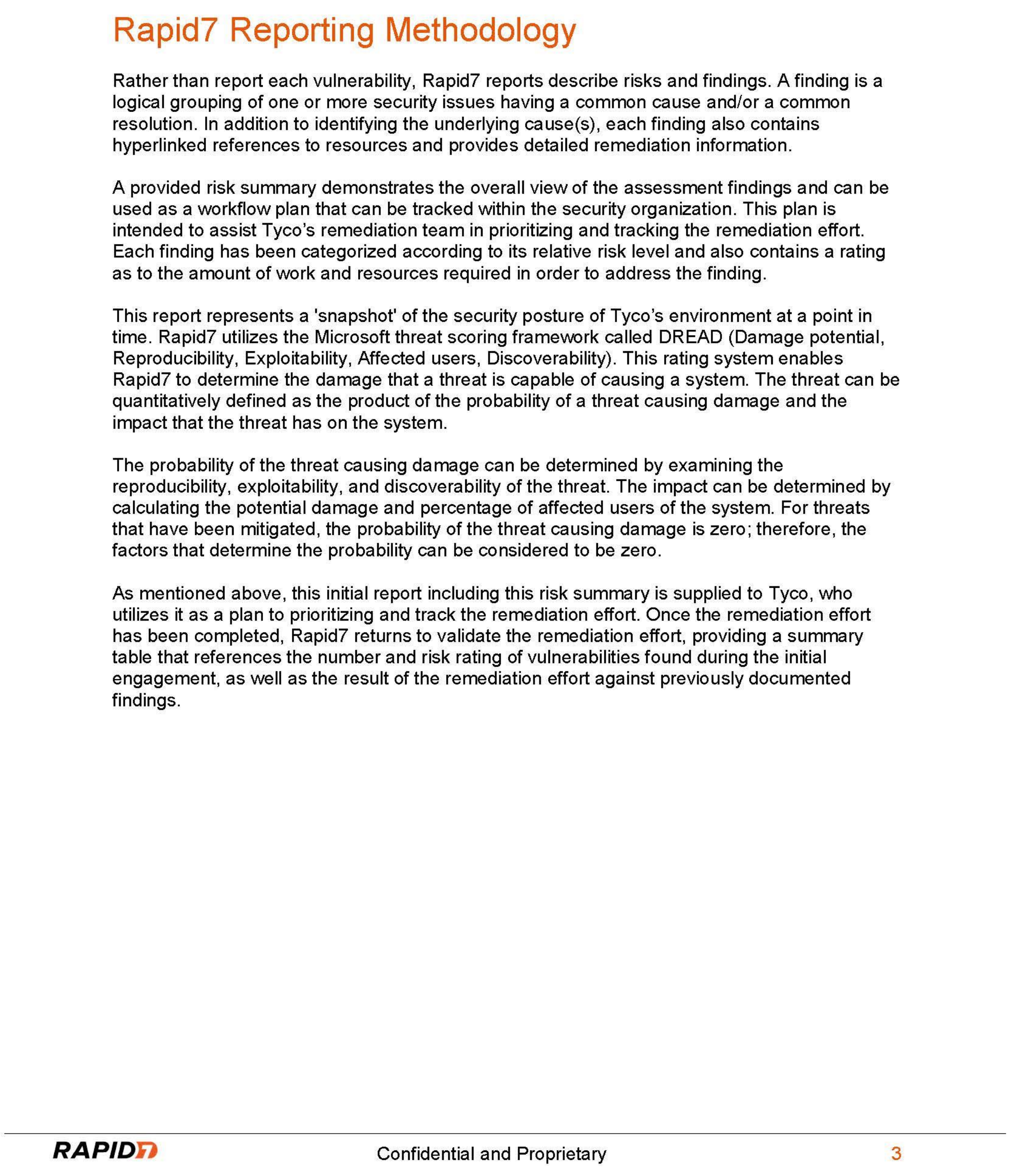
Risk ratings are based on the vulnerabilities and technical risks observed during this assessment, including:

- The ease with which a malicious actor can attack Tyco.
- The impact of the attacks on Tyco's information security.
- Tyco's ability to detect and react to attacks.
- A comparison of Tyco's security posture against other organizations of similar size.

Positive Observations

- The VideoEdge Web Application offers a limited attack surface.
- When properly configured, the VideoEdge ecosystem offers limited opportunity for attacks leveraging network communications.
- Rapid7's attempts to perform XXS attacks against the VideoEdge Web Application failed.
- All attempts to leverage XXE attacks against the VideoEdge Web Application failed.
- Rapid7 was unable to perform path traversal attacks against the VideoEdge Web Application.
- All attempts to leverage command injection attacks against the VideoEdge Web Application failed.

RAPID7 Confidential and Proprietary 2



Rapid7 Reporting Methodology

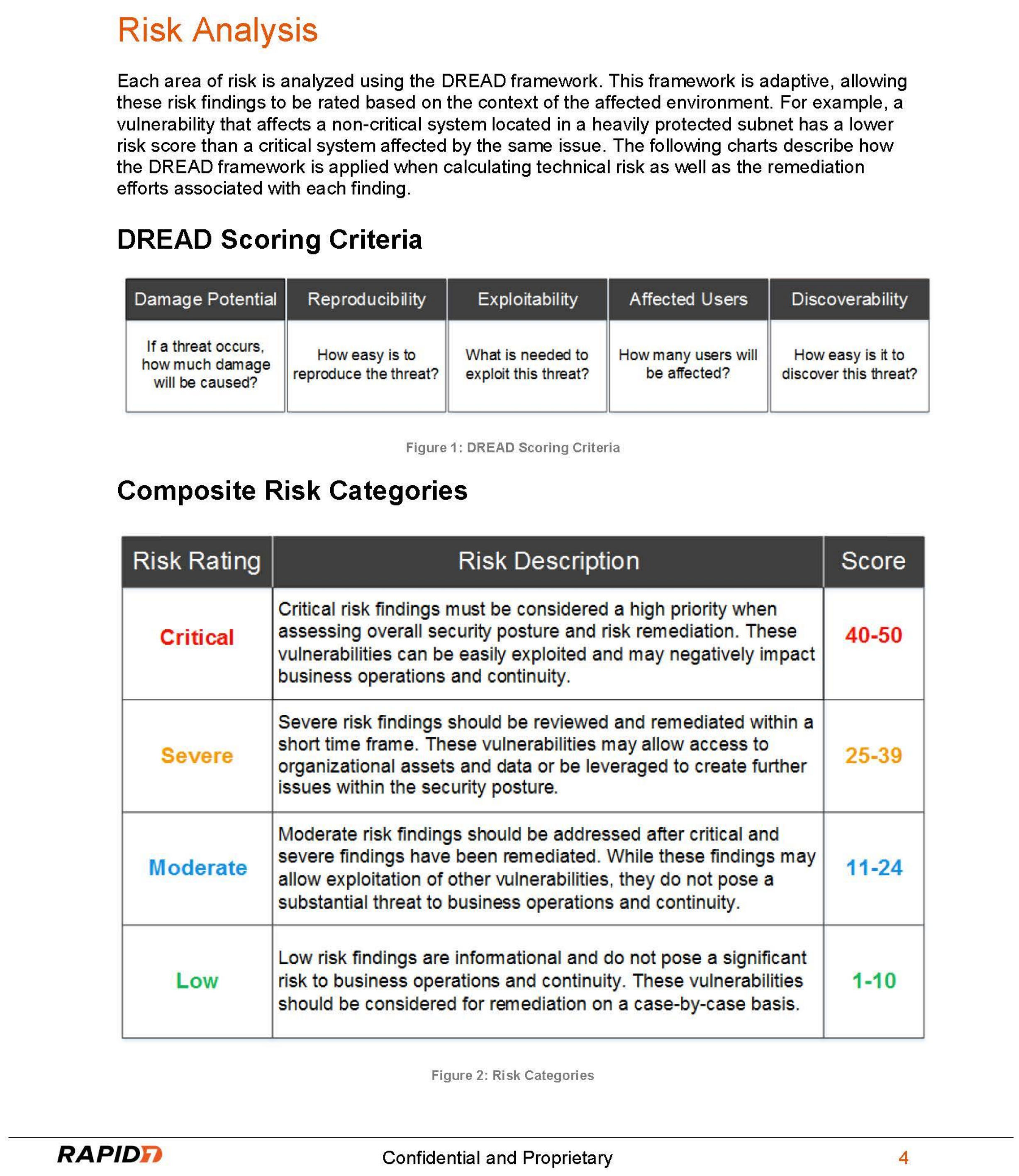
Rather than report each vulnerability, Rapid7 reports describe risks and findings. A finding is a logical grouping of one or more security issues having a common cause and/or a common resolution. In addition to identifying the underlying cause(s), each finding also contains hyperlinked references to resources and provides detailed remediation information.

A provided risk summary demonstrates the overall view of the assessment findings and can be used as a workflow plan that can be tracked within the security organization. This plan is intended to assist Tyco's remediation team in prioritizing and tracking the remediation effort. Each finding has been categorized according to its relative risk level and also contains a rating as to the amount of work and resources required in order to address the finding.

This report represents a 'snapshot' of the security posture of Tyco's environment at a point in time. Rapid7 utilizes the Microsoft threat scoring framework called DREAD (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability). This rating system enables Rapid7 to determine the damage that a threat is capable of causing a system. The threat can be quantitatively defined as the product of the probability of a threat causing damage and the impact that the threat has on the system.

The probability of the threat causing damage can be determined by examining the reproducibility, exploitability, and discoverability of the threat. The impact can be determined by calculating the potential damage and percentage of affected users of the system. For threats that have been mitigated, the probability of the threat causing damage is zero; therefore, the factors that determine the probability can be considered to be zero.

As mentioned above, this initial report including this risk summary is supplied to Tyco, who utilizes it as a plan to prioritizing and track the remediation effort. Once the remediation effort has been completed, Rapid7 returns to validate the remediation effort, providing a summary table that references the number and risk rating of vulnerabilities found during the initial engagement, as well as the result of the remediation effort against previously documented findings.



Risk Analysis

Each area of risk is analyzed using the DREAD framework. This framework is adaptive, allowing these risk findings to be rated based on the context of the affected environment. For example, a vulnerability that affects a non-critical system located in a heavily protected subnet has a lower risk score than a critical system affected by the same issue. The following charts describe how the DREAD framework is applied when calculating technical risk as well as the remediation efforts associated with each finding.

DREAD Scoring Criteria

Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability
If a threat occurs, how much damage will be caused?	How easy is to reproduce the threat?	What is needed to exploit this threat?	How many users will be affected?	How easy is it to discover this threat?

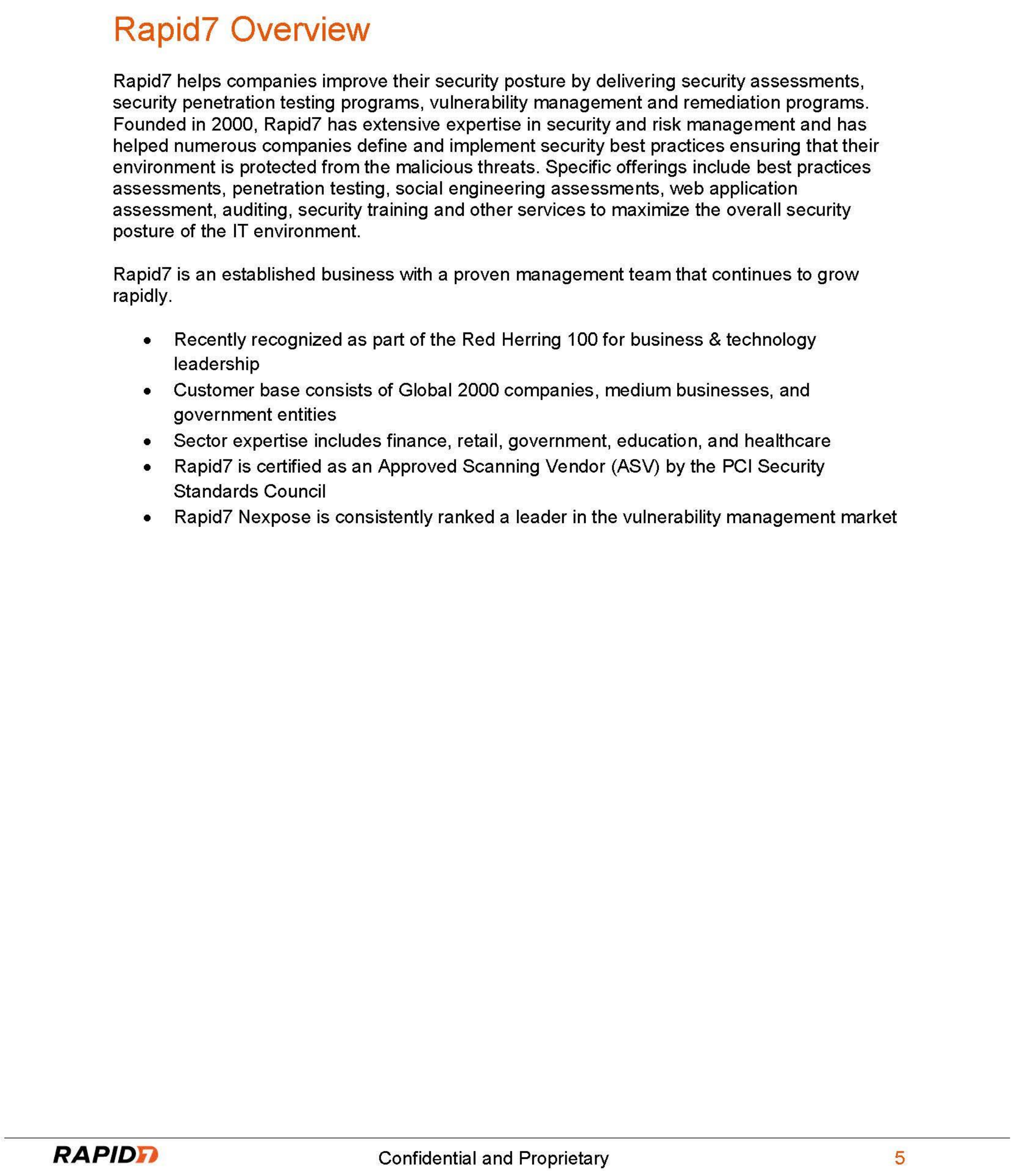
Figure 1: DREAD Scoring Criteria

Composite Risk Categories

Risk Rating	Risk Description	Score
Critical	Critical risk findings must be considered a high priority when assessing overall security posture and risk remediation. These vulnerabilities can be easily exploited and may negatively impact business operations and continuity.	40-50
Severe	Severe risk findings should be reviewed and remediated within a short time frame. These vulnerabilities may allow access to organizational assets and data or be leveraged to create further issues within the security posture.	25-39
Moderate	Moderate risk findings should be addressed after critical and severe findings have been remediated. While these findings may allow exploitation of other vulnerabilities, they do not pose a substantial threat to business operations and continuity.	11-24
Low	Low risk findings are informational and do not pose a significant risk to business operations and continuity. These vulnerabilities should be considered for remediation on a case-by-case basis.	1-10

Figure 2: Risk Categories

RAPID7 Confidential and Proprietary 4



Rapid7 Overview

Rapid7 helps companies improve their security posture by delivering security assessments, security penetration testing programs, vulnerability management and remediation programs. Founded in 2000, Rapid7 has extensive expertise in security and risk management and has helped numerous companies define and implement security best practices ensuring that their environment is protected from the malicious threats. Specific offerings include best practices assessments, penetration testing, social engineering assessments, web application assessment, auditing, security training and other services to maximize the overall security posture of the IT environment.

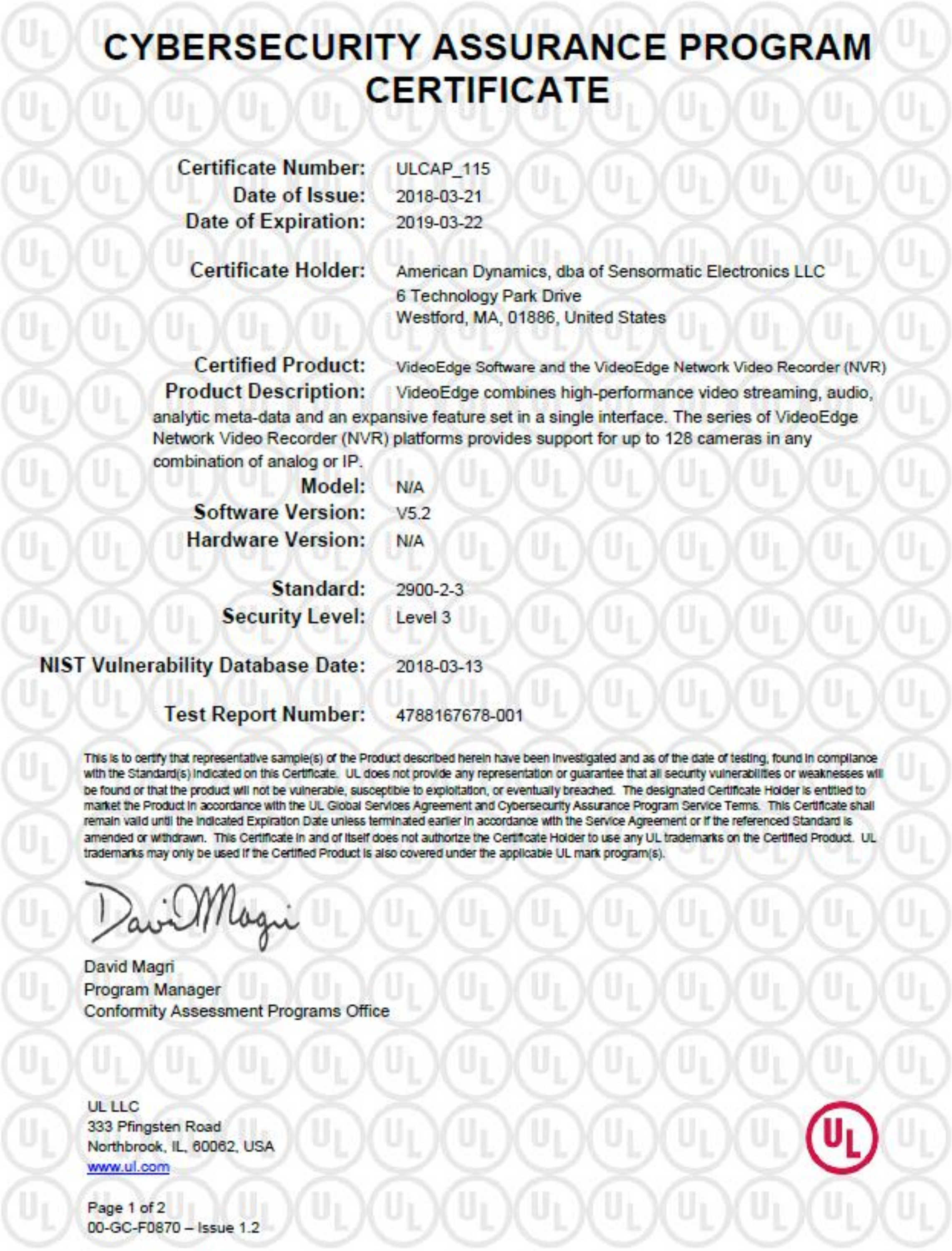
Rapid7 is an established business with a proven management team that continues to grow rapidly.

- Recently recognized as part of the Red Herring 100 for business & technology leadership
- Customer base consists of Global 2000 companies, medium businesses, and government entities
- Sector expertise includes finance, retail, government, education, and healthcare
- Rapid7 is certified as an Approved Scanning Vendor (ASV) by the PCI Security Standards Council
- Rapid7 Nexpose is consistently ranked a leader in the vulnerability management market

RAPID7 Confidential and Proprietary 5

ANNEX G – Certificates

UL2900-2-3 (Level 3)



CYBERSECURITY ASSURANCE PROGRAM CERTIFICATE

Certificate Number:	ULCAP_115
Date of Issue:	2018-03-21
Date of Expiration:	2019-03-22
Certificate Holder:	American Dynamics, dba of Sensormatic Electronics LLC 6 Technology Park Drive Westford, MA, 01886, United States
Certified Product:	VideoEdge Software and the VideoEdge Network Video Recorder (NVR)

Product Description: VideoEdge combines high-performance video streaming, audio, analytic meta-data and an expansive feature set in a single interface. The series of VideoEdge Network Video Recorder (NVR) platforms provides support for up to 128 cameras in any combination of analog or IP.

Model:	N/A
Software Version:	V5.2
Hardware Version:	N/A
Standard:	2900-2-3
Security Level:	Level 3
NIST Vulnerability Database Date:	2018-03-13
Test Report Number:	4788167678-001

This is to certify that representative sample(s) of the Product described herein have been investigated and as of the date of testing, found in compliance with the Standard(s) indicated on this Certificate. UL does not provide any representation or guarantee that all security vulnerabilities or weaknesses will be found or that the product will not be vulnerable, susceptible to exploitation, or eventually breached. The designated Certificate Holder is entitled to market the Product in accordance with the UL Global Services Agreement and Cybersecurity Assurance Program Service Terms. This Certificate shall remain valid until the indicated Expiration Date unless terminated earlier in accordance with the Service Agreement or if the referenced Standard is amended or withdrawn. This Certificate in and of itself does not authorize the Certificate Holder to use any UL trademarks on the Certified Product. UL trademarks may only be used if the Certified Product is also covered under the applicable UL mark program(s).

David Magri

David Magri
Program Manager
Conformity Assessment Programs Office

UL LLC
333 Pfingsten Road
Northbrook, IL, 60062, USA
www.ul.com

Page 1 of 2
00-GC-F0870 – Issue 1.2