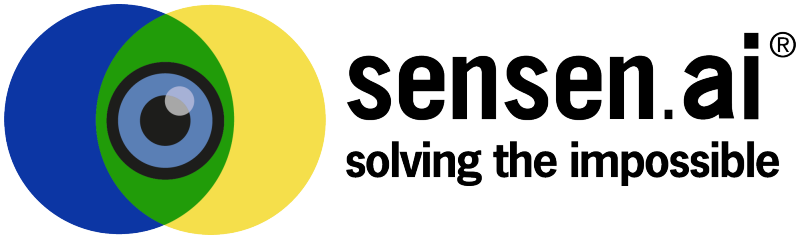

SENTRACK NETWORK INTELLIGENCE

SERVER INSTALLATION AND ADMINISTRATION GUIDE (MILESTONE XPROTECT INTEGRATION)

VERSION 1.8.2

SENSEN
support@snapsurveillance.com
http://sensen.ai

Contents

1. Introduction

This document describes the steps required to install SenTRACK Network Intelligence (SNI) and integrate it with a Milestone XProtect VMS. It also provides a reference for quick setup and commissioning of the SNI server plus common maintenance operations.

1.1 Definitions

This document uses the following definitions:

Term	Meaning
SNI Master Server	In single server deployments, the server running SenTRACK Network Intelligence (SNI); In multi-server deployments (large systems), the main server running SenTRACK Network Intelligence (SNI)
SNI Edge Server	In multi-server deployments (large sites), additional servers running SNI; not used in smaller deployments
Milestone XProtect Management (or Master) Server	The main server for the Milestone XProtect VMS
Milestone XProtect Camera (or Slave) Server	Servers responsible for recording video in the Milestone XProtect VMS
SNI	Abbreviation for SenTRACK Network Intelligence
SNI WebAdmin App Port	Port used by the SNI web application (default 80)
SNI Database Port	Port used by the SenTRACK database (default 5432)
SNI VMS User	The user account SNI uses to access the Milestone XProtect VMS
Installation Directory	The SNI installation directory

1.2 System Architecture

The SenTRACKsystem client-server architecture consists of:

- A SenTRACK Network Intelligence (SNI) Master Server
- Optionally (for larger sites), one or more SNI Edge Servers
- One workstation running theSenTRACK Network Optimizer (SNO) client
- One or more workstations running SenTRACK Client (STC), the SenTRACK Video Operator client. In the case of Milestone, the operator client can run embedded with Milestone's SmartClient.

The initial role of the SNI Master Server is to gather information from the Milestone XProtect Management (or Master) Server; this information includes cameras, camera groups and other information. The SNI Master Server also keeps track of the SNI Edge Servers, if there are any.

For smaller sites (up to 300 cameras, depending on camera resolution), SenTRACK Network Intelligence runs on a single server, the SNI Master Server. This server then accesses video from the VMS during the learning process, and makes the result of learning available to the SenTRACK clients. Figure 1.1 shows this scenario, including the network connections between the SenTRACK server and SenTRACK clients and VMS servers.

NB: The VMS Master Server in the diagrams corresponds to the Milestone XProtect Management (or Master) Server and the VMS Archivers correspond to Milestone XProtect Camera (or Slave) Servers.

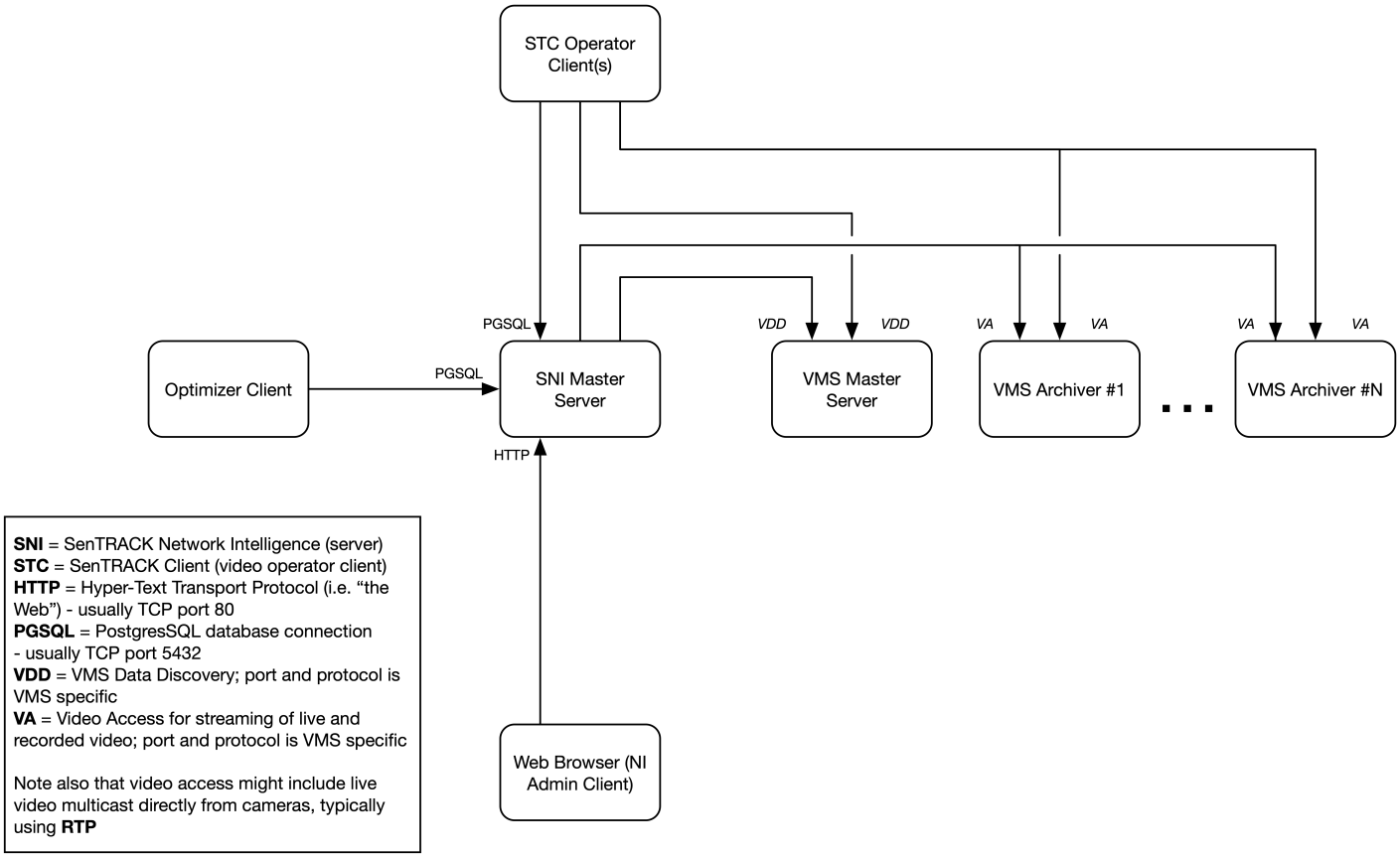

Figure 1.1: Single server architecture

For larger sites (starting at 200 or more cameras, again depending on camera resolution), SenTRACK Network Intelligence (SNI) runs on multiple servers, the SNI Master Server plus one or more SNI Edge Servers, with the SNI Edge Servers assisting the SNI Master Server with the processing required for learning. These servers then access video from the VMS during the learning process. Note that the total number of SNI Edge Servers cannot usefully exceed one per Milestone XProtect Camera (or Slave) Server, and typically there is one SNI Edge Server for every two or three Milestone XProtect Camera (or Slave) Servers. The SNI Master Server collects the learning results and makes these result available to the SenTRACK clients. Figure 1.2 shows this scenario, including the network connections between the SenTRACK servers, SenTRACK clients and VMS servers.

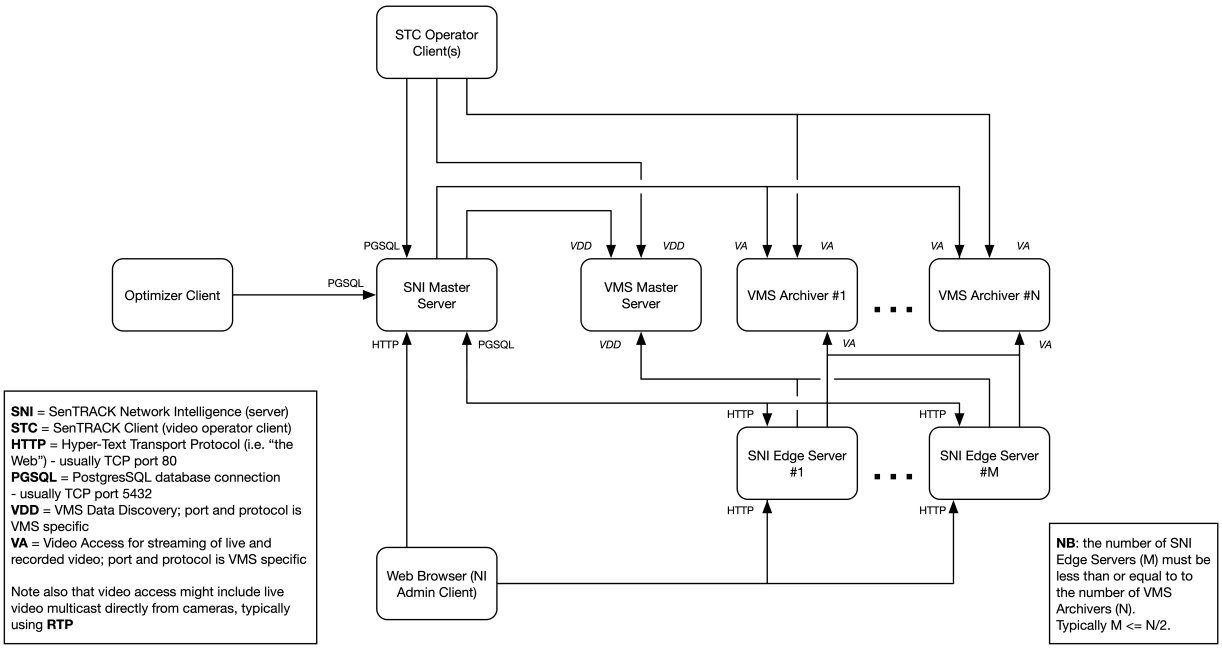

Figure 1.2: Multi-server architecture

2. Quick Start

2.1 Prerequisites

2.1.1 Operating System

SenTRACK Network Intelligence (SNI) is supported on the following platforms:

- Windows 7 64-bit
- Windows 8.1 64-bit
- Windows 10 64-bit
- Windows Server 2008 R2 and later

2.1.2 Disk Layout

It is strongly recommended that SenTRACK Network Intelligence (SNI) is installed on a disk volume (drive letter) that is separate from the volume containing the operating system and the various prerequisite packages (PostgreSQL, Apache and Python).

For small SNI installations (fewer than 200 cameras) the two volumes might be two partitions on the same physical disk or RAID array. For larger SNI installations, and particularly for the SNI Master Server in multi-server installations, it is likely that the disk volumes will be on separate RAID arrays.

2.1.3 Time Synchronisation

SenTRACK Network Intelligence (SNI) servers must utilise the same time source as the VMS and synchronise regularly. Any associated SenTRACK Client (STC) workstations must also synchronise regularly to the common time source. If possible all cameras should also be synchronised to the common time source.

2.1.4 Multi-streaming Setup

SenTRACK Network Intelligence (SNI) is able to make use of the live multi-streaming capability of Milestone XProtect Advanced (Expert or Corporate) to learn from low-resolution streams and doing so can greatly reduce the SNI server workload (or equivalently increase the server capacity in terms of number of channels). It is preferable to set up multi-streaming (using the Milestone XProtect Advanced management client) before connecting SNI to the VMS.

Details of how to set up secondary streams are given in the Milestone XProtect Advanced Administrator's Manual; as of Milestone XProtect Advanced 2015 the relevant sections are Settings tab (devices), which describes how to configure stream resolutions and other properties and Streams tab (devices), which describes how to associated camera streams with streams made available by the VMS.

Properties for the extra streams should be:

- Resolution should be the same aspect ratio as the main live stream and in addition both width and height should be at least 120 pixels (i.e. at least 120 pixels on the "short" side), the best choice for

SNI's purposes is the smallest resolution that satisfies both the aspect ratio and minimum pixels constraints;

- Frame rate should be at least 8 FPS, the best choice for SNI's purposes is exactly 8 FPS;
- Compression type can be MJPEG or MPEG4/H.264, the better choice for SNI's purposes depends on the efficiency with which the server can decode the video (typically this is MJPEG but in recent servers it may be H.264);
- The "Live Mode" for the extra stream should usually be set to "When needed" and the additional stream should not be the default;

SNI will automatically have access to all extra streams established prior to the next step. When streams are added subsequently (including when new cameras are added) or changed in Milestone XProtect VMS there are additional steps that need to be undertaken to make the streams available to SNI, see Section 3.9.2.

2.1.5 Power Plan (Windows 7 Only)

This step only needs to be performed if SenTRACK Network Intelligence (SNI) is to be installed on a computer running the Windows 7 Operating System. The default power plan for Windows 7 is "Balanced", which puts the computer to sleep after 30 minutes without user activity.

To prevent this from happening:

1. Click Start ->Settings ->Control Panel ->Power Options
2. Click the "Show additional plans" text
3. Select the "High performance" option
4. Click the "Change plan settings" link for the High performance plan
5. Set the "Put the computer to sleep" option to "Never"
6. Click "Save changes"
7. Close the Power Options window

2.1.6 Windows Media Player

If Windows Media Player has been uninstalled from Windows it must be reinstalled.

2.2 Configure Milestone XProtect VMS

2.2.1 Determine the Authentication Scenario

Customers deploying SenTRACK Network Intelligence (SNI) will be using one of three distinct authentication scenarios depending on whether Microsoft Active Directory (AD) is in use, and if so, how it is used. The three scenarios are as follows:

1. *No AD* - either AD is not being used at all or both the SenTRACK Network Intelligence server(s) and the Milestone XProtect VMS server(s) are outside the AD domain;

2. *SNI Outside AD* - the SNI server(s) are outside the AD domain but the Milestone XProtect VMS server(s) are within the AD domain;
3. *Full AD* - both the SNI server(s) and the Milestone XProtect VMS server(s) are within the AD domain;

Whichever of these scenarios applies will affect how authentication (user accounts) should be set up in later steps, in particular:

- the Milestone XProtect VMS user account that the SNI servers use to access the Milestone XProtect VMS servers (see Section 2.2.2);

and in some cases also:

- the Windows user(s) as which the SNI services run on the SNI servers.

2.2.2 Configure a Milestone XProtect VMS User

The SenTRACK Network Intelligence (SNI) services running on the SNI servers require authenticated access to the Milestone XProtect VMS servers. This is achieved via a user account within the Milestone XProtect VMS system. Typically a new user is created just for this purpose, although it is also possible to re-use a suitable user account that already exists within the Milestone XProtect VMS system.

The access required by the SNI services includes the following:

- access to information about cameras and groups within the Milestone XProtect VMS system. This should include access to all cameras and groups that are to be used within the SNI system (which can if required be a subset of the cameras and groups in the Milestone XProtect VMS system, if for some reason there are cameras and/or groups that should be excluded from the SNI system;
- access to live video from the cameras as above;
- likewise, access to recorded/archive video.

In particular, the SNI system does not require any access to make changes to the Milestone XProtect VMS system. This means that whilst an administrative account (with full access) has sufficient access to to support SNI, such an account actually has more access than is necessary, and a more restrictive account may be preferable.

Now, within Milestone XProtect VMS there are two types of users:

- *Windows Users* - which may also be Active Directory (AD) users if AD is in use; and
- *Basic Users* - which exist purely within the Milestone XProtect VMS system.

Referring to the possible authentication scenarios in Section 2.2.1:

1. in the *No AD* and *SNI Outside AD* scenarios, both types of users can bu used;
2. in the *Full AD* scenario, it may be preferable to use a Basic user as this is much less complicated. If a Windows user (which in this case will be an AD domain user) must be used then it will depend on the details of the AD configuration and advice should be obtained from support channels as to how to do this.

2.2.3 Install Milestone SmartClient and Verify Configuration

On the SenTRACK Network Intelligence (SNI) server(s), install the Milestone SmartClient and log in to it as the designated SNI VMS User, then verify that all required cameras are available for both live view and archived playback. This should also be performed on the SenTRACK client workstation(s), although this can be done after installation of SNI.

2.2.4 Verify Critical Server API Functionality

On the SenTRACK Network Intelligence (SNI) server(s) use a web browser to verify access to critical Milestone XProtect VMS API functionality.

In all cases, access to the URLs given below is subject to authentication. This means that the first time a URL is accessed the web browser will prompt for username and password; use the SNI VMS User (per Section 2.2.2) to login. Some web browsers will attempt first to login as the current Windows user, and if this succeeds (i.e. the current Windows user is a valid VMS user) then there will be no authentication prompt.

If using Milestone XProtect Advanced (Expert or Corporate), the URLs to check (with `server-addr` being the hostname or IP of the XProtect Management Server) are as follows:

- `http://server-addr/ServerAPI/ServerCommandService.asmx`
  This should produce a page headed “Server Command Service” and with first line “The following operations are supported. For a formal definition, please review the Service Description.”, followed by a long list of links.
- `http://server-addr/rcserver/systeminfo.xml`
  This should produce an XML document. Near the top of the document there should be a “userid” tag containing the username of the account used to login, in the form:
  `<userid>server-addr\username</userid>`

If using Milestone XProtect Standard (Professional or Enterprise), the URL to check (with `server-addr` being the hostname or IP of the XProtect Master Server) is:

- `http://server-addr/systeminfo.xml`
  This should produce an XML document. Near the top of the document there should be a “userid” tag containing the username of the account used to login, in the form:
  `<userid>WinNT://server-addr/username</userid>`

NB: certain web browsers (or versions thereof) are not able to perform Windows authentication with Milestone XProtect Standard (Professional or Enterprise). If authentication fails, try an alternative web browser.

2.3 Install SenTRACK Network Intelligence

Install the SenTRACK Network Intelligence server by running the SenTRACK Network Intelligence Installer. If the Windows User Account Control prompt appears, select Yes to proceed with the installation.

Select “Next” to continue past the Welcome screen.

The licence terms must be accepted in order to proceed by selecting “I Agree”. Then, any dependencies not already present on the server will automatically be installed - most of this occurs silently, but some

user interaction may be required.

2.3.1 PostgreSQL Dependency

The PostgreSQL installer asks for the administrator password to be set. You may use any password, but this password must be recorded because the SenTRACK Network Intelligence system uses it to configure the database.

Proceed through the installation using the default options except:

1. Database password must be entered and should be recorded as it will be required by the SenTRACK Network Intelligence installer.
2. TCP port 5432 (and UDP port 5432) are registered with IANA (the Internet Assigned Names Authority) as being for the use of the PostgreSQL Database. See:

   www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

   for details.

   SenTRACK Network Intelligence uses the PostgreSQL Database and defaults to the use of this port for its assigned purpose.

   Unfortunately various other software packages also make use of this port, generating a conflict. If such other software is running at the time the PostgreSQL Database installer is run (either as part of the SenTRACK Network Intelligence installer or separately) then the conflict will be detected and PostgreSQL will choose a different port (typically it will chose 5433). This alternative needs to be noted as it will be needed later.

   There is a further complication if the conflicting software is not running at the time PostgreSQL Database installer is run. In this case PostgreSQL has no way to know about the port conflict and will use its normal registered port (5432). If the later conflicting software later tries to run it will likely fail. Therefore the installation/administration guides of all other third-party software packages installed on the SenTRACK Network Intelligence server(s) need to be studied to ascertain whether they attempt to use port 5432, and if so the PostgreSQL Database installer should be directed to use an alternative port (e.g. 5433).
3. De-select the option to run Stack Builder. If you accidentally continue past this point it is safe to just cancel the installation and exit.

2.3.2 Python Dependency

If the Python dependencies cannot be installed successfully (or if a previously installed Python system ceases functioning) then a likely cause is a generic Windows issue known as a “Side-by-Side Configuration Error”. When this problem occurs it is likely that error messages related to “side-by-side” will appear in the Windows Event Viewer. Additionally if one runs the “python.exe” program (typically located in C:\Python27\python.exe) and/or the “pythonw.exe” program in the same directory, then if this issue has occurred it will display a message indicating “this application failed to start because side-by-side-configuration is incorrect”.

According to Microsoft:

> “Most Side by Side configuration errors are caused by missing C++ runtime components or corruption.”

The fix is to download and reinstall the Visual C++ Redistributable Packages. There are several of these (one for each release of Microsoft Visual Studio) and also distinct versions for x86 (32-bit) and x64 (64-bit) operating systems. The SenTRACK Network Intelligence server(s) must be running a 64-bit OS so the 64-bit versions are required.

Go to:

http://www.microsoft.com/downloads

and search for:

"Visual C++ Redistributable x64"

This will generate a list of downloads that should be installed and one of these will fix the problem (which one it is can vary).

2.3.3 Server Types

As described in Section 1.2 a SenTRACK installation consists of one SNI Master Server plus zero or more SNI Edge Servers. The SNI Master Server must be installed before any SNI Edge Servers are added.

SNI Master Server Installation

1. Enter the licence details you have been provided in the next prompt, and select "Next".
2. On the SenTRACK PostgreSQL Database Setup page, leave the server as the default.
3. Enter the password from Section 2.3.1, step 1 in the "PostgreSQL Administrator (postgres) Password" field.
4. Enter the database port used when installing the SNI Master Server (Section 2.3.1, step 2 during the installation of the SNI Master Server) in the "Port" field and select "Next".
5. Enter a secure password in the "Master Password" field and record it. This password is used when deploying multi-server installations (refer to Section 2.3.3 for details). Select "Next" when complete. Proceed with Section 2.3.4.

SNI Edge Server Installation

1. Enter the SNI Master Server details (hostname or IP address) in the database server field.
2. Enter the password from Section 2.3.3, step 5 in the "Master Password" field.
3. Enter the port from Section 2.3.1, step 2 in the "Port" field and select "Next". Proceed with Section 2.3.4.

2.3.4 Installation

1. In the SenTRACK Network Intelligence User Setup prompt, enter the username and password of the SNI VMS Userconfigured in Section 2.2.2 and select "Next".
2. Choose the Installation Directory, following the scheme outlined in Section 2.1.2.

2.3.5 Installation Complete

Select “Finish” to close the installation program. If a Windows Security Alert appears during the installation, it indicates that the Windows Firewall is enabled and some extra configuration is required:

- Open the Windows Firewall to allow Apache to communicate with the appropriate networks via the default TCP port of 80
- Open the Windows Firewall to enable PostgreSQL to communicate with these same networks via the default TCP port of 5432

2.4 Start SenTRACK Network Intelligence

To commence the configuration process, the SenTRACK Network Intelligence (SNI) server(s) should have been installed installed:

1. On the SNI Master Server, open a web browser (e.g. Internet Explorer) and browse to http://localhost.
2. You should see the “Create administrator account” page for the SNI system (Figure 2.1). If this is not what you see, even after forcing the browser to refresh the page (CTRL+F5), please refer to Section 2.4.1 for steps to identify and resolve the problem.
3. Set a SNI administrative username and password. These details should be noted as they will be required for future login.
4. Once the new account has been created, the “Setup” page is displayed.

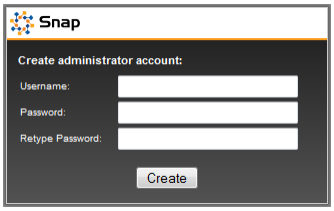

Figure 2.1: Initial view after installing SenTRACK Network Intelligence (SNI)

2.4.1 Altering the Apache HTTP Server Configuration to Avoid Port Conflict

If you do not see the “Create administrator account” page described in Section 2.4 it indicates a problem with the Apache HTTP server. A common reason for Apache not to work is that during the installation there was a warning about Port 80 being in use by another process. To fix this there are two possible solutions:

1. Port 80 may conflict with IIS (Microsoft Internet Information Services) if it is installed. If IIS is unused, uninstall it then start the Apache service through Windows Administrative Tools → Component Services.

   In Windows 10, there is a variant of IIS called “World Wide Web Publishing Service”. This will also use port 80 if it is running. If this service is unused it can be stopped in the “Services” tool: stop the service and also change its properties so as to start manually rather than automatically.

2. Modify the Apache configuration file and change the port. You will need to choose a port other than 80 for the SNI WebAdmin App to use; the port you choose must not be used by any other service.

Use netstat (Appendix C) to identify the ports currently in use.

Having chosen the port you will use you need to update the Apache configuration file. Port 8080 is a common choice since it is the standard alternative HTTP port. Note however that some versions of Milestone XProtect make use of port 8080 for internal communications, in which case you cannot use that port. Netstat will show clearly whether port 8080 is currently in use.

The Apache configuration file can be found in:

```
C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf
```

In the file, locate the line that contains “Listen 80” and change the 80 to a free port on your host. For example, “Listen 8080”.

Once done, start the Apache service named Apache2.2 through Windows Administrative Tools → Component Services.

NOTE: Re-running the SenTRACK Network Intelligence installation will modify and replace the httpd.conf file. It is up to you to ensure you re-apply any manual modification you may have made to the port number.

2.5 System Setup

This section provides details on how to setup the SenTRACK Network Intelligence (SNI) system and start the learning process. This section describes how to:

1. Configure capacity and other properties of the SNI server(s).
2. Authenticate with a remote VMS and discover its configured channels.
3. Select and activate channels (cameras) from those in the VMS.
4. Optionally, select and activate groups (of channels/cameras) from those in the VMS.
5. Optionally, organize the active channels into distinct sites.
6. Create a schedule to undertake learning on active channels.

2.5.1 Servers

The “Servers” tab is used to manage the server(s) in the SenTRACK Network Intelligence system.

Ensure that the expected SNI Edge Servers are present in the Servers table (Figure 2.2). To alter the properties of a particular server:

1. Click the name of the server
2. In the left column enter the following information:
3. Click the Update button

Field	Description
Max Channels/Archiver	Maximum number of streams to retrieve from any one Milestone XProtect Camera (or Slave) Server
Max Channels/Server	Maximum channels processed on the server
Perform Processing	Time range during which the server is active

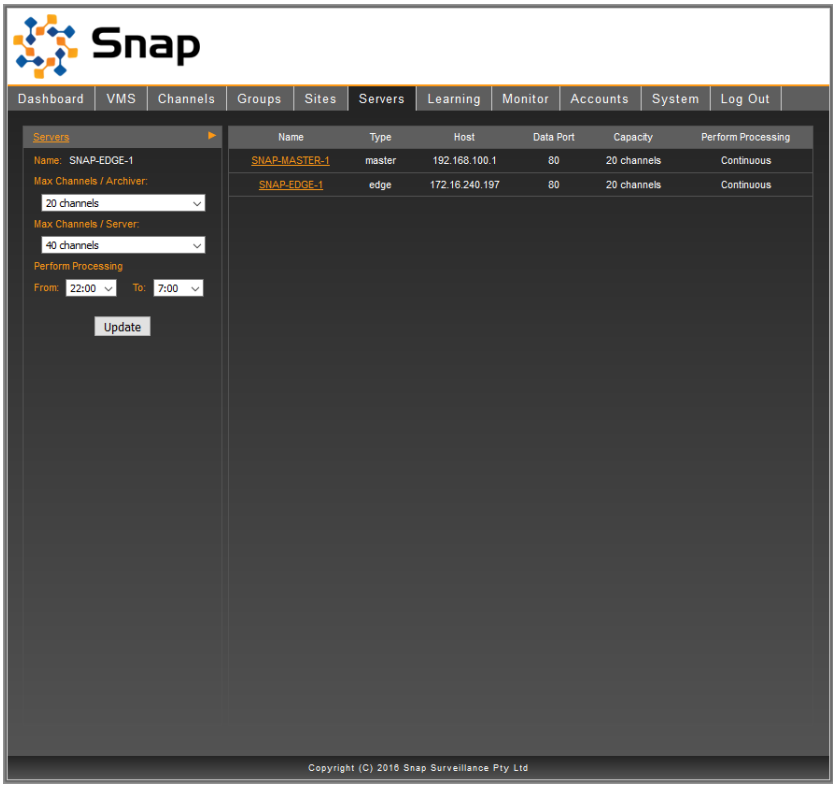

Figure 2.2: Configuring SenTRACK Network Intelligence servers

2.5.2 VMS Setup

The “VMS” tab is used to manage the connection of SenTRACK Network Intelligence (SNI) to the VMS system.

Note: Ensure the low resolution streams have been configured before continuing (Section 2.1.4).

To connect to the VMS server:

1. Enter the following information in the VMS sub-section (Figure 2.3):

Field	Description
Type	VMS type, select Milestone XProtect VMS from the drop-down list
Host Address	Address of the Milestone XProtect Management (or Master) Server (IP or Fully Qualified Domain Name, must be globally resolvable - do not use loopback IPs or names like localhost)
Port	TCP port of the Milestone XProtect Management (or Master) Server (default is 80)
Username	Username for the SNI VMS User (Section 2.2.2)
Password	Password for the SNI VMS User (Section 2.2.2)

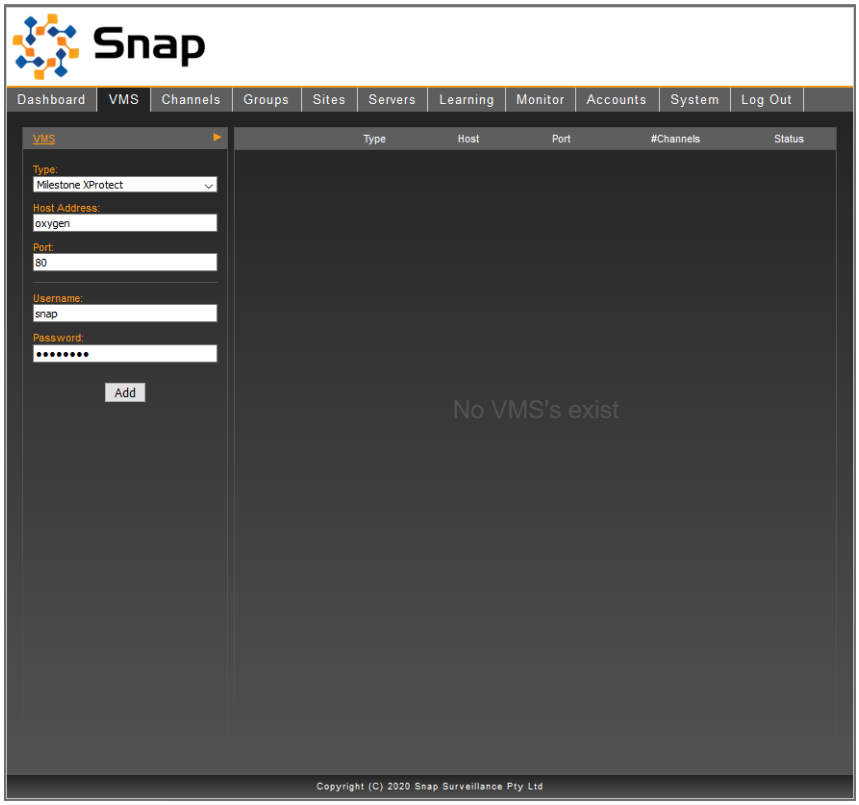

Figure 2.3: Setting up a VMS

2. Click Add. At this point, the system attempts to authenticate with the remote VMS and then discover its configured channels and the groups they belong to:

   (a) The “Status” should update to “OK” once the SNI Master Server can successfully authenticate using the provided credentials.

   (b) The “#Channels” status should display the number of channels available to the SNI system. This should be less than or equal to the number of channels in the VMS.

   (c) The “Inactive Channels” link from the left side bar should also indicate the number of newly discovered channels.

Note: This process can take several minutes if there are many hundreds (or thousands) of cameras.

2.5.3 Channel Activation

The “Channels” tab is used to manage channels (cameras).

All newly discovered channels are initially inactive. Channels are included in the SenTRACK Network Intelligence (SNI) system by adding them to the topology. In addition, you can enable learning for these cameras in the same step.

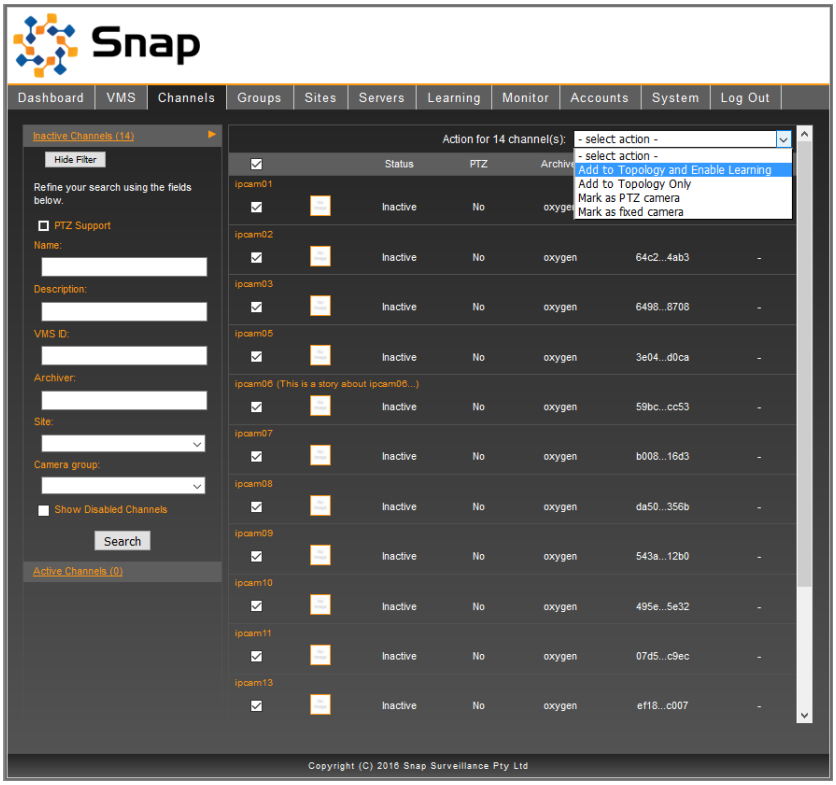

Figure 2.4: The list of inactive channels

Click on the “Inactive Channels” link from the left side bar to display all the inactive channels (Figure 2.4).

1. Select the channels to be activated.
2. In the drop down box that appears in the top right of the main view, select “Add to Topology and Enable Learning”. The selected channels will then transition into the “Active Channels” view.
3. Select the “Active Channels” link from the left side bar to display all the activated channels (Figure 2.5).

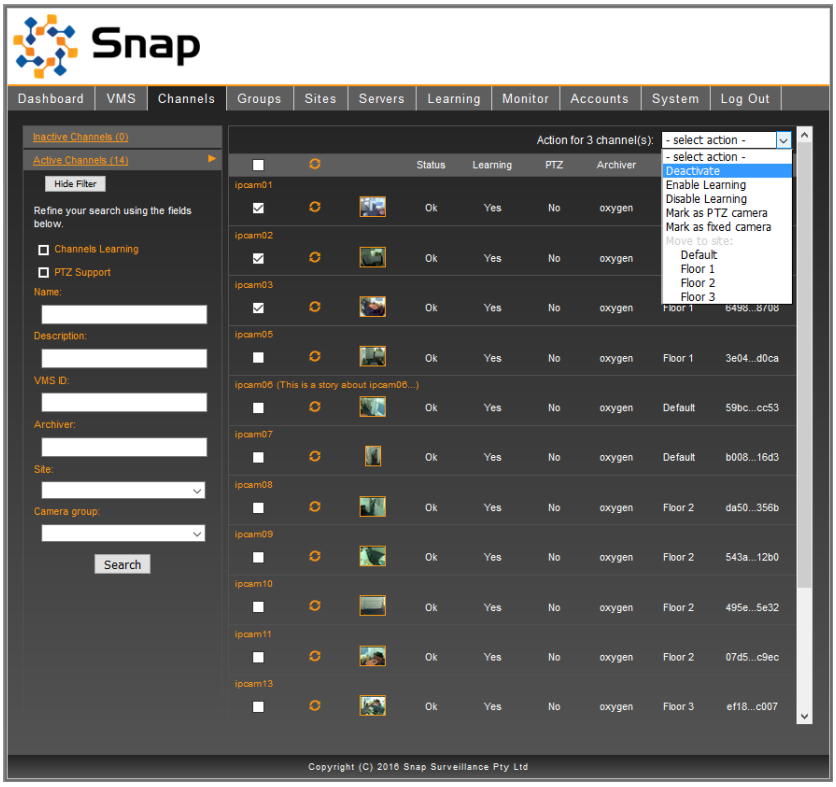

Figure 2.5: The list of activated channels

During the activation process, the SNI Master Server attempts to retrieve an image from each of the selected channels. The status column indicates the progress of each channel and the section title shows the overall progress while the retrieval is occurring. Hovering the mouse pointer over the image will display an enlarged version of the channel image.

Before proceeding, wait for the status of all channels to be OK. Failures during image retrieval typically indicates a problem with the affected channel that needs to be fixed before reliable learning can commence. To update the sample image for a channel press the corresponding circular refresh arrows (Section 3.10.2).

2.5.4 Disable Learning for Unsuitable Channels

Certain kinds of channels (cameras) do not benefit from the SenTRACK Network Intelligence automatic learning, including:

- PTZ cameras that roam around and do not return automatically to a home position;
- any other cameras lacking a single dominant field of view in which the majority (more than 90 percent) of time is spent.

After activation, these channels should be set to “Disable Learning” using the menu as shown in Figure 2.5. The result of this will be that the channels (cameras) are visible to video operators, but no links to other cameras will be learned (however links can be made manually using the SenTRACK Network Optimizer tool)

2.5.5 Group Activation

The “Groups” tab is used to manage groups of channels (cameras).

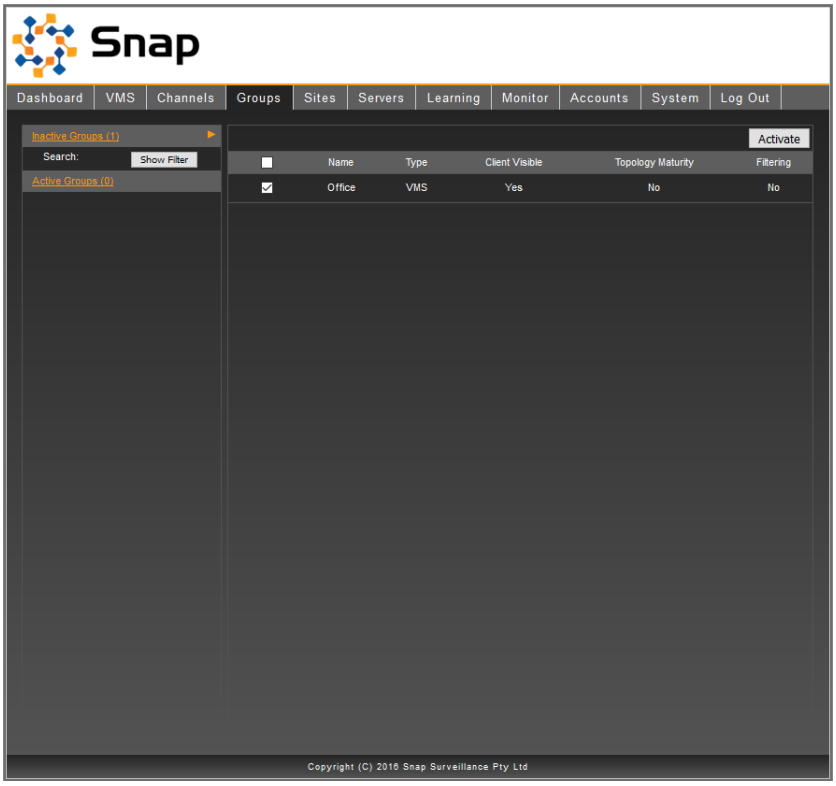

Figure 2.6: Activating group imported from the VMS

If the VMS has organized cameras into groups, then these groups will be imported as initially inactive and listed in the Inactive section of the Groups tab. The activation process is a simplified version of the process for activating channels. Once activated, the groups are available to be used in SenTRACK for various purposes (see Section 3.2 for more information about groups).

2.5.6 Sites

The “Sites” tab is used to manage distinct Sites within the SenTRACK Network Intelligence system. Sites can be used for a variety of purposes; typical purposes include:

- Completely distinct locations, such as distinct facilities/campuses within a large enterprise;
- Distinct parts of very large facilities and with minimal connection between the parts, such as the different terminals within a major airport.

Sites are a powerful concept with three main benefits applicable to large multi-site systems:

- *Enabling Progressive Rollout of Large Systems* - this means that instead of having to wait for the whole system to be ready before providing customer access, it is possible to proceed Site by Site, with customers gaining access to Sites progressively as they become ready for use. In addition to bringing forward the first point at which customers can start to use SenTRACK, this also has benefits to customer training and may help in levelling integrator/technician resource requirements for a large rollout;

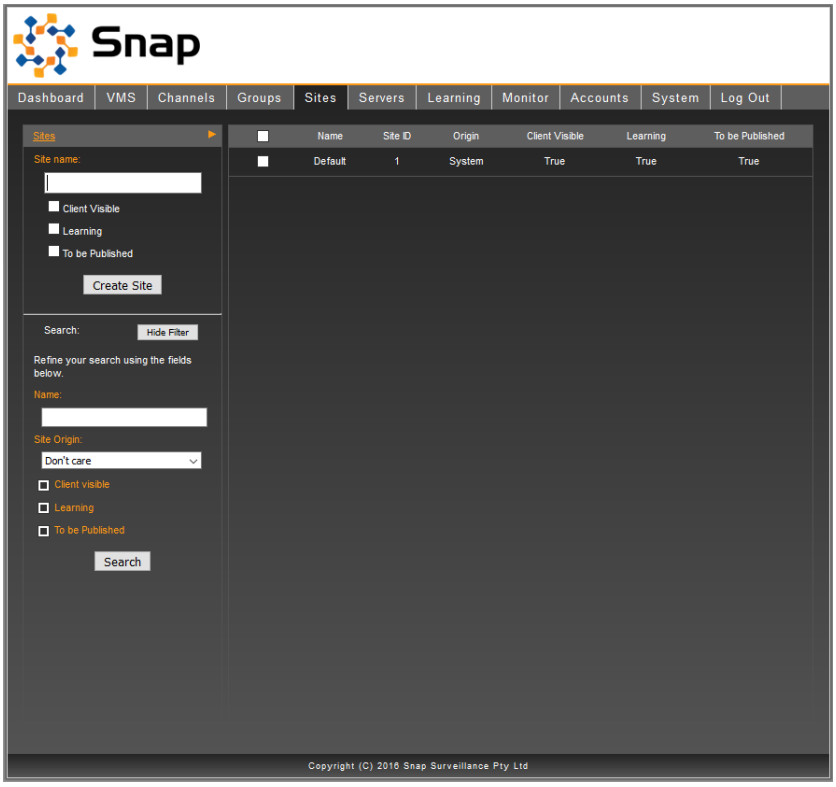

Figure 2.7: Sites tab

- *Speedup of the Learning Process* - with multiple Sites, the SenTRACK Network Intelligence learning process ignores the possibility of links between cameras belonging to different Sites. This means there is simply less learning required and in combination with appropriate use of the "learning" flag on the Sites, results in a speedup of the time required when compared to learning for all the cameras without division into Sites;
- *Organization and Simplification when using SenTRACK Network Optimizer (SNO)* - the SenTRACK Network Optimizer (SNO) tool is used after the learning process has completed. SNO has been structured to work on one Site at a time (it can switch between Sites at any time if desired) and this allows people using SNO to focus their attention, thereby being more productive.

Initially, all active channels (and any subsequently activated channels) are placed into the default Site. The default Site is initially named "default": this can be changed in the Sites tab, by selecting the Site, editing site name that appears to the left and saving the change. If you're using sites you'll probably want to use the default site for the site with the largest number of cameras (and rename it accordingly).

The Sites tab can also be used create and delete Sites (note that the default Site can't be deleted).

It is strongly recommended that if Sites are to be used then they are set up at this point. In particular, if Sites are used then each camera should be assigned to its proper Site before learning is commenced for that camera.

Only cameras that have been activated can be assigned to Sites. If it is preferred to set up only a few Sites initially, then then the recommended approach is to activate only the camera belonging to those Sties (rather than activating all cameras and leaving most of them in the default Site)

See Section 3.3 for details about Sites, including the properties that can be set on them.

2.5.7 Sites and Learning

Note that this step is only relevant when a SenTRACK Network Intelligence (SNI) system is divided into Sites.

Per Section 3.3, there is a “learning” property that can be set on Sites which control whether (and when) the Site is included in the learning process. Correct use of the “learning” property is important to achieve speedup of the learning process, which is one of the major benefits of Sites as discussed previously.

Recommendations for the use of this “learning” flag are as follows:

- it is strongly recommended that only a limited number of Sites are set to “learning” at a given time. The rationale is that is more efficient (and sometimes much more efficient) to learn a small number of Sites at “full speed” and then move on to a new subset of the Sites (learning again at full speed) instead of learning all Sites at reduced speed;
- to determine the Sites to set “learning” at a given time the following information is needed:
  - the total capacity (channels) of the SenTRACK Network Intelligence system, which is the sum of the capacities of the SenTRACK Network Intelligence servers (see Section 2.5.1); and
  - the number of learning channels (cameras) within each Site (ignoring any channels for which learning is disabled, see Section 2.5.4).

  Using this information, the recommended approach for selecting Sites to be learning simultaneously is a set set of Sites for which the total number of learning channels (cameras) on those Sites is less than 120 per cent of the total channel capacity. The fastest possible learning occurs when the total number of learning channels on those Sites is less than or equal to total capacity, but allowing up to an extra 20 per cent may allow an extra Site to included, and having a total less than the capacity is wasteful.

  Using this approach, one can plan a staged learning process consisting of a number of “rounds” where for each round a distinct set of sets in learned. The idea is for the first round to complete learning for a set of Sites, which are then available for use. One then disables learning for the first round Sites and then moves on to the second round (enabling learning for its Sites), which a different set of sites, and completes learning for them, and so on.

  There are two important special cases:

  - there may be large Sites for which the number of channels exceeds the total capacity by more than 20 per cent. Each of these needs to be learned in a round by itself;
  - conversely, there may be very small Sites (e.g. fewer than 10 channels, for example a small branch office) for which it may be reasonable to avoid learning completely (and instead just create all links manually using SenTRACK Network Optimizer). If this policy of not learning very small Sites is adopted, then these Sites should not be included in any round, and should have learning permanently disabled.

If Sites are used, then before proceeding to the next step it is important to ensure they are set up, including ensuring that the Sites in the first round of learning have the correct channels (cameras) and only those first round Sites have learning learning enabled.

2.5.8 Creating a Learning Schedule

The “Learning” tab is used to create learning schedules and review learning progress.

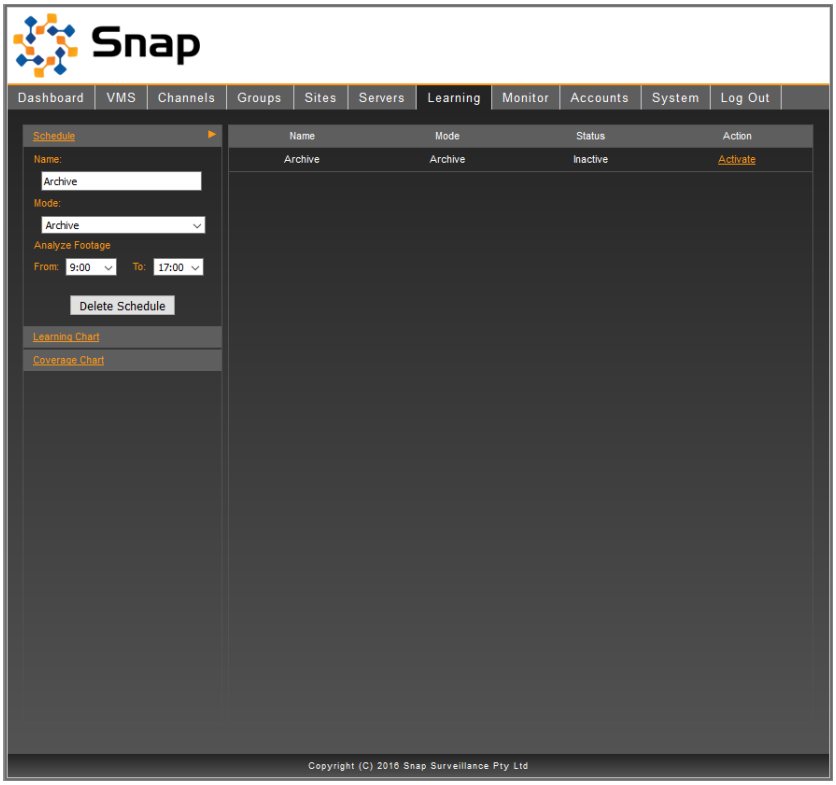

Figure 2.8: Creating a Schedule

A schedule needs to be created so that processing can begin for all channels that have been configured for learning:

1. Click the “Learning” tab.
2. Click the “Schedule” link from the left side bar to create a schedule (Figure 2.8).
3. Create a new schedule by entering the following information:

Field	Description
Name	Choose a name for easy reference
Mode	Live (recommended) or Archive
Analyze Footage	Time range of footage to analyze *

*Archive mode only. Footage is assumed to be available for the configured times.

4. Click “Create Schedule”
5. Start the schedule by clicking “Activate” in the “Action” column

The system will now schedule learning for all channels configured to learn. By clicking on the “Dashboard” tab, you can verify the state of the running system.

2.6 Verification and Next Steps

To verify that the SenTRACK Network Intelligence (SNI) system is working correctly:

1. Select the “Dashboard” tab and check that “Learning” is “Active”.
2. Check that the number of “Learning Channels” matches the server capacity.
3. Select the “Monitor” tab and verify that each channel has a non-zero value for “FPS” when running (see Section 3.12). Ideally “FPS” should be between seven and eight, but it will of course be limited by the FPS of the cameras’ video streams.
4. Check that the CPU load on the SNI server(s) is below 80 percent; if not, deactivate learning and use the “Servers” tab to reduce the capacity of the servers with too high a CPU percentage.
5. Also verify that the Milestone XProtect VMS is handling the load from serving video to SenTRACK Network Intelligence. if required, the load can be reduced using the “Max Channels / Archiver” setting in the “Servers” tab.

Next steps:

1. Create a user account with privileges to access SenTRACK Network Optimizer (SNO)(Section 3.8.1).
2. Create a user account with privileges to access SenTRACK Client (STC)(Section 3.8.1). This can be the same account as for SNO if desired. however, in this case the account must be present (with a matching password) in the Milestone XProtect VMS.
3. Log in to SNO . A dialog box should appear:
   - If it states that “No learning is available” just press the OK button.
   - If it states “There is learning available. Would you like to import it?”, just press the Cancel button.
4. Confirm that all groups from the VMS have been imported (these will be read only in SNO).
5. Switch to Topology Layout View and create an indirect manual link between two cameras using the Add Indirect Manual Link button in the toolbar on the left.
6. Publish the topology.
7. Log in to STC, jump to one of the cameras you manually linked (using the camera list) and verify that the other camera is in that camera’s peripheral set, and that live and recorded video plays correctly.
8. Log out of SNO and STC.
9. Install the Milestone SmartClient plugin following the instructions in Appendix D.
10. Once the “Last Update” time has changed (in the Dashboard), log in to SNO again and this time choose to import the new learning data. This initial learning data will likely not be mature: refer to Section 3.4 to determine when the learning is mature.
11. Ensure that the “Last Calculation”, “Last Merge” and “Last Update” times (on the “Dashboard” tab) are updated periodically (approximately every 30 minutes for a Live schedule).

3. Reference

3.1 The Dashboard

The Dashboard provides details of the running system all in one convenient location (Figure 3.1). The left side bar displays useful information for the health of the SenTRACK system and any configured SenTRACK Network Intelligence (SNI) servers. The main view provides more in-depth information about the learning status of each site. View the Dashboard regularly to obtain a health check of SNI.

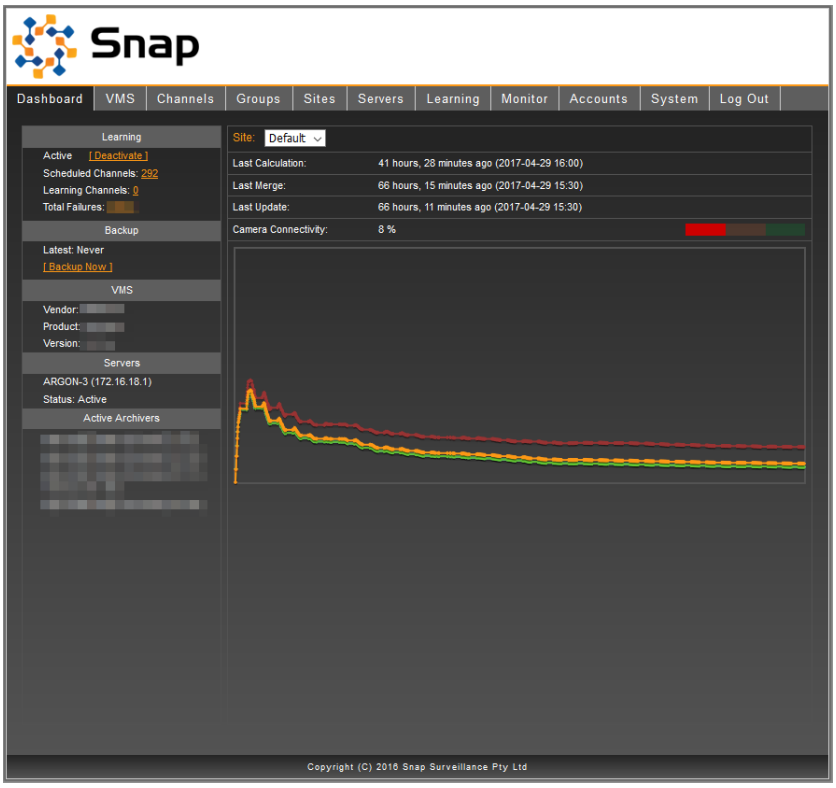

Figure 3.1: The Dashboard page

3.2 Camera Groups

Camera groups are imported from the VMS during setup, and can also be created in SenTRACK Network Optimizer (SNO). The origin of each group is displayed in the “Type” column of the Groups Setup page (Figure 3.2).

Once all groups have been created, they can be configured in SNI. There are three attributes that can be set for a group:

Attribute	Description
Filtering	Remove autolinks emanating from the group
Topology Maturity	Include the group in topology maturity calculations
Client Visible	The group is visible in the SenTRACK clients and hence visible to operators

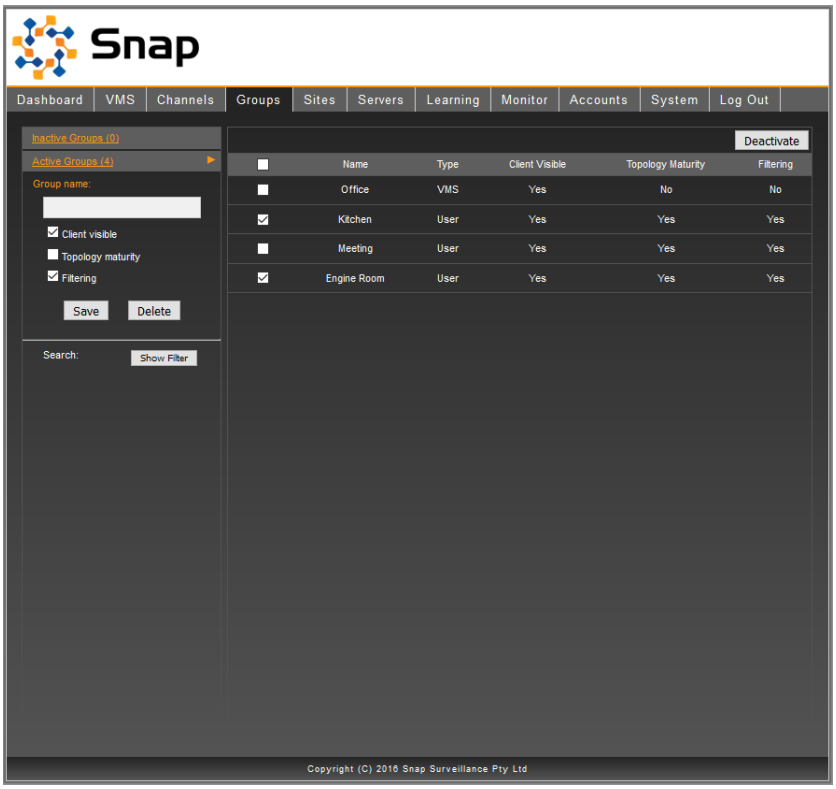

Figure 3.2: Camera group configuration

3.3 Sites

Sites can be created in SNI. Note that the “Default” Site is automatically created by the system. To create a Site:

1. Enter the name of the Site
2. Select the desired Site attributes
3. Press the “Create Site” button

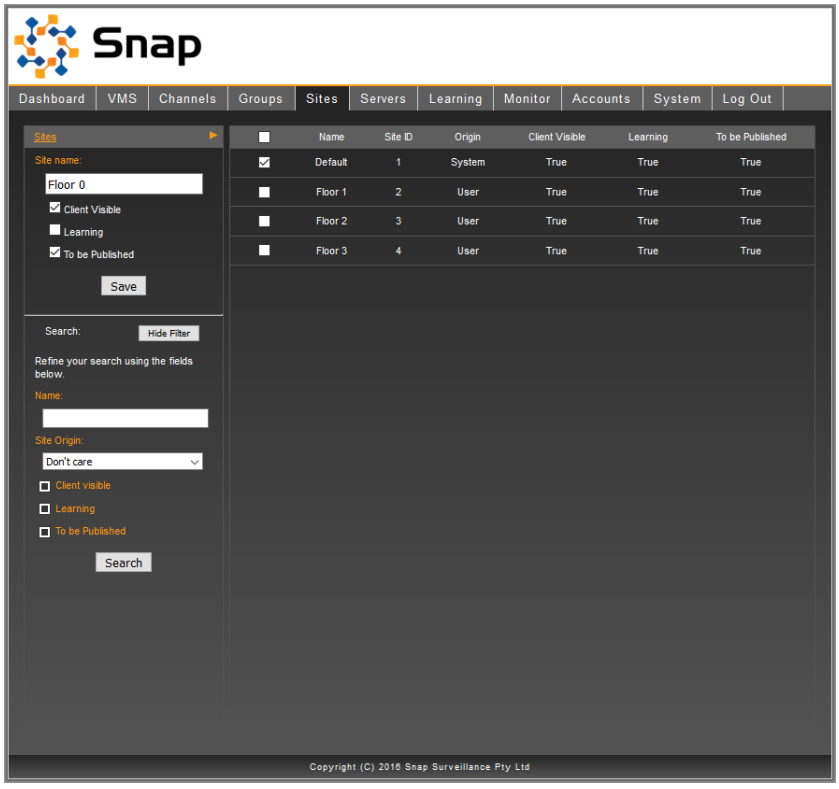

Figure 3.3: Changing Site attributes

There are three attributes that can be set for a Site:

Attribute	Description
Client Visible	The Site is currently visible in the SenTRACK Network Optimizer (SNO) tool. This should almost always be set to True.
Learning	The Site is currently included in the automatic learning process (see]2.5.7 for a discussion of the use of this property).
To Be Published	The cameras in this Site should be included in the camera topology published to operators. By setting this to false one can prevent a Site's cameras appearing before the Site is ready for use, and thus avoid confusion.

To change the attributes of a Site, select the Site in the main tab, adjust the settings as required, and then press the "Save" button (Figure 3.3). This process can also be used to rename a Site, including the "Default" Site.

3.4 Learning Maturity

It is essential that automatic learning reaches a level of maturity before commissioning using SenTRACK Network Optimizer (SNO) can proceed.

Learning maturity proceeds through three phases:

- Immature - the initial phase; during this phase the overall connectivity increases towards a peak
- Maturing - after the connectivity has reached a peak it starts to diminish
- Mature - the connectivity has stabilized; it has stop diminishing significantly (as it was during the Maturing phase) and is now varying only slightly (both up and down) around a stable value

The Camera Connectivity statistic in the main section of the Dashboard indicates the latest connectivity value for the selected site. The chart shows the historical variation of this value; by inspecting this chart one can see which phase of learning maturity has been reached.

Clicking on the chart shows a full size version of this chart (Figure 3.4).

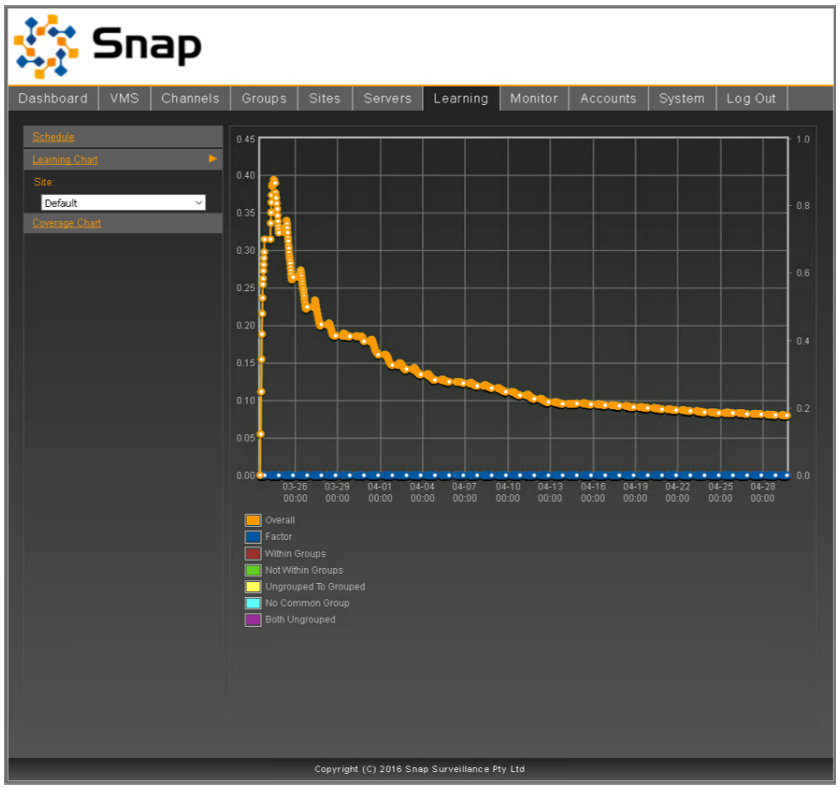

Figure 3.4: The detailed Learning Maturity chart with no Topology Maturity groups configured

The more detailed chart for each site can also be accessed in the Learning tab.

3.4.1 Topology Maturity and Camera Groups

If no “Topology Maturity” groups have been set up (see Section 3.2), the the Learning chart will resemble Figure 3.4:

- Observe how the “Overall” line initially rises towards a peak. This is the “Immature” phase.
- Subsequently, it falls from the peak, but jump up and down a bit. This in the “Maturing” phase.
- Eventually it flattens out and stops falling significantly (it may continue to fall slightly). This is the “Mature” phase.

The point at which the learning transitions from “Maturing” to “Mature” is to some extent a matter of judgement and experience. In the example shown there is a clear reduction in the rate of decrease at

around 04-13 (i.e. 13th April) and this would be the first good candidate for the transition point.

If “Topology Maturity” groups have been set up then the chart will contain more information (and will look more complicated). It will resemble Figure 3.5.

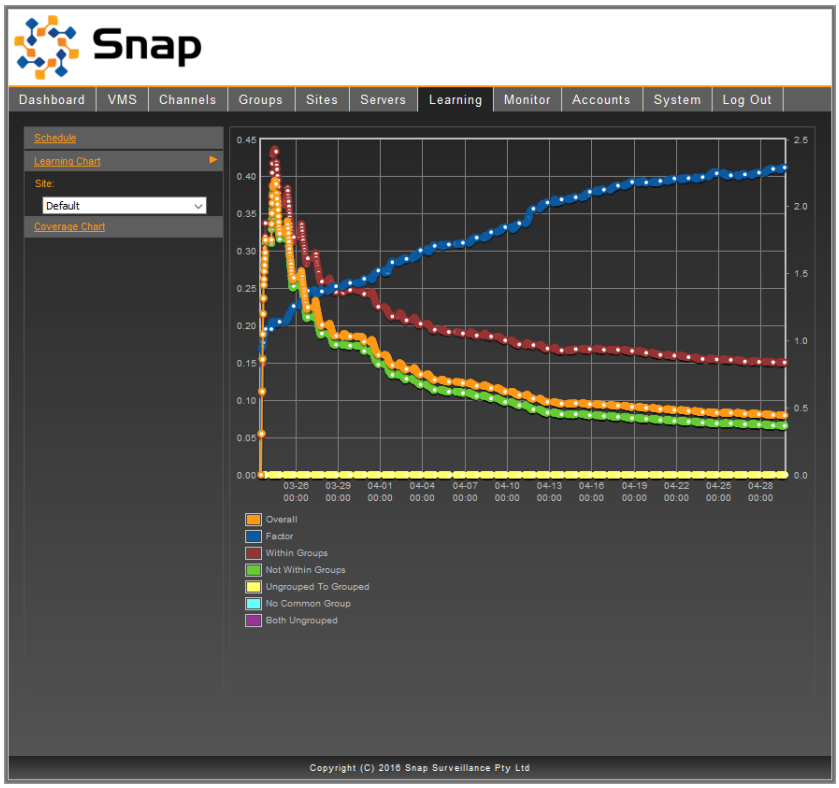

Figure 3.5: The detailed Learning Maturity chart with some Topology Maturity groups configured

In addition to the “Overall” curve (which behaves as above), the next most important information is in the “Factor” curve, which is the ratio of connectivity likelihood between:

- Pairs of cameras that are in the same group, and
- Pairs of cameras that are in different groups (or no group).

If “Topology Maturity” groups have been set up (see Section 3.2) and most cameras are in at least one such group, then the likelihood of links between pairs of cameras in the same group should be significantly higher than the likelihood of links between pairs of cameras that are not in the same group. This is reflected in a value for “Factor” that is significantly higher than 1.0 (on the right hand scale). The “Factor” curve will rise towards a value (greater than 1.0) and then flatten out, providing a further indication that learning has entered the “Mature” phase.

Note that this use of groups to assist in assessing learning maturity can be undertaken retrospectively: it is not necessary to create groups in advance. Instead as groups are added (and removed and changed) in SenTRACK Network Optimizer (SNO) and the changes are saved, the learning history is recalculated to reflect the current grouping. Also note that it is not necessary to place all or even most cameras in groups; in fact a single group with a small set of cameras is often enough and three or four such groups (as long as they are from different areas of the site) provides more than enough information in most cases. There may of course be other reasons to create a comprehensive set of groups in SNO.

3.5 Learning Coverage

The Learning Coverage detail chart for each site can be accessed in the Learning tab. This chart shows the number of frames for which pairs of cameras have been considered for learning (Figure 3.6). Max shows the highest value: at least one pair of cameras have been considered for this many frames. Mean shows the average number of comparisons across all pairs. 50% of the pairs have been considered at least the number of frames given by the 50% (a.k.a. median) value; similarly 75% of the pairs have been considered at least the number of frames given by the 75% value, and so on. Min shows the lowest value: all pairs of cameras have been considered for this many frames; note that in large networks this (and the 99% value) can be zero if cameras are offline for long periods of time.

A good rule of thumb is that once the 95% value exceeds about 100,000 frame comparisons then learning is likely to be sufficient. Note also the adding and removing cameras can alter the coverage results.

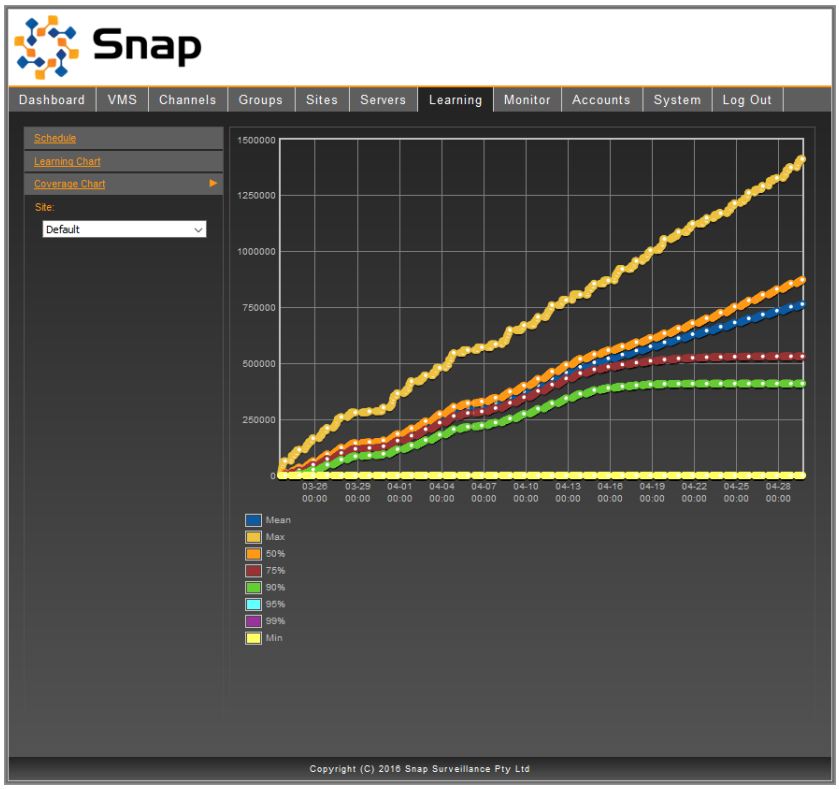

Figure 3.6: The Learning Coverage detailed chart

3.6 Backup/Restore

It is good practice to backup the database periodically. It is strongly recommended to perform backups as part of a regular health check.

3.6.1 System Backup

To backup the contents of the database:

1. Select the “Dashboard” tab

2. Locate the “System Backup” item in the “Status” section and click on the “Backup” link

The time of the latest backup should now be displayed in that item. Alternatively:

1. Select the “System” tab
2. Click the “Backup Now” link that appears in the side panel (Figure 3.7)

Details of the backup should now be displayed in the “Restore Points” main window. A page reload (F5) may be required to refresh the restore points list.

Note: Backup files are stored locally in the folder [Installation Directory]/backups.

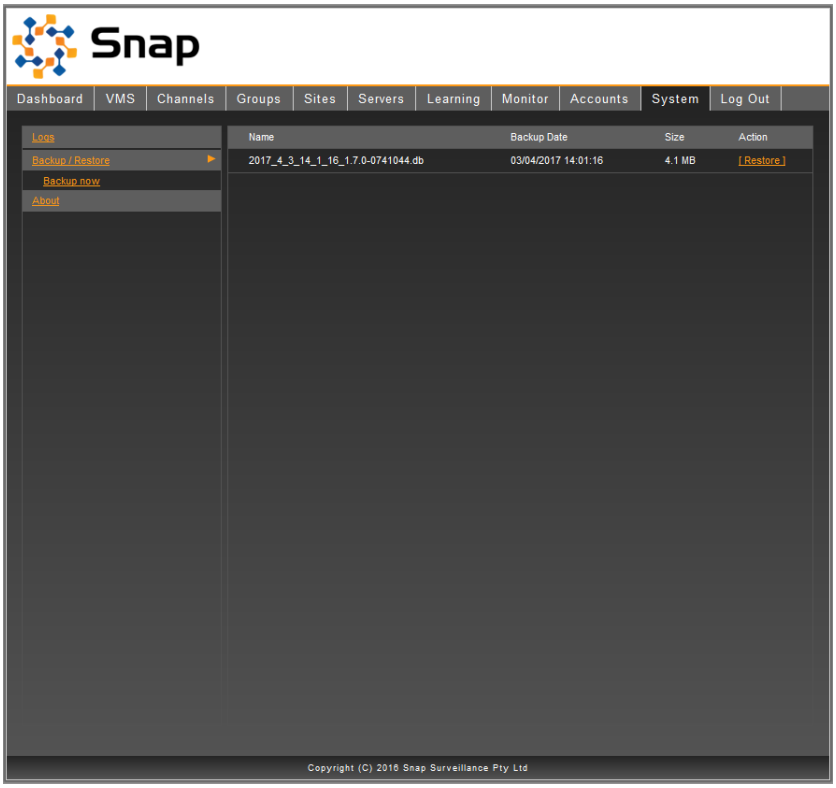

Figure 3.7: The System Restore page

3.6.2 System Restore

To restore the database to a previously saved restore point:

1. Select the “System” tab
2. Click on the “Backup/Restore” section from the side panel (Figure 3.7).
3. In the “Restore Points” main window, choose the appropriate restore point and click “Restore”.

Note: The database can only be restored using backups from the same version of SNI. The list of restore points contains only valid database backups.

3.7 System Shutdown

3.7.1 Normal Shutdown Procedure

Before powering down any SenTRACK Network Intelligence (SNI) server, it is good practice to stop the schedule and wait a short time for the learning to complete.

To stop the schedule:

1. Select the “Dashboard” tab
2. Locate the “Current” item in the “Status” section and click on the “Deactivate” link.

The SNI server can now be powered down using the normal Windows procedure.

3.7.2 Windows Service Shutdown Procedure

The SenTRACK Network Intelligence (SNI) system runs as a service on Windows. In the case of a system failure, the service can be stopped (and restarted again) to help determine the cause. An inspection of the log files generated by the system may be required to achieve this. See Section 3.13.1 for details.

To stop the service:

1. Click the Windows Start button and click on “Run...”
2. In the text box provided, type “services.msc” and press enter
3. In the services list displayed, locate the “SenTRACK Network Intelligence Service” item and select it
4. Click the “Stop” link from the left panel
5. Wait for the service to come to a complete stop
6. Click the “Start” link from the left panel to start the service again

3.7.3 Emergency Shutdown Procedure

If emergency shutdown is necessary, it is safe to power off the SenTRACK Network Intelligence (SNI) server without following the procedure described in Section 3.7.1.

3.8 Managing User Accounts

User accounts allow SenTRACK Network Intelligence (SNI) to control access to the clients and video footage. This section describes how to add and remove users, change user passwords, and modify user privileges and permissions.

3.8.1 Adding Users

Access to SenTRACK Network Optimizer (SNO) and SenTRACK Client (STC) is restricted to users created in SenTRACK Network Intelligence (SNI). For STC users, these credentials are used to access video footage from the VMS, so they must also match a valid VMS user.

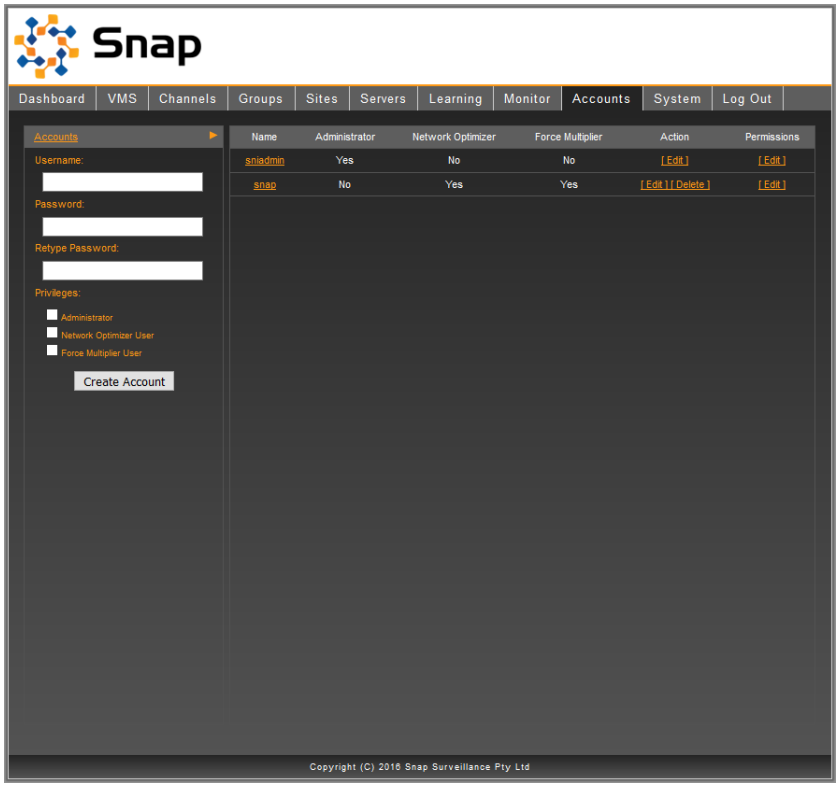

Figure 3.8: The System Accounts page

To create users:

1. Select the “Accounts” tab
2. Enter the details of a VMS user account (for example, the account configured in Section 2.2.2), ensuring the passwords match.
3. Select the “Network Optimizer User” and/or “Force Multiplier User” privileges
4. Click the “Create Account” button

3.8.2 Removing Users

To remove users:

1. Select the “Accounts” tab
2. In the “Action” column in the Accounts table, click the “Delete” link (Figure 3.8)

3.8.3 Changing User Passwords

To change a user’s password:

1. Select the “Accounts” tab
2. In the “Action” column in the Accounts table, click the “Edit” link (Figure 3.8)
3. Enter the new password using the fields in the left side panel

4. Click the “Save Account” button

3.8.4 Modifying User Privileges

To change a user’s privileges:

1. Select the “Accounts” tab
2. In the “Action” column in the Accounts table, click the “Edit” link (Figure 3.8)
3. Adjust the relevant privileges
4. Click the “Save Account” button

3.8.5 Modifying User Permissions

To change a user’s permissions:

1. From the “Accounts” page, find the row with the user to modify and click “Edit” in the permissions column.
2. The permissions page is now displayed for the user (Figure 3.9)
3. The permissions can be changed by selecting a policy in each column column for each row. The default permission applies no explicit override.
4. Select “Save Permissions” once the desired configuration is achieved to store the settings.

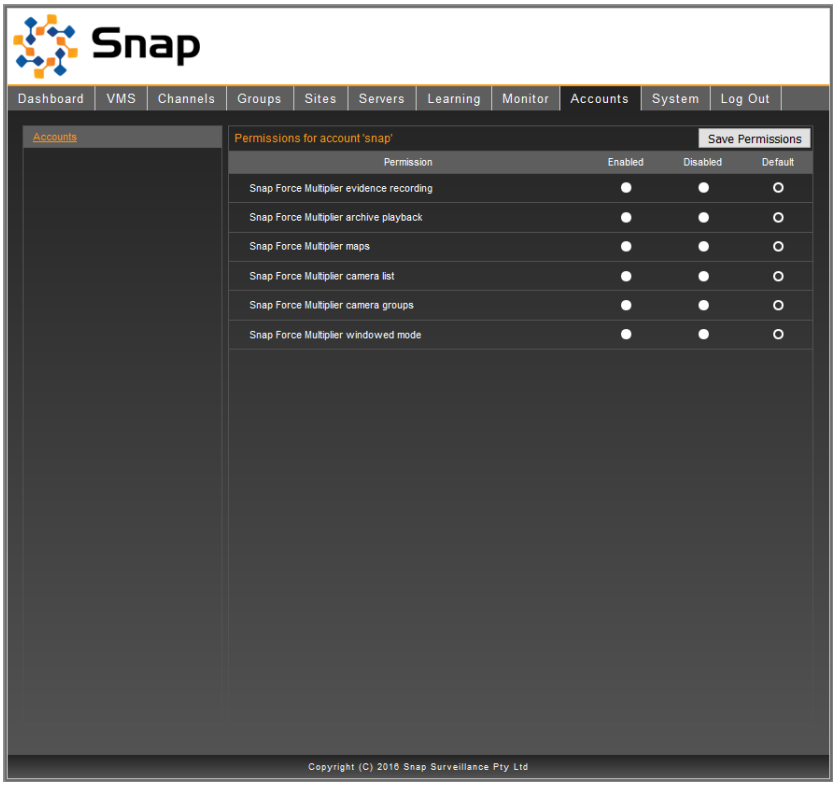

Figure 3.9: The Account Permissions page

3.9 Managing the VMS

3.9.1 Synchronising Channels and Groups

To synchronise the SenTRACK Network Intelligence (SNI) channel list and group membership with that of the VMS:

1. Select the “VMS” tab
2. Click on the circular refresh arrows next to the VMS in the main table

Any new channels will appear in the Inactive Channels section of the Channels tab. Any channels that have been removed from the VMS will also be removed from the SNI system. Group membership will also be updated.

3.9.2 Making extra streams available to SNI

Assuming that extra low-resolution streams have been configured in the VMS per the guidelines given in Section 2.1.4, those extra streams then need to be made available to SNI:

1. SNI needs to be made aware of the extra streams. To do this simply use the process for Synchronising Channels and Groups (Section 3.9.1)
2. The resolution of the extra streams needs to be discovered. This is tied to the process of retrieving sample images (see Section 3.10.2) and is triggered as follows:
   (a) If the cameras for which extra streams have been defined are Inactive, simply activate them (see Section 2.5.3);
   (b) If the cameras for which extra streams have been defined are Active, reload sample images for them (see Section 3.10.2);

Note also that this same process is needed if the configuration of an extra stream is changed in XProtect.

3.9.3 Updating VMS Account Details

To modify the username and/or password of the account used by SNI:

1. Select the “VMS” tab
2. Change the username/password information in the left side panel
3. Click on the “Update” button

If the credentials are invalid an error message will alert you that authentication failed, and the stored credentials will not be changed. Otherwise, the Status field for the VMS will transition from “Authenticating” to “OK”, and the stored credentials will be updated.

3.10 Managing Channels

3.10.1 Channel Deactivation

To deactivate a channel:

1. Select the “Channels” tab
2. Click on the “Active Channels” section from the left side panel
3. Select the channels to be deactivated.
4. In the drop down box that appears in the top right of the main view, select “Deactivate”. The selected channels will then transition into the “Inactive Channels” view (Figure 2.4).

3.10.2 Updating Camera Images

The sample images can be updated at any time using the Active Channels page (Figure 2.5):

1. Select the “Channels” tab
2. Click on the “Active Channels” section from the left side panel
3. To refresh all images, click the circular refresh arrows at the top of the Active Channels table
4. To refresh individual images, click the circular refresh arrows in the relevant row of the Active Channels table

3.10.3 Adding/Removing Channels from Learning

The learning status of a channel can be modified in the Active Channels page:

1. Select the “Channels” tab
2. Click on the “Active Channels” section from the left side panel
3. Select the required channels
4. Use the “Action” selector to choose “Enable Learning” or “Disable Learning” as desired

3.10.4 Adding/Removing Channels from the Topology

Channels can be added to, and removed from, the topology in the Active Channels page:

1. Select the “Channels” tab
2. Click on the “Active Channels” section from the left side panel
3. Select the required channels
4. Use the “Action” selector to choose “Add to active topology” or “Remove from active topology” as desired

3.10.5 Cameras that Change Position

When cameras are moved, their relationship with the other cameras need to be re-established which will happen over time. This relearning can be expedited by using the following steps:

1. Select the “Learning” tab
2. Click on the “Schedule” section from the left side panel
3. Ensure the schedule is deactivated
4. Select the “Channels” tab
5. Click on the “Active Channels” section from the left side panel
6. Select the moved cameras
7. Use the “Action” selector to choose “Deactivate”
8. Select the “Learning” tab
9. Click on the “Schedule” section from the left side panel
10. Activate the schedule
11. Select the “Dashboard” tab
12. Wait until the learning data is updated again (note the time in the “Last Updated” field in the Dashboard)
13. Click on the “Deactivate” link to stop the schedule
14. Select the “Channels” tab
15. Click on the “Inactive Channels” section from the left side panel
16. Select the moved cameras
17. Use the “Action” selector to restore them to their previous state
18. Select the “Learning” tab
19. Click on the “Schedule” section from the left side panel
20. Activate the schedule

3.10.6 PTZ

To mark a camera as PTZ:

1. Select the “Channels” tab
2. Click on the “Active Channels” section from the left side panel
3. Select the channels you wish to mark as being PTZ
4. Use the “Action” selector to choose “Mark as PTZ camera”

Cameras can have the PTZ designation removed by following the same procedure, but choosing “Mark as fixed camera” instead.

3.11 Managing Schedules

To change schedules, any existing schedule must first be deleted.

1. Select the “Learning” tab
2. Click on the “Schedule” section from the left side panel
3. Ensure the schedule is deactivated
4. Click the “Delete Schedule” button in the left side panel

A new schedule can now be created:

1. Click the “Schedule” link from the left side bar to create a schedule
2. Create a new schedule by entering the following information:

Field	Description
Name	Choose a name for easy reference
Mode	Live or Archive
Analyze Footage	Time range of footage to analyze *

*Archive mode only. Footage is assumed to be available for the configured times.

3. Click “Create Schedule”
4. Start the schedule by clicking “Activate” in the “Action” column

3.12 Monitoring Channels

The details for each learning channel can be viewed in the Monitor tab (Figure 3.10).

Clicking on the channels sample image loads the detailed information for that channel (Figure 3.11).

This view provides access to the sample image retrieval log and the latest learning log.

3.13 System Information

System information can found in the “System” tab of the web application.

3.13.1 Log Files

All log files generated by the Network Intelligence system are located in the [Installation Directory]/LOGS folder. Log files generated by the Network Intelligence service can be viewed via the “System” tab:

1. Select the “System” tab
2. Click on the “Logs” sections from the side panel to view the current log file (Figure 3.12)
3. To view older log files, click on the appropriate dated log file from the left side panel

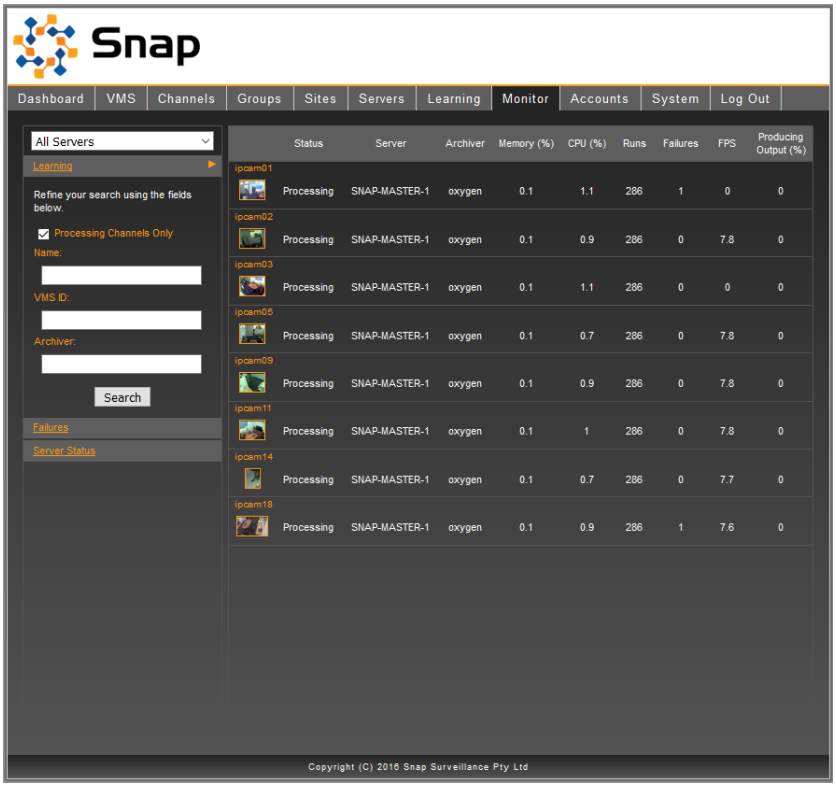

Figure 3.10: Channel monitor

4. Refine the log details displayed by altering the number of lines displayed or the log level using the drop-down boxes above the log display.

Log files generated by learning processes can by viewed via the web application from the “Monitor” tab:

1. Select the “Monitor” tab
2. Click on the image of the appropriate camera
3. In the view displayed, expand the “Channel Log” subsection to display the logs for that camera (Figure 3.13)

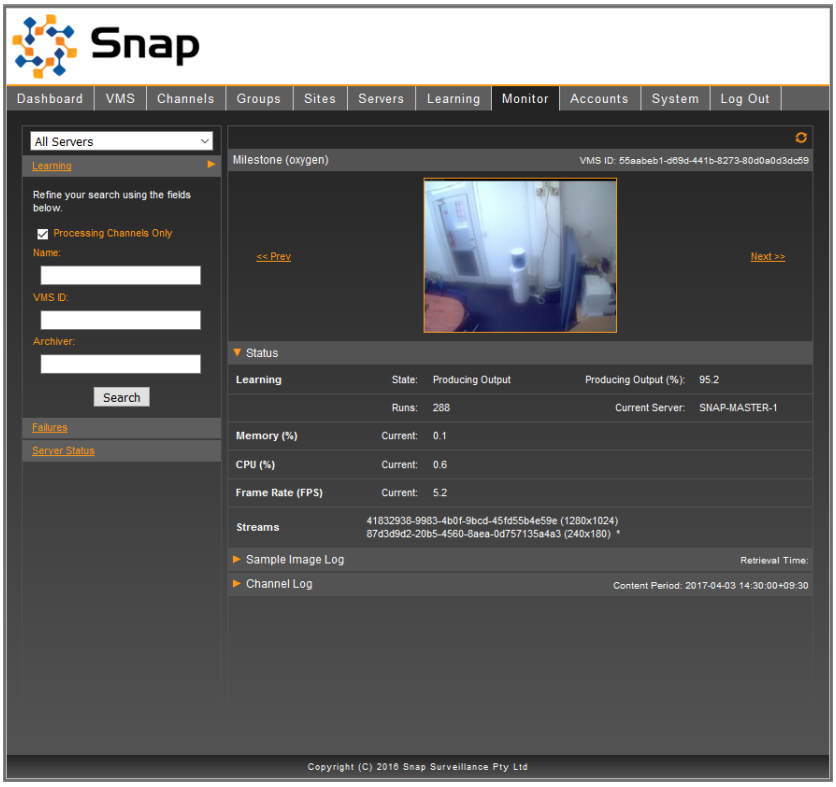

Figure 3.11: Detailed channel information

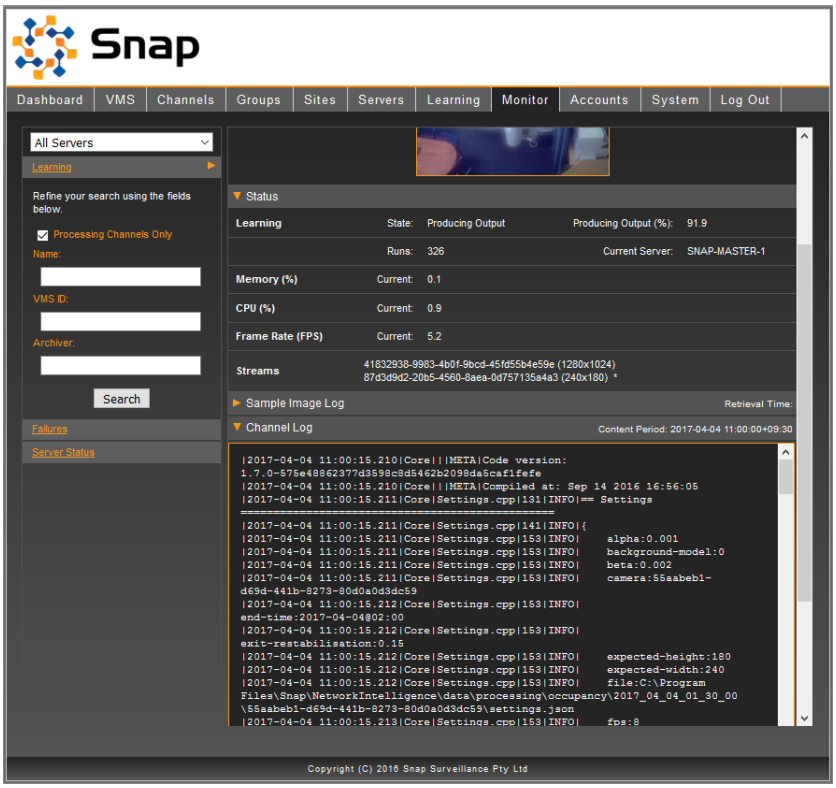

Figure 3.13: The Channel Log page

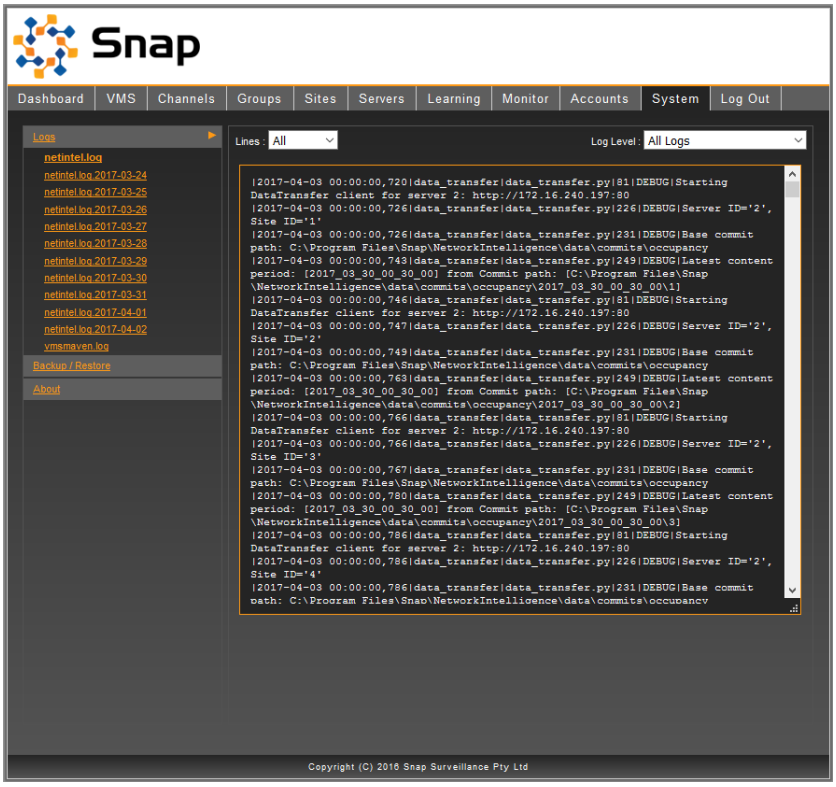

Figure 3.12: The System Log page

3.13.2 System Version and License

The SenTRACK Network Intelligence (SNI) version and license details can be found in the “System” tab.

1. Select the “System” tab
2. Click on the “About” section from the side panel

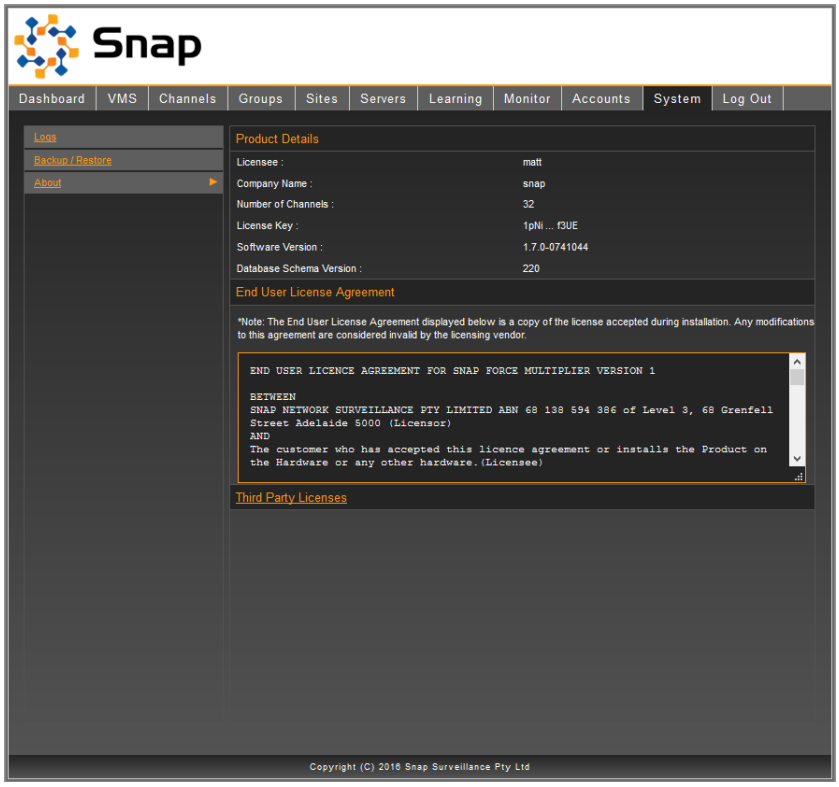

Figure 3.14: System Version and License

The system version and license details can be inspected from the “Product Details” section in the page displayed (Figure 3.14).

3.14 Upgrade SenTRACK Network Intelligence (SNI)

Existing installations of the SNI server can be upgraded by running the SNI installer. This should be performed by a service technician.

3.15 SFM API

SenTRACK Client (STC) can be controlled using an API. Set STC’s TCP listening port by specifying `"listen-port": <port number>` in STC’s settings file and connect using Telnet or similar.

The `set_play_state` command is the default (the `command` key-value pair can be omitted):

```
{
        "command": "set_play_state",
        "vms_id": "172.16.0.2_80",
        "camera_id": "e172bc75-21de-4e09-b7c9-4955b6de47dd",
        "play": {"time": "2014-04-02T01:02:03Z", "speed": -1.0 },
        "view": "Single Camera View"
}
```

this produces a response like the following (non-zero status is various types of error)

```
{
        "status": 0,
        "error_message": "OK"
}
```

The `play` component can also be `live`, and the `view` component can be `Peripheral View`:

```
{
        "command": "set_play_state",
        "vms_id": "172.16.0.2_80",
        "camera_id": "e172bc75-21de-4e09-b7c9-4955b6de47dd",
        "play": "live",
        "view": "Peripheral View"
}
```

The `get_play_state` command is:

```
{
        "command": "get_play_state"
}
```

this produces an output like:

```
{
        "status": 0,
        "error_message": "OK",
        "vms_id": "172.16.0.2_80",
        "camera_id": "e172bc75-21de-4e09-b7c9-4955b6de47dd",
        "play": {"time": "2014-04-02T01:02:03Z", "speed": -1.0 },
        "view": "Single Camera View"
}
```

A. VMS Connection Troubleshooting

Establishing and maintaining a connection to the Milestone XProtect Management (or Master) Server is a critical step. Various problems can arise and these need to solved to enable SenTRACK Client (STC) to function. The table below lists the error messages that are provided and the recommended troubleshooting steps.

Error Message	Troubleshooting Recommendation
The name “host-name” given for the Milestone XProtect Management (or Master) Server could not be resolved to an IP address.	1. Check the name is spelled correctly; in particular if you intended to enter an IP address check that it is validly formatted. 2. Check whether the SNI Master Server has a DNS server set. 3. If there is a DNS server, consult that server’s administrator as to why the given name does not resolve. 4. If there is no DNS server check that the name appears in the local name resolution mechanism (HOSTS file etc.).
The SNI Master Server’s network interface is disconnected, disabled or faulty.	1. Ensure that a cable is plugged in to the SNI Master Server’s network interface and that that cable is plugged into active network infrastructure. 2. Check that the SNI Master Server’s network interface is enabled (in the server’s operating system). 3. Check that the SNI Master Server’s network interface has a valid IP address. 4. Check for operating systems messages indicating the SNI Master Server’s network interface card (NIC) is faulty.

Continued on next page

Error Message	Troubleshooting Recommendation
Attempted to connect to server named “host-name” at IP address *IP-address*; the connection timed out. **or** Attempted to connect to server at IP address *IP-address*; the connection timed out.	1. Check that the SNI Master Server can communicate with another server on the network which you know to be functional (e.g. a file server). 2. If a Host Name is given in the error message then check it is the correct Host Name for the Milestone XProtect Management (or Master) Server. 3. Check that the IP address given in the error message is the correct IP address for the Milestone XProtect Management (or Master) Server. 4. On the SNI Master Server, use the “ping” command to test connectivity to the IP address for the Milestone XProtect Management (or Master) Server. 5. Consult the administrator of the Milestone XProtect Management (or Master) Server to ensure that it is not overloaded and thus unable to respond in time. 6. Consult your network administrator to undertake more advanced diagnosis.
Attempted to connect to server named “host-name” at IP address *IP-address* on TCP Port number *port-number*; the connection was refused. **or** Attempted to connect to server at IP address *IP-address* on TCP Port number *port-number*; the connection was refused.	1. If a Host Name is given in the error message then check it s the correct Host Name for the Milestone XProtect Management (or Master) Server. 2. Check that the IP address given in the error message is the correct IP address for the Milestone XProtect Management (or Master) Server. 3. Check that the Port number given in the error message is the correct port for the Milestone XProtect Management (or Master) Server. 4. Consult the administrator of the Milestone XProtect Management (or Master) Server to ensure that it is indeed running on the server with the given address and at the given port. 5. If there is a firewall running on either of the SNI Master Server or the Milestone XProtect Management (or Master) Server, or on the network between the two, consult the relevant firewall administrators to ensure that outbound connections are permitted from the SNI Master Server to the Milestone XProtect Management (or Master) Server at the given port. 6. Consult your network administrator to undertake more advanced diagnosis.

Continued on next page

Error Message	Troubleshooting Recommendation
The Milestone XProtect Management (or Master) Server named “host-name” at IP address *IP-address* denied authentication of the user named “user-name” with the supplied N-character password. **or** The Milestone XProtect Management (or Master) Server at IP address *IP-address* denied authentication of the user named “user-name” with the supplied N-character password. **or** The Milestone XProtect Management (or Master) Server named “host-name” at IP address *IP-address* on TCP port number *port-number* denied authentication of the user named “user-name” with the supplied N-character password. **or** The Milestone XProtect Management (or Master) Server at IP address *IP-address* on TCP port number *port-number* denied authentication of the user named “user-name” with the supplied N-character password.	1. Verify that the username and password are correct. 2. If a Host Name is given in the error message then check it is the correct Host Name for the Milestone XProtect Management (or Master) Server. 3. Check that the IP address given in the error message is the correct IP address for the Milestone XProtect Management (or Master) Server. 4. If a TCP Port number is given in the error message then check that it is the correct port for the Milestone XProtect Management (or Master) Server. 5. Consult the administrator of the Milestone XProtect Management (or Master) Server to ensure that the specified user satisfies the prerequisites given in Section 2.2.2 of this guide.

Continued on next page

Error Message	Troubleshooting Recommendation
The server named “host-name” at IP address *IP-address* did not respond as a Milestone XProtect Management (or Master) Server should. **or** The server at IP address *IP-address* did not respond as a Milestone XProtect Management (or Master) Server should. **or** The server named “host-name” at IP address *IP-address* on TCP port *port-number* did not respond as a Milestone XProtect Management (or Master) Server should. **or** The server at IP address *IP-address* on TCP port *port-number* did not respond as a Milestone XProtect Management (or Master) Server should.	1. If a Host Name is given in the error message then check it is the correct Host Name for the Milestone XProtect Management (or Master) Server. 2. Check that the IP address given in the error message is the correct IP address for the Milestone XProtect Management (or Master) Server. 3. If a TCP Port number is given in the error message then check that it is the correct port for the Milestone XProtect Management (or Master) Server. 4. Consult the administrator of the Milestone XProtect Management (or Master) Server to ensure that it is indeed running on the server with the given address and at the given port.
VMS type has not been specified, connection cannot proceed.	1. Ensure that the correct VMS type is selected in the drop-down menu of the Setup→VMS page.

Also it is possible that the connection to the Milestone XProtect Management (or Master) Server succeeds but there are unexpected values in the retrieved information.

Problem	Troubleshooting Recommendation
Number of channels in the VMS connection is zero or unexpectedly low	1. Consult the administrator of the Milestone XProtect Management (or Master) Server to ensure that the user has access to all expected channels (cameras etc.)

Finally if the incorrect VMS Type has been specified and a connection commenced it is necessary to to reinstall in order to choose the correct VMS Type. To do this uninstall SenTRACK Network Intelligence (choosing to remove data), then reinstall.

B. Sample Image Retrieval Troubleshooting

SenTRACK Network Intelligence (SNI) obtains sample images in order to verify that it is able to connect to the VMS and access live video. Typically if video can't be access to retrieve sample images then it means there are problems that need to be solved before commissioning can proceed. The Sample Image Log for each camera contains detail about the retrieval of sample images, including any problems encountered, and can be access through the detailed camera view in the Monitor page (see Section 3.12).

Issue	Troubleshooting Recommendation
No sample images obtained at all and Status is "Failed" for all	1. Ensure native client live video access (as below) for several of the cameras. 2. Ensure network connectivity (as below) from the SNI Master Server to each of the Milestone XProtect Camera (or Slave) Server. The Milestone XProtect Camera (or Slave) Server for each camera is given in the Active Channels page entry for that camera. 3. Inspect the Sample Image Log for each of the cameras, noting any errors and warnings.
No sample images obtained from a particular Milestone XProtect Camera (or Slave) Server and Status is "Failed" for all cameras from that Milestone XProtect Camera (or Slave) Server. Note that the Milestone XProtect Camera (or Slave) Server for a given camera can be seen in the Active channels list.	1. Ensure network connectivity (as below) from the SNI Master Server to the Milestone XProtect Camera (or Slave) Server. 2. Ensure native client live video access (as below) for several of the cameras from that Milestone XProtect Camera (or Slave) Server. 3. Inspect the Sample Image Log for each of the cameras, noting any errors and warnings.
Individual cases where no sample image obtained and Status is "Failed"	1. Ensure native client live video access (as below) for the failed cameras. 2. Inspect the Sample Image Log for each of the cameras, noting any errors and warnings.
Poor quality sample image or "noise" in sample image	1. Check the image quality in the native VMS client and correct any problems observed. 2. Retry retrieval of the sample image.

Ensuring Native Client Live Video Access and Sample Image Access

A key tool in troubleshooting sample image access is running the native VMS client as the SNI VMS User (the user specified in the Setup→VMS page), since if video isn't accessible via the native VMS client it won't be accessible to SenTRACK Network Intelligence . The following process can be used to ensure such access:

1. If the native VMS client is not installed on the SNI Master Server but is already installed on some other workstation, then login on that client as the SNI VMS User and check live video access for several cameras:
    - if live video **cannot** be viewed then consult with your Milestone XProtect Management (or Master) Server administrator to make such video available, then try refreshing the sample images (see Section 3.10.2) for the camera(s) you checked.
2. Install the native VMS client on the SNI Master Server.
3. Login on that client as the SNI VMS User and check live video access for several cameras:
    - if live video **cannot** be viewed then consult with your Milestone XProtect Management (or Master) Server administrator to make such video available, then try refreshing the sample images (see Section 3.10.2) for the camera(s) you checked.

Note also that in large SenTRACK Network Intelligence (SNI) systems with multiple SNI servers this procedure can also used to ensure native client live video access on the other SNI servers.

Ensuring Network Connectivity from the SenTRACK Network Intelligence (SNI) Ser to Archivers

In many VMS systems live video is obtained via Archivers, rather than direct from the cameras. Some VMSes support direct transmission of live video from cameras via multi-cast, usually as an option with a fallback to obtain the video via the Archiver. And of course all recorded video is obtained from the Archivers. Therefore it's important to ensure that SNI servers can access the Archivers over the network. Use the following process:

1. Run the Windows "Command" tool.
2. In the command tool, run the "ping" command (separately for each Milestone XProtect Camera (or Slave) Server), specifying the name of the Milestone XProtect Camera (or Slave) Server as the command line argument to "ping". If "ping" is able to translate the name of the Milestone XProtect Camera (or Slave) Server into an IP address it will list the translated address in its output. If there are problems then "ping" will report various error messages. Use the following steps to diagnose problems:
    (a) If "ping" indicates that the name of the Milestone XProtect Camera (or Slave) Server could not be resolved then consult your network administrator to resolve the problem.
    (b) If "ping" can resolve the name of the Milestone XProtect Camera (or Slave) Server it will print the resolved IP address. Verify that this is the correct IP address for the relevant Milestone XProtect Camera (or Slave) Server. If it is incorrect then consult your network administrator to resolve the problem.

(c) Sometimes “ping” may report that the given name of the Milestone XProtect Camera (or Slave) Server resolves to more than one IP address. This is typically problematic, particularly if the first/default IP address is not correct (per the previous point). Consult your network administrator to resolve this problem.

(d) If after resolving the Milestone XProtect Camera (or Slave) Server name to the correct IP address, “ping” reports “no route to host”, “host unreachable” or similar then consult your network administrator to resolve this problem.

C. Using netstat to Identify Used Ports

You can use the “netstat” command to find out which ports are **currently** in use, but note that it is possible that the port you choose may be required for some service that only runs intermittently. To use netstat, open command prompt and run:

```
netstat -o -a
```

The output of the netstat program is shown in Figure C.1.

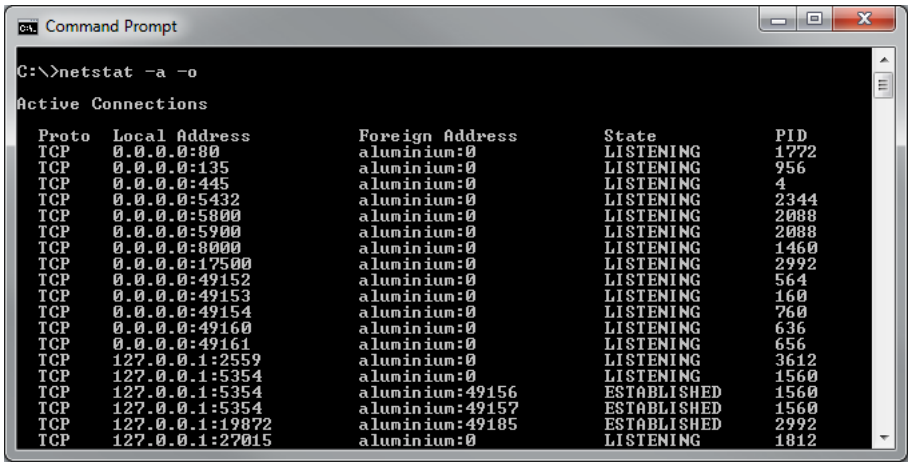

Figure C.1: Typical output of the netstat program

Each line in the netstat output relates to one port currently in use on the system. The address of the port is listed in the “Local Address” column, and the protocol being used on the port is shown in the “Proto” column. The netstat output in Figure C.1 shows TCP port 80 is already in use (0.0.0.0:**80**).

D. Installing the SmartClient Plugins

SenTRACK Client (STC) can run as a tab within the Milestone SmartClient.

Pre-requisites

The SenTRACKclients (at least SenTRACK Client) should be installed and working (i.e. should run in stand alone mode from the Start menu).

There are two plugins:

- SnapForceMultiplierPlugin is the core plugin; and
- MilestoneSessionManagerPlugin is used to integrate SnapForceMultiplierPlugin with the Milestone SmartClient.

The installation process for the two plugins is the same (and both are required). The description below focuses on the SnapForceMultiplierPlugin.

Installation Procedure

1. Extract the ZIP file of the plugin (either the 32 bit or 64 bit, as appropriate) to your Desktop. The result will be a folder with a name starting with "SnapForceMultiplierPlugin" (the end of the name depends on whether it's 32 or 64 bit; some ZIP programs tend to extract single-folder archives inside another folder. The "SnapForceMultiplierPlugin" is the one that is needed, not the containing folder) and containing two files:
   - ForceMultiplier.dll
   - plugin.def
2. Locate the "MIPPlugins" folder inside the Milestone SmartClient installation. This will normally be:
   - `C:\Program Files\Milestone\XProtect Smart Client\MIPPlugins`, or
   - `C:\Program Files (x86)\Milestone\XProtect Smart Client\MIPPlugins`
3. Copy the "SnapForceMultiplierPlugin. . . " folder from step 1 into the "MIPPlugins" folder.
4. Repeat above steps for the MilestoneSessionManagerPlugin.
5. (Re)Start the Smart Client and log in. The "Force Multiplier" tab should appear at the top (to the right of the standard "Live" and "Playback" tabs and typically between "Sequence Explorer" and "Alarm Manager"). NB: when Smart Client is loading it may instead display a security message related to the "ForceMultiplier.dll" file. In this case the "ForceMultiplier.dll" needs to be unblocked. To do this (depending on security policies it may be necessary to perform these steps as an administrator):
   (a) Use Windows Explorer to Navigate to the "SnapForceMultiplierPlugin. . . " folder inside the "MIPPlugins" folder (from step 3)
   (b) Select the "ForceMultiplier.dll" file icon and run "Properties" from the right click menu; this will have an option to unblock the DLL.

6. Once the “Force Multiplier” tab is visible it can be clicked on. If the logged in Milestone user is running the plugin for the first time (i.e. they have not already run it from some other machine elsewhere on the network) then it is necessary to do some user-specific configuration (and the “Force Multiplier” tab will display a message indicating the need to do this). The procedure is:
   (a) In Smart Client, open the “Options” panel (using the “Star” icon, which is usually in the top right of the window).
   (b) Select the “Force Multiplier” section in the list on the left.
   (c) The username should be entered, including the Active Directory domain component (if any).
   (d) The corresponding password should be entered (twice)
   (e) The “Force Multiplier Directory” entry is not editable but verify that it points to the directory in which the standalone client is installed. If the “Force Multiplier Directory” entry is not displayed or refers to a directory that has been deleted then it will be necessary to run the SenTRACK client installer again to reinstall the client. Steps 1-4 do not need to be repeated however.
   (f) The plugin can now be used (by the logged in Milestone user).