



American Dynamics

From Tyco Security Products

VideoEdge Security

User Guide

Document Version 2.0

August 2015

Notice

The information in this manual was current when published. The manufacturer reserves the right to revise and improve its products. All specifications are therefore subject to change without notice.

Copyright

Under copyright laws, the contents of this manual may not be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent of Tyco Security Products.

© 2015 Tyco Security Products. All Rights Reserved.

American Dynamics

60 Congress Avenue

Boca Raton, FL 33487 U.S.A.

Customer Service

Thanks you for using American Dynamics products. We support our products through an extensive worldwide network of dealers. the dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers should contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the Web at www.americandynamics.net.

Trademarks

Windows® is a registered trademark of Microsoft Corporation. PS/2® is a registered trademark of International Business Machines Corporation.

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco Security Products. will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco Security Products are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

License Information

Your use of this product is governed by certain terms and conditions.

VideoEdge Security Overview

Introduction

Tyco Security Products range of video products include information security controls and features designed to protect the device/system and enforce the security policies of the customer organization. These security controls and features are available to be enabled and configured on the respective devices.

About this Document

This Security Features Guide describes the VideoEdge NVR security functions and associated features. The document provides information on how these features work, guidelines for their use and how these features interact with one another. The selection and application of these product-specific controls, in conjunction with other network security controls provided by the host network, supports the creation of a system that meets information security best practices, organization security policies and applicable FISMA technical controls. It is the organization's responsibility to select, enable, configure and/or apply these controls to achieve the desired level of security in accordance with the organization's security policies and as part of their overall IT security infrastructure.

Certain security features are provided as device settings and configurations. Other features are provided as actions available to a user which may support a customer's security policies and required security controls.

For each security feature, this document provides a description of the feature, how to enable, configure or invoke the feature, guidelines for using the feature and how the feature interacts with other security features.

Applicable Software Versions

The information and procedures contained in this document relate to the following software versions:

- VideoEdge V4.7

VideoEdge

VideoEdge is a scalable enterprise IP video surveillance solution. It is designed as an open platform solution supporting a range of third party hardware, storage, video devices, and clients, allowing users to manage their video surveillance servers and edge devices as a single logical system.

The VideoEdge (NVR) manages the IP encoder and camera devices, records the video onto its configured storage devices, and provides clients with secure access to live and recorded video and audio. Users can use a web browser interface (NVR Administration Interface) or the victor rich-client application software to configure the NVR or access the video/audio streams.

Purpose of the NVR

The NVR is the backbone for an IP-based video security system. The NVR uses TCP/IP communication to access and control the hardware networked to it. The server can be controlled directly by logging into its Administration interface homepage using a web browser or accessing it via the victor rich-client application software. When configured worldwide access to the NVR gives it excellent portability, that is any place where with a personal computer with internet access to the web, provides access to the video security system.

An NVR provides control over all the features of the surveillance and security hardware networked to the NVR.

The NVR is available as either a complete software/hardware solution, or as a software-only product that transforms a standard computer hardware system into an advanced and powerful NVR server. The NVR software is a hardware-

independent platform. It supports major-brand IP cameras and encoder devices, integrates into a TCP/IP networking environment, turning an ordinary PC or server into an Enterprise Network Video Recorder.

victor Network Video Management System

victor is part of a powerful Network Video Management System that includes advanced policy management, health monitoring, Smart Search, instant playback, and more, ensuring the security and safety of your entire organization whether a single site, or a multi-location, globally dispersed enterprise.

The “open” architecture of the victor Digital Video Management System line is designed so that each component can operate independently, and can interact with software applications from other product lines. The victor Digital Video Management System line includes products to address the needs of a wide range of users.

As the architecture is open, it is independent of specific hardware platforms. The NVR does not require an existing operating system as it includes it’s own Linux-based operating system that can support a variety of different hardware platforms. The Figure below shows how the NVR fits into the victor Network Video Management System.

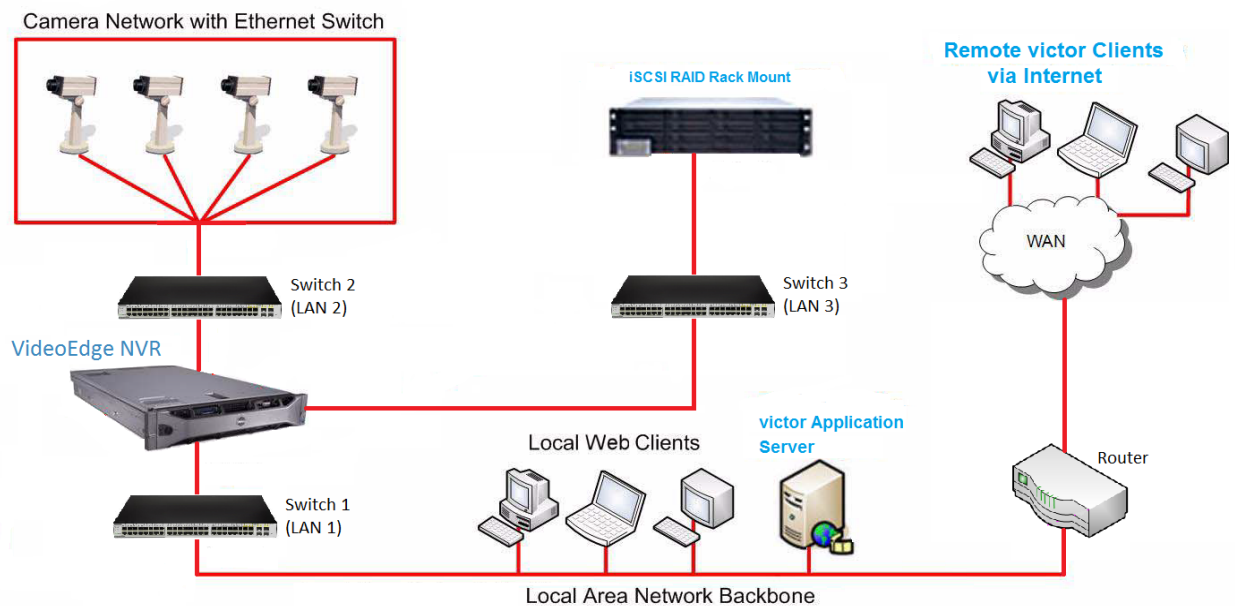
Device/System Security Overview

Overview

This section provides the background on the overall operation of the security controls in the system so that users can then understand the options and actions of individual security-relevant commands.

Device/System Environment

Figure 3-1 VideoEdge Architecture



Definitions of Terms

The following terms and acronyms may be used within this document:

VideoEdge NVR Administration Interface: Access to the VideoEdge NVR Administration Interface is provided on the VideoEdge Client's Side Bar to provide access to the VideoEdge NVR's configurable settings.

VideoEdge NVR Certificate: When using HTTPS communication, a certificate is required. VideoEdge NVR supports creation of a self-signed certificate and creation of a certificate request that can be used to obtain a certificate from a third-party Certificate Authority (CA).

Self-signed Certificate: For users with a lower security requirement, you can create a self-signed certificate which can then be installed on victor Unified Client and victor site manager allowing HTTPS communication between the VideoEdge NVR and the client.

CA-Signed Certificate: VideoEdge NVR supports the creation of a certificate request which can be used to obtain a signed certificate from a third-party Certificate Authority (CA). The signed certificate can then be installed on the system.

HTTP: HyperText Transfer Protocol, the communications protocol used to connect to Web servers on the Internet or on a local network (intranet).

HTTPS: HyperText Transfer Protocol with SSL Encryption. It is the most popular network protocol for establishing secure connections

VNC: Virtual Network Computer. VNC remote access to the VideoEdge operating system can be enabled or disabled using the Security Configuration command.

XRDP:Microsoft Remote Desktop Protocol, XRDP is a Microsoft protocol that allows remote access a device.XRDP remote access to the VideoEdge operating system can be enabled or disable. using the Security Configuration command.

DAC: Discretionary Access Control, is a method of restricting access to objects based on the identity of the user account. For example, an administrator account will have more privileges than a guard account. Refer to victor Configuration and User Guide and/or VideoEdge Hybrid Installation and User Manual for a breakdown of role privileges.

SSH: Secure Shell (SSH) is a cryptographic network protocol for secure data communication.

SSHD: Secure Shell Daemon, is a secure network service that is used to let you log into a remote computer running an SSH Server.

SSL: Secure Sockets Layer is a protocol for transmitting information privately over the internet.

NVMS: Network Video Management System.

TLS: Transport Layer Security is the successor to SSL.

NAT: Network Address Translation is a methodology for mapping private IP addresses to a public IP address and port. NAT can be used to hide the details of the internal network or to share a single public IP address between multiple internal addresses. The NAT router in a network will keep a table of registered IP addresses and when a private IP address requests access to the network the router selects an IP address.

System Security Administrator

VideoEdge has multiple user credentials or roles which dictate varying levels of access and interaction with the software. The following roles allow configuration of the security features on their respective software:

VideoEdge NVR Administration Interface

- admin - Default user account with read/write access to the NVR Administration Interface/VideoEdge Client/victor Web LT.
- support - Support user account which provides a set of diagnostic tools for use by American Dynamics Technical Support. The password for this account can be changed using the procedure later discussed in this user guide.

VideoEdge Embedded Operating System

- root - Default user account with read/write access to the NVR's embedded Linux OS.
- support - Support user account which can be used by American Dynamics Technical Support for SSH system access and diagnostics. The password for this account is unique to each NVR and is derived by American Dynamics Technical Support from the platform's support ID. The password can not be changed, however remote SSH access can be prevented by disabling the SSH Remote Access service using the procedure later discussed in this user guide or by not connecting the NVR to the internet.

Note:

This account is not the same as the VideoEdge NVR Administration Interface support account.

Security Functions, Features and Commands

Overview

This section details the security features which are present in VideoEdge, their related commands and procedures for configuration.

VideoEdge Security Configuration Menu

The following commands are available under the VideoEdge Security Configuration menu.

Note:

NVR-generated certificates (self-signed and CA-signed) and certificate signing requests use the SHA-256 algorithm in VideoEdge 4.7+ providing enhanced security.

Certificate Authority Settings

The “Certificate Authority Settings” section allows an intermediate certificate authority to be installed on the NVR for use in signing the NVR’s certificate. It is the responsibility of the customer to deploy the appropriate certificate chain to client computers. The uploaded certificate authority should be PEM-encoded and should contain the CA certificate and encrypted private key.

Certificate Remote Access System Password System Use Banner LDAP Security Audit

Certificate Authority Settings

You may install an intermediate certificate authority for use when creating certificates.

Install intermediate CA certificate and key

It is critical that the certificate authority remains secure at all times. We recommended that you generate it with an encrypted private key and upload it using the browser on the NVR, or ensure that you are using HTTPS.

CA private key is encrypted:

Decryption Password:

Upload intermediate CA certificate (pem format):

After you install the Certificate Authority, the details of the CA are visible on the Certificates Page.

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

Create Certificate

Create Certificate Signing Request ?

Installed certificates

Subject: C=IE, ST=Munster, L=Cork, O=Tyco, CN=BEL-CORK-47
Issuer: C=IE, ST=Munster, L=Cork, O=Tyco, CN=BEL-CORK-47
Valid From: May 5 15:13:48 2015 GMT
Valid Until: May 4 15:13:48 2016 GMT



Click to Delete

CA Details

Procedure 3-1 Installing a Certificate Authority

Note:

It is recommended that you use the browser on the NVR, or access the page using HTTPS, when installing the intermediate CA. This is to protect the decryption password from interception on the network.

Step	Action
1	Select System .
2	Select Security Configuration . The Certificate page opens.
3	(Optional) Select the CA private key is encrypted checkbox if required. a Enter the Decryption Password in the field.
4	Click Browse .
5	Navigate and select the required .PEM file.
6	Click Open .
7	Click Install .

- End -

When you generate a new certificate for the NVR, you can choose to use the installed CA to sign the certificate. To automatically include IP addresses from the certificate or certificate request, select the "Allow IP Addresses" checkbox.

Create certificate

Certificate parameters

Country: UK *

State or province:

Locality:

Organisation:

Organisational Unit:

Common Name: NVR01.test.com *

Subject Alternative Name: NVR01.test.com *

Allow IP Addresses:

Validity: 365 days (1..9999) *

Fields marked * are mandatory.

Signing

There is an intermediate certificate authority installed. You have the option of using this to sign the certificate.

CA signed Self signed

OK Cancel

CA-signed certificates can be identified in the "Installed certificates" section of the "Certificate" page, under "Issuer" details.

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

Create Certificate

Create Certificate Signing Request ?

Installed certificates

Subject:	C=UK, CN=NVR01.test.com
Issuer:	C=GB, ST=Down, O=Tyco, OU=AD, CN=intermediate CA encrypted/emailAddress=f@g.com
Valid From:	Mar 11 15:43:36 2015 GMT
Valid Until:	Mar 10 15:43:36 2016 GMT

Click to Delete

Certificate Details

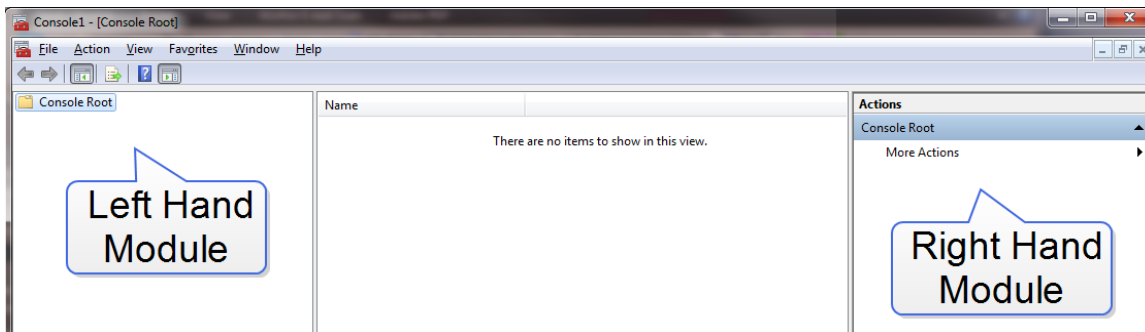
Installing Root and Intermediate Certificates

When using an installed CA or using a 3rd Party CA you will be required to install the Root and Intermediate certificate on your victor Unified Client PC.

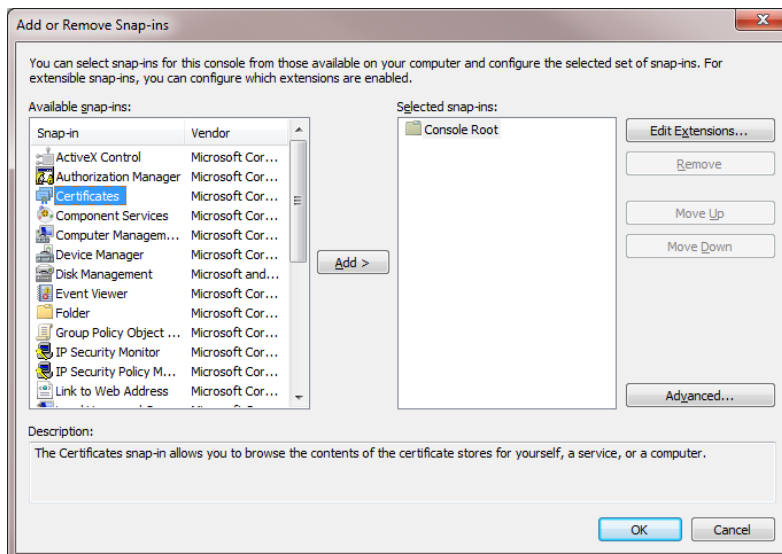
Procedure 3-2 Installing Root / Intermediate Certificates

Step Action

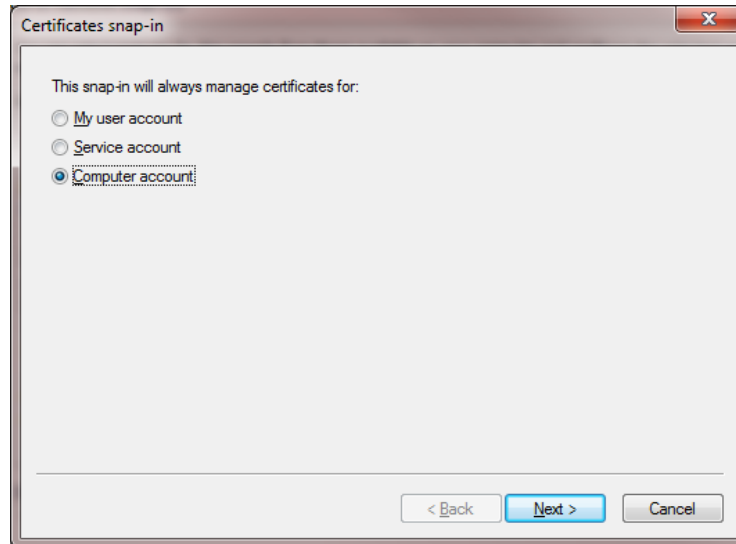
- 1 Open Microsoft Management Console (MMC). **Windows Button > MMC > Return**
MMC will launch.



- 2 In MMC select **File > Add/Remove Snap-In**.
- 3 Select **Certificates** from the Available snap-ins.



- 4 Click **Add >**.
The Certificates snap-in Wizard launches.
- 5 Click the **Computer Account** option button.



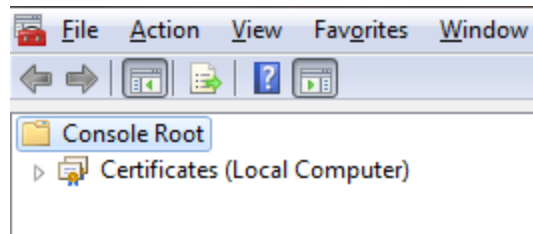
6 Click **Next**.

7 Click the **Local Computer** option button (selected by default).

8 Click **Finish**.

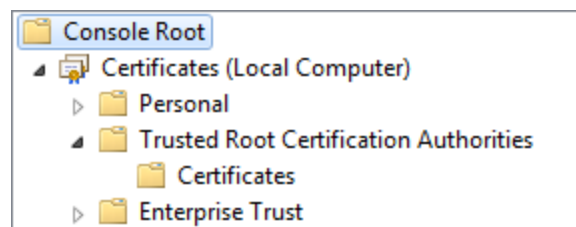
9 Click **OK**.

A certificates dropdown menu will appear under the Console Root. Located on the left hand module of MMC.



10 Select the **Certificates** menu dropdown .

11 Select **Trusted Root Certification Authorities** dropdown.

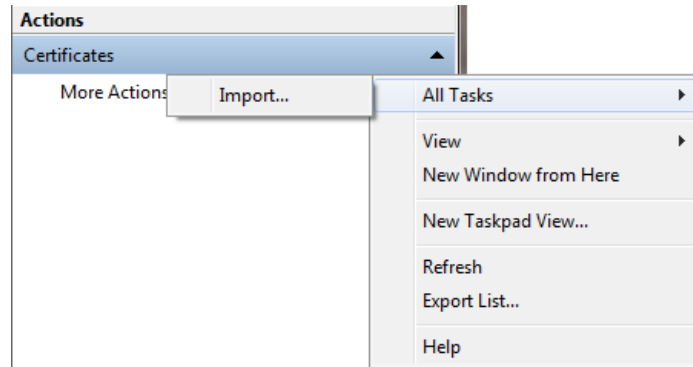


12 Select **Certificates**.

13 Select **More Actions**. Located on the right hand module of MMC.

14 Navigate to **All Tasks**.

15 Select **Import...**

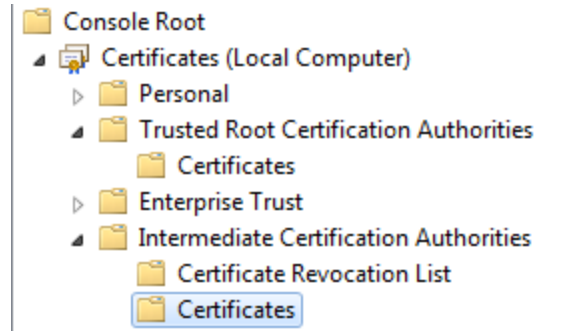


The Certificate Wizard launches.

- 16 Click **Next**.
- 17 Click **Browse**.
- 18 Navigate to your Root Certificate and click **Open**.
- 19 Click **Next**.
- 20 Click **Next**.
- 21 Click **Finish**.

A message stating "import was successful" displays.

- 22 Under certificates menu on the left hand module of MMC, select **Intermediate Certification Authorities**.
- 23 Select **Certificates**.

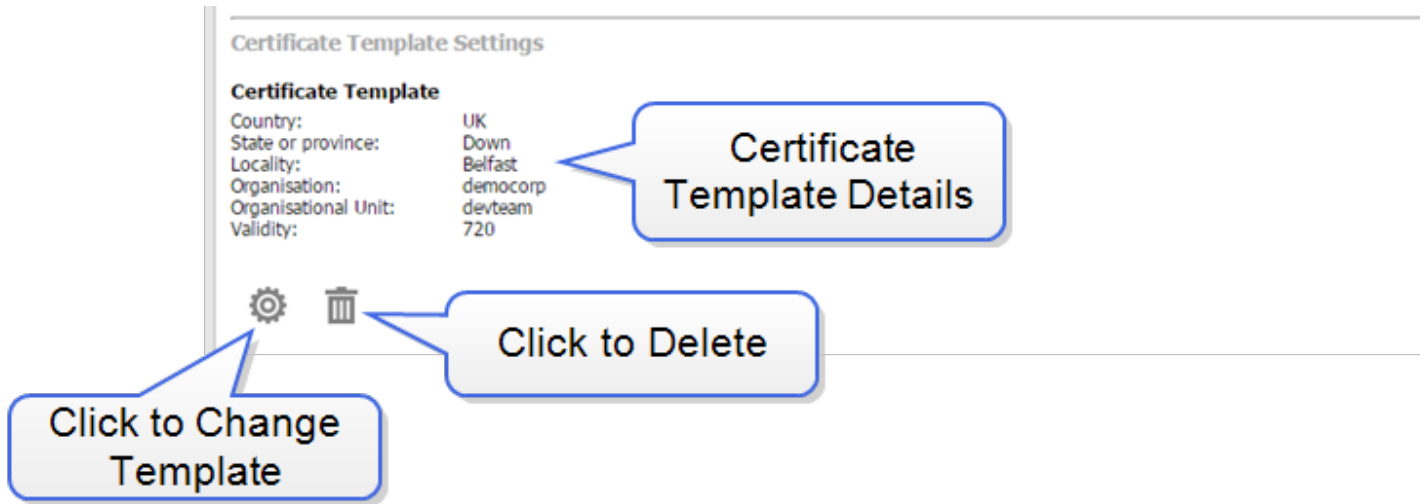


- 24 Select **More Actions**. Located on the right hand module of MMC.
 - 25 Navigate to **All Tasks**.
 - 26 Select **Import...**
- The Certificate Wizard launches.
- 27 Click **Next**.
 - 28 Click **Browse**.
 - 29 Navigate to your Intermediate Certificate and click **Open**.
 - 30 Click **Next**.
 - 31 Click **Next**.
 - 32 Click **Finish**.

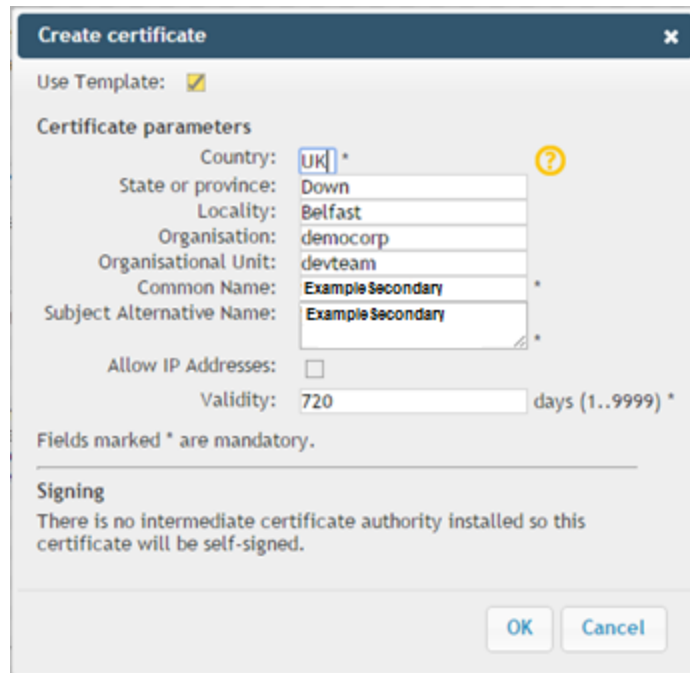
A message stating "import was successful" displays.

Certificate Template Settings



You can define a template for use when generating certificates or certificate signing requests.



When a template has been specified, you will have the option to use it when creating a certificate or certificate signing request.



Procedure 3-3 Create a Certificate Template

Step	Action
1	Select System .
2	Select Security Configuration . The Certificate page opens.
3	Select  The Edit certificate template window opens.
4	Enter the Country Code .
5	(Optional) Enter the State or province .
6	(Optional) Enter the Locality .
7	(Optional) Enter the Organisation .
8	(Optional) Enter the Organisational Unit .
9	Enter the Validity .
10	Click 


- End -

Certificate Automatic Generation

Certificate automatic generation can be enabled and disabled, using the option button. A certificate template must be created before you can enable certificate automatic generation. If the certificate template is deleted, certificate automatic generation will be disabled. By default, certificate automatic generation is disabled.

When automatic generation is enabled, the NVR will generate a new certificate when it detects that the certificate does not contain all of the names and IP addresses that are currently configured on the NVR. When a certificate is automatically generated, it is created with the certificate template.

Procedure 3-4 Enabling Certificate Automatic generation

Step	Action
1	Select System from the main menu.
2	Select Security Configuration . The Certificate page opens.
3	Scroll to the Certificate Automatic Generation section of the page.
4	Click the Enabled option button.
5	Click 

- End -

Certificate Settings

Note:

The use of self signed or CA approved certificates is not enabled by default.

Description

When using HTTPS communication, a PKI certificate is required to provide secure encrypted communications and authenticate the NVR to the connecting device. VideoEdge supports the creation of a self-signed certificate or use of a certificate provided by a 3rd-party Certificate Authority. A certificate sourced from a 3rd-party Certificate Authority typically provides a higher level of security than a self-signed certificate.

Configuration/Commands

Create or request a certificate.

Creating a self-signed certificate

The following procedure describes how to create a self-signed certificate.

Figure 3-1 Certificate Page

Certificate Remote Access System Password System Use Banner LDAP Security Audit

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

Create Certificate

Create Certificate Signing Request ?

Installed certificates

Subject: C=IE, ST=Munster, L=Cork, O=Tyco, CN=BEL-CORK-47
Issuer: C=IE, ST=Munster, L=Cork, O=Tyco, CN=BEL-CORK-47
Valid From: May 5 15:13:48 2015 GMT
Valid Until: May 4 15:13:48 2016 GMT

Click to delete currently installed certificate



Summary displays the current installed certificate. Will appear blank when default certificate is in use

Procedure 3-5 Creating a self-signed certificate

Step	Action
1	Select System from the main menu.
2	Select Security Configuration . The Certificate page opens.
3	Click Create Certificate .
4	Enter the Country code in the field.

Note:

The country code must be entered as per the standard SSL Certificate Country Code.

- 5 (Optional) Enter the **State or province** in the field.
- 6 (Optional) Enter the **Locality** in the field.
- 7 (Optional) Enter the **Organization** in the field.
- 8 (Optional) Enter the **Organizational Unit** in the field.
- 9 Edit the **Common Name** if required.
- 10 Edit the **Subject Alternative Name** if required.
- 11 Edit the **Validity** if required.
- 12 Click 
The new certificate is activated.
- 13 Click  and restart your browser.

- End -

Creating a request for a signed certificate

The following procedure describes how to create a certificate request required to obtain a certificate from a 3rd-party Certificate Authority.


Procedure 3-6 Creating a certificate request

Step	Action
------	--------


- 1 Select **System** from the main menu.
- 2 Select **Security Configuration**.
The Certificate page opens.
- 3 Click **Create Certificate SigningRequest**.
- 4 Enter the **Country** code in the field.

Note:


The country code must be entered as per the standard SSL Certificate Country Code.

- 5 (Optional) Enter the **State or province** in the field.
- 6 (Optional) Enter the **Locality** in the field.
- 7 (Optional) Enter the **Organization** in the field.
- 8 (Optional) Enter the **Organizational Unit** in the field.
- 9 Edit the **Common Name** if required.
- 10 Edit the **Subject Alternative Name** if required.
- 11 Click 
The certificate request is displayed in PEM format.

12 Copy and paste the request into email or alternative file for sending to the CA.

13 Click 

Note:

A summary of the certificate request will be displayed on the Certificates page. To delete an awaiting certificate request, click 

- End -

Uploading a Signed Certificate

The following procedure describes how to install a certificate obtained from a 3rd-party Certificate Authority.

Procedure 3-7 Uploading a Signed Certificate

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select System from the main menu. |
| 2 | Select Security Configuration .
The Certificate page opens. |
| 3 | Click Browse . |
| 4 | Use the windows file explorer to located the signed certificate. |
| 5 | Click Open . |
| 6 | Click Install . |

- End -

Remote Access Services

Note:

SNMP, SSH, VNC and XRDP are enabled by default.

Description

The SNMP, SSH, VNC and XRDP services allow remote access to the VideoEdge operating system. These services can be enabled or disabled independently.

The following procedure describes how to enabled and disable these services.

Configuration/Commands

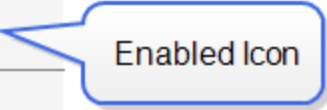
Enable or disable a remote access service.

Procedure 3-8 Enabling and Disabling Remote Access Services

Step	Action
------	--------

- 1 Select **System** from the main menu.
- 2 Select **Security Configuration**.
The Certificate page opens.
- 3 Select the **Remote Access** tab.
- 4 Navigate to the Remote Access Services table.

NAME	ENABLED
SNMP	<input checked="" type="checkbox"/>
SSH	<input checked="" type="checkbox"/>
VNC	<input checked="" type="checkbox"/>
XRDP	<input checked="" type="checkbox"/>



- 5 De-select the respective Enabled button to disable the service. Select the Enabled button to enable the Service.
When a selection is made, a dialog box opens to confirm the selection..
- 6 Click **OK**.

- End -

Remote Web Access

Note:

Remote Web Access Services are enabled by default.

Description

The Remote Web Access services allow access to the VideoEdge web interface using multiple platforms / sessions. These services can be enabled or disabled independently.

The following procedure describes how to enabled and disable these services.



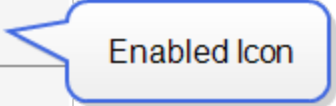


Configuration/Commands

Enable or disable remote web access.

Procedure 3-9 Enabling/Disabling and Restricting Remote Web Access

Step	Action
------	--------

- 1 Select **System** from the main menu.
- 2 Select **Security Configuration**.
The Certificate page opens.
- 3 Select the **Remote Access** tab.
- 4 Navigate to the Remote Web Access table.

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

- 5 Click the **Enabled** icon in the entry you want to enable or disable remote access.
A dialog box opens.
- 6 Click **OK**.

- End -

Web Server Protocol Configuration

Note:

The web server supports HTTP and HTTPS protocols by default. The HTTP Port has a default value of 80 and the HTTPS Port has a default value of 443.

Description

VideoEdge NVR supports remote access via HTTP and HTTPS web protocols. When the HTTPS protocol is used, communication is secured via TLS using the certificate hosted by the NVR. Two options are provided. "HTTP and HTTPS" permits communication by either protocol. Using this option, the client browser selects the protocol. The "HTTPS only" selection only permits use of the HTTPS protocol. The "HTTPS only" selection provides the most security. The communication type on the VideoEdge NVR can be configured by assigning bespoke HTTP and HTTPS ports. If HTTPS communication has been selected between the VideoEdge NVR and victor this will ensure that data is sent encrypted.

Configuration/Commands

Configure the web interface protocol and communication ports.

Procedure 3-10 Editing the Web Server Configuration

- | Step | Action |
|------|---|
| 1 | Select System from the main menu. |
| 2 | Select Security Configuration .
The Certificate page opens. |
| 3 | Select the Remote Access tab. |
| 4 | Navigate to the Web Server Ports and Protocols section. |

Figure 3-2 Web Server Ports and Protocols

Web Server Ports and Protocols

Communication: HTTP and HTTPS HTTPS only

HTTP Port:

HTTPS Port:



Default Values

- 5 Select the **HTTP and HTTPS** option button.
Or
Select the **HTTPS only** option button.
- Enter the **HTTP port** you want to use in the field.
 - Enter the **HTTPS port** you want to use in the field.

Note:

You can only configure one value at a time. To edit the HTTP Port and HTTPS port value you must edit one and save before you can edit the other.

- 6 Click

- End -

System Password

Note:

The system password is 'root' by default.

Description

VideoEdge NVR provides the ability to change the local root account password. The root account provides full administrative access to the NVR's embedded operating system. Changing the root system from the default password and making it unique enhances the security of the product.



Caution

It is highly recommended that you change the root password.

Configuration/Commands

Change the system password used by the 'root' account.

Note:

The System Password page must run under HTTPS.

Procedure 3-11 Changing the System Password

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select System from the main menu. |
| 2 | Select Security Configuration .
The Certificate page opens. |
| 3 | Select the System Password tab. |
| 4 | (When viewing in HTTP Only) Click Change to HTTPS .
A browser warning page displays to state there is a problem with the website's security certificate. This warning only displays when the default NVR certificate or a certificate not signed by a trusted root CA is installed. |
| 5 | Select Continue to this website (not recommended) . |
| | <hr/> Note:
Wording may differ between browsers. <hr/> |
| 6 | Enter the Current Password . |
| 7 | Enter the New Password . |
| 8 | Re-enter the New Password in the Confirm Password field. |



Caution

It is extremely important that you remember this password. If the password is lost/forgotten you will have to re-install the system to regain root access.

- | | |
|---|---|
| 9 | Click  |
|---|---|

System Use Banner

Note:

The System Use Banner is not populated by default.

Description

VideoEdge NVR provides an optional configurable System Use notification Banner that can be configured to be displayed before a user logs on to the system either locally or remotely before granting access to the system.

The System Use Banner wording can be customized to provide organization-specific privacy and security notices consistent with applicable laws, executive orders, directives, polices, regulations, standards and guidance.

Configuration/Commands

Configure system use notification banner.

Procedure 3-12

Configuring the System User Banner for non-XDRP Clients

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select System from the main menu. |
| 2 | Select Security Configuration .
The Certificate page opens. |
| 3 | Select the System Use Banner tab. |

Figure 3-3 System Use Banner Field

Configure the System Use Notification Banner for non-XRDP clients

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

🗑 ✕

Configure the System Use Notification Banner for XRDP clients

Upload a 256 color Bitmap image file for XRDP

NOTE: XRDP clients may be sensitive to the bitmap image size. Please make sure you test it and adjust the image size properly when necessary.

System Use Notification Banner Image File:

Current System Use Notification Banner Image for XRDP:



Note:

The format entered in the system use banner field is preserved in both the VideoEdge Administrator

Interface login page and during operating system login. When logging into an NVR operating system account locally or via VNC, the login window will display the use banner in a justified format.

- 4 Enter the required notifications in the text field.

Note:

If the text field is empty, the System Use Banner will not be displayed during login.

- 5 Click 

- End -

Procedure 3-13 Configuring the System User Banner for XDRP Clients

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select System from the main menu. |
| 2 | Select Security Configuration .
The Certificate page opens. |
| 3 | Select the System Use Banner tab. |
| 4 | Click Browse .
A file explorer window opens. |
| 5 | Select the file you want to use for the System Use Banner. |

Note:

Only bitmap files are supported. Some XDRP clients may be sensitive to the .bmp image size.

- | | |
|---|-----------------------------------|
| 6 | Click Open . |
| 7 | Click Upload XRDP Banner . |

- End -

LDAP Configuration

Note:

LDAP is not configured by default.

Description

VideoEdge allows the use of a Lightweight Directory Access Protocol (LDAP) server to administer user credentials for the Administration Interfaces and VideoEdge Clients of multiple NVRs. This minimizes configuration and management of user credentials on each NVR by sharing one centralized server.

Note:

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

VideoEdge LDAP supports the use of active directory and a secure connection. For secure connections a valid LDAP server certificate must be provided in order to log in or to retrieve a list of LDAP groups on the LDAP Roles page.

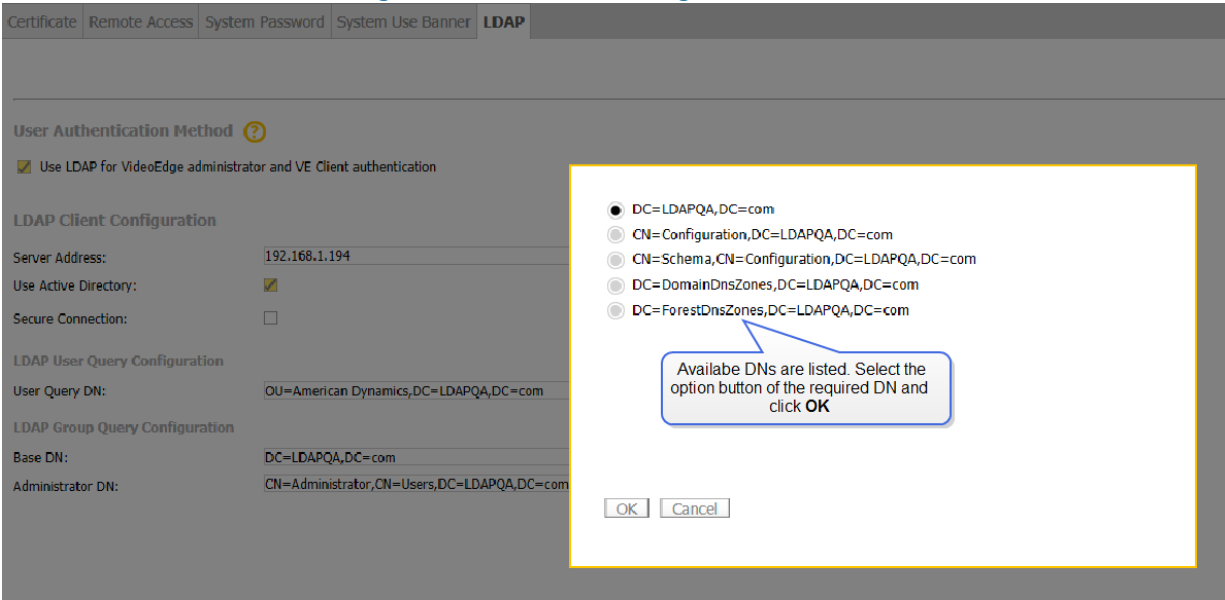
Configuration/Commands

Configure LDAP server.

Procedure 3-14 Enabling LDAP Support

Step	Action
1	Select System from the main menu.
2	Select Security Configuration . The Certificate page opens.
3	Select the LDAP tab.
4	Select the Use LDAP for VideoEdge administrator and VE Client authentication checkbox.
5	Enter the LDAP Server IP address in the Server Address field.
6	(Optional) If using Active Directory on the LDAP server, select the Use Active Directory checkbox.
7	(Optional) Select the Secure Connection checkbox. A menu item and warning displays at the bottom of the page prompting 'A valid LDAP server certificate must be installed in order to log in securely as an LDAP user.'
8	Click Browse to search for the LDAP server certificate. A file explorer window opens.
9	Navigate to the required location and select the certificate.
10	Click Open .
11	Click Install . A dialog box displays to notify the success of the installation.
12	Click OK .
13	Enter the User Query DN in the field. <hr/> Note: The User Query DN should be the distinguished name of the organizational unit that the user belongs to. <hr/>
14	Enter the Base DN in the field. Click Fetch DN to view a list of available Base DNs.

Figure 3-4 Fetch DN Configuration Window




Note:

The Base DN is the starting point for the search. Only groups within the specified Base DN will be retrieved. The value must be a distinguished name that currently exists in the database.

- 15 Enter the **Administrator DN** in the field.

Note:

The Administrator DN is used to authenticate to the server. The value must be a distinguished name with the authority to search for groups. This is the sole purpose of the Administrator DN.

- 16 Click 

- End -

Security Audit

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

- Role Settings
- User Settings
- Linux User Settings
- Web Server Ports and Protocols
- Remote Access
- Certificate Settings
- Certificate Authority Settings
- System Robustness

Camera Security Groups

Description

In order to communicate, a camera's and the VideoEdge NVR's communications and security settings must be compatible to allow them to interoperate. When an IP camera is added to a VideoEdge NVR, the NVR initially uses the manufacturer's default communication and security settings to communicate with the camera. VideoEdge NVR provides the ability to change the NVR's camera interface settings by creating a Security Group with a security level assignment. An NVR Security Group with settings compatible with the settings of the cameras in the group will enable communication between the grouped cameras and the NVR.

One of the following three security levels, as defined below, can be assigned to a Security Group:

Low

Passwords will not be encrypted and all traffic will be sent unencrypted and eavesdroppers on the network may be able to intercept commands.

Medium

The VideoEdge NVR and the camera will communicate through HTTP. Passwords will be sent encrypted but all commands will be sent unencrypted and eavesdroppers on the network may be able to intercept these commands.

High

The VideoEdge NVR and the camera will communicate by HTTPS/SSLv3.

Configuration/Commands

Configure secure camera communication using the VideoEdge NVR.

Note:

1. You can opt to assign a different port for camera communication instead of the defaults which are listed.
 2. Some handlers will not support HTTPS. Please refer to the camera handler release notes for further details.
 3. The Security Groups feature does not change the password on the camera. is used to configure the password used
-

by the VideoEdge NVR to communicate with cameras.

4. The Security Group password and the camera(s) password must match. The password on the camera(s) must be changed prior to changing the corresponding Security Group password. Otherwise, the corresponding cameras will not be able to connect to the VideoEdge NVR.

5. Port number: This is either the HTTP or HTTPS port number which has been specified for communication. The default port number will be used to communicate with the camera unless you specify a port. The port number on the corresponding cameras must be correctly configured for communication to be established.

Procedure 3-15 Creating a Security Group

Step	Action
------	--------

1	Select Devices from the main menu.
---	---

2	Select Security . The Security tab displays.
---	--

3	Select  The Security Group window opens.
---	--

4	Enter a Group Name .
---	-----------------------------

5	Enter a Description .
---	------------------------------

6	Enter a Username .
---	---------------------------

7	Enter a Password .
---	---------------------------

Note:

This is the password that will now be used by the NVR to connect to the cameras in this security group.

8	Confirm the password in the Confirm Password field.
---	--



9	Select Advanced .
---	--------------------------

10	Select the Security Level from the dropdown.
----	---

11	Enter the Port number.
----	-------------------------------

Note:

Ensure the **Default** checkbox is selected if you want to use the default port number.

12	Select the cameras you want to assign to the security group by using the  and  buttons.
----	---

13	Click 
----	---

Note:





Cameras connected to the NVR via an encoder that are associated with a security group must all have the same password. Configuring the security group for one camera connected by an encoder will result in all cameras on that encoder being assigned the same password. A message opens warning that multiple cameras will be updated.

- End -

Editing a Security Group

Security groups can be edited using the security tab.

Procedure 3-16 Editing a Security Group

Step	Action
1	Select Devices from the main menu.
2	Select Security . The Security tab displays.
3	Select  in the group record you want to edit. The Security Group window opens.
4	Edit the Group Name as required.
5	Edit the Description as required.
6	(Optional) Select the Set Username/Password checkbox. Enter a Username . Enter a Password . Confirm the password in the Confirm Password field.
7	Edit the Security Level using the dropdown as required.
8	Edit the Port as required.
9	Select the cameras you want to assign to the security group by using the  and  buttons.
10	Click  .

- End -

Deleting a Security Group

When you delete a security group, the NVR will try to communicate with the cameras that were in this group, using the manufacturer's default password.

In order for the NVR to successfully communicate with the cameras that were in this group, you must change the password for each camera back to the manufacturers default password, using the direct camera web interface, or reassign the cameras to a new security group.

Procedure 3-17 Deleting a Security Group

Step	Action
1	Select Devices from the main menu.
2	Select Security . The Security tab displays.

3 Select the checkbox in the security group record that you want to remove.

4 Click 

- End -

Users and Roles

VideoEdge NVR provides the ability to configure user-specific credentials. Each user can be assigned a role type which denotes its permissions and lockout options.

You can also configure role permissions for LDAP groups which have been configured on your LDAP server.

Users


Description

The Users page allows management of user credentials for customized user types for the nine default user types i.e. softwareadmin, admin, nvrgroupadmin, operator, snmpuser, support, viewer1, viewer2 and viewer3. The default user types cannot be deleted.

Note:

The NVR's default user types are also the basis of the role permissions for the NVR.

Each user of the NVR should be assigned a separate user account. User accounts should not be shared by multiple users.

New users can be added by clicking . You can assign a bespoke username and password for a new user. The user's role can be selected from the **Role** dropdown list, the following options are available:

- **softwareadmin** - Allows access to the software update page only. This credential is used solely for carrying out software updates and installing camera handler packs. The default password for this role is **softwareadmin**
- **admin** - Allows viewing and editing of the VideoEdge Administration Interface and full functionality of the VideoEdge Client. The default password for this role is **admin**
- **operator** - Allows viewing of the VideoEdge Administration Interface and full functionality of the VideoEdge Client. The default password for this role is **operator**.
- **support** - The support user role is solely for the use of American Dynamics Technical Support.

Note:

User roles viewer1, viewer2 and viewer3 do not provide access to the NVR administration Interface, they only provide access/permissions for use with VideoEdge Client and victor Web LT.

- **viewer1** - Allows full functionality of the VideoEdge Client. Unable to view or edit the VideoEdge Administration Interface. The default password for this role is **viewer1**
- **viewer2** - Allows full functionality of the VideoEdge Client with exception of Analog (Real) PTZ. Unable to view or edit the VideoEdge Administration Interface. The default password for this role is **viewer2**
- **viewer3** - Allows full functionality of the VideoEdge Client with exception of Analog (Real) and Digital PTZ, Still Image Capture and Clip Export. Unable to view or edit the VideoEdge Administration Interface. The default password for this role is **viewer3**



The following user types are for use with the NVR groups functionality only and can not be assigned to custom user credentials:

- **nvrgroupadmin** - This user credential is used for communication between NVRs in a group. The default password for this role is **nvrgroupadmin**
- **snmpuser** - This user credential is used for SNMP communication between NVRs in a group. The default password for this role is **snmpuser**

Configuration/Commands

Create new users, reset user passwords, change default role passwords.

Procedure 3-18 Add New User

Step	Action
1	Select System from the main menu.
2	Select Users andRoles . The Users page displays.
3	Click  The Add New User window opens.
4	Enter the user name in the Username field.
5	Enter the password in the New Password field.
<hr/> Note: With enhanced password validation disabled: There is no minimum length restriction for usernames or passwords. Usernames may only contain upper and lower case letters and the digits 0-9. Passwords may only contain upper and lower case letters, the digits 0-9, space, and the symbols [] () { } \$ # + - _ ~ * % With enhanced password validation enabled additional restrictions are applied, refer to the Roles section for further information.	
6	Re-enter the password in the Confirm Password field.
<hr/> Note: When entering the user name and password note the use of upper and lower case. The user will be required to enter their user name and password as it has been entered at this stage.	
7	Select the role from the Role dropdown.
8	Click 

- End -

Reset a Password


User accounts with admin privileges can reset the password of user accounts which have been created using the Add New User button.

Note:

You do not need to know the current password to complete this function.


Procedure 3-19 Reset a Password

Step	Action
------	--------

- 1 Select **System** from the main menu.
- 2 Select **Users and Roles**.
The Users page displays.
- 3 Select  beside the User name you want to edit the password for.
The edit window opens.
- 4 Select the **Reset Password** checkbox.
- 5 Enter the new password in the **New Password** field.

Note:

It is good practice to choose a password consisting of a combination of upper case letters, lower case letters, numbers and special characters.

- 6 Confirm the new password by entering it in the **Confirm Password** field.
- 7 (Optional) Select a new role from the **Role** dropdown.
- 8 Click 


- End -

Changing the Default Role Passwords

The passwords for the softwareadmin, nvrgroupadmin, operator, snmpuser, viewer1, viewer2 and viewer3 roles cannot be reset. The password can however be changed by a user with admin privileges.

Procedure 3-20 Changing the Default Role Passwords

Step	Action
------	--------

- 1 Select **System** from the main menu.
- 2 Select **Users and Roles**.
The Users page displays.
- 3 Select  beside the User name you want to edit the password for.
The edit window opens.
- 4 Enter the new password in the **New Password** field.

Note:


It is good practice to choose a password consisting of a combination of upper case letters, lower case letters, numbers and special characters.

- 5 Confirm the new password by entering it in the **Confirm Password** text box.

6 Click 


- End -

Remove a User

User accounts with admin privileges can remove user accounts using the  button. Only user accounts which have been created can be removed, default user roles can not be removed from the NVR.

Procedure 3-21 Remove a User

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select System from the main menu. |
| 2 | Select Users and Roles .
The Users page displays. |
| 3 | Select the checkbox(es) next to the users you want to remove. |
| 4 | Click 
A dialog box opens. |
| 5 | Click OK . |
-

- End -

Roles

Description

VideoEdge NVR provides role-based security features that apply to all user accounts assigned with the corresponding role. The Roles page allows configuration of the following role-based security features. These include:

- **Inactivity Lockout Interval** - Number of days of account inactivity after which an account is locked..
- **Failed Login Lockout Policy** - There are three login lockout policies available for use; None, Lockout and Delay. When Lockout is enabled the account will be locked if the account performs the configured number of consecutive failed login attempts. When Delay is selected, the account will be locked in accordance with the configured number of consecutive failed login attempts and subsequently unlocked (i.e., able to log in) after the configured period of time.
- **Auto Logout** - Automatically logs out the account after a configured period of inactivity.
- **Enhanced Password Validation** - If enhanced password security is enabled, the assigned password must meet the following criteria:
 - Password must consist of a minimum of 7 characters
 - Password must not be a duplicate of the previous 3 passwords associated with that credential
 - Password must differ by a minimum of 3 characters from the previously assigned password

- Password must obey at least 3 of the following rules -
 - Must contain an uppercase letter
 - Must contain a lowercase letter
 - Must contain a number
 - Must contain a special character e.g. ? ! # \$ and so on

Note:

By default, these security features are not configured.



Caution

Care should be taken to ensure that you do not lose or forget account passwords when all NVR accounts are set to Lockout. If the passwords for each of the accounts were to become unknown, access to the NVR Administration Interface could be lost.

Configuring Additional Security features on Roles

Configuration/Commands

Configure additional settings on roles.

Procedure 3-22 Configuring Additional Security on Roles


Step	Action
1	Select System from the main menu.
2	Select Users and Roles . The Users page displays.
3	Select the Roles tab.
4	Select  of the role you want to edit. A configuration window opens.
5	Select Lockout from the Lockout Policy dropdown.

Figure 3-5 Lockout Selected

Rolename: admin

Lockout Policy: Lockout

Retry Limit: 3 (1-50) ⓘ

Enable Auto Logout:

Enhanced Password Validation: Disabled ⓘ

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



Enter the number of failed password attempts in the **Retry Limit** field that are required for the account to lockout. (Minimum 1, maximum 50)

Or

Select **Delay** from the Lockout Policy dropdown.

Figure 3-6 Delay Selected

Rolename: admin

Lockout Policy: Delay

Retry Limit: 3 (1-50)

Retry Delay (minutes): 1 (1-4320)

Enable Auto Logout:

Enhanced Password Validation: Disabled

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

Enter the number of failed password attempts in the **Retry Limit** field that are required to cause a lockout or a lockout delay before the user can re-attempt to enter their credentials.

Enter the number of minutes in the **Retry Delay** that are to pass before the user can re-attempt to enter their credentials. (Minimum 1, maximum 4320)

- 6 (Optional) Select the **Enable Auto Logout** checkbox.

Figure 3-7 Auto Logout Selected

Rolename: admin

Lockout Policy: None

Enable Auto Logout:

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

Enhanced Password Validation: Disabled

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

(Optional) Enter the **Auto Logout Interval (minutes)** in the field. (Minimum 5, maximum 60)

- 7 To enable Enhanced Password Validation, select **Enabled** from the dropdown.

- 8 Click 

- End -

Locked Accounts

Description

When an account is locked, the user can no longer access the NVR Administration Interface (Provided this function is permitted by their configured role). The NVR's Lockout Policies also apply to the VideoEdge Client and victor Unified Client.

Note:

Accounts cannot be manually locked.

Should an account be locked or delayed, the account will be unable to access the VideoEdge Client or access the NVR Administration Interface through victor Unified Client or a web browser. A locked account can quickly be identified using the Users table in the Users page; locked accounts are indicated by a locked padlock symbol.

Accounts can be unlocked by a user with either the admin or support role assigned to their account. Accounts can be unlocked directly from the Users table or by using the edit icon located with each table entry in the Users page.


Note:

User accounts which have been assigned the admin or support role can only be unlocked by other admin or support role accounts.

Configuration/Commands

Unlock Locked Accounts.

Procedure 3-23 Unlocking Accounts from the Users Table

Step	Action
1	Select System from the main menu.
2	Select Users and Roles . The Users page displays.
3	Select  in the user credential row you want to unlock. A dialog window opens stating 'This will unlock the account named: xxxx'
4	Click OK .

- End -

Procedure 3-24 Unlocking Accounts using the Edit Icon


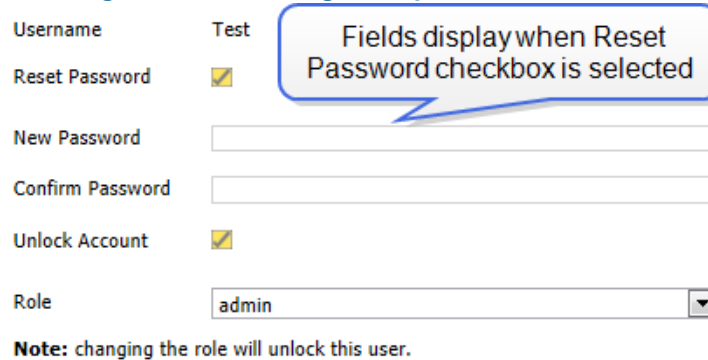
Step	Action
1	Select System from the main menu.
2	Select Users and Roles . The Users page displays.
3	Select  in the user credential row you want to unlock.
4	(Optional for bespoke user credentials) Select the Reset Password checkbox when logged in as an admin or support user to create a new password for the locked user account.

Figure 3-8 Unlocking a Bespoke User Credential



Username Test

Reset Password


New Password

Confirm Password

Unlock Account

Role admin

Note: changing the role will unlock this user.

- 5 Select the **Unlock Account** checkbox to unlock the account.
- 6 (Optional) Select the **Role** from the dropdown if you want to assign a new role to the account.
- 7 Click 

- End -

Linux Operation & Additional Configuration

Overview

This section details the use of the VideoEdge NVR's embedded operating system and additional configuration.

Disable SSLv3 in Apache

Note:

SSLv3 is disabled by default in VideoEdge v4.7+

To mitigate the POODLE (CVE-2014-3566) vulnerability, file configuration steps are provided to disable SSL 3.0 on the VE NVR Apache server.

The POODLE vulnerability allows an attacker to steal information over time by altering communications between an SSL client and its server (also known as a man in the middle attack, or MITM). Successful exploitation of this vulnerability can result in an attacker exposing data encrypted between an SSL 3.0 compatible client and a SSL 3.0 compatible server. Overall, the issue is relatively difficult to exploit. In VE NVR, it can be addressed by performing the following steps:

Note:

This procedure only applies to NVR - external client communications. With this procedure applied, the NVR will still communicate with cameras using SSLv3.

Procedure 3-1 Disable SSLv3 in Apache

Step	Action
------	--------

- | | |
|---|--|
| 1 | SSH to the NVR as VideoEdge, or open an xterm if already logged directly onto the machine. |
| 2 | su root |
| 3 | Enter the root password - nvr |
| 4 | vi /etc/apache2/conf.d/common/adnvr_ssl_virtualhost_common.conf |
| 5 | Change the line
SSLProtocol -ALL +SSLv3 +TLSv1
to
SSLProtocol -ALL +TLSv1 |
| 6 | Restart apache
service apache2 graceful |
| 7 | From a remote machine, verify that the ssl3 protocol is not supported
openssl s_client -ssl3 -connect 192.168.122.210:443 |
| 8 | Expected error response should be:
<i>CONNECTED(00000003)</i>
<i>8031:error:14094410:SSL routines:SSL3_READ_BYTES:ssl3 alert handshake failure:s3_pkt.c:1098:SSL alert number 40</i>
<i>8031:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:534:</i> |

Changing the default password credential used for victorWeb's access to the CouchDB service

The CouchDB database service on VideoEdge has a default configuration using a static predefined username/password pair that is the same for each VideoEdge system. The following procedure provides the steps to uniquely configure the password credential for the CouchDB service.

On the victorWeb host recorder:

Procedure 3-2

Changing the default password credential used for victorWeb's access to the CouchDB service

Step	Action
1	SSH to the NVR as VideoEdge, or open an xterm if already logged directly onto the machine.
2	su root
3	Enter the root password
4	vi /opt/americandynamics/venvr/victorweb/config/victorweb_bind_inaddr_any.ini
5	Change the 'victorweb = password' (where password will either be 'cloud' or a hashed value similar to '-pbkdf2-5lkjhwei8yasdfkl345poqhwe') to your new credentials, using plain text; save the file when done.
6	Open /opt/americandynamics/venvr/victorweb/server/config.js for editing.
7	Change the couchDbAccount/access value from 'http://victorweb:cloud@localhost:5984' to 'http://username:password@localhost:5984' where username/password are the new credentials you entered in plain text in step 5 above; save the file when done.
8	service couchdb restart
9	service adnvr_nodejs restart

Adding 'noquery' to NVR ntp.conf file.

To enhance the security of NVR's NTP configuration, the command 'noquery' should be added to the ntp.conf file.



Caution

Upgrades to 4.6+ will NOT apply this update to existing config automatically, but the 4.6+ NVR will automatically apply this to all subsequent edits via the NVR Administration Interface.

Procedure 3-3 Enable NTP daemon

Step	Action
1	SSH to the NVR as VideoEdge, or open an xterm if already logged directly onto the machine.
2	su root
3	Enter the root password - root
4	# vi /etc/ntp.conf
5	Go to the bottom of the file. You will see entries like these for each configured ntp server server 176.126.242.239 minpoll 4 maxpoll 4 iburst restrict 176.126.242.239
6	Add "noquery" at the end of each "restrict" line, as follows: server 176.126.242.239 minpoll 4 maxpoll 4 iburst restrict 176.126.242.239 noquery
7	Save and exit. Restart the ntp daemon
8	# service ntp restart Shutting down network time protocol daemon (NTPD) done Starting network time protocol daemon (NTPD) done
9	Check that it is running ok # service npd status remote refid st t when poll reach delay offset jitter =====
	kvm1.websters-c 193.190.230.65 2 u 2 16 1 26.842 2.449 1.167
	lithium.constan 206.246.122.250 2 u 1 16 1 87.265 -6.403 0.851
	Checking for network time protocol daemon (NTPD): running
10	Any time the ntp servers are modified from the "Network / General" screen, the changes above will need to be re-applied.

- End -

Disable RC4 ciphers in Apache

Procedure 3-4 Disable RC4 ciphers in Apache

Step	Action
1	SSH to the NVR as VideoEdge, or open an xterm if already logged directly onto the machine.
2	su root
3	Enter the root password - nvr
4	vi /etc/apache2/conf.d/common/adnvr_ssl_virtualhost_common.conf
5	Change the line SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM to SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!RC4:+HIGH:+MEDIUM
6	Restart apache >service apache2 graceful
7	From a remote machine, verify that RC4 ciphers are not supported openssl s_client --ssl3 -cipher RC4 -connect 192.168.122.230:443 openssl s_client -tls1 -cipher RC4 -connect 192.168.122.230:443
8	Expected error response should be: 5683:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c:1098:SSL alert number 40 5683:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:534:

- End -

Secure Session Cookie Flags

Secure session cookie flags force communication through HTTPS and prevent session hijacking. In VideoEdge version 4.7+, this flag is set by default when HTTP is disabled on the admin Graphical User Interface.

Appendix A - User Best Practices

Overview

Organizational security policies should be consulted for appropriate use of the VideoEdge NVR. VideoEdge supports the basic password and computer/terminal security best practices detailed below.

VideoEdge supports these best practices.

Password Security

- It is highly recommended for security reasons that you change all the default passwords for local access and Administration Interface access, especially the NVR's root password.
- Use a combination of lowercase and uppercase letters, numbers and symbols in your password.
- Do not use phone numbers, family names or birth dates.
- Do not share your password.
- Do not write down your password.
- Do not use passwords which form a distinguishable sequence, for example MyNvrP4sswordJan, MyNvrP4sswordFeb and so on.
- Change your password periodically, avoid reusing a previous password.

Computer/Terminal Security

- If you need to be logged in but have to leave the vicinity, lock your computer/terminal.
- Log out of your account if you are leaving your computer/terminal unattended.
- Do not leave your computer/terminal unattended with sensitive information displayed on the screen.
- Ensure no one watches you when you enter your password.
- Do not install software or applications that have not been approved or authorized by your system administrator.
- Site-specific physical and network security policies should be followed to protect against unauthorized access to the NVMS components.