United VMS 8.0.5

Admin Center
Help File
Latitude
# Table of Contents

1. Getting Started ............................................................................................................. 1  
   1.1 About This File ..................................................................................................... 1  
   1.2 Using this Help File .......................................................................................... 6  
   1.3 Log On using Command Line ........................................................................ 6  
2. System Overview .......................................................................................................... 8  
   2.1 System Concepts ............................................................................................... 9  
   2.2 Server Components - Overview ......................................................................... 13  
      2.2.1 Directory Server ....................................................................................... 14  
      2.2.2 Archiver Server ...................................................................................... 15  
      2.2.3 Event Distributor (EDB) Server .............................................................. 17  
      2.2.4 Transcoder & Gateway Servers ............................................................. 17  
      2.2.5 Application Server .................................................................................. 17  
      2.2.6 Web Server ............................................................................................. 18  
      2.2.7 Update Services Server ....................................................................... 19  
      2.2.8 CaseBuilder Server ............................................................................... 19  
      2.2.9 Global Admin Server ............................................................................ 19  
   2.3 Client Applications ............................................................................................. 20  
      2.3.1 Control Center Client ............................................................................. 21  
      2.3.2 Admin Center Client ............................................................................ 21  
      2.3.3 Web Client ............................................................................................ 21  
      2.3.4 Global Client ......................................................................................... 22  
      2.3.5 Client Portal .......................................................................................... 24  
      2.3.6 Client Upgrades .................................................................................... 25  
3. AdminCenter User Interface ........................................................................................... 26  
   3.1 Dashboard .......................................................................................................... 28  
   3.2 Workspace ....................................................................................................... 32  
      3.2.1 Sidebar ................................................................................................... 32  
      3.2.2 Selection Pane / Navigation Tree .......................................................... 35  
         3.2.2.1 Logical View ..................................................................................... 37  
         3.2.2.2 Physical View .................................................................................. 40  
         3.2.2.3 System Settings View ..................................................................... 43  
   3.3 Configuration Pane - Overview ......................................................................... 46  
   3.4 Options ............................................................................................................. 47  
4. Configuration - Entities ............................................................................................... 50
Table of Contents

4.1 Analog Monitor .................................................................................................. 50
4.2 Audio Layout (Legacy) ....................................................................................... 51
4.3 Camera ............................................................................................................ 51
  4.3.1 Camera General Tab .................................................................................. 54
  4.3.2 Camera Video Settings Tab ........................................................................ 58
  4.3.3 Camera Picture Settings Tab ...................................................................... 62
  4.3.4 Camera Thermal Settings ........................................................................... 65
  4.3.5 Camera Recording Settings Tab ................................................................. 68
  4.3.6 Camera Edge Recording Tab ..................................................................... 71
  4.3.7 Camera Linked Tab ................................................................................... 73
  4.3.8 Camera PTZ Configuration Tab ................................................................. 74
  4.3.9 Camera Motion Detection Tab ..................................................................... 75
  4.3.10 Camera Analytics .................................................................................... 75
  4.3.11 Camera Privacy Mask Tab ........................................................................ 78
4.4 Camera Sequence ............................................................................................. 81
4.5 Conditional Event ............................................................................................. 83
4.6 Enterprise .......................................................................................................... 85
4.7 GIS Maps .......................................................................................................... 87
4.8 Input Pin Device ................................................................................................ 90
4.9 Map .................................................................................................................. 90
4.10 Microphone ....................................................................................................... 92
4.11 Network ........................................................................................................... 95
4.12 Output Pin Device ............................................................................................ 95
4.13 Recipients Group ............................................................................................... 96
4.14 Serial Device .................................................................................................... 97
4.15 Serial CCTV Keyboard ..................................................................................... 99
  4.15.1 Adding a new CCTV keyboard configuration ............................................ 100
4.16 Site ................................................................................................................ 101
4.17 Speaker .......................................................................................................... 102
4.18 System ............................................................................................................ 103
  4.18.1 System - General ................................................................................... 103
  4.18.2 System - System Security ...................................................................... 107
  4.18.3 System - Edge Security .......................................................................... 113
  4.18.4 System - Logical IDs .............................................................................. 115
# Table of Contents

4.18.5 System - Discovery .................................................................................. 116
4.18.6 System - Audit Trail .................................................................................. 116
4.18.7 System - Advanced .................................................................................. 117
4.18.8 System - Mass Export .............................................................................. 122
4.18.9 System - Analytics ................................................................................... 122
4.18.10 System - Actions ..................................................................................... 123
4.19 Tile Layout ...................................................................................................... 123
4.20 Timer .............................................................................................................. 123
4.21 Unit ................................................................................................................. 124
4.22 User ............................................................................................................... 127
4.23 User Group ..................................................................................................... 132

5. Configuration - Functionality ........................................................................ 137

5.1 Alarm Management ...................................................................................... 137
5.1.1 Configuring an Alarm with Cameras ....................................................... 143
5.2 Binding Cameras and Encoders .................................................................... 144
5.2.1 Configuring RTSP Support for a Camera on a TRK Unit ....................... 147
5.3 Events and Actions ....................................................................................... 148
5.3.1 Events ........................................................................................................ 152
5.3.2 System-Wide Events .............................................................................. 157
5.3.3 Actions ...................................................................................................... 158
5.4 MMS Video Support .................................................................................... 168
5.5 Motion Detection ........................................................................................... 170
5.5.1 Motion Detection Settings ....................................................................... 170
5.5.1.1 Configuring Motion Detection .......................................................... 173
5.6 Privacy Mask ................................................................................................ 189
5.6.1 Adding a Privacy Mask to a Video Scene ............................................... 189
5.6.2 Setting User Privacy Mask Permissions (Deactivate Privacy Masking) ...... 191
5.6.2.1 Changing the System-Wide Privacy Mask Password ......................... 192
5.6.3 Recovering Privacy Mask Password from an Exported Scene Recording ...... 197
5.7 PTZ Priorities ............................................................................................... 198
5.8 Tru Witness .................................................................................................. 201
5.8.1 TruWitness Mobile Camera - Android Application ............................... 202
5.8.2 TruWitness - Gateway Setup ................................................................. 208
5.9 User Management ........................................................................................ 210
# Table of Contents

5.9.1 Privileges and Access Right Configuration ......................................................... 211  
5.9.1.1 Defining Access Rights ........................................................................... 215  
5.9.1.2 Access Right Default Settings ................................................................... 217  
5.9.1.3 Privileges Default Settings, Use Cases and Scenarios ........................... 220  
5.9.2 Terminate a user session remotely ................................................................. 223  
5.9.3 User Group Wizard ......................................................................................... 224  
5.10 Tools ............................................................................................................... 228  
5.10.1 AdminCenter Wizards ................................................................................ 229  
5.10.1.1 Quick Configuration Wizard .................................................................. 229  
5.10.1.2 Camera Wizard .................................................................................... 236  
5.10.1.3 Copy Configuration ............................................................................... 242  
5.10.2 Communication Ports .................................................................................. 243  
5.10.3 Discovery .................................................................................................... 245  
5.10.3.1 Discovery - Proprietary Configuration ................................................. 248  
5.10.3.2 Discovery - Generic Camera Configuration .......................................... 253  
5.10.3.3 Supported Edge Devices ...................................................................... 254  
5.10.4 DNA Application .......................................................................................... 255  
5.10.5 Export - Background Export ..................................................................... 255  
5.10.6 Export - Mass Export ................................................................................ 260  
5.10.7 MapBuilder .............................................................................................. 266  
5.10.8 Mentor ...................................................................................................... 270  
5.10.9 Rediscovering or Replacing a Unit ............................................................... 274  
5.10.9.1 Time Synchronization ........................................................................... 277  
5.10.10 Reporting Tool .......................................................................................... 278  
5.10.10.1 Installing the Reporting Tool ............................................................... 279  
5.10.10.2 Starting the Reporting Tool .................................................................. 279  
5.10.10.3 Using the Reporting Tool ................................................................... 280  
5.10.10.4 Configuring the Reporting Tool ........................................................... 282  
5.10.10.5 Reports ............................................................................................... 284  
5.10.11 Safrun ...................................................................................................... 286  
5.10.12 Scene Tracker ........................................................................................... 287  
5.10.12.1 Starting Calibration from the AdminCenter ....................................... 288  
5.10.12.2 Calibration Wizard ............................................................................. 289  
5.10.12.3 Create a New SceneTracker View ....................................................... 296
# Table of Contents

5.10.13  SNMP ..................................................................................................... 305
5.10.13.1 Trap Filter .................................................................................. 307
5.10.14  Tile Layout .............................................................................................. 309

6. Configuration - Settings ............................................................................................ 310

6.1  Changing IP Address and Computer Name ........................................................ 310
6.2  Coverages ....................................................................................................... 311
6.3  Licensing ........................................................................................................ 313
6.4  Profiles ........................................................................................................... 318
6.4.1  Picture Profile ........................................................................................... 319
6.4.2  Video Profile ........................................................................................... 320
6.4.3  Vendor-Specific Profile ............................................................................ 322
6.5  Schedules ....................................................................................................... 322
6.5.1  Picture Schedule ..................................................................................... 324
6.5.2  Quality of Live Stream Schedule ............................................................... 325
6.5.3  Quality of Recorded Stream Schedule ....................................................... 325
6.5.4  Recording Schedule ................................................................................. 326
6.5.5  Attached Entities Tab ............................................................................... 327

6.6  Software Components ...................................................................................... 327

7. Configuration - Server Components ......................................................................... 329

7.1  Application Server ............................................................................................ 329
7.2  Active Directory ............................................................................................... 331
7.3  Archiver .......................................................................................................... 334
7.3.1  Monitoring of Storage Tampering Attempts .............................................. 345
7.3.2  Archiver Failover ...................................................................................... 346
7.3.3  Archiver Status Check and Notification ...................................................... 349
7.3.4  Export - Background Export ...................................................................... 354
7.4  CaseBuilder .................................................................................................... 358
7.4.1  Cases - CaseBuilder Features .................................................................... 359
7.4.2  Adding a CaseBuilder Server .................................................................... 360
7.4.2.1  CaseBuilder Data Location Folder Setup .............................................. 366
7.5  Database ......................................................................................................... 366
7.5.1  Backing Up a Server Database .................................................................... 368

7.6  Directory ....................................................................................................... 370
7.6.1  Directory Failover ..................................................................................... 371
# Table of Contents

7.7  Event Distributor (EDB) .................................................................................................................. 372
7.8  Gateway Server .............................................................................................................................. 372
7.9  Global Admin Server Component ................................................................................................. 375
7.10 Map Server .................................................................................................................................... 377
7.11 Mail Server ..................................................................................................................................... 378
7.12 Transcoder ...................................................................................................................................... 379
7.13 Transcoder - Web Publishing ......................................................................................................... 386
7.14 Web Server Setup .......................................................................................................................... 392
7.15 Update Services Server .................................................................................................................. 394
# 1 Getting Started

**Welcome to This File**  
**Using this Help File**  
**Log On using Command Line**

## 1.1 About This File

Welcome to the United VMS 8.0.5 Admin Center Help File.  
**Note:** Changes to this file were compiled on 12/22/2019 and introduced after Application Build No: 6127  

### Summary of latest changes:

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Summary</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Analytics</td>
<td>Sep 2018</td>
<td>Added description of basic analytics and behavior with motion detection</td>
<td><a href="#">Basic Analytics</a></td>
</tr>
<tr>
<td>Updated Privileges screen shot to include Output pin</td>
<td>Sep 2018</td>
<td>Updated Privileges screen shot to include Output pin</td>
<td><a href="#">Privileges</a></td>
</tr>
<tr>
<td>Added conditional Event feature</td>
<td>Sep 2018</td>
<td>Added Conditional event feature</td>
<td><a href="#">Logical View Conditional Event</a></td>
</tr>
<tr>
<td>Removed “feature set” from dashboard</td>
<td>Sep 2018</td>
<td>Removed the Feature Set line from the Dashboard screenshot</td>
<td><a href="#">Dashboard</a></td>
</tr>
<tr>
<td>Added button for collapse all</td>
<td>Sep 2018</td>
<td>Added info about new “collapse all” button. Updated screenshots too</td>
<td><a href="#">Selection Pane / Navigation Tree</a></td>
</tr>
<tr>
<td>Updated CCTV keyboard info</td>
<td>July 2018</td>
<td>Added commands list for new FLIR CCTV keyboard</td>
<td><a href="#">Controlling the ControlCenter via CCTV Keyboard</a></td>
</tr>
<tr>
<td>Added Alarm Predefined Clear Descriptions to alarms management</td>
<td>June 2018</td>
<td>Added Alarm Predefined Clear Descriptions to alarm management section</td>
<td><a href="#">Alarm Management</a></td>
</tr>
<tr>
<td>Remote Control Center entry revised</td>
<td>June 2018</td>
<td>Description updated</td>
<td><a href="#">Remote Control</a></td>
</tr>
<tr>
<td>Updated &quot;change password&quot;</td>
<td>June 2018</td>
<td>Updated edge change password screenshot with &quot;confirm password&quot; option</td>
<td><a href="#">System - Edge Security</a></td>
</tr>
</tbody>
</table>
## Change | Date | Summary | Links
--- | --- | --- | ---
screenshot |  |  |  
Updated Transcoder page | June 2018 | Updated outdated info on Transcoder page | Transcoder
Edited Web Server Section | Mar 2018 | Only one Web Server may be defined | Web Server
Map Definition | Mar 2018 | Browse button added to Map File setup. | Map GIS Maps
Archiver Storage | Mar 2018 | Text in Archiver Storage Span window was updated. | Archiver
Privacy Mask | Mar 2018 | Editing Window for Privacy Mask redesigned. | Camera Privacy Mask Tab Adding a Privacy Mask to a Video Scene
Live Streaming - Unicast TCP Streaming option | Oct 2017 | Archivers, and cameras which support Unicast TCP streaming may be set to use this stream connection option | System/General/Stream Connection Types Camera General Tab - Stream Connection Types
Edge Security | July 2017 | 2 Warnings: 1. Changing password on a PTZ which is in an active Control Center session will result in loss of PTZ capability. Admin Center operator must ensure correct PTZ Driver is selected. 2. If the user has Quasar Gen II and/or IOI-HD units, then if firmware is upgraded then Certificates must be reloaded. | When Using Change Password on PTZ Cameras Reload Certificates when updating firmware on Quasar Gen I and IOI-HD
Licensing | June 2017 | Licensing Web Site link for new installations changed (effective mid July 2017) | Licensing
System Security | June 2017 | Setting the parameter 'Using Secured Edge Connection' applies to new units, rediscovered units and firmware upgrades | System - System Security
Timer | June 2017 | Timer entity moved to Logical View | Timer
<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Summary</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Security - Edge Device Security</td>
<td>May 2017</td>
<td>Note added that Certificates must be loaded before enabling TLS</td>
<td><a href="#">System - System Security</a></td>
</tr>
<tr>
<td>Timer</td>
<td>April 2017</td>
<td>Timer Entity added in Physical View</td>
<td><a href="#">Timer</a></td>
</tr>
<tr>
<td>Unit Credentials</td>
<td>Apr 2017</td>
<td>Change to text of the Credentials Required field, and warning message added.</td>
<td><a href="#">Unit</a></td>
</tr>
<tr>
<td>Improved Discovery Process</td>
<td>Mar 2017</td>
<td>Unified discovery of FLIR devices, easier camera attachment</td>
<td><a href="#">System - Discovery</a></td>
</tr>
<tr>
<td>Transport Layer Security (TLS) for Edge Devices</td>
<td>Mar 2017</td>
<td>Ability to secure control communications with edge devices. Manage edge device connections</td>
<td><a href="#">System - System Security</a>, <a href="#">System - Edge Security</a></td>
</tr>
<tr>
<td>Password Management</td>
<td>Mar 2017</td>
<td>Manage password status</td>
<td></td>
</tr>
<tr>
<td>Licensing</td>
<td>Mar 2017</td>
<td>The Licensing page has changed, and a new Licensing Site is used.</td>
<td><a href="#">Licensing</a></td>
</tr>
<tr>
<td>Thermal Analytics Setup in Admin Center</td>
<td>Mar 2017</td>
<td>Setting up analytics for FC-ID range</td>
<td><a href="#">Camera Analytics</a></td>
</tr>
<tr>
<td>Timer Entity</td>
<td>Mar 2017</td>
<td>New entity allows Triggering Events by Timer</td>
<td><a href="#">Timer</a></td>
</tr>
<tr>
<td>Administration of Users across Multiple Systems</td>
<td>Mar 2017</td>
<td>Global Admin Server is now a standard feature</td>
<td><a href="#">Global Admin Server</a></td>
</tr>
<tr>
<td>Directory Backup Schedule</td>
<td>Dec 2016</td>
<td>User can specify frequency for backups of directory information</td>
<td><a href="#">Directory Backup Schedule</a></td>
</tr>
<tr>
<td>Status of FoD Backup information</td>
<td>Dec 2016</td>
<td>Failover directory screen edited to make it clear that the field regarding synchronization indicates whether changes that have been made to the Directory are already backed up or not</td>
<td><a href="#">Directory Failover</a></td>
</tr>
<tr>
<td>'Directory failed to synchronize'</td>
<td>Dec 2016</td>
<td>New event added - 'Directory failed to synchronize'</td>
<td><a href="#">Server Entity Events</a></td>
</tr>
<tr>
<td>Change</td>
<td>Date</td>
<td>Summary</td>
<td>Links</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Analytics Events</td>
<td>Nov 2016</td>
<td>Updated list of supported Events to include Analytics-related events</td>
<td>Events</td>
</tr>
<tr>
<td>Recorder License</td>
<td>Nov 2016</td>
<td>New license type authorizes connection of FLIR Recorders</td>
<td>Dashboard</td>
</tr>
<tr>
<td>Supported Browsers</td>
<td>Oct 2016</td>
<td>Listed supported Browsers</td>
<td>Web Server</td>
</tr>
<tr>
<td>Camera Thermal Settings Tab</td>
<td>Oct 2016</td>
<td>When a Thermal Camera is selected in the Camera Configuration page, a new Tab allows the user to set parameters for the Thermal image.</td>
<td>Camera Thermal Settings</td>
</tr>
<tr>
<td>Dual Sensor Cameras</td>
<td>Oct 2016</td>
<td>Dual Sensor cameras show as two separate entries in the Selection/Navigation Pane</td>
<td>Camera</td>
</tr>
<tr>
<td>Connecting DVRs</td>
<td>July 2016</td>
<td>FLIR Digital Video Recorders (DVRs) are now integrated into the system. DVRs are capable of receiving input from multiple cameras, allowing the cameras to be viewed in real time, storing the videos remotely, and retrieving the recordings for viewing through the systems.</td>
<td>DVRs</td>
</tr>
<tr>
<td>Panoramic Lens Cameras</td>
<td>July 2016</td>
<td>Configuring the Quasar Gen 2 and other panoramic-lens cameras</td>
<td>Lens Configuration</td>
</tr>
<tr>
<td>Binding Cameras and Encoders</td>
<td>June 2016</td>
<td>How to associate Cameras and Analytics Encoders</td>
<td>Binding Cameras and Encoders</td>
</tr>
<tr>
<td>Supported Devices</td>
<td>June 2016</td>
<td>Link to updated list of Supported Devices</td>
<td>Supported Edge Devices</td>
</tr>
<tr>
<td>File information</td>
<td>May 2016</td>
<td>This new topic was introduced so that users could see the file status and have a summary of relevant recent changes.</td>
<td>(This topic)</td>
</tr>
<tr>
<td>Change</td>
<td>Date</td>
<td>Summary</td>
<td>Links</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Transcoder Archiver Tab</td>
<td>May 2016</td>
<td>Link from the application to this topic was updated</td>
<td>Transcoder</td>
</tr>
<tr>
<td>Camera Discovery Parameters</td>
<td>May 2016</td>
<td>The Quasar Fish-eye camera model was added. Adjustments to list of Plug-ins.</td>
<td>Camera General Tab / Lens Configuration Discovery - Proprietary Configuration</td>
</tr>
<tr>
<td>Camera Discovery Parameters</td>
<td>May 2016</td>
<td>The Generic Camera Plug-in was updated</td>
<td>Discovery - Generic Camera Configuration</td>
</tr>
<tr>
<td>Log On using Command Line</td>
<td>March 2016</td>
<td>Allows Clients to log on using Command lines, for example where there is no keyboard access to a remote computer.</td>
<td>Log On using Command Line</td>
</tr>
<tr>
<td>FLIR Branding</td>
<td>March 2016</td>
<td>The United VMS 7.0 suite was re-branded.</td>
<td></td>
</tr>
</tbody>
</table>

Please note: This is not a formal Change Register - the list is included so that users can quickly access Topics that contain new or changed information.

Quick Links to key sections of the Help File:

<table>
<thead>
<tr>
<th>System Overview</th>
<th>AdminCenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration - Entities</td>
<td>Configuration - Functionality</td>
</tr>
<tr>
<td>Configuration - Settings</td>
<td>Using this Help File</td>
</tr>
</tbody>
</table>

File information:

Source file: Latitude Admin Center Help File 8.0.5.pdf

Date compiled: Sunday, December 22, 2019

Please note: This is a reference to the Source File for the Help system. It is not accessible from User systems.
1.2 Using this Help File
The system has a context-sensitive Help function, with specific information such as explanations about icons used, how to add, edit or delete entries, default values, cautions and notes where required.

Open the Help file by clicking on a Help system icon
1. Right-click anywhere in the Table of Contents, and select Open all to see the full Table of Contents.
2. This opens the full Table of Contents, so you can see all the material that is available.
3. Use Search to find specific words or phrases.
4. Use Favorites to bookmark Help pages that you want to access frequently.

1.3 Log On using Command Line
The Admin Center is normally loaded on the local machine by the user by clicking on the Admin Center icon.
For some instances it may be convenient to start the application and log in using the Command line.

Note:
1. The processes described below will not work if the Admin Center is already running on the workstation.
2. Each of the following instances refers to a NEW installation. For systems that have been upgraded from previous versions, the file path begins:
   C:\Program Files (x86)\DVTEL...

Admin Center Log On to a single directory
The following syntax is required:
C:\Program Files (x86)\Latutude\AdminCenter\AdminCenter.exe
-u="admin" -p="password" -s="server-address"

Admin Center Log On to multiple directories
Where multiple directories are needed, the addresses of all the required servers should be entered:
C:\Program Files (x86)\Latutude\AdminCenter\AdminCenter.exe
-u="admin" -p="password" -s="server-address1 server-address2 server-address3 ..."

Logging On via Command Line using Encrypted Password

Caution When using Command Line Log On, the text and arguments of the process are readable to any operator of the target Admin Center machine. In order to prevent exposing the normal User password, it is recommended to use the following process that creates an encrypted version of the password.

In order to encrypt a password:
1. Open CMD
2. Enter command:
   cd C:\Program Files (x86)\Latutude\Tools\PasswordEncryptor
3. Enter command:
   Latutude.PasswordEncryptor.exe Password
4. Go to C:\Program Files (x86)\Latutude\Tools\PasswordEncryptor folder
5. The file “encrypted.txt” contains your encrypted password

Using the Encrypted Password
In the Logon instructions above, use the text in the encrypted.txt file as the password in the Password argument.
This password text will only work for the Command Line Log On. If an operator tries to use this encrypted password to gain regular access to a client workstation through the Login screen, it will not be accepted.
2 System Overview

Latitude is a network-based video and audio management system comprised of servers, client workstations, connected media units (e.g. encoders, decoders, cameras, domes, etc.) and additional optional components, such as external storage modules, and sensors. The system provides a single, highly customizable client application, **ControlCenter**, for viewing live and archived media, alarms and interactive maps. It supports all matrix-style features such as sequencing and guard tours. A second client application, **AdminCenter**, allows for robust management of every aspect of the system, including camera and recording parameters, user privileges, alarm behaviors and much more.

Latitude is designed for maximal scalability and flexibility in order to enable any combination of remote and local monitoring and archiving. The system topology diagram below illustrates a typical setup such as might be used by a customer such as a retail bank that has multiple small- or medium-sized branches, a large centralized data center and a separate security office. Note that monitoring is not limited to the security office in this example -- it can be performed by local personnel at the branches or by any user that connects to the system from within the corporate network or via the Internet (using a Transcoder and Gateway server, not shown in the diagram below).

The system is built on open standards to allow integration with a wide variety of additional devices and systems via its System Development Kit (SDK). Examples include integration to PTZ devices, access control systems, content analysis systems, and building automation systems.
2.1 System Concepts

Capabilities and Scenes

Latitude implements the concept of **scene entities**, which provide users with the ability to configure most aspects of the system offline. The majority of the entities appearing in the logical tree, such as cameras, microphones, serial devices and sequences, are **scenes**. Scenes that represent external devices must be associated with a unit capability, or the unit port connecting the device (e.g. a camera) to Latitude (e.g. Encoder Video In port).

Capability entities do not have settings that can be configured in their AdminCenter configuration panes. You can, however, change the scene attached to a capability through its Context menu (right-click on the entity) in the Selection View Pane. This allows authorized users to switch cameras and other scenes between units without having to reconfigure their settings (e.g. when a unit malfunctions).

Alarms

An **alarm** is a special type of **event** that can be defined in the system for situations where an immediate operator response is usually required. For a discussion on how Events are defined, and actions are associated with them, see [Events and Actions](#).

Examples are *movement detected by a camera*, or *a signal from an external input to a camera contact* (such as from a door contact.)
## Alarm States

An Alarm can be in any one of the following states:

<table>
<thead>
<tr>
<th>Action</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm triggered</td>
<td>Alarm sensed by the system. Alarm status is <strong>ON</strong>. Alarm is sent to all specified recipients.</td>
</tr>
<tr>
<td>Alarm activated</td>
<td>Same as Alarm triggered, but this is generated by a CC operator rather than by an event sensed by the system.</td>
</tr>
<tr>
<td>Alarm accepted</td>
<td>One of the CC recipients sees that alarm is <strong>ON</strong>. Accepts the alarm. Alarm status becomes 'accepted'. Other recipients now cannot process the alarm.</td>
</tr>
<tr>
<td>Alarm cleared</td>
<td>Ends the life cycle of the alarm.</td>
</tr>
<tr>
<td>Alarm forwarded</td>
<td>A user who was a recipient for this alarm adds a new user to the list of recipients.</td>
</tr>
<tr>
<td>Alarm snoozed</td>
<td>One of the CC recipients sees that alarm is <strong>ON</strong>. By snoozing the alarm, the escalation defined for that alarm is delayed.</td>
</tr>
<tr>
<td>Alarm unaccepted</td>
<td>A user who previously 'accepted' an alarm now returns it to the list of recipients as a ‘triggered’ or ‘activated’ alarm.</td>
</tr>
</tbody>
</table>

## Alarms Life Cycle

A typical alarm life cycle is described below, showing the different Alarm Events that occur as the Alarm is raised (either by an 'Alarm triggered' action, or by a the Control Center operator clicking on 'Create Alarm') through to when the Alarm event ends ('Alarm Accepted' action).

<table>
<thead>
<tr>
<th>Step</th>
<th>Alarm Events</th>
<th>Alarm State and Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alarm Triggered (Global)</td>
<td>Alarm is triggered and immediately sent to its highest priority recipients, Alice and Bob. The number shown in both station's active alarms indicator (on the left side of the Viewing Pane toolbar) increases by one.</td>
</tr>
<tr>
<td></td>
<td>Alarm Activated (for Alice and Bob)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Alarm Snoozed (for Alice)</td>
<td>Alarm is snoozed by Alice. Once snoozed, the alarm disappears from Alice's screen and the number shown in the active alarms indicator decreases by one.</td>
</tr>
<tr>
<td>3</td>
<td>Alarm Forwarded (for Bob)</td>
<td>Alarm is forwarded by Bob to Charlie. It immediately disappears from Bob's screen and appears on Charlie's. Bob's active alarms indicator is decremented and Charlie's is incremented.</td>
</tr>
<tr>
<td>Step</td>
<td>Alarm Events</td>
<td>Alarm State and Behavior</td>
</tr>
<tr>
<td>------</td>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Alarm Activated (for David)</td>
<td>Since the alarm has yet to be accepted, it is sent to its second-priority recipient, David. The number of active alarms on his station is incremented.</td>
</tr>
<tr>
<td>5</td>
<td>Alarm Activated (for Alice)</td>
<td>The alarm reappears on Alice's screen after her (local) snooze interval (3 minutes) ends. Her active alarms indicator is incremented.</td>
</tr>
<tr>
<td>6</td>
<td>Alarm Forwarded (for Bob) Alarm Activated (for Charlie).</td>
<td>David forwards the Alarm to Bob. It immediately disappears from David's screen and appears on Bob's. David's active alarms indicator is decremented and Bob's is incremented.</td>
</tr>
<tr>
<td>7</td>
<td>Alarm Accepted (Global)</td>
<td>Bob accepts the Alarm.</td>
</tr>
</tbody>
</table>

Alarms have a number of properties that make them geared for this type of use:

- **They require a user response.** Unlike standard events, alarms remain active until they are accepted by a user. They are sent only to users configured to receive them and can be broadcast to a specific recipients group, to all recipients at once or in a staggered fashion.

- **They are automatically displayed on special " Armed for Alarm" tiles.** When alarms are triggered, they are shown in viewing pane tiles armed for alarms. A user may not replace an active alarm with other content before responding to the alarm (though the alarm may be "covered" by another alarm with a higher priority if there are more active alarms than armed tiles.)

A user is configured to use one of three possible behaviors that determine the way alarms are presented to that user — Block mode, Flat mode, or Salvo mode. See [Configuring an Alarm with Cameras](#) and Displaying a Camera on Alarm (manual and automatic).

- **They may be triggered manually or by event.** Unlike most events, alarms can be triggered from ControlCenter by a user (e.g. as a response to some suspicious activity.)

- **They allow for sequencing live video, archived video and maps within a single tile.**

**Alarm Handling**

Each alarm type is associated with a group of users, known as its recipients, as well as a notification method (either sending alarms to all recipients as soon as they are triggered or
sending them in a staggered fashion based on the recipients' priorities). There are three primary ways that a user can respond to an alarm:

- **By clearing** an alarm, a user signifies that the situation has been contained and no longer requires active monitoring by any of the users to which it has been sent. Once cleared, the alarm disappears from all client workstations, though copies of the alarm may remain in the form of client-side sequences (which are not alarms but merely sequences based on alarm displays).

- **By snoozing** an alarm, a user indicates that the alarm situation does not require immediate attention and can be handled at a later time. The alarm remains active but disappears from the user's display for a pre-configured period of time (typically a few minutes). It reappears after this interval unless the alarm has already been cleared by another user.

- **By forwarding** an alarm, a user hands off responsibility for it to another user. When an alarm is forwarded, it becomes essentially "cleared" from the perspective of the original user, who no longer has the responsibility (or even the capability) to deal with it any further. From a system perspective, however, the alarm is still active and relevant.

In addition to the alarm responses described above, there are two other alarm-related actions users may take without effecting the alarm's state:

- If an alarm procedure has been defined for the alarm type, a user may display it by clicking the procedure button in the alarms pane.

- An alarm can be "copied" onto another tile in the form of a client-side sequence. The copy, unlike the alarm itself, can be controlled by the user like a regular sequence. Additionally, it does not disappear until actively removed by the user, even once the alarm from which it was created has been accepted.

### Manually Displaying an Alarm

While alarms are typically displayed automatically on armed tiles, an active alarm that appears in a user's alarm queue can always be manually displayed on any ControlCenter tile (except an armed tile displaying another active alarm) by dragging and dropping it from the queue onto the tile.

### Privileges

Latitude 8.0 features a robust privileges model that enables administrators to control users' access to each entity in the system. The model employs positive and negative inheritance and also enables exceptions without having to change parent entity settings. To facilitate ease-of-use, it is possible to set privileges and access rights to all members of a user group and individual users.

For more information, see [Privileges & Access Rights Configuration](#).

### Active Directory

Active Directory integration enables Latitude administrators to do the following:

- Comply with IT standards by providing support for the management of Latitude users and user groups via the Active Directory instead of Latitude.

- Facilitate central user management when used with Global Latitude systems by integrating all Latitude directories with the same Active Directory service.
• Provide the option for simplified sign-in to Latitude applications. Users that are logged in to MS Windows using their Active Directory credentials have the option to launch Latitude applications without having to log in again.

In order to work with the Active Directory, the relevant license option is required. After creating an Active Directory entity, use the Windows credentials to log in to and activate the Active Directory.

The Active Directory can only be activated when there are no user groups and users defined in the system (except the default Users user groups and the System Admin user). Once the Active Directory is activated, it is impossible to add new users and user groups from within Latitude. They can only be added via the Active Directory entity. This ensures a consistent and reliable user system. New user groups and users are imported via the Active Directory entity once the Active Directory is activated.

The AdminCenter that configures the Active Directory should be able to communicate directly with the Active Directory. Therefore it is not recommended to configure Active Directory when logged in as a Remote Client.

For more information, see Active Directory Configuration.

- Transport Layer Security (TLS)

Communications between the Web Server and Web Clients can be encrypted, so that use of the Web Client does not provide unprotected access to the system. When TLS is operational, all communications between Web Server and Web Clients (video/audio content AND Control Messages) are encrypted.

The user must arrange through his IT department for a suitable Certificate to be made available.

Changes are made to the system configuration, and the User's IT department must check that the required Ports are available - See System / IP Security

2.2 Server Components - Overview

Latitude 8.0 has five primary server applications running as Windows Services.

**Directory server**

The Directory server is used to manage system configuration data, Alarm management, Incident Management and Failover. For more information on the Directors server, see Directory Server.

**Archiver**

Device management, Discovery, Video and Audio archiving, Metadata tracking, Sequence creation/management, Media routing, Failover and redundancy. For more information on the Archiver server, see Archiver Server.

**Event Distributor (EDB)**

The Event Distributor is used as an interface for passing events and actions between different Latitude components, as well as between the system and external devices and programs. For more information on the Event Distributor, see Event Distributor (EDB) Server.

- **Transcoder**

  The Transcoder is an application that converts live and archived video streams from
MPEG4 to MJPEG. For more information on the Transcoder, see Transcoder & Gateway Servers.

- **Gateway Server**
  The optional Gateway Server is used when instances of client applications such as the Control Center and Admin Center are to be connected remotely to the system. For more information on the Gateway server, see Transcoder & Gateway Servers.

- **ControlCenter**
  Client users can create, configure, research and export case files for investigative use. For more information, see Control Center.

- **Application Server**
  The Application Server allows external systems to create and run their own plug-ins that run as part of the Latitude system, and have access to the Latitude APIs. For more information, see Application Server.

- **Web Server**
  The optional Web Server is an instance of the Windows Internet Information Service (IIS) and is used to support registered users wishing to view live and/or recorded video directly from non-dedicated PCs within the organization or over the Internet. See Web Server.

- **CaseBuilder Server**
  The optional CaseBuilder Server provides a centralized location for managing and storing case files. For more information, see CaseBuilder Server.

- **Global Admin Server**
  The optional Global Admin Server allows multiple Latitude systems to share User and User Group credentials. See Global Admin Server.

### Monitoring Overall System Status
- Each computer on which any Latitude services are installed, also runs the Safrun watchdog service and its counterpart GUI application (which can be launched from the Windows System Tray).

### Databases
- The Directory, Archiver (and EDB, if the audit trail reporting feature is installed) each use an MSDE/MSSQL database. MSDE comes packaged with the Latitude software. Under some circumstances, a full MSSQL instance may be required instead.
- You can view the database size of each server. For more information, see Database.

#### 2.2.1 Directory Server
- The Latitude Directory’s primary functions are:

  **Management of system configuration data.** The Directory is the primary database of the system, holding the up-to-date configuration data - all the system entities, their components and status. It also holds other important information such as the access rights and privileges of users.

  At any one time, there will be a ‘Primary’ Directory, which is accessed by all system functions that need the most up-to-date information.
One or more ‘Failover’ Directories may be defined in the system. These are continually updated so that in the event of a failure of the Primary Directory, a Failover Directory can take over the functions of the Primary.

Even though more than one Failover Directory may be defined, in practice, only one 'becomes' the Primary in the event of a failure.

(In one particular case, more than one Failover Directory can become 'Primary' - this occurs when communication is lost between multiple sites where Failover Directories are configured. In such a case, each disconnected area that includes a Failover Directory is able to continue functioning until communication is re-established.)

Whenever a server or client application comes online, it queries the Directory for all settings relevant to its functions, including for example, whether to allow a user to log in, or which archiving schedules to follow for each camera.

When a configuration change is made, it is sent to the Directory, which updates the configuration database and generates an event -- distributed via the EDBs -- to inform other system components of the change.

**Alarm management.** Alarms are managed by the Directory, which is responsible for following the pre-configured alarm handling procedures. These procedures determine which users receive an alarm; what content is displayed for it (typically one or more live or playback scenes); and how the alarm should be escalated if notified users fail to respond in the allocated amount of time (e.g. send the alarm to other users, send an e-mail, etc).

**Incident Management.** While bookmarks are maintained by Archivers, the Directory keeps track of incidents and the bookmarks associated with them.

**Failover.** An additional 'Failover' Directory/ies can be configured to automatically take over the primary Directory's role in case of failure. The Primary (active) Directory constantly updates the Failover Directory so that the system can continue operating without interruption in the case of Directory failover.

A loss of communication with the Latitude 8.0 Directory does not cause complete system failure, even without a Failover Directory. This is because all system components maintain a locally-stored copy of their settings. You can still view live and archived media, search the archives, control PTZs and digital zoom, and view maps after the Directory fails. Directory failure does, however, prevent new users from logging on to the system, prevent any user from changing system configurations, and disables alarm functionality.

### 2.2.2 Archiver Server

The Archiver's main functions are:

- **Device management** - Every edge device (encoder, decoder, IP camera, etc.) connected to Latitude is controlled by an Archiver, which manages their video, audio and data capabilities (including I/O pins, serial ports, and PTZ drivers). While units' settings are stored by the Directory, the Archiver is the only system component that directly communicates with them. In particular, it instructs units where to send their streams -- and what quality settings to use -- based on user requests and network capabilities.

- **Discovery** - The Archiver Discovery Service handles all unit discovery in the system. Discovery works in accordance with ONVIF Profile S.
System Overview

- **Video and audio archiving** - In order to optimize media storage, the Archiver creates a system of files known as *containers*. When storing video or audio, the Archiver directs the Operating System exactly which locations to use in order to utilize the available disk space in the most efficient manner. The resulting performance improvement is especially pronounced as the disks near capacity, since the Archiver continues to have large uninterrupted blocks of space available for its use, rather than the much smaller blocks that result from natural disk fragmentation when this function is done by the Operating System.

- **Tamper-proof Storage** - The system can be set to digitally sign all stored content, thus enabling a check on the integrity of all recordings.

- **Metadata tracking** - The Archiver intelligently manages the different types of recordings -- manual, scheduled, event-driven, and alarm-driven. It supports clip locking and forced deletion of clips on expiration. It also seamlessly handles simultaneous recording of different types for the same video or audio stream. Along with maintaining information about each clip's recording triggers, the Archiver also keeps track of bookmarks and motion activity, both of which may be used to search for archived media.

- **Sequence creation and management** - The Archiver is charged with creating and distributing sequences.

- **Media routing** - Latitude uses the Archiver as a highly sophisticated bridge (or proxy) between separate multicast-enabled LANs to send high-bandwidth video to multiple client workstations. For more detail, see Archiver Media Routing.

- **Failover and redundancy** - Latitude provides a prioritized failover mechanism that allows system administrators to control which units fail over -- and which Archivers they fail over to -- under various circumstances (see here for more information). Failover can also be triggered manually for server maintenance purposes. In addition, the system supports fully redundant Archiver recording (scheduled recordings only).

- **Archiver failure notification and troubleshooting information** - The Archiver provides ongoing Archiver Status Checking that validates the Archiver is operating trouble free and able to record. If the Archiver fails the status check, notification icons appear on the cameras and devices associated to the Archiver. These notification icons not only alert AdminCenter users and help troubleshoot but also alert ControlCenter client users that the Archiver is unable to record on the indicated cameras. For more information, see Archiver Status Check and Notification.

**Performance and Scaling**

In Latitude the main process of the Archiver has been subdivided into 3 sub-processes:

- **AM (Archiving Manager)**
  The AM is responsible for the communication with the Latitude system, controlling the units (managing PTZ and picture settings), executing the planned schedules, *ad hoc* EDB tasks, and activating the ART.

- **ART (Archiver Real Time)**
  The ART is the most active part of the Archiver. Its main function is to focus on real-time activities, such as streaming and recording.

- **AD (Archiver Discovery)**
  The AD is responsible for the Discovery process.

Separating the Archiver's main tasks into the AM, ART and AD sub-processes enhances the scalability and performance of the Archiver. By default, a single Archiver is configured to sup-
port up to 70 cameras. However, the actual number supported can vary (up or down), depending on the mix of units.

For large installations, several Archivers are necessary. Multiple Archivers are also typically required for systems that have a complex network topology.

### 2.2.3 Event Distributor (EDB) Server

The Event Distributor is an interface for passing events and actions between different Latitude components, as well as between the system and external devices and programs. By assigning event processing to a dedicated server or servers, the system's ability to handle a large number of events is significantly enhanced. The latter option may be required for systems that handle a very large amount of events (typically when integrating Latitude with other event-based systems). The number of EDBs that should be used by a system depends also on its network topology and related latency considerations.

If audit trail reporting is enabled, each EDB maintains an Audit Trail database that stores information about the system events sent via the EDB.

### 2.2.4 Transcoder & Gateway Servers

The **Transcoder** is an entity that can be added to the AdminCenter. It allows any of the available camera scenes to be made available as Capture Devices.

By registering each of the user-selected live camera scenes as independent capture devices on the local machine operating system, these video capture devices can be exploited by third party applications. A application can request from the listed capture devices a variety of standard capture device formats for features like streaming TCP video, recording, cropping, resizing, color correction, etc.

For streaming video for example, this feature coupled with available third party applications such as Windows Media Encoder or Windows Expression 4 and allow transmission to a remote client or over TCP via the Internet or a Wide Area Network (WAN). For more information, see the **Transcoder** section for setup as capture devices and then the **Web Publishing** section which has example procedures on streaming audio with two download applications offered by Microsoft Windows.

The **Gateway Server** acts as the interface between remote clients and Latitude's server applications. It handles all command and control responsibilities with clients outside the local area network and, like the Transcoder, typically relies on router port forwarding to receive external requests. The Gateway's default communication port is 7777.

See **Gateway Server**

### 2.2.5 Application Server

The Application Server hosts external plug-ins that will be loaded and run as part of the Latitude system.

An Application Server should be used whenever a plug-in does not include GUI/presentation components or Directory Logic. Typically, this would be for plug-ins that are built to allow Latitude to communicate with 3rd-party apps.

The Application Server's main functions are to:
• Provide full API functionality for external programs
• Increase scalability and stabilize core system performance by providing separate processing capability for functionality provided by external plug-ins
• Interface for applications to provide Monitoring and event notification
• Provide separate fail-over capability for non-native functions.
For setup information, see Application Server

2.2.6 Web Server
The Web Server is a dedicated application that supports Web Client functionality, allowing casual users, working either from within the organization's network environment, or logged on over the Internet, to log in to the Web Server, and then access the live and recorded material for which they are authorized.
The Web Client is supported under Windows, Linux or Mac OS-X (Snow Leopard).
The system can be set to use Transport Layer Security (TLS) to encrypt the connections to all Web Client connections. See System security / Web Security

Supported Browsers
Chrome: Version 29 and later
IE: Version 11 and later
Opera: Version 16 and later
Minimum resolution - 1280 x 800

The Web Server is not a separate entity like Archiver or Directory – it refers to the Windows Internet Information Server (IIS) component. It is shown in the Latitude Navigation tree. See Web Server Setup.
2.2.7 Update Services Server
The Update Services Server provides a central location from which client applications may download new versions of the Latitude software when required, and install them automatically.
See Update Services Server

2.2.8 CaseBuilder Server
The CaseBuilder allows privileged operators to collect and organize data into Cases, and export it in a verifiable form to a shared location outside the Latitude system, so that it can be accessed by other systems. For example, a Case may be taken off-site for third-party investigations or to a court of law.

A case can include multimedia data, such as video clips, audio clips and snapshots. It can also include Meta-data such as events, alarms, and bookmarks. The user can add attachments of any file types or URLs, as well as text descriptions to the case and its data.

The CaseBuilder server supports authorized ControlCenter users using the CaseBuilder mode to find and assemble content for occurrences such as criminal violations that are captured by the system and documented by the system users. It provides centralized storage and tracking of the Case files that are created.

An overview of CaseBuilder features and configuration is covered in more detail in the CaseBuilder section.

2.2.9 Global Admin Server
The Global Admin Server, if available in your system, is an independent Latitude server that allows User Groups and Users to be administered across multiple Latitude systems.

A stand-alone server is set up in a network location accessible to all participating Latitude systems. The correct server definitions must be created in each of the systems.

Once this is done, a User Group or User may be designated to be Global. When this is done, the following information is shared across all participating systems:

- User names and passwords
- User privileges
Notes:

1. If a User is designated to be Global but does not belong to a Global User group, they will automatically be added to a Default Global User Group.
2. The Default Global User Group cannot be deleted.
3. If a Global user is deleted on one of the participating systems, then the deletion will be replicated on the other participating systems.
4. If a Global User is deleted and the system finds that User is specified as the recipient of a system-generated email, or is designated as a recipient in an Alarm action on any of the participating systems, then the user will be restored and placed in the default Global User Group.

Setting up the Global Admin server is described in Configuration - Server Components/Global Admin Server Component

Setting up Global User Groups and Global Users is described in User Management/Global User Groups and Global Users

2.3 Client Applications

Latitude has two main client applications: ControlCenter, used to view live and archived media, search for archived media, control PTZ devices, respond to alarms, etc; and AdminCenter, used to configure system entities and settings.

The Web Client application allows casual users to log in to the Latitude system and use a subset of functionality of the Control Center. The Web Client can run in any network-connected computer running a supported Browser.

Client applications require the User to log in with a system-recognized User Name and Password. Each defined User of the system can have their own tailored set of privileges, allowing defined levels of access to each of the system's facilities. The system can be set to allow or disallow concurrent multiple log-ins by a single user.
2.3.1 Control Center Client
Control Center is the primary client application of the Latitude platform. The following are a few highlighted features:

- A highly customizable workspace, allowing authorized users and administrators a great deal of control over the look and layout of the application, from determining where panes are located on the screen to applying completely new user-designed skins.
- The ability to choose specific tiles for instant-replay, alternative content and for alarms or if a user chooses, to allow default rollover display in the next available tile.
- Multiple-source bookmarking using incidents.
- Enhanced sophisticated audio capabilities, including the ability to mix sources and associate a single source with multiple cameras.
- Combined PTZ and digital zoom controls.

The full Control Center description starts at Control Center.

2.3.2 Admin Center Client
Admin Center is the system's configuration application. It provides an efficient work flows that take advantage of the scene and profile concepts put forth by Latitude to make the setup process both quicker and more powerful. Admin Center now provides the ability to perform off-line configuration, which allows administrators to configure most system entities before the system is installed at its permanent site (the main exceptions are Latitude servers, PTZ devices and connected analog matrices).

Once the system and its edge devices (units) are installed, it can quickly be brought online by performing discovery and linking the pre-configured entities to the physical units.

The full Admin Center description starts at Admin Center.

2.3.3 Web Client
While professional security users and Control Room operators require the full-fledged functionality of the Control Center application, there are many other users who can use the browser on their computer to access the simpler Web Client for non-dedicated access to live or recorded video. The Web Client application, working through a Web Server configured as part of the Latitude system, allows them to access video from regular PCs through any of the browsers listed below, within the corporate environment, or even (with suitable Internet connection speeds), over the Internet from home or other locations.

**Supported Browsers:**

- Chrome: Version 29 and later
- IE: Version 11 and later
- Opera: Version 16 and later
- Minimum resolution - 1280 x 800

The Web Client is a simple and thin video monitoring application which provides quick and easy access to any user, by simply opening the browser at:

http://[Latitude web server URL]/webclient
The Web Client offers basic functionality and is easy to use. It supports live video monitoring and PTZ control, simple search of recorded video for playback, thumbnail visual search, and export of clips.

Users who wish to access video content using a Web Client must register a user name and password with the system administrator, who will also issue them with the required privileges to access content. After accessing the Web Server from their PCs, users log in with their user name and password, and can then access the live and recorded video that they are authorized to see.

The Web Client has its own Help File accessed from a Toolbar drop-down.

2.3.4 Global Client

Global Client is a client-side feature that allows users to connect to multiple Latitude systems from the ControlCenter and AdminCenter applications. It allows users to login to different systems using different or identical user names and passwords.

Logging In to Multiple Systems for the First Time

To connect to multiple systems for the first time, first connect to a single Directory in one of the Latitude client applications.

Next, log in to additional systems by going to System — Connect... in the ControlCenter or System — Connect... in the AdminCenter.
Connecting AdminCenter to an additional system

Connecting ControlCenter to an additional system

The system shows the regular login box for the chosen Client application.

Once you enter a **Username**, **Password** and the **Directory** computer name, the application will log in to the new Directory in addition to the one to which it is already connected. You will then see two trees (without a common root) in the AdminCenter **View Selection** Pane and ControlCenter **Navigation** Pane.

**Logging In to Multiple Systems in the Following Login Attempts**

After connecting to any system for the first time, the login information is saved. In the following login attempts, it is possible to globally connect to previously connected systems. Select the check boxes of the (multiple) desired directories to which the user previously connected from the Directory or gateway drop-down list, and click OK to connect to multiple directories at once.

**Logging Out of a System**

To log out of a system, go to File>System>Disconnect>[System Name] in ControlCenter or System>Disconnect>[System Name] in AdminCenter.
Limitations

The Global Client feature does not give the systems any additional "knowledge" of each other on the server side. It is not designed to "connect" distinct systems, but rather to give users the ability to conveniently use multiple systems simultaneously. As a result, the following capabilities are not available in Global Client mode:

- A scene from one system cannot be played (or played back) using an analog monitor or speaker that belongs to another system.
- An incident involving scenes from multiple systems cannot be created.
- A layout saved in the ControlCenter may only contain scenes from its own system (i.e. scenes that appear under the same System in the Navigation Tree).
- When connecting to multiple Directories in the ControlCenter, it is possible to switch systems (i.e. control different directories) from a CCTV keyboard if it is connected to the ControlCenter (but not if it is connected to a serial port of an encoder/decoder).

2.3.5 Client Portal

Latitude supports a Client Portal, allowing authorized users to easily download local copies of the Admin Center and Control Center Client Applications.

In addition, Users who wish to run the Control Center Client without a permanent installation on their computers may use the Quick Control Center Application.

To access the Client Portal, use your browser to access <ServerName>/Clientportal
Choose the required option and complete the process as guided by the installation instructions.
The Installation file is downloaded, and the normal Control Center or Admin Center Login screen is displayed. The user can then enter the IP address of the Latitude system - when connected to an internal network, connection is to the Directory server address (or the All-in-One system). When connecting from an outside network, connection is through the Gateway server.

2.3.6 Client Upgrades
Latitude Versions are issued from time to time, and require new or upgraded licenses. The user downloads the full software build and runs either a New Installation or an Upgrade. Latitude versions are identified by the first two sets of numbers in the full version number shown on the Admin Center Dashboard and the Control Center Splash Screen, or in the About screen accessed from either the Admin Center or Control Center Main Menu.

The Client Upgrade process is described in Upgrade Services Server
3 AdminCenter User Interface

AdminCenter is United VMS 8.0.5's system administration application. It is used to configure virtually every aspect of the system, from its largest building blocks, such as Archivers and Networks; to basic parameters such as picture brightness, video format and user names. The application is designed to allow administrators to maximally utilize Latitude's robustness while minimizing the need to specify countless settings to achieve the desired effects. To achieve this, AdminCenter introduces a number of powerful new concepts:

**Dashboard**
The dashboard provides a managerial snapshot on various system-wide activities and settings. By looking at the dashboard, the user is able to view the status and data of the different components managed via the AdminCenter.
For more information, see [Dashboard](#).

**Sidebar**
The sidebar enables quick access to filtered views of the Latitude trees as well as easy activation of common tasks. The sidebar can be hidden using the collapsing method.
For more information, see [Sidebar](#).

**Scenes**
A scene is a logical entity comprised of one or more system capabilities, such as cameras, sequences and serial ports (but not units, which are collections of capabilities). Unlike a capability, a scene has no inherent physical properties, but merely serves as a label for some combination of linked capabilities that do. This provides a powerful level of abstraction that has a number of advantages:

1. More robust association between system capabilities. Audio and video from separate units may be streamed to the same tile, for example, or a camera may be shown with audio in one scene and without in another, allowing the system administrator to control which users have access to the "enhanced" scene.
2. Off-line configuration. The use of scenes provides system integrators with the ability to pre-configure most of the system's settings before going on site. The only steps that must then be performed at the system's permanent location are discovering units and linking their capabilities to pre-configured scenes.
Profiles
Profiles are user-defined groups of settings that may be applied to various entities, typically, though not always, through the various Settings tabs' relevant camera entities.

Enterprises
Enterprises provide the ability to partition the system into independently-managed "sub-systems" that share most of their resources. The crucial feature of an enterprise is that it is associated with its own set of users, including an enterprise system administrator, which do not "see" the system outside their enterprise and are invisible to users in other enterprises (but not to users at the root of the System). See here for more information on enterprises.

Enhanced Scheduling
Latitude supports a number of different schedule types, including picture and motion detection schedules. All schedule types in the system are defined by a combination of two basic parameters, a profile and a coverage (or super coverage).
3.1 Dashboard

Upon starting the AdminCenter, the Dashboard view appears, providing a managerial snapshot on various system-wide activities and settings. By clicking the desired option on the Sidebar, you can access the workspace.

An overview of the following information appears in the dashboard:

- **Cameras** - All cameras currently defined in and attached to the system, and detailed data on the currently defined cameras.
- **Users** - The number of currently defined and logged on users. By clicking on **Logged on Users**, an Operator with the required Privileges can right-click on a selected user to access the command **Logout user**. This allows a supervisor or other suitably-configured operator to terminate a user session remotely.
- **Archivers and Storage** - The number of currently defined Archivers and all video devices attached to them, and detailed data on the currently defined storage.
- **Recording Video Quality** - The recording video quality Profiles currently defined in the system.
- **Database Health** - The database size, log size and status of the servers currently defined in the system.
- **License Information** - Detailed information about the license currently activated for the system, including the activation key.

It is possible to access more detailed information by clicking the links in the Channels and Archivers and Storage boxes.
In addition, it is possible from the Dashboard to repair cameras that are inaccessible or not recording.

**Cameras**

In the Cameras box, it is possible to view the following options:

- all cameras of the system
- all inaccessible cameras of the system
- all recording cameras of the system

By clicking the (Total) or (Inaccessible) links, you can drill-down to view the detailed list of cameras and their status.

The list contains the following information:

- **Icon** - indicates the status of the camera (inaccessible, recording or idle)
- **Name** - the camera name and IP address
- **Recording** - the status of the camera (inaccessible, recording, idle or repairing)
- **Archiver** - the name of the Archiver to which the camera is attached

To return to the Dashboard, click the button in the Cameras box or click System on the sidebar.
To repair an inaccessible camera

1. Access the desired camera by clicking Cameras (Total) or Cameras (Inaccessible) on the dashboard.
2. Right-click the failed camera, and then select Repair.
3. The system will attempt to repair the camera accessibility.

Archivers and Storage

In the Archivers and Storage box, it is possible to view the following options:
- all Archivers defined in the system
- all storage defined in the system

By clicking each option and you can drill-down to view the detailed list of Archivers and cameras attached to the Archivers, and the storage units and their status.

To view the Archivers and the attached cameras

1. Access the list of Archivers by clicking Archivers in the Archivers and Storage box.

The list of all Archivers appears.

The list contains the following information:
- Icon - indicates the status of the Archiver (connected or disconnected)
- Name - the Archiver name and IP address
- Cameras - the number of cameras attached to the Archiver
- CPU - the percent of CPU usage of the Archiver
- Memory - the commit charge of the machine that the Archiver is running on
- Throughput - the Network traffic of the Archiver
2. To view the cameras attached to the Archivers, click the row of the desired Archiver. The list of cameras connected to the selected Archiver is shown.

3. To return to the dashboard, click the button in the Archivers and Storage box or click System on the sidebar.

**To view the Storage units**

1. Access the list of Storage units by clicking Defined Storage in the Archivers and Storage box.

![Defined Storage Screen](image)

The list of defined storage of the system appears, listed according to Archivers.

![Storage Units Screen](image)

The list contains the following information:

- Icon - indicates the status of the Archiver (connected or disconnected)
- Name - the Archiver name and IP address to which the storage is allocated
- Locations - the number of storage locations
- Storage - the storage size

2. To return to the dashboard, click the button in the Archivers and Storage box or click System on the sidebar.

**To repair an inaccessible camera**

It is possible to repair the camera accessibility by drilling down to the relevant cameras from the Storage.

For more information, see [To repair an inaccessible camera](#).
3.2 Workspace

The AdminCenter workspace is comprised of three regions:

Sidebar
The Sidebar provides quick access to filtered views of the Latitude trees as well as easy activation of common tasks.

Selection Pane
The Selection Pane provides various views of the system as a whole and is used to browse to entities in order to see their detailed parameters and to configure them if necessary. The Tabs and Panels displayed in the Selection Pane change depending on the type of entity selected.

Configuration Pane
The Configuration Pane is used to configure the entity selected in the Selection Pane.

3.2.1 Sidebar
The Sidebar enables quick access to filtered views within Latitude as well as easy activation of common tasks. The Sidebar can be hidden using the collapsing method that is commonly used in Latitude. The Sidebar consists of the following icons and sub-menus:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name/Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="System Link" /></td>
<td>System</td>
</tr>
<tr>
<td>Logical View</td>
<td>Logical View</td>
</tr>
<tr>
<td>Physical View</td>
<td>Physical View</td>
</tr>
<tr>
<td><img src="image" alt="System Settings" /></td>
<td>System Settings</td>
</tr>
<tr>
<td><img src="image" alt="Video" /></td>
<td>Video</td>
</tr>
</tbody>
</table>
System
When the System button on the Sidebar is clicked, the Dashboard appears. The dashboard provides a managerial snapshot on various system-wide activities and settings. Using the drop-down menu of System, you can access to the following options:

- Connect - Connect to Latitude systems
- Disconnect - Disconnect from currently connected Latitude systems
- Change Password - Change the existing password of the AdminCenter
- Tools - Display the Options dialog box.
- Check for Updates - Allows the user to apply the latest updates where necessary. See Update Services server
- Help - Display the Online Help
- About - Display the version of the AdminCenter
- Exit - Exit the AdminCenter

Logical View
When clicking the Logical View button on the Sidebar, the system's Logical View appears. The Logical View is used to browse through, create, and manipulate logical entities. You can also copy entity configurations and export field reports.

Physical View
When clicking the Physical View button on the Sidebar, the system's Physical View appears. The Physical View is used to browse through, create and perform actions on physical entities. You can also backup databases, add camera sequences, add matrices, replace entities with...
either new or existing entities, perform manual failover, end failover, and copy the unit configuration.

**System Settings**

When clicking the System Settings button on the Sidebar, the System Settings View appears. The System Settings View is used to browse through, create, and remove “helper” entities (entities used to configure logical and physical entities) and alarms. Using the drop-down menu of System Settings, you can directly access the following entities:

- Profiles
- Schedules
- Coverages
- Software Components
- License
- Alarm Types

**Video**

Clicking the Video button on the Sidebar causes the Video entities defined in the system appear in the Logical Tree. Using the drop-down menu of Video, you can directly access either Cameras or Analog Monitors.

**Audio**

When clicking the Audio button on the Sidebar, the Audio entities defined in the system appear in the Logical Tree. Using the drop-down menu of Audio, you can directly access either Microphones or Speakers.

**Users and Groups**

When clicking the Users and Groups button on the Sidebar, the users and user groups defined in the system appear in the Logical Tree. Using the drop-down menu, you can directly access the Recipients Groups, User Groups and Users defined in the system.

**Servers**

When clicking the Servers button on the Sidebar, the system's Server applications appear.

**Applications**

When clicking the drop-down menu of the Applications button on the Sidebar, you can access other applications. Only those applications that are installed will appear in the drop-down menu; some applications require separate installation. You will be automatically logged in to the selected application with the currently logged in user name.

The following applications can be accessed provided they are installed on your system:

- Control Center - Access the ControlCenter
- Discovery Networking Assistant (DNA) - Access the DNA Application
- Reporting Tool - Opens the Reporting tool page which is an application that provides reports on past Latitude events by querying the audit databases maintained by the Latitude EDB servers (e.g. reports on User Logon, Entity Configuration, Incident, Alarm, Equipment Failure, and Server Monitoring)
- **Map Builder** - Accesses the Map Builder which is an application that allows the creation of full-featured security maps that can be used by the operator for command and control on a graphic image that provides a layout overview of a physical security array of devices. (e.g. An aerial photo with camera icons.)

**Discovery**

When clicking the **Discovery** button on the Sidebar, the Physical tree is displayed and the **Discovery** tab appears.

**Wizards**

When clicking the drop-down menu of the Wizards button on the Sidebar, you can access the following wizards to assist you in the configuration process of the AdminCenter:

- **Quick Configuration Wizard** - Access the [Quick Configuration wizard](#)
- **Camera Wizard** - Access the [Camera Wizard](#)
- **Copy Configuration Wizard** - Access the [Copy Configuration wizard](#)
- **User Group Wizard** - Access the [User Group Wizard](#)

### 3.2.2 Selection Pane / Navigation Tree

The **Selection Pane** provides general views of the entities in the system, depending on what part of the system needs to be displayed.

The different views are accessed directly via the **Sidebar**, or by selecting a view from the drop-down window at the top of the Selection Pane.

![Logical View]

The different views help the user by displaying only those entities or components that are required tasks related to them:

- **Physical view** relates to activities that are concerned with the connections of devices to their hosts
- **Logical view** highlights the way the installation is arranged by the user - i.e. Entities are grouped by sites, etc
- **System Settings view** shows Profiles, Schedules, Coverages, Software Components, License and Alarm Types
- **Video view** shows only Cameras and Analog monitors
- **Audio view** shows only Speakers and Microphones
- **Users and groups view** shows Recipients Groups, User Groups and Users
- **Servers view** shows Archivers, Directory Servers, EDBs, Gateway Servers, CaseBuilder Servers and Transcoders
- **Discovery view** shows a Physical view, and displays the Discovery parameters in the Viewing Pane

**Note**: When the Selection Pane drop-down is first used, it will only show the Physical, Logical and System Settings Views. If the user accesses any other view using the Sidebar, the corresponding entries are added to the drop-down options.
Toolbar icons for the View Selection Pane:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Drop-down list&gt;</td>
<td>The drop-down list is used to switch between previously accessed views (general and entity-specific) during the same login instance. The list is cleared once you log off.</td>
</tr>
<tr>
<td>🔄</td>
<td>Click this button to refresh the entity tree.</td>
</tr>
<tr>
<td>🕹️</td>
<td>Click this button to sort and group the entity tree.</td>
</tr>
<tr>
<td>🌐</td>
<td>Click this button to access the Copy Configuration wizard.</td>
</tr>
<tr>
<td>✖️</td>
<td>Click this button to Delete an entity</td>
</tr>
<tr>
<td>✫</td>
<td>Click this button to add an entity to the currently selected location</td>
</tr>
<tr>
<td>🕸️</td>
<td>Right-click this button to select the desired tree filtering properties.</td>
</tr>
</tbody>
</table>

Icon State Symbols

The *state* of entities in the Navigation tree is reflected in their icons.

<table>
<thead>
<tr>
<th>Icon state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚡️</td>
<td>Entity being recorded.</td>
</tr>
<tr>
<td></td>
<td>Icons of Offline entities are shown grayed out.</td>
</tr>
<tr>
<td>🕹️</td>
<td>Disconnected entity</td>
</tr>
<tr>
<td>🎤</td>
<td>Entity linked to a microphone</td>
</tr>
<tr>
<td>🌐</td>
<td>input/output pin device in an abnormal state.</td>
</tr>
<tr>
<td>🌐</td>
<td>input/output pin device in an unknown state.</td>
</tr>
<tr>
<td>✖️</td>
<td>Archiver for this entity failed..</td>
</tr>
</tbody>
</table>
3.2.2.1 Logical View

The Logical View is used to browse through, create and manipulate logical entities. Actions on the entities displayed may be performed using contextual right-click options.

**To access the Logical View, click the Logical View button in the Sidebar.**
### Entity | Icon | Description | Right Click Options
--- | --- | --- | ---
**System** | ![System Icon] | System - The entity that represents the entire system and is used to configure system-wide parameters and launch unit discovery. | Add [any logical entity], Disconnect from System and Export Field Report. |
**Enterprise** | ![Enterprise Icon] | An enterprise is a part of the system associated with entities (including users) and its own password and locking policies. | Add [any logical entity except Enterprise], Copy Configuration and Remove. |
**Site** | ![Site Icon] | A site is a grouping of logical entities, typically based on their location. | Add [any logical entity except Enterprise or User] and Remove. |
**ControlCenter** | ![ControlCenter Icon] | A ControlCenter that resides in the same directory/System system as the AdminCenter. | Remove |
**ControlCenter Monitor** | ![Monitor Icon] | A monitor controlled remotely via a ControlCenter residing within the same directory/System system as the AdminCenter. | Remove |
**Conditional Event** | ![Event Icon] | A conditional event combines two sources as the trigger for subsequent VMS operations | Copy Configuration and Remove. |
**User** | ![User Icon] | A user of the system has a number of attributes, including a name, password and privileges. | Copy Configuration and Remove. |
**Camera** | ![Camera Icon] | A camera is any NTSC or PAL analog video capture device that can be connected to an encoder’s video input port (an IP camera thus consists of a video input port and a camera). | Copy Configuration, Remove and Camera Wizard. |
**PTZ Camera** | ![PTZ Icon] | A camera with Pan-Tilt-Zoom capabilities (the icon changes from a regular camera icon once PTZ settings are configured). | Copy Configuration and Remove. |
**Analog Monitor** | ![Analog Icon] | An analog monitor connected to a decoder’s video out port. | Copy Configuration, Remove, Connect Camera and Connect Sequence. |
<table>
<thead>
<tr>
<th>Entity</th>
<th>Icon</th>
<th>Description</th>
<th>Right Click Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Playback</td>
<td>🎬</td>
<td>A playback session that can be viewed on an analog monitor.</td>
<td>Remove</td>
</tr>
<tr>
<td>Map</td>
<td>🌍</td>
<td>An HTML page that can be created and edited in the AdminCenter and viewed in a ControlCenter tile. It may contain links to various System entities, such as alarms and cameras.</td>
<td>Remove.</td>
</tr>
<tr>
<td>Microphone</td>
<td>🎤</td>
<td>A microphone connected to a unit's audio input jack.</td>
<td>Copy Configuration and Remove.</td>
</tr>
<tr>
<td>Speaker</td>
<td>🎧</td>
<td>A speaker connected to a unit's audio output jack.</td>
<td>Copy Configuration, Remove and Connect Microphone.</td>
</tr>
<tr>
<td>Tile Layout</td>
<td>📢</td>
<td>A ControlCenter tile arrangement in which each tile may be associated with an arming state and a video, video and audio, or map source.</td>
<td>Remove.</td>
</tr>
<tr>
<td>Audio Layout</td>
<td>🎧</td>
<td>A ControlCenter audio tile arrangement in which each tile may be associated with an audio source as well as various audio settings, such as volume and solo.</td>
<td>Remove.</td>
</tr>
<tr>
<td>Camera Sequence</td>
<td>🎥</td>
<td>A video stream managed by an Archiver that is comprised of live video selected in sequence from different cameras based on user-defined parameters (sources, dwell time, etc.)</td>
<td>Copy Configuration and Remove.</td>
</tr>
<tr>
<td>SceneTracker View</td>
<td>🎥</td>
<td>A scene comprised of a number of cameras that are &quot;stitched&quot; together using Latitude's built-in SceneTracker application.</td>
<td>Remove.</td>
</tr>
<tr>
<td>Input Pin Device</td>
<td>🌈</td>
<td>An input connected to a unit's input pin.</td>
<td>Remove.</td>
</tr>
<tr>
<td>Output Pin Device</td>
<td>🌈</td>
<td>An output connected to a unit's output pin.</td>
<td>Remove.</td>
</tr>
</tbody>
</table>
### Entity Icon Description Right Click Options

<table>
<thead>
<tr>
<th>Entity</th>
<th>Icon</th>
<th>Description</th>
<th>Right Click Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipients</td>
<td>🔄</td>
<td>A group of users that receive email notifications concerning actions and events.</td>
<td>Remove</td>
</tr>
<tr>
<td>Group</td>
<td>🔄</td>
<td>A group of users that receive email notifications concerning actions and events.</td>
<td>Remove</td>
</tr>
<tr>
<td>Serial Device</td>
<td>🔄</td>
<td>A device connected to a unit via one of its serial ports that is <em>not</em> a PTZ motor.</td>
<td>Remove</td>
</tr>
<tr>
<td>Serial CCTV</td>
<td>🔄</td>
<td>A device that provides a way to control the video display on analog monitors as well as GUI monitors (tiles of ControlCenter applications).</td>
<td>Remove</td>
</tr>
<tr>
<td>Keyboard</td>
<td>🔄</td>
<td>A device that provides a way to control the video display on analog monitors as well as GUI monitors (tiles of ControlCenter applications).</td>
<td>Remove</td>
</tr>
</tbody>
</table>

The analog monitor **Connect Camera** and **Connect Sequence** options and the Speaker **Connect Microphone** option allow an administrator to specify a default scene to be sent to the monitor or speaker.

### 3.2.2.2 Physical View

The Physical View is used to browse through, create and perform actions on physical entities.

Entities that are only viewable in the Physical View include the following: **Audio In Port, Audio Out Port, Input Pins, Output Pins, Video In Ports**, and **Video Out Ports**.

Actions on the entities displayed can be performed using contextual right-click options.

To access the Physical View, click the Physical View button in the Sidebar.

![Physical View Diagram](image-url)
<table>
<thead>
<tr>
<th>Entity</th>
<th>Icon</th>
<th>Description</th>
<th>Right Click Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>![system_icon]</td>
<td>System - the entity that represents the entire system and is used to configure system-wide parameters and launch unit discovery.</td>
<td>Add Archiver, Add Archiver Failover Group, Add Directory, Add Network, Add EDB, Add Gateway Server, Add Mail Server, Add Network, Add Transcoder, Disconnect ➤ System and Export Field Report.</td>
</tr>
<tr>
<td>Directory</td>
<td>![directory_icon]</td>
<td>A service charged with managing the other server application as well as maintaining a database of all system settings (see Server Applications for more information on the Directory).</td>
<td>Backup on Local Machine, Backup on Server, Become Primary Directory, Perform Synchronization, Remove and Shutdown.</td>
</tr>
<tr>
<td>Directory (Failover - Standby)</td>
<td>![directory_fallback_icon]</td>
<td>This Directory is defined as a failover unit, and is currently in standby mode</td>
<td></td>
</tr>
<tr>
<td>Directory (Failed Sync)</td>
<td>![directory_sync_error_icon]</td>
<td>Changes have been made to the Active Directory, and this Failover Directory has not yet saved the changes to its database</td>
<td></td>
</tr>
<tr>
<td>Directory (Inaccessible)</td>
<td>![directory_access_error_icon]</td>
<td>This failover Directory has been defined, but it currently not accessible within the system</td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td>![directory_active_icon]</td>
<td>The directory that holds the user accounts and groups in the organization This is the 'current' Directory.</td>
<td>Remove, Synchronize Now</td>
</tr>
<tr>
<td>Archiver</td>
<td>![archiver_icon]</td>
<td>A service that manages units, archives video and audio, proxies media between networks and manages sequences (see Server Applications for more information on the Archiver).</td>
<td>Add Camera Sequence, Add Matrix, Add Unit Manually, Attach Existing Camera Sequence, Backup on Local Machine, Backup on Server, End Failover, Failover, Refresh Configuration from Directory, Remove and Shutdown.</td>
</tr>
<tr>
<td>Archiver Failover Group</td>
<td>![archiver_fallback_icon]</td>
<td>A group of Failover Archivers that facilitates their management.</td>
<td>Remove</td>
</tr>
<tr>
<td>Unit</td>
<td>![unit_icon]</td>
<td>An encoder, decoder, recorder or IP camera with some component.</td>
<td>Remove, Reboot and Detach from Archiver.</td>
</tr>
<tr>
<td>Entity</td>
<td>Icon</td>
<td>Description</td>
<td>Right Click Options</td>
</tr>
<tr>
<td>-----------------</td>
<td>------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Video Input</td>
<td><img src="image" alt="icon" /></td>
<td>A combination of video, data and audio capabilities.</td>
<td></td>
</tr>
<tr>
<td>Camera</td>
<td><img src="image" alt="icon" /></td>
<td>A camera is any NTSC or PAL analog video capture device that can be connected to an encoder's video input port (an IP camera thus consists of a video input port and a camera).</td>
<td>Copy Configuration, Detach, Remove and Camera Wizard.</td>
</tr>
<tr>
<td>PTZ Camera</td>
<td><img src="image" alt="icon" /></td>
<td>A camera with Pan-Tilt-Zoom capabilities (the icon changes from a regular camera's once PTZ settings are configured).</td>
<td>Copy Configuration, Remove and Camera Wizard.</td>
</tr>
<tr>
<td>Video Output</td>
<td><img src="image" alt="icon" /></td>
<td>A decoder's video output port.</td>
<td>Replace attached camera with a new camera and Replace attached camera with an existing camera.</td>
</tr>
<tr>
<td>Analog Monitor</td>
<td><img src="image" alt="icon" /></td>
<td>An analog monitor connected to Video Output.</td>
<td>Remove and Detach.</td>
</tr>
<tr>
<td>Audio Input</td>
<td><img src="image" alt="icon" /></td>
<td>A unit's audio input port.</td>
<td>Replace with New/Existing Microphone.</td>
</tr>
<tr>
<td>Microphone</td>
<td><img src="image" alt="icon" /></td>
<td>A microphone connected to an Audio Input.</td>
<td>Copy Configuration, Detach and Remove.</td>
</tr>
<tr>
<td>Audio Output</td>
<td><img src="image" alt="icon" /></td>
<td>A unit's audio output port.</td>
<td>Replace with New/Existing Speaker.</td>
</tr>
<tr>
<td>Speaker</td>
<td><img src="image" alt="icon" /></td>
<td>A speaker connected to an Audio Output.</td>
<td>Copy Configuration, Remove and Detach.</td>
</tr>
<tr>
<td>Input Pin</td>
<td><img src="image" alt="icon" /></td>
<td>A unit's input pin.</td>
<td>Replace with New/Existing Input Pin.</td>
</tr>
<tr>
<td>Input Relay</td>
<td><img src="image" alt="icon" /></td>
<td>An input connected to an Input Pin.</td>
<td>Copy Configuration, Remove and Detach.</td>
</tr>
<tr>
<td>Output Pin</td>
<td><img src="image" alt="icon" /></td>
<td>A unit's output pin.</td>
<td>Replace with New/Existing Output Pin.</td>
</tr>
<tr>
<td>Output Relay</td>
<td><img src="image" alt="icon" /></td>
<td>An output connected to an Output Pin.</td>
<td>Copy Configuration, Remove and Detach.</td>
</tr>
<tr>
<td>Entity</td>
<td>Icon</td>
<td>Description</td>
<td>Right Click Options</td>
</tr>
<tr>
<td>----------------------</td>
<td>------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Serial Port</td>
<td>🌐</td>
<td>A unit's serial port.</td>
<td>Add Serial CCTV Keyboard, Add Serial Device, Attach Existing CCTV Keyboard, Attach Existing Serial Device and Copy Configuration.</td>
</tr>
<tr>
<td>Serial Device</td>
<td>🌐</td>
<td>A device connected to a unit via one of its serial ports that is not a PTZ motor.</td>
<td>Copy Configuration, Remove and Detach.</td>
</tr>
<tr>
<td>Camera Sequence</td>
<td>📸</td>
<td>A video stream managed by an Archiver that is comprised of live video selected in sequence from different cameras based on user-defined parameters (sources, dwell time, etc.)</td>
<td>Copy Configuration, Remove and Detach from Archiver.</td>
</tr>
<tr>
<td>Mail Server</td>
<td>💌</td>
<td>The server responsible for dispatching notifications.</td>
<td>Remove</td>
</tr>
<tr>
<td>Matrix</td>
<td>🌐</td>
<td>An analog matrix connected to and controlled by an Archiver.</td>
<td>Remove Matrix and Detach from Archiver.</td>
</tr>
<tr>
<td>Network</td>
<td>🌐</td>
<td>A user-defined network used to configure the Archiver.</td>
<td>Remove</td>
</tr>
<tr>
<td>EDB</td>
<td>🌐</td>
<td>Latitude's event distribution service (see Server Applications for more information on the EDB).</td>
<td>Backup on Local Machine, Backup on Server, Remove, Shut Down and Refresh Configuration from Directory.</td>
</tr>
<tr>
<td>Gateway Server</td>
<td>🌐</td>
<td>The service used by remote clients to connect to the Latitude system.</td>
<td>Remove, Shut Down and Refresh Configuration from Directory.</td>
</tr>
<tr>
<td>Transcoder</td>
<td>🌐</td>
<td>A service charged with transcoding video from MPEG4 to MJPEG (typically for transmission over the Internet to remote clients).</td>
<td>Remove, Shut Down and Refresh Configuration from Directory.</td>
</tr>
</tbody>
</table>

### 3.2.2.3 System Settings View

This System Settings View is used to browse through, create and remove "helper" entities (entities used to configure logical and physical entities) and alarms.
To access the System Settings View, click the **System Settings** button on the Side-bar.

To create an entity in the System Settings View, right-click the entity's category (e.g. Coverages, Profiles, etc.) and choose **Add [specific entity type]**.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Icon</th>
<th>Description</th>
<th>Right Click Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Types</td>
<td></td>
<td>An entity that can be triggered either manually or based on predefined events and is shown on armed tiles only based on alarm display settings. An alarm is distinguished from simple events in that it requires a user response.</td>
<td>Copy Configuration and Remove</td>
</tr>
<tr>
<td>Coverage</td>
<td></td>
<td>A period of time during the week (Sunday-Monday, 12:00 AM-11:59 PM), effective from a start date to an end date (if specified) and used to define schedules.</td>
<td>Remove</td>
</tr>
<tr>
<td>Super Coverage</td>
<td></td>
<td>A positive and negative combination of coverages, used to define complex schedules (e.g. all weekdays except holidays).</td>
<td>Remove</td>
</tr>
<tr>
<td>PTZ Driver</td>
<td></td>
<td>The software used to control a PTZ from Latitude.</td>
<td>Remove</td>
</tr>
<tr>
<td>Keyboard Driver</td>
<td></td>
<td>The software used to control a keyboard from an Latitude client.</td>
<td>Remove</td>
</tr>
<tr>
<td>Matrix Driver</td>
<td></td>
<td>The software used to control a Matrix from Latitude.</td>
<td>Remove</td>
</tr>
<tr>
<td>Unit Driver</td>
<td></td>
<td>The software used to control a unit from Latitude.</td>
<td>Remove</td>
</tr>
<tr>
<td>Entity</td>
<td>Icon</td>
<td>Description</td>
<td>Right Click Options</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>External Action Types</td>
<td>🗂️</td>
<td>An entity used for integration purposes by SDK users.</td>
<td>Add External Action Type, Copy Configuration and Remove</td>
</tr>
<tr>
<td>External Event Type</td>
<td>🗂️</td>
<td>An entity used for integration purposes by SDK users.</td>
<td>Add External Event Type, Copy Configuration and Remove</td>
</tr>
<tr>
<td>Video Profile</td>
<td>📃️</td>
<td>A profile used to define a set of video quality settings. The video profiles are based on supported camera types and configuration parameters and appear as child entities under the Profile branch.</td>
<td>Copy Configuration</td>
</tr>
<tr>
<td>Recording Profile</td>
<td>📃️</td>
<td>A profile used to define how long after being recorded a media clip may expire.</td>
<td>Copy Configuration and Remove</td>
</tr>
<tr>
<td>Picture Schedule</td>
<td>📃️</td>
<td>A schedule, comprised of a Coverage and a Recording Profile, used to associate a time period with picture quality settings.</td>
<td>Copy Configuration and Remove</td>
</tr>
<tr>
<td>Recording Schedule</td>
<td>📃️</td>
<td>A schedule, comprised of a Coverage and a Recording Profile, used to associate a time period with recording settings.</td>
<td>Copy Configuration and Remove</td>
</tr>
<tr>
<td>Quality of Recorded Stream Schedule</td>
<td>📃️</td>
<td>A schedule, comprised of a Coverage and a Recorded Video Quality Profile, used to associate a time period with recorded video quality settings.</td>
<td>Copy Configuration and Remove</td>
</tr>
<tr>
<td>Quality of Live Stream Schedule</td>
<td>📃️</td>
<td>A schedule, comprised of a Coverage and a Live Video Quality Profile, used to associate a time period with motion detection settings.</td>
<td>Copy Configuration and Remove</td>
</tr>
</tbody>
</table>
3.3 Configuration Pane - Overview

The configuration pane is used to edit and view entity settings. While its look changes based on the entity whose information it displays, there are some characteristics shared by all variations of the pane.

Tabs
The pane presents one or more Tabs in a horizontal row, with the entity name and path display directly below. Click on a Tab to display all the information relative to that Tab.

In all Tabs, there is a standard list of toolbar icons: (from left to right): Save, Undo, Previous, Next and Help.

The selected tab provides access to all the parameters related to that tab.

Panels
Most tabs are further subdivided into horizontal panels each headed by a panel title bar. Each panel deals with a particular group of parameters.

Because there are often more parameters than can be displayed on a single screen, panels can be opened or minimized by clicking on the up- and down-arrow icons on the right of the panel title bar.

Panel Closed
Clicking this icon opens the panel.
3.4 Options

Using the *Options* menu, it is possible to set the view and login settings of the AdminCenter.

To access the *Options* menu, expand the drop-down menu of *System*, and then select *Tools -- Options*.

**Setting the View Settings**

The View Settings option is divided into Layout and Advanced settings.

- The dashboard
- The last viewed layout before logging out of the system

In the *View Settings -- Advanced* dialog box, you can set whether or not the status bar appears and at what interval it gets refreshed.

**To set Layout settings**

1. Expand the drop-down menu of *System*, and then select *Tools -- Options*.
   - The *Options* dialog box appears.
2. Expand the *View Settings* branch and click *Layout*.
3. To determine which layout appears at start-up, select the desired layout -- the dashboard or the last viewed layout.
4. Click *OK*.
To set Advanced Layout settings
1. Expand the drop-down menu of System, and then select Tools -- Options. The Options dialog box appears.
2. Expand the View Settings branch and click Advanced.
3. To display the status bar, select the Use status bar check box.
4. Set the desired interval at which the status bar gets refreshed.
5. Click OK.

Setting the Login Settings
In the Login Settings dialog box, you can set whether or not to remember the login settings.

To set Login settings
1. Expand the drop-down menu of System, and then select Tools -- Options.
2. The Options dialog box appears.
3. Click the Login Settings branch.
4. To remember the last used logins settings the next time you log in, select the Remember login settings check box.
5. Click OK.
Setting the PTZ Message Settings

In the PTZ dialog box, you can set whether or not to a message will be displayed, informing the user that a PTZ lock is about to be overridden.

1. Expand the drop-down menu of System, and then select Tools -- Options.
2. The Options dialog box appears.
3. Click the PTZ branch.
4. To display the Override PTZ Lock message when overriding the PTZ lock, select the check box.
5. Click OK.
4 Configuration - Entities

This section covers the Configuration screens of each of the Entities that can be defined in the system:

- Analog Monitor
- Audio Layout (Legacy)
- Camera
- Camera Sequence
- Enterprise
- GIS Maps
- Input Pin Device
- Map
- Microphone
- Network
- Output Pin Device
- Serial Device
- Serial CCTV Keyboard
- Site
- Speaker
- System
- Timer
- Unit
- User
- User Group
- Recipients Group
- Tile Layout

4.1 Analog Monitor

The analog monitor configuration pane contains the following tabs: General and Actions.

General

The General tab is used to name the analog monitor, enter a description for it, and define a few basic additional parameters. The tab is divided into three panes - Information, Configuration and Links.

Information

The Information pane contains one non-editable information field:

- Connected -- Indicates whether the analog monitor is connected to an accessible unit. An analog monitor may be shown as disconnected either because its unit is for some reason inaccessible or because it has yet to be connected to a unit (a typical situation when performing off-line configuration).

Configuration

The Configuration pane is used to configure several basic settings:
• Name - A generic name is given to every monitor scene when it is first created by the user or the system (see Configuration in the Latitude). It is highly recommended that you give your monitor a meaningful name.

• Description - An optional field used to provide a description of the monitor.

• Connected unit - This non-editable field lists the unit to which the monitor is connected.

• Connected port - This non-editable field lists the video input to which the monitor is connected.

• Video output format - Select NTSC/PAL

• Scene Name is indicated - Check this box if Scene information is required.

• De-blocking filter - This check-box is used to specify whether a deblocking filter should be applied to video sent to the monitor.

• Deinterlacing mode - This check-box is used to specify whether video shown on the monitor should be optimized for deinterlacing mode.

• Brightness - Use this field to adjust the brightness of any video displayed on the monitor.

Links
In the Links pane, an external speaker can be associated with a monitor so that audio from camera scenes with linked audio can be played along with the video. Clicking the drop-down opens an item browser that displays only speakers (and their logical locations).

Actions Tab
See Events and Actions.

4.2 Audio Layout (Legacy)
Older Latitude systems may have separate Layouts defined for Audio scenes. These may still be used, but no new Audio Layouts may be defined.

The audio layout configuration pane is used only to view or modify an audio layout's name and description. All other configuration is performed through ControlCenter (see Creating Layouts).

Note: On older systems, to create an audio layout, the user had to use AdminCenter: In the view selection pane (logical view), right-click the System icon, an enterprise or a site and select Add Audio Layout.

4.3 Camera
A camera represents any video source connected through a unit's video input. The Camera configuration pane allows the user to define the video input settings. The pane contains the following tabs: General, Video Settings, Picture Settings, (or Thermal Settings if this is a Thermal Camera), Recording Settings, Edge Recording, Linked, PTZ Configuration, Motion Detection, (or Analytics if this is an Analytics Camera) Privacy Mask, and Actions.

Note when deleting Scenes
When deleting Scenes, the recorded clips of these scenes will remain in the Archiver, virtually inaccessible. They will gradually expire, unless they were locked. Therefore, when deleting a
scene (which is not the same as *detaching* a scene, making it an 'offline scene'), its recordings should be deleted as well.
A scene which is a part of SceneTracker scene or otherwise part of a compound scene (e.g. an audio scene that is connected to a video scene) should not be deleted.

**Adding a Camera**

To add a camera, perform one of the following options:

- **Use the Camera Wizard.** This option is advisable when multiple cameras are added. The Camera Wizard guides you, step by step, through the camera configuration procedure. To access the Camera Wizard, click the **Wizards** button on the Sidebar, and select **Camera Wizard**. For more information, see **Camera Wizard**.

- **Access the Discovery** tab by clicking **Discovery** on the Sidebar. The discovered camera(s) then have to be configured in the various tabs listed below. For more information, see **Discovery**. This option can be used for the addition of single or multiple units.

- **Add a camera manually** directly to the required Archiver. Access the Physical View by clicking **Physical View** on the Sidebar. Right-click the required Archiver, and select **Add Unit Manually**. Define the unit type and necessary parameters. This option is only advisable for a single or a small number of cameras.

**Note on integrated Multisensor cameras**

When a Multisensor camera that is integrated into Latitude (such as the FLIR PT series) is added, two separate entries are created in the Selection Pane - one for the Visible camera, and one for the Thermal.

When accessing the Multisensor camera's Settings page, a **Picture Settings Tab** or a **Thermal Settings Tab** will be displayed, depending on which entity is selected.

**Replacing a Camera**

It is possible to replace a camera with an existing or a new camera.

- **Access the **Physical View** by clicking **Physical View** on the Sidebar. Expand the tree in the navigation tree and select the **Video in port** node of the required camera. Right-click the Video-in port and select the required option -- replace with an existing or a new camera.
4.3.1 Camera General Tab

The General tab is used to name a camera, enter a description for it, and define a few basic additional parameters. The General tab is divided into multiple panels — Preview, Information, Configuration, Multicast Configuration, Stream Connection Types, Image, Lens Configuration and GIS Positioning.

Preview

A preview of the selected camera streaming video is displayed. (Live video).

The Web Access link allows the user to access the camera's web page to make changes to its direct settings (if applicable for the selected camera).

Note: Changes made through the Web interface are normally not accessible through the AdminCenter interface, and are not stored in AdminCenter - thus if the camera is reset, such settings have to be re-entered manually.

If the video for this camera has Privacy Masking configured, you can right-click and enable and disable the mask on this preview.
Information

This pane contains two non-editable information fields:

- **Connected** -- Indicates whether the camera is connected to an accessible unit. A camera may be shown as disconnected either because its unit is for some reason inaccessible or because it has yet to be connected to a unit (a typical situation when performing off-line configuration).
- **Signal state** -- Indicates the status of the camera video signal.
- **Recording state** -- Indicates the camera is currently being recorded.
- **Device Driver** -- Indicates the device driver of the camera
- **Model** -- Indicates the camera model and firmware

Configuration

This pane is used to configure several basic settings:

- **Name** -- A generic name is given to every camera scene when it is first created by the user (in the case of an off-line camera created for off-line configuration) or the system. It is highly recommended that you give your camera a meaningful name.
- **Description** -- An optional field used to provide a description of the camera or the view it provides.
- **Connected unit** -- Non-editable field - lists the unit to which the camera is connected.
- **Connected port** -- Non-editable field - lists the video input to which the camera is connected.
- **Archiver** -- This non-editable field lists the Archiver to which the camera is attached.
- **Video source format** -- The system supports the NTSC and PAL standards.
- **Exposure mode** -- This is the type of exposure mode of the camera. (This is a camera dependent feature/setting.)
- **Low light behavior type** -- Setting that indicates what the camera behavior is when its sensors detect low light. (a.k.a. Day/Night mode). (This is a camera-dependent feature/setting.)

Multicast Configuration

This pane is used to set the multicast parameters:

- **Stream 1 IP** -- The IP address of the first multicast stream
- **Stream 2 IP** -- The IP address of the second multicast stream
- **Port** -- These non-editable fields list the ports of the respective streams.

Stream Connection Types
Configuration - Entities

This pane is used to configure how streams are sent from the unit - in unicast or multicast UDP, or, for live streaming, optionally using Unicast TCP if supported by the unit. You can set the transmission methods of the live and recording streams and of the client connection separately.

**Archiver Live Stream Type**

Unicast UDP is the default method.

**Unicast TCP Live streaming**

If the camera supports TCP, the user has the option of selecting this mode. 

**Note:** If the camera does not support TCP streaming, then the option does not appear in the option dropdown.

Camera supports TCP streaming

Camera does not support TCP streaming

**Note on using Unicast TCP Option**

For this setting to be used, it is critical that all Directories and Archivers in the system have a version of Latitude that supports the Unicast TCP Live Streaming option installed, before attaching and configuring units that will use the setting. If one or more Archivers in the system are using versions that do not support Unicast TCP, (for example Archivers designated as Fail-over resources that have not yet been upgraded), or if for any reason the version is uninstalled so that an earlier version which does not support Unicast TCP will run, this setting might interfere with live video from units on these Archivers. Users should be aware of this limitation, and should always ensure that all Directories and Archivers are on the newer version, and should always manually reset relevant units before executing an Uninstall.

As an additional protection, the Latitude uninstall process will reset any units found with Unicast TCP selected, to Unicast UDP. Details of which versions support particular facilities may be found in the Release Notes.

**Archiver Recording and Client Connection types**

When Client connection type is set to Unicast, it will always receive the stream from the Archiver. When it is set to Multicast, the stream will be sent directly from the unit if the network architecture allows it, and sent from the Archiver otherwise.

Both streams must be set to Multicast when using redundant recording.

**Image**

This panel is used to handle the image viewed from the camera. It can be rotated and switched to a mirror image.

The panel is enabled for cameras that support this feature.
Lens Configuration
This panel allows activation of panoramic ("Fish-eye") lens capability, when a suitably-equipped camera (such as the Quasar Gen 2), is used or where the associated camera is fitted with a suitable lens.
The Enable Panoramic Lens Configuration check-box in the Camera/General tab is used to enable the capability. Depending on the type of camera, the applicable list of parameters is shown.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Brand</strong></td>
<td>Quasar, Immervision, Sentry</td>
</tr>
<tr>
<td><strong>RPL Number</strong></td>
<td>Select the appropriate Lens Model (Only shown if Immervision)</td>
</tr>
<tr>
<td><strong>Position</strong></td>
<td>Ceiling, Ground, Wall (not available for Sentry)</td>
</tr>
<tr>
<td><strong>Anti-Aliasing</strong></td>
<td>Enable/Disable (Not available for Sentry)</td>
</tr>
<tr>
<td><strong>Calibrate</strong></td>
<td>(Only required for Sentry)</td>
</tr>
</tbody>
</table>

Cameras with panoramic lenses, when used with special associated software which is integrated into the Latitude system, allow the user to ‘plunge’ into the picture. Layouts can be created in the Control Center allowing the user to see multiple views from a single camera, covering a full 360° x 180° field of view.

Select the applicable parameters from the drop-downs and click Save to apply. For an example of setting up views for this type of camera, see Panoramic Camera.

**GIS Positioning**

Allows the camera's GIS positioning co-ordinates to be entered, to be used in Maps, etc.

### 4.3.2 Camera Video Settings Tab

This tab is used to configure the camera's live and recording video settings. The Video Settings parameters affect the quality of the video stream used for live display, such as frames per second (FPS) and resolution.

Video settings may be applied in one of two ways: by attaching predefined coverage settings, or by creating custom coverage settings, which may utilize either predefined or custom profiles (along with predefined coverages).

Only one instance of the AdminCenter can configure the video settings at a time. It is recommended when you are finished making configurations, that you save them and not leave the Video Settings tab sit open and idle with the selected camera exclusively locked for configurations. If you have other AdminCenter tasks, you can select your next configuration entity or tab or if you are finished, logout from the AdminCenter.

To conserve bandwidth, you may disable an encoder’s dual-streaming functionality for the camera. To do so, click the check box labeled **Recorded quality same as live quality** in the Recording tab of the Settings pane.
If supported on the scene, you can disable **Recorded quality same as live quality** to allow configuring the Record quality settings independently. Not all cameras and units support separate Live and Recording streams. If the unit was discovered with **Create separate scene for each encoder**, this will not be supported as the dual streams are treated as separate cameras.

**Preview**

In the *Preview* pane, you can view the video stream of the camera. Click the *Actual Size* button to view a large display of the video stream. The camera's stream type, Bit rate, Frame rate, Stream source IP and Resolution are displayed with the video preview.
To configure the Live and Recorded Video Settings

Video settings - Live

1. If not selected, click the sub tab **Live**.
2. If you want to create a custom Coverage, follow the steps below

   Click \( \text{Create coverage} \), in the Create coverage dialog that appears, do the following:

   a. Type a name in the Name field
   b. Type an optional description in the Description field
   c. From the Date Range fields, select a beginning date. If a specific end date is required, uncheck the Effective indefinitely box, and enter the required end date
   d. In the Day and Time grid, hold down the CONTROL key and click and drag to highlight the times that the coverage schedule will include.
   e. When finished, click OK.
   f. Repeat this step for each Coverage you want to create.

   1. Select Coverage definitions as follows:

   a. Click \( \text{Select Coverages} \) and in the Select Coverages dialog that appears, click on the coverage icon next to the Coverage name, verify the Day and Time highlights are what you need, and click OK.
**Note:** If none of the available Coverage definitions provide the schedule you need, in the Select Coverages dialog, click Cancel, go to step 2., create the Coverage you need and then redo this step.

**Tip:** It works best to configure each Coverage with its paired Profile before adding another Coverage. Complete steps 3-5 before adding the next Coverage.

b. Select a Profile option from the Profile menu.
If you selected the Profile option **Custom**, do the following
(The availability of these settings may vary among proprietary camera types and whether the camera was added as ONVIF):

i. From the **Resolution** menu, select a resolution option.
ii. To adjust the frames per second (fps), click and drag the Frame Rate slider to increase or decrease the number of frames per second.
iii. From the Compression Quality menu, select the option for the level of compression quality to use. Select Custom if you want to use the Advanced settings to define custom compression (encoding) settings.

2. To optionally modify the Advance Settings, click the Advance Panel (expand button).
Check the Advanced settings check-box, and do the following as needed:

   a. Adjust the settings slider for Bit-Rate, Key frame interval and Quality.
   b. From the Compression menu, select the compression to use.
   c. From Rate control mode menu, select the rate control mode to use.

**Note:** Advanced settings vary based on the camera model and whether the camera was added as proprietary or ONVIF. For more information on the Advanced settings of your camera, refer to the manufacturer’s documentation.

1. Click **Actual Size**, and in the video dialog that appears, review the image quality and make adjustments to your settings as needed. Click **Close** when complete.

2. Repeat step 3 through 5 for each Coverage/Profile pair.

3. Click the sub tab Recorded, and if you want to use the identical settings you just made in the Live sub-tab, assure Record quality same as live The Recording Settings screen appears.
   -OR-
   If you want to define different Recorded settings, clear Record quality same as live field and repeat steps 2 through 6 only in on the Recorded tab quality settings.

4. When finished, click and leave the tab by selecting another item in the navigation tree or exit the AdminCenter. (This is required to prevent the camera from being locked in a configuration holding status.)

**Notes:**
- To set your own Video settings, select Advanced in the General tab. This stops the operation of the Bit Rate Calculator.
If you select a Profile, the settings and values default to the predefined and the tab settings are disabled.

5. Select Save As to publish a profile. It will appear in the System Settings menu.

To remove a video setting

To remove a video setting, select it from the Coverages drop-down list, and click the Remove button.

Summary

In the Summary pane, all configured video settings are listed, displaying which coverage is currently active. Only one set of coverage settings can be active for each of the video settings.

4.3.3 Camera Picture Settings Tab

The Picture Settings tab is used to configure the camera’s picture settings. The Picture Schedule parameters affect the image quality, such as brightness and contrast.

Note: When a Thermal camera is selected, the Picture Settings tab is replaced with the Thermal Settings Tab.

Picture settings may be applied in one of two ways: by attaching predefined coverage settings, or by creating custom coverage settings, which may utilize either predefined or custom profiles (along with predefined coverages).
**Preview**

In the Preview pane, you can view the video stream of the camera.

**Settings**

In the Settings pane, you can perform the following procedures:

**To add a picture setting**

1. Choose a Coverage
   a. To use an existing Coverage:
      i. Click and in the Select Coverages dialog that appears, click on the coverage name, double check the Day and Time highlights are what you need, and click OK.
   
      **Note:** If none of the available Coverage definitions provide the schedule you need, in the Select Coverages dialog, click Cancel, go to step a. and create the Coverage you need and then redo this step.
Tip: It works best to configure each Coverage with its paired Profile before adding another Coverage. Complete steps b. before adding the next Coverage.

b. To create a Custom Coverage, click . In the Create Coverage dialog that appears, do the following:
   i. Type a name in the Name field.
   ii. Type an optional description in the Description field.
   iii. From the Start date menu, select a beginning date.
   iv. In the Day and Time grid, hold down the CONTROL key and click and drag to highlight the times that the coverage schedule will include.
   v. When finished, click OK.
   vi. Repeat this step for each Coverage you want to create.

2. Select a Profile option from the Profile menu.

If you selected the Profile option Custom, do the following:

Note: The availability of these settings may vary among proprietary camera types and whether the camera or not was added as ONVIF.

- To modify the Saturation, Hue, Contrast, or Brightness setting, in the General Settings area, click and drag the respective slider right to increase or left to decrease the respective value.
  The effects of setting changes to video image will be reflected in the video image displayed at the right.
  Note: If Saturation is disabled and set to 0, the Advanced Setting Color Enable is automatically turned off. To enable the use of the Saturation, the Advanced settings must be enabled and the Color Enabled setting selected.
- To optionally modify the Advance Settings, open the Advanced panel by clicking on the arrow .
- Enable the Advanced Settings check-box

- Adjust the settings as needed. (Advanced settings vary based on the camera model and whether the camera was added as proprietary or ONVIF. For more information on the Advanced settings of your camera, refer to the manufacturer’s documentation.)
• If you want to optionally save the custom settings to a profile for selection from the Picture Settings Profile menu (available to all cameras), click **Save As** and in the dialog that appears enter a Profile name and click **OK**.
  
a. Repeat step a) through b) for each Coverage/Profile pair.

3. When finished, click ☐️ and leave the tab by selecting another item in the navigation tree or exit the Admin Center.

**To remove a picture setting**

To remove a picture setting, select it from the Coverages drop-down list, and click the **Remove** button ✗.

**To define the Day Night mode**

For **Pro Line A** edge devices the **Day Night** mode is supported. These predefined settings enable the quick definition of the Picture settings for edge devices used on specific times of the day. The possible settings are **Day**, **Night** or **Advanced**.

In the **Picture Setting** tab **Advanced** pane, select the desired **Day Night** mode from the drop-down list -- **Day**, **Night** or **Advanced**.

- **Day mode** - Configures the camera to use the day setting of the Day/Night mode.
  (Depending on the camera, this may include enabling color)
- **Night mode** - Configures the camera to use the night setting of the Day/Night mode feature.
  (Depending on the camera, this may include disabling color or switching to IR features).
- **Advanced mode** - Saturation parameter can be enabled by selecting the Color enabled check box. If it is not selected, the scene will be black and white.

In the **Day** mode, you can adjust the Saturation level.

If you select the **Advanced** mode, select the **Color enabled** check box to have a colored scene or do not select it for a black and white scene.

**Summary**

In the Summary pane, all configured picture settings are listed, displaying which coverage is currently active.

Only one set of coverage settings can be active for a picture settings.

**4.3.4 Camera Thermal Settings**

**Note:**

This Tab is only shown when the selected Entity is a Thermal Camera. If Analytics are supported, then the screen will include an Analytics Tab.

When the selected entity is a Thermal camera, the **Picture Settings** Tab is replaced with this **Thermal Settings** Tab.

This tab shows a preview window with the current setup of the camera, and allows the user to set up Coverages and Profiles.
Preview
In the Preview pane, you can view the video stream of the camera, and see the basic camera-set On-Screen Display (OSD) information, the current Driver in use, and the Camera Model information. The OSD information is described in more detail below in the Actual Size View.

The Enable OSD check-box toggles the OSD information set by the AdminCenter
The Show AGC ROI check-box allows the user to show/hide the area used to control the Thermal Auto Gain Control (when a Custom Profile has been stored)

Actual Size View
Clicking on the Actual Size button opens a more detailed view.
Camera OSD information
The camera OSD information is set up through the Web interface, and varies according to the firmware of the particular camera model. A typical default display is shown in the example above. Setup and changes to the Onscreen Display details shown in the preview window are made through the camera’s web interface.

Latitude Stream Parameters
The following standard information is shown in the Latitude-generated OSD:
- Stream type, Bitrate, Frame rate, Stream Source, Resolution

Settings
The camera is initiated with the system default settings, and all settings are disabled until a Coverage and Profile are associated with the camera.

Coverage
The process for setting up a Coverage is as described in the Picture Settings Tab.
Profile
The parameters that may be set up in a Profile are:

**Color Palette** - The drop-down allows a choice of stored color tables that define different ways to display the Thermal image. Each camera model may have its own set of color palettes. The user should select the palette most suited to the particular situation.

Security cameras will most often display scenes using palettes that provide white-on black or black-on-white images, while for display of industrial images, the color alternatives might be more useful.

The examples below show how a particular camera (in this case, a PT-334 Thermal Head) display the same Thermal scene using different look-up tables.

![Lookup Tables](image)

**DDE** - (Digital Detail Enhancement) refers to a built-in capability to enhance the thermal images, making it easier to show transitions between different temperature ranges.

- **Auto** or **Manual**. **Auto setting** allows the settings made in this Tab to be used, while **Manual** allows the settings made through the camera’s web page to be retained.

**DDE Gain** - Slider setting. When DDE is set to Automatic, the user can change the DDE setting here without using the camera's Web Page.

**AGC** - (Automatic Gain Control): Each camera model may have its own set of AGC settings. The user should select the setting most suited to the particular situation. Typical settings are **Manual**, **Linear**, **Plateau**, **Once Bright**, **Auto Bright**, etc.

**AGC ROI** - AGC Region of Interest - Similar to AGS settings. Each camera model may have its own set of AGC ROI choices. Depending on where the camera is situated, an appropriate ROI should be selected. (For example, where part of the camera's field of view includes the sky, one would normally use setting that excludes this part of the image. Typical settings are **Custom** (allowing the user to 'paint' the desired ROI), **Full Screen**, **Horizontal OPT**, **Sky OPT**, **Center 75 Percentage**, **Center 50 Percentage**, etc.

4.3.5 Camera Recording Settings Tab
This tab is used to configure the camera's recording settings. The Recorded Quality parameters affect the quality of the video stream used for recorded video display. Recording settings may be applied in one of two ways: by attaching predefined coverage settings, or by creating custom coverage settings, which may utilize either predefined or custom profiles (along with predefined coverages).
Preview
In the Preview pane, you can view the video stream of the camera.

Settings
In the General panel, you can perform the following procedures:

To add a recording setting

1. If you want to create a custom Coverage, click in the Create coverage dialog that appears, do the following:
   a. Type a name in the Name field.
   b. Type an optional description in the Description field.
   c. From the Start date menu, select a beginning date.
   d. In the Day and Time grid, hold down the CONTROL key and click and drag to highlight the times that the coverage schedule will include.
   e. When finished, click OK.
   f. Repeat steps a - e for each Coverage you want to create.
2. Select Coverage definitions as follows:
   a. Click and in the Select Coverages dialog that appears, click on the coverage name, double check the Day and Time highlights are what you need, and click OK.
Note: If none of the available Coverage definitions provide the schedule you need, in the Select Coverages dialog, click Cancel, go to step a. and create the Coverage you need and then redo this step.
Tip: It works best to configure each Coverage with its paired Profile before adding another Coverage. Complete steps b-d before adding the next Coverage.

b. Select a Profile option from the Profile menu. If you selected the Profile option Custom, do the following (The availability of these settings may vary among proprietary camera types and whether the camera was added as ONVIF).

c. To adjust the life span of the recorded video, click and drag the Recording life span slider to increase or decrease the numeric value and then from the calendar unit (Days, Weeks, Months, or Years).

d. Repeat step a) through c) for each Coverage/Profile pair.

3. When finished, click and leave the tab by selecting another item in the navigation tree or exit the AdminCenter. (This is required to prevent the camera from being locked in a configuration holding status.)

To remove a recording setting
To remove a recording setting, select it from the Coverages drop-down list, and click the Remove button.

Recordings Lifespan
This pane is used to specify the amount of time before each type of recording clip will be labeled as 'eligible to be overwritten' provided the option to stop recording when space is full is not enabled in the System settings General tab.

- Schedule Recording lifespan -- Regular scheduled recording clips
- Redundant recording lifespan -- Duplicate recordings, initiated by the Archiver Redundant recording feature
- Motion detection recording lifespan -- Recording clips resulting from 'Record on Motion' settings
- Other recording triggers lifespan (Alarm, Action and Manual) -- Corresponding recordings
- Force deletion of expired recordings -- This check-box allows the system's administrator to force recordings from the camera to be erased once expired even if storage space is not needed. This function is useful for administering large multi-enterprise systems and for ensuring the timely removal of sensitive video clips
- Manual Recording timeout -- The default length of recording for clips initiated by the user initiating Manual recording (from the Navigation Tree or Viewing Tile Context Menus)

Summary
In the Summary panel, all configured recording settings are listed, displaying which coverage is currently active. Only one set of coverage settings can be active for a Recording Setting.
4.3.6   Camera Edge Recording Tab

The Edge Recording Tab defines parameters for cameras with Storage-on-the-Edge (SOE) that are supported by Latitude.

**Note:** If the camera is not supported, the page will be grayed out and cannot be enabled. See limitation regarding password change and security mode, if applicable, prior to configuration.

### Configuring Edge Recording

Ensure that the SD card is only formatted and mounted according to the specific cameras installation guide.

1. Define Storage for Edge Recording on the Archiver to which the camera is connected. See Archiver/Storage/Storage Location for Edge Recordings for instructions.
2. Optional: Define Video Profile for edge recording under System Settings/Profiles
3. In the camera's Recording Settings tab, add a coverage of "Always" Recording.
   
   **Note:** The recorded profile must have an "Always" Recording schedule. Event based schedules can result in edge recording storage to fill up quickly.
4. In the Edge Recording Tab:
   a. Click the check-box "Enable recording on the edge"
   b. Under Configuration > Profile, Select "Same as recorded profile" or a custom defined profile
**Note:** For older Axis cameras with Edge Recording, a custom profile or predefined Axis SOE profile must be selected. Defined profiles are only supported for a joint live/recorded stream

c. Select the Clean-up policy to be used by Latitude when storage in the camera is full.

![Profile Selection](image)

**Note:** It is recommended to use the "overwrite" option due to the limited space available on SD storage

d. Save

⚠️ **Important:** The VMS manages time for Edge Recording. The user should not make any time related changes in the camera web page. Doing so can disrupt the edge recording.

**SD Card Information:**
When using a supported Axis camera, the system will report that the Storage Location's status is Ready, and will show the total space available on the system for recordings. It may take up to one minute before this information appears.

![SD Card Status](image)

**Supported FLIR Cameras:**
CF-6308, Ariel Gen II (including CC-3103), Ariel Gen III, CP-6302, CM-6308-P1-I

**Limitations:**
1. If Edge Recording is recording and user changes password or changes security mode under System > Edge Security recording and offload will stop
   a. Workaround:
      Secure and change password prior to setting up Edge Recording configuration. If password must be changed, Edge Recording should be disabled, then the password changed and then re-enabled.

2. If a FLIR camera is set to record on the edge and is factory defaulted, the user must disable edge recording and then re-enable and save.

3. When the camera is set on “Always” Recording with SoE, if the user changes the camera’s video configuration (e.g. resolution), there might be a small gap in the recording. An example of this is when using boost upon alarm.

**Notes:**
1. Latitude does not support audio for Edge Recording
2. Latitude's ability to apply this storage policy is limited. For example, the camera may have more specific parameters regarding overwriting its storage. If in doubt, consult the camera's documentation.
3. Recordings might be corrupted if the unit shuts down due to power loss.
4. Using Axis SOE-enabled cameras: - Axis recommend formatting the SD card using the EXT4 format type.

4.3.7 Camera Linked Tab
This tab is used to link and unlink microphones and speakers to the camera scene. The Available box shows which scenes are available to link while the Linked box lists the scenes already linked. Use the single arrows to link or unlink scenes individually and the double-arrows to link or unlink all scenes at once.
4.3.8 Camera PTZ Configuration Tab

This tab is used to specify the data communication and protocol parameters for PTZ cameras. In addition, it contains a PTZ controller (identical to the one found in ControlCenter), which can be used to set presets and patterns; change iris, focus and speed settings; and access the camera’s on-screen menu.

In the Summary pane, you can add PTZ schedules.

PTZ schedules can be created based on presets and patterns.

To set a PTZ schedule

1. In the Driver configuration pane, enable the PTZ functionality by selecting the Enable PTZ functionality check box.
2. Configure a PTZ driver.
   After at least one preset or pattern is configured, the Add is enabled in the Sum-
   mary pane.
3. Click **Add** to add and set a PTZ schedule based on the selected preset or pattern.
4. In the **Summary** pane, set the desired coverage from the drop-down list.
5. In the **Preset/Pattern** column, select the desired preset or pattern for which the
   schedule is created from the drop-down list.
6. Click the Save icon to save your settings.

**4.3.9 Camera Motion Detection Tab**

The Motion Detection screen allows you to define the Coverage - the time during
which the Motion Detection will be active, and configure detection of movement and
change within a Region of Interest (ROI) on supported cameras. For more informa-
tion on Motion Detection, see the Motion Detection Overview section.
See Motion Detection.

**4.3.10 Camera Analytics**

The FLIR FC-ID Series cameras support Analytics, and these can be configured directly
rather than by having to use the camera's Web interface.
For information about cameras that support Basic Analytics (Ariel Gen III,
-6308, etc) see Basic Analytics
The following facilities are available:

**Analytics Status**
The user can set the status of the Analytics in the camera (Just as this can be done from the Control Center using the Context Menu)

**Armed/Disarmed**
Change the status of the Analytics.

**Clear**
Clear all Analytics data, events, alarms (not Settings).

**Configuration Source**
Analytics settings created and stored in the system are accessed when this switch is set to **System**.
When set to **Web**, the screen will show the current settings that were created using the camera’s Web interface. These cannot be edited in this page, and are therefore shown as **Disabled**.

### Rules Tab

The user can create three types of Analytic Rules

#### Create Rule

Clicking on an icon allows the user to use the mouse to create an outline of the required type in the viewing window.

Each left click adds a point to the shape. Right-clicking completes the shape. (For Intrusion Areas and Masking Areas, which are closed shapes, this is done by connecting the last drawn point to the first.)

The completed shape is shown as a shaded area and given the next available name for that type of rule. (The camera supports up to 4 Rules of each type.).

The Masking Area Rules are always shown at the end of the list.

The user selects a rule in the **Rules** column, and then the characteristics of each individual rule can be set in this **Rules Settings** column.

A selected rule may be deleted by clicking the trash icon.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Type</th>
<th>Rule Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📚</td>
<td>Intrusion Area</td>
<td></td>
</tr>
<tr>
<td>⬅️</td>
<td>Tripwire</td>
<td>In addition to the criteria above, the user can select a ‘direction’ to monitor.</td>
</tr>
<tr>
<td>🕐</td>
<td>Masking Area</td>
<td>Masking areas are used to define areas that should be excluded from the analytics.</td>
</tr>
</tbody>
</table>
Configuration - Entities

**Depth Calibration Tab**

- **Automatic**: The Cameras determines the depth of the scene
- **Manual**: Allows the user to create a calibration plane using the mouse
- **Disabled**: No Depth Calibration is used

**Relearn**: Clicking the relearn button clears the previous Depth Calibration and runs it again (Can take several minutes)

**General Settings Tab**

This tab allows the user to set how the Analytics will be displayed when the camera is viewed.

![General Settings Tab](image)

**Show Object Detection**

* **No boxes**: doesn't show a bounding box around moving targets, even if they trigger an event
* **Classified boxes**: shows a black bounding box around targets that have been classified, for example Human. When it triggers an event it will change to white
* **All boxes**: shows a black bounding box around all moving targets, it changes to white when it triggers an event

**Show Lines**: When selected it will show tracking lines, when not selected it does not.

**Show regions**: When selected, draws regions in black (when a region or tripwire is active it changes to white) When not selected, shows no regions

As a general recommendation, we suggest enabling drawing **Regions** and **classified boxes**.

**4.3.11 Camera Privacy Mask Tab**

The Privacy Mask screen is for configuring the option privacy mask feature which allows administrators the ability to block viewing of regions of a video scene when viewed by some or all operators using the xx.

The mask is a password-protected on-screen display that can only be removed by authorized users.

**Notes**:

1. When a clip is exported in .avi format, the mask is embedded in the recording, and cannot be removed.
2. Privacy Masks are not normally used on PTZ cameras.
- **Adding/Editing a Mask**

Upon opening the tab, a camera preview window is shown. An Edit/View toggle button allows the existing mask to be displayed, or a new/existing mask to be created/edited.

Once a mask is defined, it will be shown in all <ControlCenter> tiles displaying the camera. The <ControlCenter> operator can open the context menu in the tile (by right-clicking in the tile), and may then be able to clear the privacy Mask, provided that operator has the **Allow** privilege set in **User Rights and Privileges**.
Setting a Password for removing/showing the Privacy Mask

A single, system-wide password is set by a system administrator in the System Screen/Advanced tab/Privacy Masking Password panel
4.4 Camera Sequence

A camera sequence is a display mode wherein several cameras are shown cyclically, each for a predefined amount of time. Sequences in Latitude are managed by an Archiver, though the cameras belonging to the sequence need not necessarily be archived or managed by the Archiver as well. The sequence configuration pane contains the following tabs: General and Actions.

General

The top section of this tab is used to enter the sequence's Name, Description and Client connection type, which has the same meaning for sequences as for cameras. It also provides two important pieces of information about the sequence: its controlling Archiver (if any), and its Multicast address.
There are two ways to create a new **Camera Sequence**:

- **From the Physical view**: Right-click on an **Archiver**, and select 'Add Camera Sequence'. The Archiver from which the Camera Sequence was created will automatically be assigned to control this Sequence.

- **From the Logical view**: Right-click on the **System** icon, and select 'Add Camera Sequence'.

  **Note**: When the Camera Sequence is created from the Logical View, it will not be active until an Archiver is selected to be the controller for the Sequence. This can be done either:
  
  - from the drop-down 'Archiver' field in the Camera Sequence window, or
  - by right-clicking on an Archiver in the Physical view, selecting 'Attach existing camera sequence', and then selecting the Camera Sequence to be attached.

To select and add cameras to the sequence, open the **Selected Cameras panel**.
Add or remove cameras from the list using the Add or Remove buttons

Change the order within the sequence with the Promote and Demote buttons

Each camera’s dwell time is specified by clicking its Time column. Similarly, a PTZ command may be entered for a camera through the drop-down menu that appears for each highlighted row in the PTZ Command column.

**Actions**

See [Events and Actions](#).

### 4.5 Conditional Event

The Conditional Events feature combines two sources as the trigger for subsequent VMS operations. The VMS administrator sets an action to only be performed when two originating events occur within a given time duration.

**General**

The **General** tab is used to Name, enter a description of, and configure event conditions.

**Condition**

**Events must occur within X seconds** (default: 10 seconds, range: 1-3600 seconds): Duration in which both configured events should occur for this condition to be met.
Other event must NOT occur within 10 seconds (default: 10 seconds, range: 1-3600 seconds): Duration after one of the configured events has occurred, in which the other event must NOT occur for this condition to be met.

- If In Order is checked, the event in the 2nd row must NOT occur.
- If In Order is not checked, one of the two configured events should occur but the other one must NOT occur.

In Order (default: checked): If checked, the configured events must occur by the order in which they were defined in the list for the condition to be met. If unchecked, the order in the list would not matter.

Source Events Table: A conditional event’s condition is comprised of two source events, represented in a two-rows table with one row per event. Clicking a row will show dropdown controls allowing to uniquely select the event of interest for that row.

Up/Down buttons: Allow the user to quickly reorder the table rows. These buttons will only be visible when ‘By Order’ is checked.

Supported Source Event Types are only those associated with the following Entity Types:

- Alarm
- Camera
- Conditional event
- External Data Entity
- External Entity
- Input pin device
- Microphone
- Output pin device
- Server
- Speaker
- Timer
- Unit
- User

By selecting one of these entity types in the leftmost column of the table, the rest of the columns will automatically adjust. For example, when selecting “Camera” in the left column, the middle column will include all cameras in the system, and the rightmost column will only include camera-associated event types, such as “motion on”.

Configuration - Entities
Notes:

1. Identical rows (events) are not allowed.

2. Partially filled rows are not allowed.

3. When an Entity participating in a conditional event is removed from the system, that conditional event will never be met again. No warning will be provided, but when entering the configuration page of such a conditional event entity, the corresponding cells in the Source Events Table will appear as empty. The administrator may then choose to select new source events and save, or remove that conditional event entity altogether.

Actions
To configure actions to be performed when the condition is met, follow the below steps:

1. Navigate to the Actions tab of the Conditional event entity
2. Right click the “Condition met” event and add actions from the list. You may add multiple actions to a single “Condition met” event.

For more information, see Events and Actions.

4.6 Enterprise
An enterprise is a part of the system associated with logical entities (including users and an enterprise system administrator) as well as its own password and locking policies (note that an enterprise may not control a system component such as an Archiver or unit, as these are physical entities). Entities are placed inside enterprises.
in the same way that they are added to sites -- by dragging and dropping them in the view selection pane. The enterprise configuration pane is primarily used, therefore, to configure password and locking policies.

**General**

The **General** tab is used only to name the enterprise and enter on optional description for it.

![General tab](image)

**Password Policy**

**Note:** The default setting is that Rules are Disabled.
4.7 GIS Maps

To use the Default GIS Map

When the IIS service 'Mapping Services' is enabled, the system will contain an entity called 'Default GIS Map'.

1. From the sidebar, select Logical View.
2. Select the entity Default GIS Map

The default parameters are shown below.

These Latitude and Longitude parameters are for the general New York area. The 'Eye Altitude' is an indication of the standard Google Maps zoom factor. '1' is maximum zoom out and shows the entire hemisphere. Higher zoom values will initially show less area and more detail.
3. Check required KMZ files if 3D images are to be displayed.
4. Check **Show video when hovering** to enable Control Center operators to be able to view a small tile of the cameras’ videos when viewing the map on the Control Center (see Viewing GIS Maps in ControlCenter/Viewing Tile).
5. Select cameras that are to be shown on the map. (Note: Cameras will only appear here if they have been assigned GIS co-ordinates in their definitions).

**To Create a GIS Map Entity**

1. From the sidebar, select **Logical View**.
2. Right click on the System entity, and select **Add GIS Map** from the drop down list.
3. In the **GIS Map** tab, enter Longitude and Latitude co-ordinates and Altitude. Check required KMZ files if 3D images are to be displayed.
4. Check **Show video when hovering** to enable Control Center operators to be able to view a small tile of the cameras’ videos when viewing the map on the Control Center (see Viewing GIS Maps in ControlCenter/Viewing Tile).
5. Select cameras that are to be shown on the map.
6. In the **General** tab, enter a **Name** and a **Description** for the GIS Map.
4.8 Input Pin Device
An input pin device represents any device (e.g. a sensor) connected to a unit's input pin. Its configuration pane contains the following tabs:

**General**
The only setting that can be configured in this tab, other than the input pin device's **Name** and **Description**, is its **Normal state**, which by default is set to **Closed**.

**Actions**
See [Events and Actions](#).

4.9 Map
A map is an HTML page that can be created and edited in the AdminCenter and viewed in a ControlCenter tile. It may contain links to various System entities, such as alarms and cameras.

To create a Map which contains a site and cameras, use the [MapBuilder](#). This creates an internet page which is kept on the Web Server.

The Map entity consists of a **General** tab where the map is generated. It is then modified (links and backgrounds are added) in the **MapBuilder** tab.

The system allows you to build a [Map Entity](#) or a [GIS Map Entity](#)

**Create a Map Entity**
1. In **Logical View**, right click on System and select **Add Map**.

The system opens a new Map entity
2. Fill in the **Name**, **Description** and **URL** for the new map.  
   (If using a local map file, use the **Browse** button to navigate to the desired file.) 
3. Click **Test**. The Map is displayed in the **Browser** pane and added to the **Logical View** entity list. 
4. If applicable, check the **Enable Global Positioning** box, and enter **Longitude** and **Latitude** information (decimal, 0-180)
4.10 Microphone

A microphone represents any audio source connected through a unit’s Audio Input. Its configuration pane contains the following tabs: General and Actions.

To place a microphone on a recording schedule, add it to the schedule using the Attach tab in the schedule’s configuration pane (Recording schedules cannot be attached through the microphone tab).

General

The General tab is used to name the microphone, enter a description for it, define its technical and recording settings, and attach it to a speaker, if applicable (e.g. when Latitude is integrated with an intercom system). The pane is divided into four sections.
Information
This section contains two non-editable information fields:

- **Connected** -- Indicates whether the microphone is connected to an accessible unit. A microphone may be shown as disconnected either because its unit is for some reason inaccessible or because it has yet to be connected to a unit (a typical situation when performing off-line configuration).

- **Recording state** -- Indicates the microphone is currently being recorded.

Configuration
This section contains a number of settings configuration fields:

- **Name** -- A generic name is given to every microphone scene when it is first created by the user or the system (see Configuration in the Latitude Configuration Pane). It is highly recommended that you give your microphone a meaningful name.

- **Description** -- An optional field used to provide a description of the microphone.

- **Connected unit** -- This non-editable field lists the unit to which the microphone is connected.

- **Connected port** -- This non-editable field lists the audio input to which the microphone is connected.
• **Sampling rate** -- A measure of the audio encoding's quality. The available options are 8, 16, and 24 KHz. Make sure the unit your microphone is connected to supports your selected rate.

• **Data format** -- The algorithm used to digitize audio from the microphone. The available formats are PCM, ULA W and GSM.

• **Channel** -- Audio can be captured in Mono or Stereo.

• **Input type** -- Set this field to Line In if your device is not a microphone but some other audio device. Otherwise, use Microphone.

• **Mode** -- Two microphone operating modes are supported: in Full Duplex mode, audio is transmitted continuously; in Push to Talk mode, audio is transmitted only when the microphone button is clicked in ControlCenter (or the equivalent key is pressed on a PTZ keyboard that supports PTT functionality).

• **Sensitivity** -- The sensitivity of the audio encoding.

• **Force deletion of expired recordings** -- This check-box is used to set the system to delete recordings from the microphone as soon as they expire even if storage space is not needed. This function is useful for administering large multi-enterprise systems and for ensuring the timely removal of sensitive clips.

**Stream Connection Types**

This section is used to configure whether live streams are sent from the unit in unicast or multicast. You can set the transmission methods of the viewing and recording streams separately. When **Client connection type** is set to unicast, it will always receive the stream from the Archiver. When it is set to multicast, the stream will be sent directly from the unit if the network architecture allows it and sent from the Archiver otherwise.

Both streams must be set to multicast when using redundant recording.

**Manual Recording**

This section is used to specify two recording parameters for manual recordings:

• **Recording lifespan** -- The minimum amount of time for which a manually recorded clip from the microphone will remain in storage (as long as the Stop Recording When Space is Full option is checked in the Latitude Configuration Pane).

• **Recording duration** -- The amount of time a clip will be recorded when a user clicks the record button in ControlCenter.

**Links**

An external speaker can be linked to the microphone by selecting it from the Linked speaker field.

**Actions**

See Events and Actions.
4.11 Network

The **Network** entity is used to define network parameters for use by Archivers. Its configuration pane consists of a single tab with two sections: **Name and Description** and **Network**.

Setting **Base IP Address** and **Subnet Mask** values should be done in consultation with the user's IT department and FLIR Inc support staff.

**Technical Note:** Minimum requirement is that the last octet binary value ends with zero.

4.12 Output Pin Device

An output pin device represents any device (e.g. a door buzzer, siren) connected to a unit's output pin. Its configuration pane contains the following tabs: **General** and **Actions**.

**Note:** When the Change Output Pin State to Abnormal action is set to zero (0), the state changes momentarily to abnormal and then back to normal.

**General**

The only setting that can be configured in this tab, other than the output pin device's **Name** and **Description**, is its **Normal state**, which by default is set to **Closed**.
Actions

See [Events and Actions](#).

4.13 Recipients Group

The recipients group entity is used to create a list of a number of users to which email notification can be sent when actions or events occur. Recipient's Groups are added in the [Users and Groups](#) view by right-clicking on the System icon or an Enterprise icon, and then selecting Add Recipient Group.

![Image of Admin Center showing Add Recipient Group option]

**Note:** This can also be done from the Logical or Physical views.
Name and Description
This section is used to configure the following parameters:
- **Name** -- The name of the recipients group entity.
- **Description** -- An optional description of the entity.

Select Users
Add the desired users from the *Available Users* list to the *Selected Users* list.

4.14 Serial Device
A serial device represents any device other than a PTZ camera connected to a unit's serial port. Its configuration pane contains the following tabs:

General
This tab contains the following panes:
**Information**, which shows the device's connection state and includes configurations,
**which displays the communication parameters used by Latitude to communicate with
the device (via the serial port of the unit to which it is connected)
Information
This section contains one non-editable information field:

- **Connected** -- Indicates whether the serial device is connected to an accessible unit. A serial device may be shown as disconnected either because its unit is for some reason inaccessible or because it has yet to be connected to a unit (a typical situation when performing off-line configuration).

Configuration
This section is used to configure several basic settings:

- **Name** -- A generic name is given to every serial device when it is first created by the user or the system (when a unit is discovered). It is highly recommended that you give your device a meaningful name.
- **Description** -- An optional field used to provide a description of the serial device.
- **Mode** -- The communication protocol used by the device and its connected unit's serial port (note that some units have ports that support multiple protocols, e.g. RS422 and RS485. Such ports can only support one protocol at any given time).
- **Connected unit** -- This non-editable field lists the unit to which the serial device is connected.
- **Connected port** -- This non-editable field lists the unit serial port to which the serial device is connected.
• **Data bits, Parity, Stop bits and Bit rate** -- These are low level communication parameters that should be set to match those of the serial device (as specified in the device's technical manuals).

**Actions**
See [Events and Actions](#).

### 4.15 Serial CCTV Keyboard

CCTV keyboards can be used with Latitude when connected to a PC or to a serial port of a unit or of an encoder.

To use the CCTV keyboard with a PC, the ControlCenter application must be installed on the PC.

To use the CCTV keyboard without a PC, the keyboard has to be connected to a unit/encoder via its serial port.

In addition, you can integrate a third party system that uses keyboard emulation by connecting it to a unit.

Latitude supports 50 active keyboards connected to a single system.

See [Adding a new keyboard configuration](#) regarding how to connect the CCTV keyboard to a unit.

See [Working With Keyboards](#) regarding how to connect a CCTV keyboard to a PC with ControlCenter.

See [Controlling the Remote ControlCenter via CCTV Keyboard](#) regarding how to use a CCTV keyboard to control a Remote ControlCenter.
4.15.1 Adding a new CCTV keyboard configuration

1. On the Sidebar of the AdminCenter, click the Physical View button.
2. In the View selection pane, expand the tree until you reach the serial port of the unit to which a CCTV keyboard is to be connected.
3. Right-click the serial port, and then select Add Serial CCTV Keyboard.
4. In the Configuration pane, define the CCTV keyboard parameters in the General tab:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Configuration</td>
<td>Name</td>
<td>Enter/modify the name of the CCTV keyboard. The default name includes the name of the unit to which the CCTV keyboard is attached.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Enter a description. This field is optional.</td>
</tr>
<tr>
<td>Keyboard Configuration</td>
<td>Associated User Identity</td>
<td>Select the user identity associated with the CCTV keyboard from the drop-down list. The actual keyboard user will inherit the same privileges as the specified user.</td>
</tr>
<tr>
<td></td>
<td>Keyboard Protocol</td>
<td>The manufacturer and the model of the keyboard. Select the protocol which the CCTV keyboard supports from the drop-down list — such as American Dynamics, enter value Keyboard v0.1 or PelcoKBD 300A.</td>
</tr>
<tr>
<td></td>
<td>External System Behavior (Access Control)</td>
<td>Select this check box only if you are defining a keyboard for the purpose of interfacing with a third party system (such as an access control system). Do not select this option otherwise.</td>
</tr>
<tr>
<td></td>
<td>Keyboard should beep</td>
<td>Clear this check box to prevent the keyboard from beeping (upon failed actions).</td>
</tr>
<tr>
<td></td>
<td>Do not remove selected camera upon 2nd switch</td>
<td>When connecting a camera to a monitor that is already displaying that camera, the default behavior is not to remove that camera. If this option is cleared, the camera will be removed at every second connection attempt. (This action is suitable for keyboards without the Clear key.)</td>
</tr>
<tr>
<td>Serial Configuration</td>
<td>Mode</td>
<td>The mode of the serial port — RS232, RS422 4-wire, RS485 2-wire or RS485 4-wire</td>
</tr>
<tr>
<td></td>
<td>Connected Unit</td>
<td>The unit to which the keyboard is connected</td>
</tr>
<tr>
<td></td>
<td>Connected Port</td>
<td>The serial port to which the keyboard is connected</td>
</tr>
<tr>
<td></td>
<td>Archiver</td>
<td>The Archiver to which the keyboard is connected</td>
</tr>
<tr>
<td></td>
<td>Data bits</td>
<td>The number of bits in transmitted data</td>
</tr>
<tr>
<td></td>
<td>Parity</td>
<td>The parity of the serial port — odd, even, or no parity check. Most communication devices do not use parity.</td>
</tr>
<tr>
<td></td>
<td>Stop bits</td>
<td>The number of stop bits in each transmission</td>
</tr>
</tbody>
</table>
### Bit rate
The data rate that the serial equipment operates at. Possible values range from 1200 bps to 230,400 bps (transmitters) or to 115,200 bps (receivers).

5. In the *Actions* tab, define the desired actions for the following events: *Accessibility Lost* and *Accessibility Recovered*.

#### 4.16 Site

_Sites_ provide a way of organizing most types of logical entities into groups, analogous to the way folders in an operating system are used to organize files. Sites may be added at the level of the System, Enterprises, and Sites (Sites within Sites). They are often, though not always, used to organize entities based on their "real-world" locations.

To create a site, right click the location (Latitude, enterprise or site) in which you would like to place the site and choose *Add site*.

Give the site a **Name** and (optional) **Description** in its configuration pane.
Move entities into the site by dragging and dropping them onto the site's icon back in the View Selection Pane (Logical View). Once a Site has sites within it, these are shown as Child Entities.

4.17 Speaker

The speaker configuration pane contains the following tabs: General and Actions.

General

The General tab is used to name the speaker, enter a description for it, and define a few additional parameters. The pane is divided into two panes.

⚠️ When a speaker and a camera are linked to form a compound scene, the link is created in the camera configuration pane; when a speaker and a microphone are linked, the link is created in the microphone configuration pane.
Information
This pane contains one non-editable information fields:

- **Connected** -- Indicates whether the speaker is connected to an accessible unit. A speaker may be shown as disconnected either because its unit is for some reason inaccessible or because it has yet to be connected to a unit (a typical situation when performing off-line configuration).

Configuration
This pane contains a number of settings configuration fields:

- **Name** -- A generic name is given to every speaker scene when it is first created by the user or the system (see Configuration in the Latitude Configuration Pane). It is highly recommended that you give your speaker a meaningful name.

- **Description** -- An optional field used to provide a description of the speaker.

- **Connected unit** -- This non-editable field lists the unit to which the speaker is connected.

- **Connected port** -- This non-editable field lists the audio input to which the speaker is connected.

- **Audio Mode** -- Two working modes may be specified through this drop-down menu: **Full Duplex**, for constant audio transmission, and **Push-to-Talk**, which mutes the speaker when a connected microphone is being used (the typical configuration for an integrated intercom system).

- **Volume** -- The volume bar (or input box to its right) is used to set the audio stream volume, which can also be adjusted individually by ControlCenter users.

Actions
See [Events and Actions](#).

4.18 System
The **System** is the entity that represents the 'root' of the entire system and is used to configure system-wide settings. Its configuration pane contains the following tabs: **General, System Security, Edge Security, Logical IDs, Discovery, Audit Trail, Advanced, Mass Export**, Analytics, and **Actions**.

4.18.1 System - General
The **General** tab consists of the following panels: Configuration, Behavior When Recording Space is Full, Video, Time, Child Entities, System PTZ Priorities, Stream Connection Types, Alarms, Failover Archiver, Concurrent Login, and Directory Backup Schedule.
Configuration

This pane is used to configure the following parameters:

- **Name** - The name of the System entity.
- **Description** - An optional description of the entity.
- **System ID** - The logical ID used for keypad navigation in the <ControlCenter>. See Working with Keyboards for more information.

Behavior When Recording Space is Full

Two options are available for handling recording when an Archiver's allocated space is depleted and all its archived clips are unexpired:

- **Stop recording** - In this mode, the Archiver stops recording new clips to prevent non-expired ones from being overwritten before their expiration date.
- **Overwrite next expiring recording** - The Archiver overwrites archived clips by order of expiration from earliest to latest (except for locked clips, which are never overwritten.)
Video

This pane is used to configure the following parameters:

- **Recorded quality same as live by default** - When this check box is selected, the system automatically sets the recorded video quality as high as the live video quality
- **Auto Start Stream** - When this check box is selected, the system automatically starts video streaming.
- **Default Video Source Type** - Indicates the TV standard default - NTSC or PAL
- **Enable Dynamic Transcoding** - Enabling this feature allows Archivers to use a Transcoder when streaming to clients that are not part of that Archivers' set of networks (i.e. the list of networks defined on that particular Archiver/Networks Tab). See Transcoder/Mixed Mode
- **Manual recording termination warning** - This field is used to control how long before manual recording is scheduled to end the record button of the <ControlCenter> tile showing the camera will start blinking.
- **Use recorded/Edge Recording stream in Adaptive Streaming** - This check box allows the user to enable the ability to include the configured recording/edge recording stream in the Adaptive Streaming capability.

Time

The Time section is not currently supported and will be updated in a future version
For more information, see Time Synchronization.

Child Entities

This pane lists all child entities of the system. These are the servers, networks, etc. that are all configured under this System.

System PTZ Priorities

This pane is used to configure the System PTZ priorities.

- **System priority** - Determine the priority level of the system by using the slider or entering the desired value in the field
- **System vs user idle interval** - Set the idle interval of the system after which the current user can take control of a PTZ session
• **User vs user idle interval** - Set the idle interval of the user after which another user can take control of a PTZ session

  For more information, see [PTZ Priorities](#).

**Stream Connection Types**

This pane is used to set the connection type of the Archiver (live and recording) and the client applications. *(unicast, multicast (UDP), best available or Unicast TCP connection type)*

![Stream Connection Types](image)

**Note on using Unicast TCP Option**

For this setting to be used, it is critical that all Directories and Archivers in the system have a version of Latitude that supports the Unicast TCP Live Streaming option installed, before attaching and configuring units that will use the setting.

If one or more Archivers in the system are using versions that do not support Unicast TCP, (for example Archivers designated as Fail-over resources that have not yet been upgraded), or if for any reason the version is uninstalled so that an earlier version which does not support Unicast TCP will run, this setting might interfere with live video from units on these Archivers. Users should be aware of this limitation, and should always ensure that all Directories and Archivers are on the newer version, and should always manually reset relevant units before executing an Uninstall.

As an additional protection, the Latitude uninstall process will reset any units found with Unicast TCP selected, to Unicast UDP.

Details of which versions support particular facilities may be found in the Release Notes.

**Alarms**

This pane is used to enable/disable color coding for alarms management.

**Note:** Users of the `<ControlCenter>` who are logged in at the time of changing this setting will need to log out and log back in for changes to take effect.

**Failover Archiver**

This pane is used to enable the failover archiver behavior of replacing a lower priority failover archiver in a failover situation.

**Concurrent Login**

When checked, this option only allows the user to be logged in to the system once at any one time. This applies to all instances of Control Center, Web Client and/or Mobile App that may be running at that time.

**Directory Backup Schedule**
The user can set the parameters for the system to make automatic backups of the Directory. Backup information is then available to support staff if the Directory needs to be recovered - for example, after a ‘Directory failed to synchronize’ event.

4.18.2 System - System Security
The System Security Tab has the following panes: Edge Security Settings, Web Security, Users Password Rules, User Password Change.

Edge Security Settings

TLS for Edge Devices – Policy

Establishing and applying these facilities requires support in the system and from the edge devices themselves. The table below shows the current facilities supported.
## TLS for Edge Devices – Choosing the options

The user sets under what conditions Edge Devices may communicate with the system. Terms used here:

**Secured Connection** - Communication uses HTTPS and encryption to ensure integrity of messages and guard against malicious users.

**Self-signed - Certificate** is generated by the camera (or unit), rather than by a third-party Trusted Certificate Authority.

---

### Before enabling 'Use secured edge connections'

Certificates must be loaded into the cameras BEFORE enabling this option.

1. Use the cameras' web pages to check if the target camera/s have an **Enable/disable SSL** option, and if so, ensure that is it **enabled** (e.g. Ariel Gen 2)
2. Use the web page to upload certificates or generate self-signed certificates.
3. If you use the Edge Device Security screen option 'Generate Self-signed certificate', please note that this is not supported by all manufacturers.
4. Once certificates have been loaded, you can check that they are correctly set up by accessing the camera's web page through **https**.

---

<table>
<thead>
<tr>
<th>Product Type</th>
<th>Discovery method</th>
<th>TLS support</th>
<th>Confirm User-set Password</th>
<th>Change Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLIR cameras</td>
<td>FLIR Plug-in</td>
<td>Yes*</td>
<td>Yes</td>
<td>Yes**</td>
</tr>
<tr>
<td>Arecont, Axis, Bosch, Panasonic, Pelco, Sony</td>
<td>Proprietary plug-in</td>
<td>No*</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ONVIF-compatible cameras</td>
<td>ONVIF plug-in</td>
<td>Yes***</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Notes:

* TLS connection can be established if supported by the unit as well as the VMS
** Changing password is supported for: FLIR core cameras, Quasar Gen II cameras, Ariel cameras and ioi HD cameras
*** Assuming the camera supports TLS

In future versions, as the capabilities of edge devices are enhanced, and as new device plug-ins are developed, this table will be updated.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use secured edge connection if available:</td>
<td><strong>IMPORTANT:</strong> APPLIES UNITS IN THE CASES SHOWN - Other Units already in the system are not affected. 1. If this option is enabled the Archiver will try to establish a secured connection with the camera. If it succeeds then all the communication with the camera will be encrypted. 2. Discover using FLIR Plug-in or ONVIF method. 3. Units must support HTTPS and have certificate already loaded, or have already created their own self-signed certificate.</td>
</tr>
<tr>
<td>Block communications for devices using unsecured connection, but allow user to secure them</td>
<td><strong>APPLIES TO ALL UNITS.</strong> Archiver will block all communication from units except those actions that are required in order to set up secured connections. (More strict)</td>
</tr>
<tr>
<td>Block communications for devices using untrusted certificates, but allow user to replace them</td>
<td><strong>APPLIES TO ALL UNITS.</strong> Archiver will block all communication from units except those actions that are required in order to replace the certificates. (Most strict)</td>
</tr>
</tbody>
</table>

**Note:**
1. When activating these rules, keep in mind that ‘Use secured edge connection’ applies only to new edge devices that are being discovered, Rediscovering units, and updating firmware on units – when reconnecting to devices already in the system, without rediscovering, this is not enforced.
2. The two ‘block devices’ rules are always enforced – devices that do not meet the criteria, including those that are already connected, will be blocked.

3. When changing the 2nd and third parameters (Block units with unsecured connection or Block units with untrusted connections), the units are reinitialized by the Archiver, and there may be a delay before the units become accessible again. Users should allow time for units to become available before continuing.

4. When Changing passwords, special care must be taken on PTZ units. (See When using Change Password on PTZ Cameras)

5. When Updating Firmware on Quasar Gen II and IOL HD units - If Secure communications are enforced (Certificates in use), then operators must reload certificates on the units after the firmware upgrade.

**Web Security**
This panel allows the user to activate and deactivate TLS (Transport Layer Security) encryption between the Web Server/Transcoder and any Web Clients that are in use.
**Note:**
The following steps must be completed before activating TLS.
1. In order to use this facility, the User's IT department must arrange for a suitable TLS Certificate to be accessible to the system.
2. The requisite ports must be available. The required ports use default settings chosen by the system, and the user should verify with the IT department that these ports are available. See Transcoder - Server Configuration / Secured Port

**Setting up TLS**
The IP Security panel initially shows two buttons.

Only the 'Load TLS Certificate' button is enabled. Clicking on this button opens an Explorer window where the user can select a TLS Certificate to be used.

Select the .pfx file (that was previously acquired by your IT department), and click Open. You will be asked for the Password associated with this Certificate.
When a valid password has been entered, the system returns to the main parameter screen, and this now shows the options to Replace or Remove the TLS Certificate, and the name of the issuer of the Certificate.

The display returns to the System Parameter screen. The user must Save the changes.

Once the changes have been saved, the system will restart Web Client connections, and all subsequent communications with Web Clients will be encrypted. The https connection and secure icon show in Web Client address bars:

**Replacing or Removing the TLS Certificate**

Once a Certificate is in use, the user is shown these options.

The Replace option may only be used when an alternative Certificate is available. The Remove option results in TLS encryption being discontinued, and further WebClient traffic is in the clear. The user must confirm this action before it is carried out.
Users Password Rules
This panel allows you to create rules regarding passwords across the system. Settings include the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable rules</td>
<td>Enables/disables the use of the password rules on this tab.</td>
</tr>
<tr>
<td>Allow password to be identical to user name</td>
<td>When disabled enforces a password policy that the user cannot enter a password that is identical to the user name.</td>
</tr>
<tr>
<td>Minimum length</td>
<td>When set to a value other than 0, enforces a password policy that new passwords must be greater than or equal in length to the value entered.</td>
</tr>
<tr>
<td>Minimum number of letters</td>
<td>When set to a value other than 0, enforces a password policy that new passwords must contain a greater than or equal number of alpha characters than the value entered.</td>
</tr>
<tr>
<td>Minimum number of digits</td>
<td>When set to a value other than 0, enforces a password policy that new passwords must contain a greater than or equal number of numeric characters than the value entered.</td>
</tr>
<tr>
<td>Prohibited Passwords</td>
<td>This is a password disallow list that can be added to include invalid passwords. Forbidden passwords can be listed here to prevent users from using them if they are considered to pose a security risk, to be too common, or known to be exposed and no longer secure.</td>
</tr>
<tr>
<td>Users may not change passwords</td>
<td>When selected, a password policy is enforced globally across the system to prevent any password changes.</td>
</tr>
</tbody>
</table>

User Password Change
Allows the Administrator to set whether Users may or may not change their passwords.
4.18.3 System - Edge Security

This page allows for the current Security mode for all units and where applicable, allows the Administrator to change settings.

Note: Changing Edge Device Security Settings depends on the unit's inbuilt capabilities, and on the method that was used to discover the unit.

Security Mode and Certificate changes can only be made on units that are covered by the FLIR Core Products plug-in, or were discovered as ONVIF units having the necessary ONVIF profile to support these actions.

For all other listed devices, the buttons 'Set Security Mode', and 'Generate Self-Signed Certificate' will be disabled (greyed-out).

Similarly, the 'Change Password' button is only enabled for units that support password changes.

A special warning message is added when the system includes Quasar Gen II and/or IOI-HD units:

The table displays the following:
- Icons indicate the security status of the device:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Unit connection is secured, but does not have trusted certificate</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Unit is fully secured (Secured connection and trusted certificate)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Unit has security warning (see list below)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Unit is unsecured</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Unit is blocked</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Unit is inaccessible</td>
</tr>
</tbody>
</table>

- The device name
• Whether the device connection to the archiver is secured or not
• If secured, the expiration date of its certificate
• Whether or not its password has been set by the user or is still set at the factory default.

**Note:** Units discovered using the ONVIF plugin will show ‘Unknown’ as the plugin does not provide a method that can determine if a ‘new’ password has been used or if the user entered a value that corresponds to the manufacturer’s default password.

• The status of the last action initiated for that device.

When a device in the table is selected, any applicable security alerts for the selected device are displayed, and the available changes to security status are enabled.

### Security Actions

Three Security Actions are shown above the table:

- **Set Security Mode**
  This option allows user to set desired security settings for edge devices.

- **Generate Self-Signed Certificate**
  This option is available to request that the unit generate a self-signed certificate (if supported by the camera) in order to apply TLS security.

- **Change Password**
  This options allows an authorized user to change the password on a camera.

![Change Password dialog](image)

**Notes:**

1. Each of these Security actions can be applied to one or more entries in the table. The actions are only enabled if they are available for the device or devices selected, i.e. If more than one entry in the table is selected, only actions that are available for all selected devices will be enabled.

2. When the user has Quasar Gen II and/or IOI-HD units, the following warning message will always be displayed:

   ![Warning message](image)

3. When using Change Password on PTZ Cameras:

   The Change Password functionality interrupts an open PTZ session, and can affect PTZ functionality.
Admin Center operators who wish to change password on PTZ cameras should follow these steps:

1. Go to **Edge Security** page, and change the password

2. Go to the **Camera/PTZ Configuration** page (shown here).

3. Carefully note which **PTZ Driver is in use** for the camera (circled).

4. Disable **PTZ Configuration** (Uncheck)

5. Save the change.

6. Re-enable **PTZ functionality** (Check), using the driver that was in use (Choose from the drop-down menu).

7. Save the change.

### 4.18.4 System - Logical IDs

#### Logical IDs Tab

This tab allows you to change various logical entities' logical IDs, which are used when referencing the entities through PTZ keyboards.
The system allows you to select a family of devices, and then make changes to Logical IDs within that family.

To change an entity's ID, select its type from the Logical ID Family drop-down menu, click its New Logical ID cell in the table, and type in the new ID. 

**Note:** Duplicate IDs are not allowed for entities of the same family.

### 4.18.5 System - Discovery

The Discovery tab is used to discover all units -- encoders, decoders and IP cameras -- and assign them to Archivers.

See [Discovery](#) for further details.

### 4.18.6 System - Audit Trail

This tab is used to control which events, if any, are stored in the EDBs' Audit Trail databases. These databases can then be used to generate reports about user activity, alarms, equipment
configuration changes, and other system events using standard reporting tools such as Crystal Reports.

The following parameters must be configured for audit trail reporting:

- **Enable auditing** - Click this check-box to enable the audit trail feature.
- **Event storage lifespan** - The amount of time data should be stored in the database. **Note**: If the database is expected to grow larger than MSDE’s limit of 2GB, a full version of MSSQL must be used instead.
- **Storage overrun policy** - This field controls how the database behaves when it reaches its storage limit, either by overwriting data (oldest first), or by ignoring new events until space becomes available due to expiring event data.
- **Event Filtering** - This section allows you to specify which events should be archived. Use the arrow buttons to move events between the Available Events and Audited Events columns.

4.18.7  System - Advanced
The Advanced Tab has the following Panels:
- **Automatic Logout Timeout**, **Incremental Synchronization Interval**, **Server Cache Refresh**, **Application Cache Refresh**, **Maintenance**, **Cache Validation interval**, **Event Response Time**.

The first 7 panels are as follows:
- **Automatic Logout Interval** - The automatic logout interval applies to logins from Admin Center and Control Center Clients, SDK, and system servers which become disconnected unexpectedly (i.e. without sending a logout request to the Directory server). This can happened, for example, due to network disconnection or unexpected shutdown. Once a disconnection is identified, the Directory server will hold the login session for a ‘grace period’ as defined by this setting. Only after the grace period expires will the system execute a logout. The grace period defines the minimum time before the logout will occur - in practice the time will usually be somewhat longer. This setting does not apply to Web Client logins, as these connections are handled by IIS.
- **Incremental Synchronization Interval** - The length of the interval between database synchronizations.
- **Server Cache Refresh** - How frequently server applications obtain updated settings from the Directory.
- **Application Cache Refresh** - How frequently client applications obtain updated settings from the Directory.
- **Maintenance** - The minimum amount of time between successive executions of periodic maintenance tasks such as unit/component polling. This parameter overrides the Polling interval set via the General tab if its value is higher.
- **Cache Validation Interval** - The length of the interval between cache validations.
- **Event Response Time** - The maximum amount of time the system components may wait before responding to an event.  
  The next 5 panels are as follows:

- **Stream UDP Port Range** - The Archiver and Client port ranges.  
  **Note:** Changing ports requires an Archiver restart
- **Keep Alive** - How long polling intervals and reply timeouts are kept alive
- **Quality of Service** - Determines the priority given to various communication components
- **Client Detection and Recovery of Stream Failure** - define parameters for stream loss detection (client application)
- **Archiver Detection and Recovery of Stream Failure** - define parameters for stream loss detection (Archiver application)

The remaining panels are as follows:
• **Privacy Mask Password** - This is an optional feature that must be licensed. This setting provides the ability to change the password that will be embedded in DVT exported files by the <ControlCenter> user when they export a video clip that has a Privacy Mask applied. This password remains permanently attached to the exported file at the time it is exported. The default setting is: 1234.

For

• **Motion Detection** - The Re-arm Timeout setting defines the minimum time that must elapse after a Motion Off event before a new Motion On event will be reported for the same unit.

• **Automatic Client Updates** - This panel allows the user to set up where the Automatic Client Updates Server function/s is/are installed. The appropriate **Custom Installation** must have been run on the machines selected in this panel. For more details, see **Update Services Server**

• **Mapping Services** - This panel allows the user to set up where the Mapping Services Server function/s is/are installed. The appropriate **Custom Installation** must have been run on the machines selected in this panel. For more details, see **Map Server**
4.18.8 System - Mass Export
See Mass Export.

4.18.9 System - Analytics
AdminCenter integrates Analytics-capable cameras, and allows system responses such as alarm triggering to be activated by status messages from the cameras. Additionally, specific IP-camera models may be configured to provide a video stream to Analytics-capable encoders. The Analytics Tab allows the user to select cameras to be used in this mode, and to associate them with the required encoders.

For more detail, see Binding Cameras and Encoders
4.18.10 System - Actions
See Events and Actions.

4.19 Tile Layout

Tile Layouts allow users to set up predetermined layouts to be used on Control Center Monitors.

**Note:** Tile Layouts are created and managed in the xx

Creating and Saving Layouts.

Use the **Add Layout** icon in the xx Viewing Pane Toolbar to create a new Layout.

Once a new Layout has been opened, the **Save Layout** icon is enabled. When the user has completed setting up the new Layout (i.e. choosing a tile layout, adding cameras, camera sequences, maps, etc.), then the new Layout must be saved so that when it is invoked again, the same content will be available.

4.20 Timer

A Timer entity can be defined by clicking 'Add Timer' in the system context menu (Logical View).
The Timer page allows the user to name the timer and set up a single or a recurring time.

Using the Timer Entity
The Timer will typically be used to Arm and Disarm Analytics entities, so that the system is not burdened with multiple alarms during known busy periods.
Users may find additional uses for the Timer, depending on their individual needs.

4.21 Unit
A unit, also known as an edge device, refers to any external device controlled by an Latitude Archiver. The most common types of units are encoders, decoders and IP cameras (which contain built-in encoders).
Conceptually, a unit may be thought of as a collection of physical capabilities recognized by the system, namely video inputs and outputs, audio inputs and outputs, serial ports and input/output pins. Each physical capability is used by a corresponding device, which is represented by a logical entity -- a unit’s video output, for example, is connected to an analog monitor, while its serial ports are used to communicate with serial devices such as PTZ motors and keyboards.
The unit configuration pane contains the following tabs: General, Network, Clock and Actions.

General
The General tab consists of two sections, Information, which contains only non-editable fields, and Configuration, where the password and failover priority of the unit are configured.
Information
This section contains information about the unit's connection state, uptime, model and firmware version.

Configuration
The Name and Description fields can be edited.

The Requires credentials checkbox shows whether or not username and password are required when accessing the unit. This is set by the system during the Discovery process. The user can, in some cases, edit this field. (If not, it is disabled).

Note: Care should be if considering changing this setting.

If the user un-checks it and saves the setting, the unit's credentials in the system will be cleared and cannot be recovered.

If the user tries to change this setting, a warning notice is shown:

```
! WARNING

CAUTION: Changing this setting will clear the saved credentials and can disrupt communications to the device. Are you sure you want to change this?
```

The Failover Priority field is used to determine which unit will be the first to be moved to the Failover Archiver (and thus saved) when the Archiver responsible for the unit fails. The parameter can be set from 1-100, where 1 is the lowest priority level and 100 is the highest. By default, the priority is set to 100.

Note: Priority is only enabled for encoders.
Network
This tab also consists of an Information section and a Configuration section.

**Information**
This section lists the unit's MAC Address.

**Configuration**
This section can be used to change the unit's IP address (and Network), to set it to accept its network settings from a DHCP server, and to change its communication Port.

**Clock**
This tab allows you to view and change the unit's date, time and time zone. For more information, see Time Synchronization.
Actions
See Events and Actions.

4.22 User
The user configuration pane is used to specify the account settings associated with Latitude users. It contains four tabs: General, Login, Privileges and Actions.

To access User configuration, click the Users and Groups button in the Sidebar.

To add a user, right-click the System icon, and then select Add User.

Note: When the Active Directory is activated, new users can only be added via the Active Directory.

Every new user is automatically added to the default user group called Users and can then be added to additional user groups. Alternatively, a user can be added from within a user group, thereby automatically belonging to that group. Since a user can be related to more than one user group, the user privileges can be merged. The user’s private privilege are merged with the privileges of all the groups related to the user. The merged privilege settings of a user are called effective privileges. For more information, see Privileges.

A user can be related to more than one directory. The user privileges can be changed locally or globally (in one or all directories). For more information, see Privileges.

Note: A newly created user does not have access privileges to the AdminCenter unless the user was created from within a group with Admin privileges. In order to enable the user the access to the AdminCenter, the privilege to access the AdminCenter has to be set to Allow in the Privileges tab.

General
The General tab is used to enter basic information about the user, including the user’s name and contact information and the user groups the user belongs to.
Note on Global Users and Global User Groups (when available in your system)
The 'Global' check-box is only enabled when the system is connected to a Global Admin server.
When a group of systems are connected to a Global Admin Server, then User Groups can be shared across all connected systems.
To make a User Group or a User Global, simply check the check-box alongside the name, and Save the information.

⚠️ The name entered in this screen represents the user's "real" name, not the system user name. It is case sensitive and may contain spaces and other special characters.

User PTZ Priority
In the PTZ Priority pane, set the PTZ priority level of the user.

To set the PTZ priority level:
- Select the Inherit from parent (user group) check-box to set the level to the highest priority (lowest numeric value) between all the User Groups to which the
user belongs

or

- Select a priority level using the slider by entering the desired value in the field
  (whereas which 1 is the highest priority and 100 is the lowest).

For more information, see PTZ Priorities.

Alarms Display Mode

In the Alarms Display panel, you can set whether or not this user should simply inherit
the Display mode that will be used from the User Group to which he/she belongs, or
not.

If not, then one of the three modes must be selected. For an explanation of how the
different modes function, see Viewing Modes for View Modes for Alarms

Login

The fields in this tab are used to configure the user's login parameters (user name
and password).
Access Rights

Define the user access rights across the system. For more information, see Access Rights.
Define the user privileges across the system. For more information, see Privileges.
Layouts
Assign the user layouts from the available layouts.

Actions
Define the user-related actions and events. For more information, see Events and Actions.

4.23 User Group
The User Group entity represents a group of users with the same set of privileges.

When creating a user group, it is possible to select predefined group privilege sets that can later be changed or fine-tuned. See User Group Wizard

Selecting predefined group privilege sets eases the privilege setting process for user groups greatly. The privilege sets acts as basis that can be adjusted instead of defining a set of privileges from scratch.

There are predefined group privileges to for the following typical user group types:
### Privilege Set Description

<table>
<thead>
<tr>
<th>Privilege Set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Admin</td>
<td>Unlimited authorization in the AdminCenter and ControlCenter</td>
</tr>
<tr>
<td>Standard Admin</td>
<td>Full authorization in the AdminCenter and ControlCenter except creating and editing users and removing system components</td>
</tr>
<tr>
<td>Advanced User</td>
<td>Full authorization in the ControlCenter.</td>
</tr>
<tr>
<td>Standard User</td>
<td>Full authorization in the ControlCenter except setting presets, accessing the PTZ menu and making changes to layouts</td>
</tr>
<tr>
<td>Guest</td>
<td>View live video feed in the ControlCenter only</td>
</tr>
<tr>
<td>Undefined</td>
<td>No authorizations</td>
</tr>
</tbody>
</table>

After creating a user group, a new user added to the group will have the same privileges settings as the whole group. The privileges of an existing user can vary from the privileges of the user group.

It is possible to first create a user group and then add one user at a time. In addition, you can add existing users to an existing user group. You can also create a new user that will added to the desired user group.

To access the User Group configuration, access the Physical View (for example by clicking the **Users and Groups** button in the Sidebar), and then click the desired user group.

To add a user group, right-click the System icon, and then select **Add User Group**, or click ![Add User Group](add_user_group_icon) in the tool bar, and select **Add User Group**. In addition, you can add a user group by right-clicking the desired Enterprise and then selecting **Add User Group**.

Alternatively, you can create a user group, using the **User Group Wizard**.

A default user group called Users is created by default for each business location (enterprise). The privileges settings of this user group are set to undefined and can be changed. Every new user is automatically added to this user group and can then be added to additional user groups.

Since a user can be related to more than one user group, the user privileges will be merged. The user’s private privilege are merged with the privileges of all the groups related to the user. The merged privilege settings of a user are called effective privileges. For more information, see **Privileges**.
When removing a user from a user group, the user's effective privileges change accordingly.

If a user only belongs to one custom user group only and is removed from this user group without being removed from the system, the user automatically becomes a member of the default user group *Users*. The default user group cannot be removed.

When removing a user group, all its member automatically become member of the default user group *Users*.

The User Group entity contains two tabs: **General** and **Login**.

**Note:** When the Active Directory is activated, new user groups can only be added via the [Active Directory](https://example.com).

### General

The **General** tab is used to enter basic information about the user group, including the user group’s name and description, to add existing users to the user group and to create new users that then are automatically added to the user group.

In addition, the PTZ priority of the user group can be determined. To set the PTZ priority level select a priority level using the slider by entering the desired value in the field (whereas which 1 is the highest priority and 100 is the lowest). For more information, see [PTZ Priorities](https://example.com).
Note on Global Users and Global User Groups (when available in your system)
The 'Global' check-box is only enabled when the system is connected to a Global Admin server.
When a group of systems are connected to a Global Admin Server, then User Groups can be shared across all connected systems.
To make a User Group or a User Global, simply check the check-box alongside the name, and Save the information.
To create a new user

1. In the General tab of the desired User Groups entity, click **Create New User**.

   The User Details dialog box appears.

![Create New Users dialog box]

2. Enter the following information: Name, user name, password, password confirmation and e-mail address.

3. Click **OK**.

   The new user is automatically added to the user group.

**Privileges**

Define the user group privileges across the system. For more information, see Privileges.
5 Configuration - Functionality

This section covers the Configuration screens of each functionality that can be defined in the system

- Alarm Management
- PTZ Priorities
- Binding Cameras and Encoders
- Tru Witness
- Events and Actions
- User Management
- MMS Video Support
- Tools
- Motion Detection
- Privacy Mask

5.1 Alarm Management

Technical Publications Alarm Management capabilities provide an interface to monitor, review and manage alarm events via the Control Center.

Alarms can originate from Technical Publications 's video software itself, or from any third party application integrated with Technical Publications . Access Control, Intercom, ANPR and Fence systems are already integrated with Technical Publications. The alarms sent by those systems are channeled to and received by Technical Publications.

Technical Publications’s Control Center provides elaborate tools for the operator to control and manage alarms. An alarm control pane displays the list of active alarms with priority and detailed status information. Alarms can also be configured to automatically display video, both live and playback as well as display associated procedures and related maps.

Using the Technical Publications MapBuilder tool and Java script, maps can be created to support Alarm Management. When presented in Control Center, those maps provide visual representation of alarm location and status thus allowing Control Room operators to monitor alarms from multiple sources.

Alarm Configuration

Alarms are defined in Technical Publications under the System Settings tree.

To access Alarm Types, expand the System Settings drop-down menu in the Side-bar, and then select Alarm Types.

The Alarm Type configuration pane is used for general alarm configuration, attaching alarms to camera or recipients and defining actions for triggered alarms.

Each alarm has the following properties, described in detail below: General, Cameras, Recipients and Actions.

For information about alarms and alarm handling, see Alarms.
To add a new Alarm Type, right-click on the **Alarm Types** entry in the System Settings Navigation window and select **Add Alarm**.

**Note:** You should ensure that a suitable **Coverage** exists for the new Alarm Type before trying to add it.

The relevant characteristics of each Alarm are configured in their respective Tabs, described below. Click each Tab title to see further details.

### General Tab

The General Tab is made up of the following panels:

- **Configuration panel**

  The *Configuration* panel is used to configure the following settings:
  
  - **Name** -- The name of the alarm type.
  - **Description** -- An optional description of the alarm type.
  - **Pre-alarm coverage** -- During the coverage specified in this field, the Archiver will maintain temporary recordings for the cameras associated with the alarm to insure the system's ability to record or play them back with the pre-alarm times specified in the **Cameras** tab.
  - **Procedure URL** -- Location of Web Page associated with this Alarm. The ControlCenter user has a **Show Procedure** button in the alarms Pane to call up this display.
- **Priority** -- This parameter determines the order in which alarms will be displayed when the number of active alarms exceeds that of armed tiles in the ControlCenter layout (1 represents the highest priority).

- **Dwell time** -- This parameter determines how many seconds each viewable scene associated with the alarm type (see the Cameras tab) is shown before the tile switches to the next scene in the list.

- **Rearming threshold** -- The minimum time, in minutes, that must pass between the activation of two instances of the alarm.

- **Procedure URL (Map)** -- Each alarm can have one associated URL (any web page or map) that is commonly used to display a procedure to the operator. In Technical Publications, there is an option to automatically switch the procedure URL/Map to a tile when the alarm is being displayed or let the operator decide whether to display it (by clicking the Procedure button in the Control Center Alarms Pane).

**Color Coded Priority** -- (A color swatch box) Priorities are from 1-100. Color coding automatically paints priorities 1-33 in red, 34-66 in yellow and 67-100 in blue. Color coding is a configurable system option and can be turned off, if required.

### Rearmed After panel

In this panel, you can set how often an alarm will be rearmed — unlimited or limited (in which case the parameter value needs to be set).
- rearmed after previous alarm is cleared
- limited

### Automatic Clear panel

The fields in this pane may be used to configure the system to automatically acknowledge alarms that have not received a response in a timely manner as well as to automatically delete records of old acknowledged alarms.
- automatically clear after
- delete cleared alarms after

### Alarm Predefined Clear Descriptions

This pane is used to predefine descriptions used to clear alarms. When "force adding description on clear" is checked, the predefined descriptions entered here will display during an alarm in CC in a drop down. This is in addition to the free-text field used to enter a non-predefined description.
When this option is unchecked, the section will greyed out.

Cameras Tab

This tab is used to associate cameras with the alarm type. It contains an **Item Browser**, which shows the attachable entities, and a table of the entities attached to the alarm type.
You can move entities to and from the table using the and buttons. For each entity you associate with the alarm, you need to specify whether and how it should be displayed and/or recorded. The Live View column is used to indicate whether you would like to see a live view from each camera upon alarm. The Recording and Playback columns have similar check-boxes but also contain input boxes that are used to enter start and end times, in seconds, relative to when the alarm is triggered.

You can change the order in which cameras and other playable entities are shown with the and buttons.

The Digital Preset column allows fixed cameras to trigger predefined digital presets when the alarm is triggered. When the alarm is triggered and the live cameras view populates an armed tile, the selected digital preset will initiate. In order to select a digital preset, either Live or Playback must be selected and the camera must have configured presets.

Note: If a camera is bound to an ioi TRK, the presets are disabled and therefore will not show until it is unbound.
Click to open **Recipients Tab**

This tab is used to specify which users receive alarms of the alarm type and how they are sent -- to all the recipients at once or sequentially.

To add/remove a user to the alarm's recipients, select it in the Item Browser and use the buttons. If the alarm is sent out sequentially, the order recipients receive it is based on their Priority. A user will receive an alarm only if all higher priority recipients have not responded to it. The **Escalation timeout** parameter determines how much time must pass before the alarm is sent to the next lower priority user(s). In the example above, if the members of “Team 1” do not respond within 60 seconds, then alarms of this type will be passed to the “System Owners System Administrator”.

Click to open **Actions Tab**

Latitude fires events to indicate that an alarm is triggered, activated, accepted, cleared or any other change in the alarm status. The administrator can configure automatic actions, such as sending an email notification or switching the state of output pins to events that indicate changes in an alarm status. See [Events and Actions](#) and [Alarms](#).
5.1.1 Configuring an Alarm with Cameras

The following procedure shows how to create an alarm and configure it to display multiple cameras in the ControlCenter on alarm.

If you want color coded alarms based on alarm priority, go to the Physical View>System General tab and under Alarms, select *Enable color coding in alarms management*

**To configure an Alarm with cameras**

1. From the Side-Bar menu click **System Settings** and then in the Navigation Tree right-click **Alarm types** and select **Add alarm type**.
   
2. If not displayed, click the **General** tab and do the following:
   
   a. Type an **Alarm Name** and optional **Description** in the appropriate field.
   
   b. From the **Pre-alarm** coverage menu, select a coverage.
   
   c. If there is a procedural URL for the alarm, in the **Procedure URL** field, enter the URL "file:" or path to the HTML content and select/unselect **Auto display procedure URL**.
   
   d. In the **Dwell time** field, enter the time and select the units from the menu.
   
   e. In the **Priority** field, enter the priority level of the alarm.

   If you have "Enable color coding in alarms management" enabled in the System settings, a color swatch box will show the color that will highlight the Alarm in the ControlCenter when the alarm is listed.

   f. Select either **Rearm after the previous alarm is cleared** or **Limited** and set the limited number and time unit to use.
   
   g. To configure the alarm to automatically clear (no user intervention), select **Automatically clear after** and set the number and time units to delay before auto-clearing. **Note:** The video we are going to attach will not display if the alarm is cleared before it can be display. After an alarm is cleared the alarm video display is canceled.

   h. To have cleared alarms deleted, select **Delete cleared alarms after**, enter the number and select the time unit from the menu for delaying the deletion.

3. Click the **Cameras** tab and do the following:

   a. From the camera scene tree, select a camera to add and click [ ]
   
   b. In the selected cameras table, click the camera row for the added camera. Three check-boxes appear on the row.
   
   c. To enable the camera to display (automatically on-alarm or on demand when the alarm is clicked) mark the check-box in the **View Live** column. (Required for it to appear in the on-alarm display cycle of the ControlCenter.)

   d. To enable the camera to automatically record on alarm (if it is not already recording at the time) mark the check-box in the **Record** column.

   - To change the pre and post alarm recording times or recorded file lifespans, click the hyperlink and in the dialog that appears enter the number and time intervals for each and then click **OK**.

   e. To enable the camera to automatically playback on alarm of pre-alarm video, mark the check-box in the **Playback** column.

   - To change the pre and post alarm playback times, click the hyperlink and in the dialog that appears enter the number and time intervals for each and then click **OK**.
f. Repeat steps a. through e. for each camera.
g. To sort the Live View and Playback enabled cameras to a custom order in the cycle, select the camera row and click \( \text{ up arrow} \) to move it forward (up) in the play order or click \( \text{ down arrow} \) to move it towards the back of the cycle sequence (down).

4. Click the **Recipients** tab and do the following:
   a. Select **All recipients at the same time** or **Sequentially by priority** (rollover based on priority) and set the delay time in seconds in the **Escalation timeout** field.
   b. From the Recipients tree, select a User group or User to add and click \( \text{ add} \).
   c. If you selected **Sequentially by priority**, click the number in the Priority column for the added User or User Group and set the priority (one being the highest priority).
   d. Repeat steps a. through c. for each User or User Group you want to add.

5. Click the **Actions** tab and optionally configure one or more actions. For more information, see **Events and Actions**.

6. When finished, click \( \text{ save} \).

**Note:** The on-alarm automatic display of a "View Live" video requires that the Control Center user has at least one viewing tile that is in ‘Armed for Alarms’ state.

To arm a tile or tiles for ‘Armed for Alarms’ status, the Control Center user must click on the tile number of the tile/s that are to be used for displaying on-alarm live content until the tile number turns red and the icon rollover shows ‘Armed for Alarm’ (lower left-hand corner of the viewing tile).

**Note:** The tile number of a tile that is in normal state must be clicked twice. A tile that is in ‘Armed for alternative content’ state (yellow tile number) needs to be clicked once.

This method applies for all Alarm Display modes - Block mode, Flat mode, or Salvo mode.

### 5.2 Binding Cameras and Encoders

The camera and the TRK-101/TRK-101-P are bound to each other from the Latitude AdminCenter.

This ‘binding’ enables functionality such as using the encoder to provide providing Analytics on the camera scene, or allowing PTZ tracking of moving objects.

- Before binding a fixed camera, make sure that the camera is configured as a fixed camera in the Camera Type section of the TRK-101/TRK-101-P Camera > Type & Model page.
- If your fixed camera has Digital PTZ functionality, it must be disabled in Latitude because you must have a fixed Field of View in order for the analytics to work properly.

**To bind the TRK-101 or TRK-101-P to the camera if a fixed camera is discovered as a PTZ camera**

1. Select the top-level **System** in the Camera Tree.
2. Select the **Analytics tab**.
3. Select the camera that you want to bind from the Available Camera list.
4. Use the arrow button to add it to the Camera table.

**Caution:** Make sure that the TRK unit is not attached to Latitude.

5. In the table, do the following:
   a. In the Connection Type column, from the drop-down list, select Decoder, Manual RTSP or Analog. (Decoder mode will only show for supported cameras).
   b. In the Analytic Device IP column, enter the IP address of the TRK unit that you want to attach to the PTZ camera.
      i. If you select Decoder, the configuration is automatic.
      ii. If you select Manual RTSP, click the RTSP Setting button. If the TRK-101 is connected to a FLIR camera, the IP address is displayed automatically in the Analytic Device IP column. If the camera is not displayed automatically, enter the full RTSP address string after the camera’s IP address in the RTSP Settings dialog box. For example, if the FLIR camera’s RTSP URL is “rtsp://<ip>/ch0”, enter “/ch0” in the Camera RTSP Stream URL text box.
If authentication is required for the RTSP connection, select the **Authorization Required** check-box. Then enter the **User Name** and **Password** in the respective text box. Click **OK**.

---

**Unit Information Table**

**Note**: The Auto Rearm feature will be implemented in a future release.

6. Click **Save**.
7. Click **Arm/Disarm** or arm the unit from ControlCenter. The camera is displayed as Armed in the Arming Status column of the Camera table. The Analytics function starts to operate after the camera is armed and OK is displayed in the Analytics Status column.
8. From the **Setup > Depth** screen of the TRK unit's web interface, configure the analytic settings.
Once binded, the "set" and "Edit" preset buttons will be disabled. Presets should be set and edited from the TRK.

If the camera is streaming on a joint live/recorded stream (i.e record same as live) the TRK will automatically use and configure the second stream to be used for analytics.

If the camera is set to separate streams, the recorded stream will need to meet the requirements needed for the TRK (D1 resolution).

*Note:* Do not use VGA resolution on the camera in PAL format on CP-4221 cameras.

5.2.1 Configuring RTSP Support for a Camera on a TRK Unit

The video stream of the camera is viewed on the TRK unit via an RTSP connection. Each supported camera has its own syntax for the URL that attaches it to the RTSP server. The URL is entered in the TRK-101/TRK-101-P Setup > System > Unit Information screen. See Figure 4: Unit Information Screen. in the TRK Web Interface.

The syntax for each supported camera follows. For "<ip>", enter the camera’s IP address.

**FLIR F-Series and FC-Series (ID, R, and S)**

rtsp://<ip>/ch0

**FLIR TCX**

rtsp://<ip>/cam/realmonitor?channel=1&subtype=1&proto=Onvif

**Quasar**

rtsp://<ip>/h264_2

*Note:* Quasar uses Stream 2 for RTSP streaming ("h264_2").

**Axis**

rtsp://<ip>:<rtsp_port>/axis-media/media.amp?videocodec=h264&audio=0&camera=1&fps=<fps>&compression=50&resolution=640x480&videobitrate=<bitrate>&videobitratepriority=quality&videokeyframeinterval=<keyframe_interval>

Where:
- `<rtsp_port>` – used rtsp port (default 554)
- `<fps>` - frames per second required
- `<bitrate>` - desirable bitrate (bit per second should be set to 1500 and 1000 for static rules)
- `<keyframe_interval>` - desirable interval between key frames (GOP) in frames

*Note:* Used VGA resolution (640x480)

**Example:**

rtsp://10.70.20.179:554/axis-media/media.amp?videocodec=h264&audio=0&camera=1&fps=25&compression=50&resolution=640x480&videobitrate=1500&videobitratepriority=quality&videokeyframeinterval=50
Note: The stream number is not defined as a parameter in the Axis syntax. The above parameters are configured directly in the Insert RTSP stream URL text box on the TRK-101/TRK-101-P Setup > System > Unit Information screen. No additional configuration is required in the camera.

Sony
rtsp://<ip>/media/video2

Note: Sony uses Stream 2 for RTSP streaming (“video2”). Before entering the URL, the video stream parameters must be configured on the camera’s web page. The video stream parameters cannot be configured in the Insert RTSP stream URL text box on the TRK-101/TRK-101-P Setup > System > Unit Information screen.

Bosch
rtsp://<ip>/video?inst=2

Note: Bosch uses Stream 2 for RTSP streaming (“video?inst=2”). Before entering the URL, the video stream parameters must be configured on the camera’s web page. The video stream parameters cannot be configured in the Insert RTSP stream URL text box on the TRK-101/TRK-101-P Setup > System > Unit Information screen.

5.3 Events and Actions
An event is a general type of occurrence registered by Latitude, either system-related (e.g. unit discovered) or user related (e.g. incident created). An action is a response to an event that may be configured to happen whenever an event occurs during a given coverage. Multiple actions may be configured for each event, including actions of the same type. For example, a start record action may be configured with different timeout and/or time-to-live parameters for different coverages.

Events/Actions can be configured for entities whose configuration panes have Actions tabs, including most logical and physical entities as well as alarm types. The events and actions available in the Actions tab are not user configurable.

Note: Under some circumstances, however, new types of actions can be added for an entity when the System Development Kit (SDK) is used to provide custom facilities in the system.

See the list of possible Events that are available for Peripheral Entities, Server Entities and the special case of System Events/Actions.
To assign an Action to an event

An entity's Actions tab contains a list of the event types pertinent to the entity. Right-clicking an Event in the list opens a list of possible Actions.

Once an action is created (or an existing action is focused), the right side of the pane displays fields for configuring the action. These include the Coverage during which the event/action relationship should be effective, plus other settings that vary based on the type of action being configured. For a "Start Recording" action, for example, you must configure which entities are recorded and the recordings' Recording lifespan, Timeout and Video Profile (if applicable).
To record several entities using different parameters, create several “Start Recording” actions instead of just one.

The event Settings Screen allows you to define event behaviors to attach to related camera, recording, communication and associated user actions events.

The list of events and action options available in the right click menu are extensive and include settings that will not be discussed in this document. If you would like to learn more about the event and actions settings and configuration, see the Latitude User Documentation.

The Actions Tab has the following features:
If you want to delete a created Action configuration, you can right-click on it and select Delete from the shortcut menu.

For details of the different parameters required for different types of Actions, see Actions.

**To Configure an Action to an Event**

1. Select either Logical View or Physical View and then in the Navigation Tree, select the entity associated to the event you want to configure.
2. Click the Actions tab.
3. In the Actions tab configuration area, right-click on the event in Events and Actions, and select the Action to add from the shortcut menu.
   The Action you selected displays as a child entity below the selected Event in the Events/Actions area and the settings for the Action appear in the display area.
4. From the Coverage menu, select an existing Coverage.
   **Tip:** If the Coverage you want is not defined, you will need to define in the System Settings. You can come back and change the Coverage attached to the event.
5. Enter the required settings and click Save.

**WARNING:** When using Actions that will operate external devices, by activating or triggering them automatically from the system, ensure that all safety and security considerations are applied.

Never connect devices to the automation of the system that pose a security or safety risk.
Additionally, consideration for **manual overrides** should be given in instances when the system is operating normally, down, restarting, restored, or malfunctioning. If an event is configured to automate operation, all users of the system with access to the system should be informed and properly trained on the behavior of operating and triggering these events and actions as well as procedures to assure safety and conformance during fire, emergency, power outages, or malfunction. Administrators of the system must take full responsibility for assuring proper use and safety precautions for unseen events that can occur within any automation they design.

**Special cases - System-wide events:**
Most events/actions have a 1:1 relationship between the source of the event and its associated action. However, there are two additional modes that should be taken into account:

- Events which could occur in any one of a number of cases, but should always have the same effect. Example - any camera tamper event should always trigger an alarm - it should not be necessary to define the camera-tamper event for each camera separately.
- Events that could generate multiple alarms, but only refer to a single incident - example - if an Archiver becomes unavailable, not only is 'Accessibility Lost' triggered from the Archiver, but it will also be triggered for all cameras attached to that Archiver.

For this reason, a special class of **System-wide events** can be defined, where only one event will be generated even though the event may be triggered by anyone of many entities, or only one event is reported even though many different units may have the same status.

### 5.3.1 Events

**Peripheral Entities Events**

<table>
<thead>
<tr>
<th>Events</th>
<th>Camera</th>
<th>PTZ Camera</th>
<th>Camera Seq.</th>
<th>Analytics device*</th>
<th>Microphone</th>
<th>CCTV K/B</th>
<th>Input pin</th>
<th>Output Pin</th>
<th>Analog Monitor</th>
<th>Speaker</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility lost</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Accessibility recovered</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Add Serial Device</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Analytics - Camera shift</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Analytics - Fence detection</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Analytics - Intrusion ended</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Analytics - Intrusion started</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Analytics - Loitering detected</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Analytics - Object removed</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Analytics - Tripwire detection</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Analytics - Unattended object</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>Camera</td>
<td>PTZ Camera</td>
<td>Camera Seq.</td>
<td>Analytics device*</td>
<td>Microphone</td>
<td>CCTV K/B</td>
<td>Input pin</td>
<td>Output Pin</td>
<td>Analog Monitor</td>
<td>Speaker</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------</td>
<td>------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>------------</td>
<td>----------</td>
<td>-----------</td>
<td>------------</td>
<td>----------------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>Analytics - Vehicle stopped</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Archived stream switch off</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Archived stream switch on</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bookmark created</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bookmark updated</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera signal lost event</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera signal recovered event</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clip locked</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clip unlocked</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Live stream switch off</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Live stream switch on</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master recording ended</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master recording failed</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master recording started</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media snapshot exported</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin set to abnormal state</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin set to normal state</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ locked</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ locked overridden</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ moved to preset</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ pattern ended</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ movement ended</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ movement started</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ pattern started</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ session ended</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ session started</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTZ unlocked</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recording clip export ended</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Events | Camera | PTZ Camera | Camera Seq. | Analytic device* | Microphone | CCTV KB | Input pin | Output Pin | Analog Monitor | Speaker | Comments
---|---|---|---|---|---|---|---|---|---|---|---|---
Recording clip export started | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Recording ended | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Recording started | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Scene motion off | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Scene motion on | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
SD card restore session ended | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
SD card restore session started | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Source Filter streaming started | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Source Filter streaming stopped | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Tampering camera event | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Technician session ended | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Technician session started | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Zone motion off | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Zone motion on | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0

* for ioimage and FLIR devices with these capabilities

Server Entities Events/Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Archiver</th>
<th>Directory</th>
<th>EDB</th>
<th>Gateway</th>
<th>Transcoder</th>
<th>Web Server</th>
<th>Mail Server</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility lost</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Accessibility recovered</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Archiving resumed</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Archiving stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ART lost</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ART recovered</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Audit Log purged</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Backup started</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connection to database</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Action</td>
<td>Archiver</td>
<td>Directory</td>
<td>EDB</td>
<td>Gateway</td>
<td>Transcoder</td>
<td>Web Server</td>
<td>Mail Server</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------</td>
<td>-----------</td>
<td>-----</td>
<td>---------</td>
<td>------------</td>
<td>------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>lost</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection to database recovered</td>
<td></td>
<td>o</td>
<td>o</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containers initialized</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database corrupted event</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database valid event</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory failed to synchronize</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory server licensed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory server unlicensed</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defective containers percentage abn</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery lost</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery recovered</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failover ended</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failover started</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mass export job added</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mass export job removed</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mass export job updated</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shut down</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Storage location corrupted</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage location down</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage location restored</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage location tampered</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage utilization abnormal</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
System Entity events

The following Actions/Events are defined for the System entity (Root).

**Note on System-wide events:** Normally, if an 'Alarm Triggered' Action/Event is defined for a specific entity, the resulting Action/s will only be executed when that particular entity triggers the alarm. However, if 'Alarm Triggered' for the System Action/Events is used, then the alarm will be triggered for any alarm that is raised in the system.

<table>
<thead>
<tr>
<th>Event</th>
<th>S.W.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm cleared</td>
<td>o</td>
</tr>
<tr>
<td>Alarm triggered</td>
<td>o</td>
</tr>
<tr>
<td>ART lost</td>
<td>o</td>
</tr>
<tr>
<td>ART recovered</td>
<td>o</td>
</tr>
<tr>
<td>Camera Accessibility lost</td>
<td>o</td>
</tr>
<tr>
<td>Camera Accessibility recovered</td>
<td>o</td>
</tr>
<tr>
<td>Camera signal lost event</td>
<td>o</td>
</tr>
<tr>
<td>Camera signal recovered event</td>
<td>o</td>
</tr>
<tr>
<td>Connection to database lost</td>
<td>o</td>
</tr>
<tr>
<td>Connection to database recovered</td>
<td>o</td>
</tr>
<tr>
<td>Database corrupted event</td>
<td>o</td>
</tr>
<tr>
<td>Database valid event</td>
<td>o</td>
</tr>
<tr>
<td>Defective containers percentage abnormal</td>
<td>o</td>
</tr>
<tr>
<td>Email sent</td>
<td>o</td>
</tr>
<tr>
<td>Incident created</td>
<td>o</td>
</tr>
<tr>
<td>Incident updated</td>
<td>o</td>
</tr>
<tr>
<td>Master recording failed</td>
<td>o</td>
</tr>
<tr>
<td>Server Accessibility lost</td>
<td>o</td>
</tr>
<tr>
<td>Server Accessibility recovered</td>
<td>o</td>
</tr>
<tr>
<td>Shut down</td>
<td>o</td>
</tr>
<tr>
<td>Storage location corrupted</td>
<td>o</td>
</tr>
<tr>
<td>Storage location down</td>
<td>o</td>
</tr>
<tr>
<td>Storage location restored</td>
<td>o</td>
</tr>
<tr>
<td>Storage utilization abnormal</td>
<td>o</td>
</tr>
</tbody>
</table>
### 5.3.2 System-Wide Events

The following Actions/Events are defined for the System entity (Root).

**Note:** Normally, if an 'Alarm Triggered' Action/Event is defined for a specific entity, the resulting Action/s will only be executed when that particular entity triggers the alarm. However, if 'Alarm Triggered' for the System Action/Events is used, then the alarm will be triggered for any alarm that is raised in the system.
### 5.3.3 Actions

The system-defined Actions that can be initiated for any Event are listed below. Right-clicking on an Event shows the list of available Actions, and selecting an action opens a panel in which the user can define the required parameters for that Action.

The system does not limit the user to define only one Action per Event. Multiple instances of Actions can be defined with different parameters.

The following Actions are supported:
- Analytics - switch to auto mode
- Change output pin state to abnormal
- Change output pin state to normal
- Clear camera analytics
- Create Incident
- Execute external Action
- Go to PTZ preset
- Play audio on speaker
- Play video on monitor
- Reset recording quality
- Run a PTZ pattern
- Send email
- Set recording quality
- Start recording
- Stop recording
- Switch content to ControlCenter
- Trigger alarm

**Analytics - switch to auto mode**
Applies specifically to ioimage PTZ camera - after Manual PTZ changes, causes camera to return to executing stored Pattern

**Change output pin state to abnormal**

*Note: To control a device attached to an Output Pin, the device must be explicitly defined by right-clicking on an Output Pin port in the Physical View, and selecting either Add Output pin device or Attach existing Output pin device.*

![Physical View](image)

When selecting this Action, all devices that have been defined will be shown in the **Available Items** window.

![Available Items](image)

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more devices to be **Attached** to this action.
3. Set the **length of time** that the state is to be maintained.
   (Note: default is zero, so if you don't change it, nothing will happen.)
Change output pin state to normal
Uses the same parameters as 'Change to abnormal', but with no parameter for how long it should stay in that state - 'normal' is the default state.

Clear camera analytics

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **Analytics cameras** to be **Attached** to this action.
Create Incident

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more devices to be Attached to this action.
3. Enter an Incident tile (An error message is given if this field is left blank.)

Execute External Action

This allows the Action to initiate External Actions that have been defined using the Systems Settings/External Actions screen.

To define a new External Action type, click on **System Settings** in the Sidebar, and then, in the Navigation tree, right-click on **External Action types**.

Once the External Action type has been defined, Actions that invoke it can be defined.
1. Select the **Coverage** during which the action is to be in effect.
2. Select the **Action type** from the Action type drop-down.
3. Add the **String** and/or **Integer parameters** if required for this type of Action.

---

**Go to PTZ preset**

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **PTZ cameras** to be **Attached** to this action.
3. From the list of Presets for the selected PTZ camera, choose the PTZ Preset to be used.
Play audio on speaker

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **Speakers** to be **Attached** to this action.
3. Select one **Audio Source** (i.e. Microphone) from the drop-down to be used as input.

Play video on monitor

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **Monitors** to be **Attached** to this action.
3. Select one **Video Source** (i.e. Camera) from the drop-down to be used as input.
Reset recording quality

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **Cameras** to be **Attached** to this action.
3. Set the **Post-Event timeout**.

Run a PTZ pattern

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **PTZ cameras** to be **Attached** to this action.
3. From the list of PTZ Patterns for the selected PTZ camera, choose the Pattern to be used.

Send email

*Note: An E-Mail Server must be defined in order for the system to send emails.*

See [Mail Server](#)
1. Select the **Coverage** during which the action is to be in effect.
2. Select the **Recipients** to receive the email.
3. If required, modify the Subject, Prefix and/or Suffix.

**Set recording quality**
1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **Cameras** to be **Attached** to this action.
3. Set the **Duration** for which the Recording Quality is to be changed
4. Select the **Recording Profile** to be used.

**Start recording**

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **Cameras** to be **Attached** to this action.
3. Set the **Duration** for which the Recording is to be made.
4. Select the **Recording Profile** to be used.

**Stop recording**

1. Select the **Coverage** during which the action is to be in effect.
2. Select one or more **Cameras** to be **Attached** to this action.
3. Set the **Post Recording Time**.

**Switch content to ControlCenter**

1. Select the **Coverage** during which the action is to be in effect.
2. Select the Control Center to which the content is to be sent.
3. Select the source of the **Content** from the drop-down.

![Content Source](image)

4. Select the **Monitor** of the Control Center to be used, and the **Tile** in which it is to be shown (or choose **First available tile**).
5. If applicable, select the **Digital Preset** to be applied.

**Trigger alarm**

1. Select the **Coverage** during which the action is to be in effect.
2. Select the **Alarm type/s** to be attached to this Action.

![Alarm Trigger](image)
5.4 MMS Video Support

The Microsoft Media Streaming (MMS) plug-in is aimed at receiving video streams from Microsoft’s streaming server into the Latitude system. This feature is useful for users who want to monitor and record video streams from internet sources or 3rd party systems (provided that there is a Windows Media Server streaming them).

**To Discover an MMS Video Stream (can only be done manually)**

1. From Admin Center sidebar, click *Physical View*.
2. Right Click on *Archivers* and select *Add Units Manually* from the drop down list. The *Add Units Manually* dialog box appears.

   ![Add Unit manually dialog box](image)

   - Check the *Host Name* radio button and fill in the Archiver server host name (not the IP address)
   - In the *Unit Type* combo box select the *MMS Plug-in Discovery* option.
   - In the *Camera URL* edit box fill in the *URL* of the video stream.

3. Check the *Host Name* radio button and fill in the Archiver server host name (not the IP address)
4. In the *Unit Type* combo box select the *MMS Plug-in Discovery* option.
5. In the *Camera URL* edit box fill in the *URL* of the video stream.
Stream Connection Types
The MMS plug-in supports only one stream per camera. If a user selects an MMS Camera option in the Admin Center's General tab, the Archiver Recording Stream Type is disabled.

In the Archiver live stream type drop down field, two stream connection types are available:

1. Multicast (default): with this connection type, each client receives an independent stream from the Windows Media Server Multicast when viewing an MMS camera. Because of specific stream configuration generated in the Windows Media Server, by setting this connection type, a client will be able to receive video faster than using the other connection type (Unicast-UDP).

2. Unicast-UDP: When choosing this connection type, the Archiver will get the stream from the web server and proxy the stream to the clients. This connection type is required, for example, when the clients do not have connectivity to the Windows Media Server (e.g. the client have no internet connectivity and the WMS is available over an internet connection).

Note: In both cases, the actual streaming mechanism is TCP/IP and not RTP/UDP.

The third field in this category, Client connection type is relevant only when the ‘Unicast-UDP’ option is selected, and determines how the Archiver proxies the video to the client.

Video Source Connectivity
In the common use case scenario, the video stream is received from a Microsoft Media Server located on a remote site. Latitude cannot control the video quality or the connectivity.

This includes cases such as the lens being out of focus, the Microsoft Media Server not transmitting video (resources problems) or a poor internet connection. The best way to diagnose video quality issues is viewing the MMS stream with Windows Media Player. By comparing the video quality in Windows Media Player to the video quality in Latitude one can understand if the issues are related to the connection with Microsoft Media Server or from to Latitude.

Note: Microsoft Media Server can be configured to limit the duration of a stream (for resource protection purposes). Latitude restarts the stream every time this duration expires. This may take few seconds (depending on the stream connectivity).
5.5  Motion Detection

Motion Detection refers to the system's ability to ‘notice’ movement. This allows the system to bring the motion to the attention of users, and start predefined processes in the system. Typical examples are:

- Trigger an Alarm that requires operator attention
- Start recording so that the activity is saved for review, without the overhead of recording a static scene all the time
- Bookmark the event in a recording, so that it can easily be found later
- With certain cameras it is also possible to monitor a scene in low-resolution and switch to high resolution when movement is detected. This reduces overall bandwidth demand in the system. Where continuous recording is required, scenes not showing motion above a certain threshold can be recorded in low resolution. This reduces overall storage consumption.

Motion detection is normally set up using the capabilities of the cameras themselves (‘edge-based’).

The parameters for setting up basic edge-based motion detection are described here.

Note: The Latitude system also supports archiver-based motion detection – for more information on this see the Help system.

Overview
- Motion Detection Settings
- Configuring Motion Detection
- Edge-Based Motion Detection Configuration
- Archiver-based Motion Detection Guidelines
- Motion Detection Behavior with Basic Analytics
- Advanced Configuration Guidelines

5.5.1  Motion Detection Settings

In order to avoid the recording of all storing and viewing of static video clips, which take up time and storage space, Latitude enables the users to focus their attention and resources on video clips in which motion has been detected. Additionally, in Live viewing, it is usually not possible for operators to monitor all cameras in real time, and it is possible to set up the system so that when motion is detected in a scene, a real-time alert is created which can perform actions such as triggering an alarm and/or forcing the affected camera to be displayed at a viewing station.

Activating recording and sending alerts upon detecting motion are among the main — but not exclusive — benefits of this function.

Configuring motion detection parameters varies depending on the mode and type in question.

- Motion Detection Modes
- Motion Detection Zones
- Motion Detection States
- Motion Detection Parameters
Motion Detection Modes
Motion detection can be utilized in two different modes —
**Edge-device based** via the camera itself.
**Archiver based** via the Latitude Archiver

Edge-based motion detection is performed by the edge device itself according to zones and parameters defined for each of the zones. This requires the initial configuration of zones and motion detection parameters. When a unit detects motion, it sends back the information of the zone in which motion was detected.

Archiver-based motion detection is performed by the software of the Archiver, analyzing motion data received from units. The Archiver then decides if there is any motion in a predefined zone. Note: Archiver-based Motion Detection

Motion Detection Zones
Motion detection can be directed to two different types of zones — the full screen or specific zones.

When using the full screen, the motion detection parameters are activated and can create an alert on the whole video image. A full screen basically is one zone that covers the whole video image.

When using specific zones, the motion detection parameters are only applied to the zones specified. Some camera types allow multiple zones to be defined. Zones can be defined as the *region of interest* for motion detection. By defining regions of interest, the focus is diverted from regions that should be ignored (masked).

Motion Detection States
Motion detection consists of two states — *Motion on* and *Motion off*.

The *Motion on* state means that motion was detected. When the system is in the Motion on state, the motion detection feature examines the predefined zone(s) to check whether the motion continues or ceases and remains without motion for more than 5 seconds. If the motion ceases according to the preset parameters (sensitivity and motion off threshold), the state will alternate to *Motion off*.

In the *Motion off* state no motion was detected. When the system is in the Motion off state, the motion detection feature examines the predefined area(s) to check if any motion occurs according to pre-defined parameters (sensitivity, motion on threshold and consecutive frame hit). If motion is detected, the state will alternate to *Motion on*.

Motion Detection Parameters
The Motion Detection parameters affect the state in which motion detection remains or to which it alternates.
### Parameter | Description
--- | ---
**Sensitivity** | Sensitivity describes a threshold related to the degree of change or motion of a single motion block. Archiver-based motion detection can be measured by motion vectors. The longer the distance which the motion block has passed from one frame to the next, the higher is the level of motion energy of a motion vector. A high level of sensitivity detects a motion vector with a low motion energy level. A low level of sensitivity only detects a motion vector with a high motion energy level.

**Motion On Threshold** | The threshold which, when passed, the state alternates to Motion on, i.e. when motion is detected. A frame is divided into smaller units called macro blocks. Each macro block is checked for motion. The number of macro blocks from the predefined zone, in which any change/ motion has been detected since the previous frame, are counted. The Motion on threshold is passed if a minimal percentage of macro blocks from the total number of macro blocks of a predefined zone passed the pre-defined sensitivity parameter.

**Motion Off Threshold** | The threshold according to which the state alternates to Motion off, i.e. when motion ceases. **Note**: The motion detection state does not alternate to Motion off immediately after the motion off threshold was passed. Only 5 seconds in which the motion is below the motion off threshold will the state alternate to Motion off.

**Consecutive Frames Hit** | The number of consecutive frames which should pass the motion-on threshold in order to change the state to Motion_on.

**Related Links**
Configuring Motion Detection
5.5.1.1 Configuring Motion Detection

**Edge-based**

From the system's Logical view, select a required camera and click the Motion Detection tab.

1. In the Configuration field, select a Coverage (e.g. Daytime, Always, etc.)
2. Select the Type (e.g. edge zones)
3. Define the Zones. You can select an existing zone or click on to add a new zone.
4. Optionally, click .
5. **Note**: Only certain models allow irregular (i.e. non-rectangular) zones. See Capabilities field below.
6. In the Motion Detection Parameters field set the rates for Sensitivity, Motion On Threshold, Motion Off Threshold and Consecutive Frames Hit.
   **Note**: To assist in setting up the Motion detection parameters, the user can use the Test mode drop-down under the Preview window.

   ![Motion Detection Parameters](image)

   This can be set to Idle, Display all motion, Edit zone, Test all zones, or Test zone.

**Archiver-based**
When testing all zones, if there is motion detected in one or more of the zones, the border
of the Preview window changes to red.

When the motion ceases in all zones, the border returns to clear.

When testing one test zone and motion is detected in that zone, the border of the Pre-
view window changes to red.

When motion ceases in the test zone, the border returns to clear.

7. In the Recording Upon Motion field, mark the required check-boxes (Bookmark motion
on events (if recording), Record upon motion on, Pre event recording, and Set re-
cording video profile upon motion) and set the Stop recording and/or reset profile
times for motion on/off events.

When Motion Detection is activated, recording will start when the recording threshold is
triggered for the number of frames selected.

The Set recording video profile upon motion and Stop recording and/or reset profile
parameters allow the user to set up an automatic sequence to stop recording (and revert to
normal state if an alternative profile was selected) after the defined time has elapsed.

- If motion on is selected, this results in a recording, or changing the profile, starting from
  the motion-on event, for the preset duration.
- If the motion off option is selected, then once recording starts or the change of profile is
  made, it will continue until the off-motion event is detected, plus the time defined.

8. In the Capabilities field, you can view the system's motion detection capabilities and their
settings.

Notes:

1. If Bookmark motion on events is selected, bookmarks will only be created if the unit con-
cerned is currently recording. If the unit is not recording, no bookmark will be created when
motion is detected.

2. The Set recording video profile upon motion parameter allows the user to select a record-
ing profile to be used when motion is detected, using the profiles predefined in the Latitude
system for the manufacturer or defined by the user as ‘Custom Profile’.

3. The Stop recording and/or Restore profile parameter is only enabled if either Record upon
motion or Set recording profile on motion is selected.

To assign an action, such as sending an alarm, to the Motion Detection States, right-click the
desired state in the Actions tab and select the desired action.

Note: You can filter the actions based on coverage that is not related to the coverage filter of the
motion detection. For example, you can set the motion detection coverage to Always and the motion de-
Detection related action, such as sending an alarm, to Sundays only. In this scenario, motion will be detected at all times but alarms will only be sent on Sundays. See Archiver-Based Motion Detection Configuration.

**Configuring Edge-Based Motion Detection**

Edge-based motion detection is supported for zones only. For edge-based zone motion detection, zones must be configured via the Motion Detection tab in the AdminCenter, and all relevant actions must be defined in the corresponding Actions tab. All other parameters are defined in the edge device's settings, using a standard Internet browser.

**Note:** The name of each zone in the web interface must match the name in the AdminCenter.

In the Internet browser, enter the camera IP. The installation of the relevant software is prompted and, when authorized, started automatically. The zones must be defined one by one by specifying the edge-device applied Motion Detection Parameters. See Edge-Based Motion Detection Configuration.

### 5.5.1.1.1 Edge-Based Motion Detection Configuration

Latitude supports edge device motion detection configuration via the Admin Center where the cameras have this functionality integrated.

The web interface motion detection configuration.

Both existing motion detection options are explained in the work-flows below.

**Configuring Motion Detection on Edge Devices via the Admin Center**

**Configuring Ariel Encoders**

The following steps set out how to configure one or more cameras for Motion Detection when using an Ariel-range encoder.
1. Selecting the Encoder and opening its Web Page

From the Physical or Logical view, open the Navigation tree for the required encoder, and select the camera to be configured.

Click on the Web access link to open the browser for the camera.

Log on to the Camera web page.

(Default user name admin, password 1234)

The Camera Web Page opens, with a list of attached cameras in a navigation list on the left of the screen. Select the camera to be configured.
The selected camera's Live View is displayed.

2. Click the **Configuration Tab**
   The camera's **Configuration Tab** is displayed.

   ![Configuration Tab](image)

   Click on the + symbol next to **Camera Settings** in the Navigation tree, to access the Motion Detection parameters.

3. **Configuring the Motion Detection Zone**
   Use the Channel No. drop-down to display the parameters of the required camera. The se-
4. Check the **Enable Motion Detection** box. This enables the Drawing parameters.
5. With the Area Settings selected, click on **Draw Area** and use the mouse to outline the area/s to be monitored for motion.
6. Set the sensitivity to the required value (1-6).
7. Click **Save** to store the configuration.
   If you wish to change parameters, click **Clear All** and reconfigure the Motion Detection parameters.
8. Close the Web Browser and return to the Camera's settings in the Admin Center.
9. **Other parameters:**
   Go to Camera's **Motion Detection** tab in the Admin Center to configure the required **Coverage, Arming Schedule, Triggers**, and to provide name/s for the Regions of In-
Axis Edge Devices

1. Open the Axis edge device Web interface.
2. Log in using **root** as user name and **pass** as password.

   **Note:** These default values may be changed by the User - Make sure that a record is kept of the new values.

   Alternatively, use the link in the AdminCenter **Motion Detection** tab. Clicking this link should open the Web MD page without a login/password request.

3. In the **Setup** tab -- **Event Config** pane, select **Motion Detection**.
4. It is possible to define up to 6 motion detection zones in rectangular shape, each area with individual setting parameters.
5. The name of the Motion Detection zones in Latitude must be same as the zone names used in the Motion Detection configuration of the Web interface.
6. The **Help** link in the right corner will guide you through setting the configuration of the following parameters:
   a. Object size
b. History

c. Sensitivity

**Bosch Edge Devices**

1. Open the Bosch edge device web interface.

   Alternatively, use the link in the AdminCenter *Motion Detection* tab. Clicking this link should open the Web MD page without a login/password request.

2. In the *Settings* tab -- *Alarm* pane, select *VCA* (Video Content Analysis) or *Motion Detector*.

3. It is possible to define a single zone with a complex shape.

4. The **Help on this page** link in the bottom of this window will guide you through the configuration of the following parameters:
   a. Sensitivity
   b. Minimum object size
   c. Average (n frames) -- not in all cameras/encoders

**Sony Edge Devices**

1. Open the Sony edge device web interface.

   Alternatively, use the link in the AdminCenter *Motion Detection* tab. Clicking this link should open
   
   the Web MD page without a login/password request.

2. Log in to the *Setting* window by clicking *Setting* and using *admin* as user name and password. (These default values are suspect to change.)

   Alternatively, use the link in the AdminCenter *Motion Detection* tab. Clicking this link should open
   
   the Web MD page without a login/password request.

3. In the sidebar, select *Object Detection*, and then select the *Moving Object* tab.

4. It is possible to define up to 4 rectangular shaped motion detection zones.

5. The threshold and object size settings are common to all windows.

**Note:** Online help is not available. In order to understand Sony edge motion detection settings, refer to the Sony Security web site:


Look for the section Setting the motion/activity/object detection function towards the end of the Administrating the camera chapter.

- If the MD Configuration window is active in the IE, motion detection events will not report to <Latitude>. It is mandatory to close the IE window after the Motion Detection configuration is concluded.
- The name of the Motion Detection zones in Latitude should be *zone 1*, *zone 2*, *zone 3*, *zone 4*, corresponding to the *Window 1*, *Window 2*, *Window 3*, *Window 4* in the Sony Web Motion Detection configuration.
• 3rd generation Sony edge devices that support Motion Detection are: SNC-RX570N, SNC-RX550N, SNC-RX530N, SNC-RZ50, SNC-DF50, SNC-DF80, SNC-CS50N.
• 2nd generation Sony edge devices currently do not support Motion Detection.

Value Line Edge Devices
1. Open the Value Line edge device web interface.
   Alternatively, use the link in the AdminCenter Motion Detection tab. Clicking this link should open the Web MD page without a login/password request.
2. In the sidebar, click Configuration.
3. In the sidebar, click Motion Detection.
4. Select the Enable motion detection check box.
5. Click the New button to add a new window. At most three windows can exist simultaneously. Use the mouse to click, hold and drag the window frame to re-size or the title bar to move. Clicking on the ‘x’ at the upper right-hand corner of the window to delete the window. Remember to save in order to validate the changes.
6. Click the Save button to save the related settings. A graphic bar will rise or fall depending on the image variations. A green bar means the image variation is under monitoring level and a red bar means the image variation is over monitoring level. When the bar goes red, the detected window will also be outlined in red. Going back to the homepage, the monitored window is hidden but the red frame shows when motion is detected.

• Window Name The text will show at the top of the window.
• Sensitivity This sets the endurable difference between two sequential images.
• Percentage This sets the space ratio of moving objects in the monitoring window.
  Higher sensitivity and small percentage will allow easier motion detection.

Pro Line A Edge Devices

Edge-based Motion Detection of Pro Line A edge devices is defined as Archiver-based Motion Detection with the following differences:
• While in Test All Zones mode, the moved macro blocks are not visible.
• Zones must be rectangular-shaped.

5.5.1.1.2 Archiver-based Motion Detection Guidelines

Note: Archiver-based Motion Detection is a legacy capability which was used before cameras had the built-in capability to detect and signal motion. It is processor-intensive and therefore, where possible, the newer edge-based Motion Detection is recommended.

General Guidelines
The following guidelines are recommended for Video Motion Detection (VMD).
• It is highly recommended to first set the video profile before configuring VMD.
- If the encoder streams are not merged (i.e. ‘split’), it is important to remember that VMD configuration and run time are performed on the recording stream.

**Note:** The system automatically displays the archived stream while configuring MD.

- The Sensitivity parameter is not linear. For most scenes, sensitivity should be set to values higher than 85%.

- In most cases, the Motion On threshold and the Motion Off threshold parameter values should be set close one another. For example, if the Motion On threshold parameter is set to 10, the Motion Off threshold parameter should be set to 8 or 9.

- The Motion Off threshold parameter should be configured to be significantly lower than the Motion On threshold parameter only if the desired result is that once motion is detected, a motion level that is less than the Motion On threshold parameter will not turn off the motion (i.e. fire a motion off event).

- Unless special configuration is needed (such as Boost upon motion), it is recommended to set all VMD recordings and bookmarks via the Motion Detection tab in the AdminCenter and not via the Actions tab.

**To configure Motion Detection in the AdminCenter**

1. In the AdminCenter, in the Sidebar, select Logical View or Physical View, and then click the desired scene from the Navigation pane.

2. Click the Motion Detection tab.

3. When configuring Motion Detection settings for the first time or to add additional Motion Detection settings, click the Add next to the Coverages drop-down list.

4. Select a previously defined coverage from the Select Coverage dialog box and then click OK. For more information, see Coverages.

5. From the Type drop-down list, select the motion detection type — Archiver zones, Archiver full screen, Edge zones or Edge full screen.

6. If the Archiver zones or Edge zones type was selected, select an existing zone from the Zones drop-down list or click Add to define a new zone. Alternatively, click Import Zones to import zone definitions from another coverage within the same scene.

In addition, a zone selected from the Zones drop-down list can be removed or renamed.

7. If a Privacy Mask was configured and you have permission to remove, right-click and select Deactivate privacy mask on the preview video.

8. From the drop-down list underneath the Preview pane, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>Motion detection is not displayed in the Preview pane</td>
</tr>
<tr>
<td>Display all motion</td>
<td>Motion of all defined zones is displayed in the Preview pane</td>
</tr>
<tr>
<td>Edit zone</td>
<td>Edit the zone selected from the Zones drop-down list</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
**Test all zones** | All defined zones are visible in the Preview pane (in different shades of color) and can be tested to adjust the desired motion detection settings. The border of the Preview pane indicates that this option has been selected. Note: For Pro Line A edge-based Motion Detection, the moved macro blocks are not visible

**Test zone** | The zone selected from the Zones drop-down list is visible in the Preview pane and can be tested to adjust the desired motion detection settings

9. After selecting **Edit Zone** from the drop-down list beneath the **Preview** pane, select the specific area in which you want to detect motion, using the following buttons (it will appear as green layer):

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Rectangle" /></td>
<td>Marks a rectangle-shaped area as area of interest. In the Preview screen, mark the desired area.</td>
</tr>
<tr>
<td><img src="image" alt="Whole Screen" /></td>
<td>Marks the whole screen as area of interest.</td>
</tr>
<tr>
<td><img src="image" alt="Macro Block Erase" /></td>
<td>Erases single macro blocks from a previously marked area of interest. In the Preview screen, erase the macro blocks to be taken out of the desired area. This option is disabled for Pro Line A edge-based Motion Detection.</td>
</tr>
<tr>
<td><img src="image" alt="Macro Block Mark" /></td>
<td>Marks single macro blocks as area of interest. In the Preview screen, mark the desired area. This option is disabled for Pro Line A edge-based Motion Detection.</td>
</tr>
<tr>
<td><img src="image" alt="Clear Screen" /></td>
<td>Clear the whole screen.</td>
</tr>
</tbody>
</table>

10. In the **Motion Detection Parameters** pane, set the following parameters for the desired zone(s):

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sensitivity</strong></td>
<td>Sensitivity describes a threshold related to the degree of change or motion of a single motion block. For example, archiver-based motion detection can be measured by motion vectors. The longer the distance which the motion block has passed from one frame to the next, the higher is the level of motion energy of a motion vector. A high level of sensitivity detects a motion vector with a low motion energy level.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>A low level of sensitivity only detects a motion vector with a high motion energy level.</td>
<td></td>
</tr>
<tr>
<td><strong>Motion On Threshold</strong></td>
<td>The threshold which, when passed, the state alternates to Motion on, i.e. when motion is detected.</td>
</tr>
<tr>
<td></td>
<td>A frame is divided into smaller units called macro blocks. Each macro block is checked for motion. The number of macro blocks from the predefined area, in which any change/motion has been detected since the previous frame, are counted.</td>
</tr>
<tr>
<td></td>
<td>The Motion on threshold is passed if a minimal percentage of macro blocks from the total number of macro blocks of a pre-defined area passed the pre-defined sensitivity parameter.</td>
</tr>
<tr>
<td><strong>Motion Off Threshold</strong></td>
<td>The threshold according to which the state alternates to Motion off, i.e. when motion ceases.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>The motion detection state does not alternate to Motion off immediately after the motion off threshold was passed. Only 5 seconds after the motion off threshold was passed and no further motion has been detected will the state alternate to Motion off.</td>
</tr>
<tr>
<td><strong>Consecutive Frame Hit</strong></td>
<td>The number of consecutive frames which should pass the motion on threshold in order to alternate the state to Motion on.</td>
</tr>
</tbody>
</table>

11. In the **Recording Upon Motion** pane, set the following options:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Record Upon Motion-On</strong></td>
<td>Select this check box to start recording when the motion detection state alternates to Motion on</td>
</tr>
<tr>
<td><strong>Bookmark Motion-on events</strong></td>
<td>Select this check box to create a bookmark for each motion event</td>
</tr>
<tr>
<td><strong>Pre Event Recording x Seconds</strong></td>
<td>Select this check box and set how much time before an event occurs the recording should start</td>
</tr>
<tr>
<td><strong>Stop Recording x Seconds after motion-off</strong></td>
<td>Select this check box to stop recording after a pre-defined time span passes since the motion detection state alternates to Motion off</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Recording x Seconds after motion-on</td>
<td>Select this check box to stop recording after a pre-defined time span passes since the motion detection state alternates to Motion on</td>
</tr>
</tbody>
</table>

12. In the **Capabilities** pane, you can view the Motion Detection capabilities of the scene.

The configuration can be previewed in the **Preview** pane and adjusted accordingly.

**Note:** Macro blocks (in the region of interest) that passed the sensitivity threshold are marked in red. When testing a single zone and alternating to **Motion on**, the border appears red. When alternating to **Motion off**, the border remains clear. When testing all zones and one or more of the zones alternates to **Motion on**, the border appears red. When alternating to **Motion off** in all zones, the border remains clear. The different MD parameters can be changed and the change can be viewed immediately in the Preview pane.

13. Save the configuration.
14. Go to the **Actions** tab.
15. Right-click **Scene Motion On**, **Scene Motion Off**, **Zone Motion On** or **Zone Motion Off** respectively, and select the desired action for each state.

**Note:** You can filter the actions based on coverage that is not related to the coverage filter of the motion detection. For example, you can set the motion detection coverage to **Always** and the motion detection related action, such as sending an alarm, to **Sundays only**. In this scenario, motion will be detected at all times but alarms will only be sent on Sundays.

5.5.1.1.2.1 Advanced Configuration Guidelines

**Configuring VMD for Low F/R Video**

- If the frame rate (FR) is set to 1 FPS, the compression type must be set to SM4.
- Use low consecutive frame hit.
- In the Mpeg-4 format, key frames do not contain any motion information. Therefore, a high rate of key-frames may downgrade the reliability of the motion detection.

**Note:** In VSIP units, the key frame interval parameter is set to 1 every X frames while in Latitude the key frame interval is set to 1 every X seconds. There is a significant difference between the following video profiles:

1. Profile A: 25 FPS, key frame every 4 seconds
2. Profile B: 1 FPS, key frame every 4 seconds

While in profile A only 1% (1 out of 25*4=100) of the frames will not contain any motion information, in profile B, 25% (1 out of 1*4=4) of the frames will not contain any motion information.

In a low frame rate, set the key frame interval to a high value (at least 15).
Boosting to a Higher F/R Video

When boosting upon motion to a higher frame rate, the following actions should be used for the events:

- Motion On should trigger the **Start Recording** action, with an indefinite recording period.

- Motion Off should trigger the **Stop Recording** action with a Post Recording Time set to 30 seconds or as desired.

- The **Set Recording Quality** action does not offer these parameters, i.e. indefinite recording period and post recording time. Therefore it is not useful for this application.

When boosting to a profile, if the same profile is used as by the Live stream, then it will switch to the live stream. Otherwise the recording stream configuration will change on the fly. It is important to take the total encoder capability into consideration when configuring the boost.

**5.5.1.1.3 Basic Analytics**

Certain Models of FLIR cameras come with a 'Basic Analytic' feature which allows those cameras to detect analytic events and trigger actions as a result. The analytic feature uses the same functionality that is used for motion detection and can therefore only support the use of one of these features at a time.

There are several scenarios which will be effected by this behavior.

1. Enabling analytics with a configured motion zone
2. Setting a new motion zone while analytics are enabled
3. Copy Configuration from a camera to another camera with analytics enabled.

**Supported Models:**

CF-6308-00-0, CM-6308-P1-I, CM-3304-XX, CM-3308-XX, CB-3304-XX, CB-3308-XX

**Analytics Tab:**

Analytics are configured via the cameras webpage, however, there is a basic user interface for enabling/disabling, arming/disarming a camera that supports basic analytics and seeing analytics overlay.
If a motion zone is configured and the user attempts to Enable Analytics, they will be prompted by the following warning:

By clicking 'Yes' the motion zone will be disabled immediately (prior to saving) and the Analytics will be enabled upon saving.

By clicking 'No' the dialog box will close and no changes will have been made.

If no motion zone is configured, the analytics rule will be enabled and no warning will be shown.
**Note:**
Prior to enabling a rule from Admin Center, the analytics rule has to be configured via the web page.

**Motion Tab:**
If the camera's analytics are enabled and the user attempts to configure a motion zone, the following message will appear:

![Warning message](image)

By clicking 'Yes' the analytic rule from the camera will be disabled, and the user will continue with their motion detection configuration.

By clicking 'No' the dialog box will close and no changes will have been made.

If no analytic rule is enabled on the device, the motion detection settings will remain as normal and no warning will be shown.

**Copy Configuration:**
If another camera is configured with a motion zone, and the user attempts to "Copy configuration" from that camera to a camera with Basic Analytics enabled, the following message will appear:

![Warning message](image)

By clicking 'Yes' the analytic rule from the camera will be disabled, and the user will continue with their motion detection configuration.

By clicking 'No' the dialog box will close and no changes will have been made.
Note: Changing Analytics or motion detection configurations using the camera’s web page without deleting the settings from the VMS, may result in those changes being discarded when returning to the VMS.

5.6 Privacy Mask

Privacy Mask is an optional licensed feature of the Latitude that allows Administrators to block viewing of areas of the video with an overlay known as a privacy mask. This feature can be used when issues of privacy, surveillance distractions, employee usage of cameras, corporate or employee confidentiality, as well as surveillance conformance restrictions arise.

Areas of an image that are normally not needed for the security task at hand can be obscured by drawing these static visual barriers.

The Privacy Mask feature includes the password protection of these masks so that authorized users with AdminCenter assigned privileges can remove and view areas of the masked video if required.

This privacy protection and password control carries over when the video clips are exported by application of a system-wide file Privacy Mask password. Users of the exported video file who want to remove the mask must first enter the password.

Image that demonstrates how gray mask occludes viewing

If you did not already obtain the Privacy Mask feature, you can contact your FLIR Inc representative for more information.

Related Links
Licensing Privacy Mask Separately
Adding a Privacy Mask to a Video Scene
Setting User Privacy Mask Permissions (View Privacy Zones)
Default Privacy Mask Password
Changing the System-Wide Privacy Mask Password
How to Unlock a Forgotten Privacy Mask Password on an Exported DVT File

5.6.1 Adding a Privacy Mask to a Video Scene

On Latitude installations that have the Privacy Mask feature license, Administrators who have support and user privileges to edit cameras can draw Privacy Masks on the video scene by using the drawing tools on the Privacy Mask tab of the selected camera.

Note: Privacy masks can be drawn on any camera type. However, the mask is fixed with respect to the overall camera picture and does not respond to changes in the cameras field of view. Therefore:
1. Privacy Masks should not be used on PTZ cameras. 
2. If the camera moves, a previously-defined Privacy Mask may no longer cover the required area. If this occurs, either physically restore the camera's positioning or redraw the Privacy Mask.

When the Design window mode is set to View, users can right click on the window and select **Deactivate privacy mask** to check the functionality and see the hidden area of the video scene again.

![Image of Privacy Mask Configuration](image)

**To configure a Privacy Mask on a camera scene.**

1. In **AdminCenter** (Logical View or Physical View), select the camera to which you want to add a Privacy Mask.
   - The General tab of the Camera is shown in the settings area.
Note on PTZ Cameras: Privacy Masks are fixed areas in the camera's overall field of view and they cannot re-size or move in response to a PTZ's motion. Therefore, Privacy Masks should NOT be defined for PTZ cameras.

2. Click the Privacy Mask tab. (Click located to the right of the displayed tabs) until the Privacy Mask tab is displayed.)

The Privacy Mask settings are shown in the settings area.

Note: If you do not have a license for the Privacy Mask feature, the toolbar and video display are disabled.

This table describes the drawing toolbar and settings of the Privacy Mask tab:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design window mode toggle</td>
<td></td>
<td>A toggle switch for selecting what mode the current editing/viewing window is working in. When in Edit, licensed Privacy Mask users can draw and save a Privacy Mask on video scene. When in View, the scene display shows how it will display in the ControlCenter.</td>
</tr>
<tr>
<td>Mark rectangle</td>
<td></td>
<td>Click to enable the mouse to draw a rectangle-shaped region on the Preview screen, made up of small individual blocks</td>
</tr>
<tr>
<td>Mark macro block</td>
<td></td>
<td>Click to set the mouse to draw individual blocks for the mask</td>
</tr>
<tr>
<td>Unmark macro block</td>
<td></td>
<td>Click to set the mouse to erase individual blocks in the mask</td>
</tr>
<tr>
<td>Mark all</td>
<td></td>
<td>Click to mark the entire Preview image as the area of interest as masked.</td>
</tr>
<tr>
<td>Unmark all</td>
<td></td>
<td>Click to erase all the marked area.</td>
</tr>
</tbody>
</table>

3. Click Edit on the toggle switch above the Design Window.
4. Use the drawing tools to draw the mask on the displayed video.
5. Click Save to save your settings.
6. Click View on the toggle switch above the design window to see the Privacy Mask (occlusive gray overlay).
   (To make changes return to step 3.)

5.6.2 Setting User Privacy Mask Permissions (Deactivate Privacy Masking)

In order for users of the <ControlCenter> to toggle the Privacy Mask on and off, they need to be granted permission for enabling and disabling the mask with the camera privilege Deactivate Privacy Masking.

If the Privacy Mask is on an exported video from another System entity, you must request the password for the file when it was generated from the owner or administrator of the DVT file.
**Note:** The permission to Deactivate Privacy Masking also grants permissions to recover passwords for users that also have permissions to AdminCenter.

### To configure user Privacy Mask access

1. In AdminCenter on the Side Bar, click **Users and Groups** and in the Navigation Tree select the user for whom you want to add or remove Privacy Mask privileges. The General tab of the Camera Settings tabs display the settings area of the workspace.
2. Click the **Privileges** tab and for the entry **Deactivate Privacy Masking** for the required Camera node, select **Allow** (permit removal of the mask when viewing) or **Deny** (do not allow removal).
3. Click \(\text{\ding{203}}\) to save your settings.

#### 5.6.2.1 Changing the System-Wide Privacy Mask Password

The Privacy Mask is a feature that allows a portion of a fixed video scene to be masked from view when the stream is shown on a monitor.

You can change the password that is used for protecting the Privacy Mask usage. This password is recorded in the Archiver stored files. The password application at export time is either historically or the current password value. Thus keeping a record of password changes is highly recommended for future use of the Disable Privacy mask feature. For more information, see **Privacy Mask Password Export Behaviors (Historical vs. Current)**.

**Note:** The Privacy Mask Password remains permanently attached to the .DVT files.

It is recommended that the system factory default value be changed to a new password. For changing the Privacy Mask Password you do not need the previous password at the time you change it to a new password.

**Note:** If you plan on exporting the data at anytime using Mass export, Background Export or CaseBuilder, the historical passwords will likely be needed. For more information, see **Privacy Mask Password Export Rules - Current or Historical**.

**Notes:**
1. Because the passwords are settings in the System and are embedded in the .DVT files, it is important to keep a record of the System entity, date and Privacy Mask password changes in the system.
2. The authentication prompt doesn't impose a limit on the attempts. Thus you may want to use strong password conventions. If a greater level of security is needed, consult an expert on how to secure access to the file itself from unauthorized use. Consider that files exported in .AVI format embed the masking in the video frames and cannot be removed.

### To Change the System-Wide Privacy Mask Password

1. In AdminCenter, on the Side Bar, click Logical View and in the Navigation Tree, select the System entity for the system you want to change the Privacy Mask password on.
2. Click the Advanced tab.
   The Advanced settings display in the settings area.
3. Expand the Privacy Mask Password heading, and select Change Password and type the new password in the New Password and Confirm password field.
4. Click \(\text{\ding{203}}\) to save your settings.
5.6.2.1.1 Privacy Mask Password Export Behaviors (Historical vs. Current)

The Privacy Mask password behavior changes depending on the manner you export. Because the Privacy Mask password can be changed yet remains historically attached to video clips when they are recorded, the behavior under the following export types are as follows:

<table>
<thead>
<tr>
<th>Where</th>
<th>Type</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>When exporting clip from the</td>
<td>Create Clip - use Source</td>
<td>The Privacy Mask password attached to the exported DVT file is the current system-wide Privacy Mask Password</td>
</tr>
<tr>
<td>Query Results or Timeline</td>
<td>video and apply current</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When performing a Background</td>
<td>Copy Clip from Archiver -</td>
<td>The export assumes the clips are being moved to an unsecure status.</td>
</tr>
<tr>
<td>Export</td>
<td>Historical static</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For each clip segment (single Archiver container), the Privacy Mask Password set at the time the clip was recorded (not exported) is enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When exporting a CaseBuilder</td>
<td>Copy Clip from Archiver -</td>
<td>The clips exported are for portable external use. The Privacy Mask Password for each clip segment (single Archiver container) set at the time the clip was recorded (not exported) is enabled</td>
</tr>
<tr>
<td>case with clips</td>
<td>Historical static</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When execution of a Mass</td>
<td>Copy Clip from Archiver -</td>
<td>The export assumes the clips are being moved to an unsecure status.</td>
</tr>
<tr>
<td>Export occurs.</td>
<td>Historical static</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For each clip segment (single Archiver container), the Privacy Mask Password set at the time the clip was recorded (not exported) is enabled</td>
</tr>
</tbody>
</table>

For more information, see Privacy Mask Password Export Rules - Current or Historical.

5.6.2.1.2 Privacy Mask Password Export Rules - Current or Historical

**CAUTION:** When exporting, the password used is not always the system-wide Privacy Mask Password at the time of export.

This section only addresses the ability of a user to remove the privacy mask while viewing an exported video clip. Users who want to simply view the files with the mask on the video clip will not be effected as there is no need to enter a password to view the clips with the privacy mask on.

When exporting a clip of video that has Privacy Mask configured on the video, the file immediately gets password protected against disabling the Privacy Mask. This password has no relation to the ControlCenter user password or permissions. If you have changed your password within the period of the exported file range, how you export those files will determine the password mechanism employed.

Export either the Current Privacy Mask Password or the Historical Privacy Mask Password at the time the file was recorded.

The Historical password for each of the files remembers the password from that time. Thus if a range of files is being exported a Historical mechanism will make each file password protec-
ted for its point in time. Depending on the number of Privacy Mask password changes that have occurred, there may be as many different passwords required to Deactivate Privacy Masking. This is because the Password is embedded in the clips being recorded during the time when the password was active.

The Privacy Mask Password is stored in the recordings made by the Archiver from the video stream of the camera. Each of these is stored in a container according to your system settings. By default the file size in this container is 80mb. When a Privacy Mask Password is changed, the new password is applied at the time the file is closed and written to the Archiver container. Thus, the password covers some video that was being buffered for recording before the file closed:

![Diagram of live stream and archiver recorded clips]

The Archiver Privacy Mask validation process for internal ControlCenter users is done via the user permissions of the ATS system. The data of the Privacy Mask Password for future offline use is kept in the clips of the containers. In the diagram above this is represented by the yellow, blue and purple data core. In the color representations of different passwords in the graphic, you can see how the password changes in the real-time with the live stream. The passwords changes in the middle of a clip not fully written to a file, are embedded in the recorded video from the start of the clip.

As of yet the three different embedded Privacy Mask passwords are not required for hiding or showing the Privacy mask for online users. It is when the recorded files are moved out of the Archiver storage that the Privacy Mask Password is implemented.

**Privacy Mask Password - "Current" password behavior**

When Exporting from a Results Query or Timeline the same video that is in the Archiver is exported with a single file Privacy Mask password whether it is the full clip or a partial. Additionally only the selected times are exported and no matter how large the clip is, it will be exported into as many files as needed based on the max size setting in the Export settings.
When Exporting from the Query Results or the Timeline pane where you can select entire clips or set video range in and out points for taking a segment. In this type of export, the embedded historical passwords are ignored and the current Privacy Mask password is used for every file created by exporting. In the example diagram that follows, two exports are represented. (one of a range and the other of the entire selected file). Only the password defined in the system advanced settings at the time of the export is applied even though the clip spans several Historical passwords. The password “ABC123” (colored purple) is used for all files exported from the Query Results or the Timeline pane export features.
Note that the file size in the above example is based on the trimmed segment or range of the video exported.

Privacy Mask Password - "Historical" password behavior

In the following example a different mechanism is used to export. In this instance the files are directly copied from the Archiver container storage as-is and the historical passwords as imbedded are simply enabled on the files being copied outside the security zone of the Archiver.

In the above instance, each file if viewed independently and the user chooses to disable the Privacy Mask, the password they will be required to enter will be the password of the clip. Thus of the five clips, the first clip requires the password 1234, the second and third clip requires the password Old#7 and the fourth and fifth requires the password ABC123.
Because the clips are all from the same source, if they are viewed in a timeline together, only the most recent password is needed for disabling the mask of both clips.

Likewise the export of clips from the CaseBuilder has the same behavior as the Mass Export, in that it copies with the password files as-is from the Archiver. Thus if the password has changed, the selection of clips will influence what password is embedded from the historical Archiver data.

Additionally, the export file size is based one-to-one with the Archiver container files. Even if the range of the clip is limited, the file size will match the container sizes of the range and not the specific in and out points of the range.

**CASEBUILDER EXPORT CASE (Range 4:02pm-4:16pm)**

<table>
<thead>
<tr>
<th>PW: 1234</th>
<th>PW: Old#7</th>
<th>PW: Old#7</th>
</tr>
</thead>
<tbody>
<tr>
<td>80MB</td>
<td>80MB</td>
<td>80MB</td>
</tr>
</tbody>
</table>

In the above example, the segments of the DVT export file that are not specified in the range, will not be viewable to the end-user. The viewing of the clip in a timeline with a disabled privacy mask can be done by selecting the clip and entering the latest historical password. In this case "Old#7".

### 5.6.3 Recovering Privacy Mask Password from an Exported Scene Recording

When you export a video clip using the various methods available, and the clip has a Privacy Mask on the scene, the exported file will require a password be entered by the viewer if the viewer wants to Disable the Privacy Password.

Because the password is attached to the file and passwords may change over time, it is important to keep track of the passwords for files generated. This being said, it is possible that the passwords may become lost or forgotten. It is important to note that the password behavior depending on the type of export used, may use either historical or the current Privacy Mask Password at the time the export was done.

If users are not clear on these behaviors, it is possible that they may be trying to use the wrong password. It is recommended that users of exported files are aware of these behaviors which are discussed in length in Privacy Mask Password Export Behaviors (Historical vs. Current) and Privacy Mask Password Export Rules - Current or Historical.

Users who have the password to disable privacy masking on the latest exported clip, can use the Timeline pane to view a number of clips together and use only the latest password to view them all and even export them to new exported files that use only the current Privacy Mask password. For more information, see How to Unlock a Forgotten Privacy Mask Password on an Exported DVT File. However, this method does not recover the password.

The AdminCenter password recovery feature allows the AdminCenter user to select an exported file and determine what if any Privacy Mask Password is used on the file. It does not allow the password in the file to be changed.

The feature only works on files that are from scenes from units that are either attached or detached from the Archivers in the System system. If a scene is deleted, the password cannot be recovered using this feature.
Files exported to any format other than DVT, will have the privacy mask embedded in the images of the video and cannot be removed.

The Password recovery feature for the Privacy Mask Password, returns four possible responses:

1. Privacy mask was not found.
   Indicates that the selected file contains a clip range that has no privacy mask defined on it's scene.
2. Scene {camera info} was not found in the system.
   Indicates that the clip and file were either generated on a different System system or the scene has been deleted and is no longer viable.
3. User is unprivileged for password recovery for scene {camera info}
   Indicates the scene exists on the current System system but the current logged in AdminCenter user does not have permissions or access to needed to reveal the Privacy Mask Password in the file.
4. Recovered Password is: {password}
   Displays the password of the file.

**To Recover a Privacy Mask Password from an Exported DVT file**

1. In AdminCenter, on the Side Bar, click Logical View or Physical View and in the Navigation Tree, select the System entity for the system that holds the attached or unattached scene that the file was generated from.
2. Click the **Advanced** tab.
   The Advanced settings will be shown in the settings area.
3. Expand the Privacy Mask Password heading, and click **Recover Password**. 
   An Open dialog displays.
4. In the Open Dialog, browse and select the clip file (*.dvt) and click **Open**. 
   A prompt will appear displaying the results.

### 5.7 PTZ Priorities

A PTZ camera is often shared between multiple users who may try operating it at the same time. Moreover, the Latitude system can be configured to automatically use the same PTZ camera, for example, move it to a preset, while users are attempting to control that PTZ camera.

In order to resolve conflicts between users and between users and the system, there is a notion of **PTZ priorities** that the administrator can configure to define the PTZ behavior in such situations.

The system also provides a means for the user to ensure that PTZ cameras return to their required positions if they are moved temporarily for some other purpose. Thus, if it is important to know if a PTZ camera has been moved from its current position, one can define event types **PTZ movement started** and **PTZ movement ended** for specific PTZ cameras, and associate a desired Action with the event. A typical use would be that, if an operator uses the manual control to move a PTZ camera, then, once the camera has been stationary for a predefined time, (which is defined as the **PTZ movement ended** event), then an Action can be invoked to return the camera to one of its Presets.

There are two ways to handle conflicts that arise when two users try to control a PTZ camera, or where the system and a user both try to control a camera at the same time:
1. **Without explicit locking** - A user can acquire control of a PTZ by simply starting to operate it. Assuming the PTZ was not in use, the system creates an implicit lock for that user on that PTZ camera. This ensures that only users with a higher PTZ User Priority (set here) can seize control of the PTZ while the first user is still operating it. The user with higher PTZ User Priority simply starts to operate it - the first user loses control over it, and the system creates a similar 'implicit' lock for higher-priority user. Because the system itself might also move a PTZ camera, it, too is given a priority, so that it can be set to take precedence over, or defer to user actions. See System Priority below. This is done with the settings in the system root (System) screen, General/System PTZ Priority pane. The time that the 'implicit' lock remains in force is set separately for System-vs-User and User-vs-User interactions.

2. **With an explicit Lock** – If the first user decided to ‘Lock’ the PTZ camera using the PTZ GUI Lock button, the camera is marked as Locked by that user, requiring a successful ‘override’ attempt from a user with a higher PTZ priority, in order to seize control over the PTZ camera. If the user attempting to move the camera has a higher priority, the following message is shown:

   'The PTZ Dome is currently locked by : <username>. Do you want to override the PTZ lock? Yes/No'.

   A user with a lower or equal priority is given the following message:

   'The PTZ Dome is currently locked by <username> and you are not authorized to take control!'

**Note**: Only a user with enabled PTZ Privileges can perform PTZ related operations.

**System Priority**

The PTZ priority level can be set for a system. The priority level of the system determines what PTZ related actions a system can perform.

- The system seizes control of the PTZ in order to go to PTZ presets or run PTZ patterns that are predefined in the system.
- When a PTZ is released (neither held nor locked), the system can seize control of the PTZ to go to presets or run PTZ patterns.
- When a PTZ is held by a user whose PTZ priority level is higher than that of the system, the system cannot seize control of the PTZ.
- When a PTZ is held by a user whose PTZ priority level is lower than that of the system, the system can seize control of the PTZ.
- When the PTZ is locked by a user, the system cannot seize control of the PTZ.

In addition, it is possible to set the interval after which a system or user can seize control of a PTZ session that was idle or held by another user.

When a PTZ is held by a user, the system has to wait until the set interval, starting when the user is idle, passes to seize control of the PTZ. For example, if the idle interval is set to 30 seconds, only 30 seconds after the last action was performed by the user holding the PTZ, can the system seize control of the PTZ.

When a PTZ is held by a user, other users have to wait until the set interval, starting when the user is idle, passes to seize control of the PTZ.
To set the System PTZ Priority level

The system priority is set in the **System** screen, **General/System PTZ Priority pane**.

- Select a priority level using the slider by entering the desired value in the field (1 is the highest priority and 100 is the lowest). The default priority is 90.
- Select the user idle interval after which the system can seize control of a PTZ held by a user. The default is 30 seconds.
- Select the user idle interval after which another user can seize control of a PTZ held by a user. The default is 5 seconds.

**User Priority**

The PTZ priority level can be set on an individual basis or based on the user group to which the user belongs.

If a user belongs to more than one user group, the priority level will be the lowest priority (highest numeric value) of all the User Groups to which the user belongs.

**Example:**

If the PTZ priority of group A is set to 1 and the PTZ priority level of user group B is 5, then the effective PTZ priority of the user is 5.

If the private PTZ priority of the user differs from that of the user group(s) s/he belongs to, the priority level will be the lowest priority (highest numeric value).

**Example:**

If the private user PTZ priority is set to 1 and the PTZ priority level of the user group the user belongs to is 3, then the effective PTZ priority of the user is 3.

To set the User PTZ Priority level

The PTZ priority of the user is set in the **User/General** screen.

- Select the **Inherit from parent (user group)** check box to set the level to the highest priority (lowest numeric value) between all the User Groups to which the user belongs

  or
• Select a priority level using the slider by entering the desired value in the field (1 is the highest priority and 100 is the lowest).

User Group Priority
The PTZ priority level can be set for a user group. To affect the users belonging to this user group, the Inherit from parent (user group) check box in the User’s General tab must be selected for each user.

To set the User Group PTZ Priority level
The user group priority is set in the User Group/General screen.
• Select a priority level using the slider by entering the desired value in the field (1 is the highest priority and 100 is the lowest).

5.8 Tru Witness
The Technical Publications TruWitness feature allows selected Android/iOS-based smartphones to be used as mobile cameras. Once the user logs in with a user name and password, smartphones can send content which will be handled in the same way as that coming from fixed cameras.
Recorded clips are tagged with user name, device manufacturer and model, and device ID. The User can optionally add up to 256 characters of text to the tag.
See TruWitness - Gateway Setup, TruWitness Mobile Camera - Android/iOS Application
5.8.1 TruWitness Mobile Camera - Android Application

In this section:
Download TruWitness application, Running the TruWitness App, TruWitness Application System Settings

Download TruWitness application
On the smart-phone, go to Google Play or the App Store, and search for TruWitness.
Select the TruWitness App, and Install.
Accept the License conditions, and Download.
When the download is completed, press Open.
The Gateway Settings screen will be shown.

![Gateway Settings Screen](image)

Ask the System Administrator for the server address and the port number to be used.
Enter the Server Address of the Latitude Server.
The Port will be set to 8082 by default. If the system uses a different port, enter the Port number.
After clicking the ‘Save’ button, the application will perform first-time video configuration.
While doing so, the application will display video from the camera for several seconds.

Running the TruWitness App
Choose the TruWitness app on the smart-phone.

Login
The User Login window will open.
Enter the **Username** and **Password**.
**Note:** The Username and Password must have previously been registered on the Latitude system.
Press **Login**

**The Home Screen**
The **Home screen** will be shown once the user is logged in

- The Device sends its GPS position to the system.
  **Note:** The GPS position is continually updated while the device is connected to the system.
  If you do not want the GPS position to be sent, you must change this in the application **Settings**

From the **Home Screen**, you can do the following actions:
**Video**, **Video+Alarm**, and **Quick Call**
You can also access the device's **Settings** by pressing the device's Menu button.

**Video**
Pressing **Video** will activate the camera and the message **Touch Screen to Send Video** will be shown.
When the user touches the screen, the message will disappear, and transmission will start. Transmission can be paused by pressing the Pause icon.

**Note:** While sending video, to enable the on-screen icons, touch the screen once. While sending video is in progress, you can send an Alarm by pressing the Alarm icon, or initiate a call by pressing the Call icon. If you start a call, recording will be suspended, but the device will remain logged in. The user can select Back to continue the transmission or Exit to stop transmitting.

**Exit**

Transmission is ended by pressing the device’s Back button. If no video was recorded then a pop-up message that reads: “Are you sure you want to exit?” is displayed, with Back or Exit options. If video was recorded the following pop-up message is displayed:

Upon exiting the transmission session, a bookmark will be created for the recorded clip with the following description: “TruWitness clip initiated by [user] from [device manufacturer] [device model] - [device ID]”

The user can tag the recorded clip prior to exiting the session. The typed text will be added to system description, as follows: “TruWitness clip initiated by [user] from [device manufacturer] [device model] - [device ID]: [user tagging]”. The user can add up to 256 characters of text.

**Video+Alarm**

The Video+Alarm function sends an alarm to the System and initiates recording.
The alarm set to the system consists of the [User Name + Device Phone Number (if available)] as set in the Application Settings.

An Alarm Type corresponding to this phone will automatically be created by the Latitude application.

Sending video will then continue as for normal Video.

**Quick Call**

You can set a predefined number set in the ‘Quick Call Phone Number’ field of the Settings.

Pressing **Quick Call** will open the device's Call App, and call the predefined number.

![Quick Call Image](image)

**Accessing other Applications**

You can access other applications while using TruWitness by pulling down the **Notification Bar**.
Note: While using the phone, or while using other device Apps, no video is sent, but TruWitness remains logged-in.

**TruWitness Application System Settings**

You can access the General Settings by pressing the device's **Menu button**

At the Login screen, press **Settings** Icon

A tools icon will appear below the Settings button.

Press **Settings** below the Tools icon

Choose **Login Settings**, **Advanced Settings**, or **About**.
Login Settings

Server Address – The server address currently stored for the system is shown. A new Server Address can be entered.

Server Port – The port currently stored for the system is shown. A new port can be entered.

Clear Login Details – Clears all login details, so that anyone subsequently using the smartphone will need to enter new credentials.

Advanced Settings

Note: The screen only shows 3 of the settings at once. Scroll up and down to see the full set.

Statistics – Selecting Statistics will cause the following details to be shown on the screen while the camera is active:

- Frame rate - Fps
- Transmission rate - Kbit/sec
- Compression method - H264 / M-JPEG
- Locations – Latitude, Longitude co-ordinates, Altitude
M-JPEG Max Resolution – Select the required resolution
  Low, Medium, High (if available on this camera model)
M-JPEG Image Quality - 1-100 slider
Email Log report – When selected, an email is sent for each session, with details of the session. In order to use this feature, the user must select the service to be used (Twitter, Gmail, etc)
Reset All Settings - Reset all settings to default
About – App. Version info

5.8.2  TruWitness - Gateway Setup
To set up the Gateway for the TruWitness feature, a Gateway Server is required, with the Mobile tab configured to support the TruWitness feature. If required, add a Gateway Server.

Adding a Gateway Server
From the Admin Center, Physical View, right-click on the system icon to open the context menu, and click on Add Gateway server.

This will open a new server with a default name New Gateway Server n
If desired, change the name, and enter a description.

Enter the address of the Server in the **Network Address** field, and click **Save**.

(You will not be able to continue with the process until the address has been saved and the system has connected to the server – see the Connected icon at the top of the Information tab)
Click on the **Enable video from mobile device** check-box. This will enable all fields in the screen.

The screen consists of 4 panels - **Network Settings, Video Settings, Recording Settings** and **Archivers**.

**Network Settings Panel**
- **Mobile routing port** – by default, this will be set to 8082. If that port is not available, ask your system administrator to allocate another port.

**Video Settings Panel**
- **Compression** – Select desired compression mode
- **Maximum resolution** – Select desired resolution
- **Note**: If there is a conflict between the resolution specified for the Gateway and that for the camera, the lower resolution will be used.
- **Maximum Bit rate (kbps)** – Use the slider to select the desired maximum bit rate.

**Recording Settings Panel**
- In **Recording schedule**, select the schedule that the Gateway will apply to all content coming from mobile devices:
  - **None** – no content from mobile devices will be automatically recorded. (At the Control Center, one can still trigger recording during a session as for any live content).
  - **Always recording schedule** – all content from mobile devices will be recorded
  - **Other recording schedules**: Other schedules may be created in System Settings / Schedules.
- **Note**: The recording schedule selected in this screen will apply automatically to all content received from mobile devices. A Control Center user can trigger or stop recording of a particular session, but upon reconnecting, that mobile device will revert to the setting made in this screen.

**Archivers Panel**
- Select one (or more) Archiver/s to collect content from the mobile devices. If more than one Archiver is selected, the system will automatically choose which Archiver to use for a particular session.

When all selections have been made, **Save** the configuration of the Gateway.

### 5.9 User Management

**Privileges and Access Right Configuration**
- **Defining Access Rights**
- **Access Right Default Settings**

**Defining Privileges**
- **Privileges Default Settings, Use Cases and Scenarios**

**Terminate a user session remotely**

Global User Groups and Global Users
5.9.1 Privileges and Access Right Configuration

Privileges

The Privileges Configuration model allows administrators to control access by users to virtually every functionality for every entity in the system. It uses positive and negative inheritance but also allows for creating exceptions without having to change the settings of parent entities. To facilitate ease-of-use, it is possible to set Privileges to all members of a user group and individual users.

Latitude enables the administrator to apply a set of Privileges on a group of users via the Privileges tab of the user group entity.

There are 3 privilege definitions -- Allow, Deny and Undefined. By default, all privilege settings are set to Undefined. Privileges set to undefined are the same as privileges set to deny.

Privileges are applied to both user groups and users. Privileges are granted to the different functions available in the system.

On how to set privileges for the different user constellations, see Defining Privileges:
- To define privileges set of a user group
- To define privileges set of a single user

Privileges are applied to the different functions available in the system; i.e., it is possible to "allow" the user the privilege to create camera bookmarks or "deny" the user the privilege to acknowledge alarms.

In the Privilege tab, privileges are applied to various functions within the Admin Center and Control Center. If one of the functions is set to Undefined, parent group privileges are applied (the name of the parent group is listed in the Inherited From column).
Note: In many cases, Privileges may be broken down into sub-levels. For example, a user may have overall access to Camera Privileges, or the category may be expanded and the user given only some specific privileges from the category.

For User Groups, the Privilege tab contains 3 columns that appear next to each entity: Allow, Deny and Undefined. Click within the Radio Buttons to mark the relevant column (Allow, Deny or Undefined). The radio button is colored green after selection. If unselected, they appear white. Selected (green radio button), Unselected (white).
Privilege Configuration

Since privileges are automatically inherited from parent to child entities, you should always begin setting privileges for your system with the top level entities and work your way down.

1. In the User Group or User entity, click the Privileges tab.
2. Select the required radio buttons for each entity (Allow, Deny, Undefined).
3. Click on a relevant Main Topic Entity to expand the list and display its child entities.
4. Expand each of the child entities and determine which privilege, if any, to give to the user group or user.
5. Repeat steps 2-4 for all other entities, proceeding from top to bottom.

Access Rights

The Access Rights configuration model enables the administrator to set view capabilities for the system's entities. The administrator grants Access Rights to both User Groups and Users.

For User Groups there are 3 Access Right definitions: Allow, Deny and Undefined.

An additional, 4th definition called Inherited From applies only to Users.

By default, all Access Right settings are set to Undefined. Access Rights set to undefined are the same as Access Rights that are set to deny.

Each entity can be set to Allow, Deny or Undefined. If an entity is undefined for a specific user, it automatically inherits its settings from the parent group.
In the Access Rights tab **view** privileges are granted for specific entities; i.e. instead of defining **view** privileges for the entire set of cameras or servers, the user may choose specific cameras to which **view** privileges will be applied.

Each entity can be set to Allow, Deny or Undefined. If an entity is undefined for a specific user, it automatically inherits its settings from the parent group.

When a User Group or User add an entity to the existing pool of entities, there are two setting options that can be applied to the newly added entity:

The first option is to *Automatically set (the entity) to undefined*, in which case all the access rights are 'explicit'. An entity that is dragged or added under a site which the user has access rights to will not be granted access rights. (unless the entity was specifically set to deny)

The second, is to *Automatically set (the entity) to allow*, in which case the access rights are 'inherited by types'. An entity that is dragged or added under a site that the user has access rights to, will automatically be granted with access rights.

**Access Right Configuration**

1. In the User Group or User entity, click the Access Rights tab.
2. Select the required radio buttons for each entity: *Automatically set to undefined* OR *Automatically set to allow*.

3. Select the required entity from the list to view its access rights status.

### 5.9.1.1 Defining Access Rights

**To define Access Rights for a user group**

1. Access the User Group entity, by clicking the Users and Groups button in the Sidebar and selecting the required user group.
2. Click the Access Rights tab.
3. Select the *Automatically set to undefined* radio button.
4. Set the required access rights to apply to all users of the user group.
5. Save your settings.

**Notes:**

1. Access Rights defined for User Groups cannot be Inherited From any other Group.
2. For entities that are members of Sites or Enterprises, even if ‘Automatically Set to Allow’ is selected, settings will still not be set to ‘Allow’. This is to ensure that Access Rights for entities that have been grouped into Sites and/or Enterprises are explicitly granted, and not inherited.
To define access rights for a single user

1. Access the User entity, by clicking the Users and Groups button in the Sidebar and selecting the required user
2. Click the Access Rights tab
3. Select the Automatically set to Allow radio button.

All access rights are now 'inherited by types'; an entity that is dragged (or added) under a site that the user has access rights to is automatically granted with access rights.

Disabled Radio Button

For a User belonging to a group that has Allow defined for all its entities you will not have the option of selecting the Automatically set to undefined radio button. It will appear as disabled.
5.9.1.2 Access Right Default Settings

By default, all Access Rights are set to **undefined** for any new user. Access Rights set to **undefined** are the same as Access Rights set to **deny**.

**Editing the Access Right Setting of a Specific User - Blocking view to a Site**

The administrator setting the privileges wants to change the Access Right of a specific user in this user group. For example, the administrator wants to deny the user's privileges to view a specific site/entity.

**Configuration Procedure**

The following procedure should be performed:

1. From the **User** screen, select the **Access Rights** tab.
2. Click the filter drop down icon to choose **Select none**. Only **Systems**, **Enterprises**, and **Sites** are displayed.
3. Click the radio button in the Deny column (next to the selected site entity)

The site is set to **Deny**.
5.9.1.2.1 Defining Privileges

Following are the various privilege settings procedures.

**To define the privileges set for a user group**

1. Access the User Group entity, by clicking the **Users and Groups** button in the Sidebar and selecting the required user group.
2. Click the **Privileges** tab.
3. Select **Allow**, **Deny** or **Undefined** for each entity.

**Note:** Privileges defined for User Groups cannot be Inherited From any other Group.
4. Set the required privileges settings to apply to all users of the user group.
5. Save your settings.

To define privileges set of a single user

1. Access the User entity, by clicking the Users and Groups button in the Sidebar and selecting the required user.
2. Click the Privileges tab.
3. Select Allow, Deny, Undefined. If no selection is made, the function by default is Inherited From the parent group.
5.9.1.3 Privileges Default Settings, Use Cases and Scenarios

Defaults - Users

Privileges

By default, all privileges are set to **undefined** for any new user, except for Control Center Login.

Privileges set to **undefined** are the same as privileges set to **deny**.

Defaults - User Groups

The default Privileges settings of a new user group are all set to undefined when the user group is created manually. When using the **User Group Wizard** to create the user group, there are predefined group privileges for the following typical user group types:

<table>
<thead>
<tr>
<th>Privilege Set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Admin</td>
<td>Unlimited authorization in the AdminCenter and &lt;ControlCenter&gt;</td>
</tr>
</tbody>
</table>
### Use Cases and Scenarios

The following use cases are detailed:

- **Creating a User Group with Predefined Roles**
- **Editing the Privileges Setting of a User Group** (Camera Privileges)
- **Editing the Privileges Setting of a Specific User** (Camera Privileges)
- **Blocking Access of a Specific User to the AdminCenter**

#### Use Case 1 - Creating a User Group with Predefined Roles

The administrator setting the Privileges wants to create a user group with standard user privileges.

**Configuration Procedure**

The following procedure should be performed:

1. Create a new user group, using the User Group Wizard by selecting *Wizards — User Group wizard — [the desired system]*.
2. Follow the steps of the wizard, entering the group details and selecting the required users.
3. If you want to add a new user, click **Create New User** in the **Select Users** dialog box.
4. Enter the user’s details and click **OK**.
5. Select the **Privileges Sets** of the group - **Standard User**.
6. Click **Next** until you reach the **Finish** dialog box of the wizard.

The user group now has a set of predefined privileges that can be viewed in the **Privileges** tab of the user group.

#### Use Case 2 - Editing the Privileges Setting of a User Group - Camera Privileges

Let’s assume that the administrator setting the privileges wants to change the privileges of a user group. For example, the administrator wishes to grant a user group:

- all the privileges connected to all cameras or a specific camera except for configuring the PTZ
Configuration Procedure (All Cameras)

The following procedure should be performed:

1. Access the **Privileges** tab of the User Group.
2. Set the Cameras entity to **Allow**. Automatically, all the settings under the Camera entity are set to allow.
3. Under PTZ entity, locate the **Configure PTZ** setting and set them to **Deny**.
   
   Note: By selecting the Admin Center definition itself, all the related Privileges that fall under Admin Center will be set to Deny at the same time.

4. Save your settings.

Use Case 3 - Editing the Privileges Setting of a Specific User - Camera Privileges

Let’s assume that the administrator setting the privileges wants to change the privileges of a specific user in this user group. For example, the administrator wishes to deny the user’s privileges to lock the PTZ of all cameras.

**Configuration Procedure**

The following procedure should be performed:

Access the **Privileges** tab of the user.

From the **Entity** list, locate **Cameras** and set the radio button to **Allow**.

Under **Cameras**, locate the **PTZ** entity. Set **Lock PTZ** to **Deny**.

Save your settings.

Use Case 4 - Editing the Privileges Setting of a Specific User - Blocking Access to the AdminCenter

Let’s assume that the administrator setting the privileges wants to change the privileges of a specific user in this user group. For example, the administrator wants to deny the user’s privileges to access the Admin Center.

**Configuration Procedure**

The following procedure should be performed:
1. Access the Privileges tab of the User.
2. From the Entity list, locate Admin Center.
3. Set the Radio Button to Deny.
4. Save your settings.

5.9.2 Terminate a user session remotely

There is sometimes a requirement to terminate a user session remotely. For example, operators may leave at the end of their shift and forget to log off. In order to limit the number of user sessions, it is preferable to log the operator off before new operators commence their shifts.

Authorizing a User to use this function

In the User/Privileges screen, the Logout User privilege must be enabled to allow a user to carry out this function.

Using the Logout User function

Open the Dashboard and in the Users panel, click on Logged on Users. The currently logged-on users are listed. Right-click on the user to be logged off.
Provided the Admin Center user using this function has the appropriate privilege, the **Logout User** button is displayed.
Clicking on the button will start the log out process.
The Admin Center operator must confirm the action.

The user receives a message explaining that the session has been terminated.

### 5.9.3 User Group Wizard

The User Group Wizard enables you to easily configure all required and optional settings for a new user group in the system.
The wizard can either be accessed by right-clicking the **Wizards** button on the Sidebar and selecting **User Group Wizard** and then selecting the desired system or by right-clicking an existing user group and selecting **User Group Wizard**.

**To configure a User Group using the User Group Wizard**

1. On the Sidebar of the AdminCenter, select **Wizards — User Group wizard — <the desired system>**.
2. Alternatively, in the Physical View, expand the tree and right-click the desired user group, and then select User Group wizard.

3. On the Welcome screen, click Next.
   The Group Details dialog box appears.

4. Define the name and description of the user group.

5. Select the location (enterprise) to which the user group belongs.

6. Click Next.
   The Select Users dialog box appears.

7. Select the users you wish to add to the user group from the Available Users list and move them to the Selected Users list.

8. Alternatively, click Create New User to create a new user to be added to the user group.

9. Enter the user's details in the details dialog box, and then click OK.

10. The new user is added to the Available Users.

11. Click Next.
   The Privileges Sets dialog box appears.
12. Select the desired privileges settings from a list of predefined privileges sets.

<table>
<thead>
<tr>
<th>Privileges Set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Admin</td>
<td>Unlimited authorization in the AdminCenter and ControlCenter</td>
</tr>
<tr>
<td>Standard Admin</td>
<td>Full authorization in the AdminCenter and ControlCenter except creating and editing users and removing system components</td>
</tr>
<tr>
<td>Advanced User</td>
<td>Full authorization in the ControlCenter.</td>
</tr>
<tr>
<td>Standard User</td>
<td>Full authorization in the ControlCenter except setting presets, accessing the PTZ menu and making changes to layouts</td>
</tr>
<tr>
<td>Guest</td>
<td>View live video feed only</td>
</tr>
<tr>
<td>Undefined</td>
<td></td>
</tr>
</tbody>
</table>

13. Click **Next**.
The Access Rights dialog box appears. Configure the entities to be viewed by the user.

Two options set the default behavior when new User Groups are created:
- **Automatically set to undefined** - No Access Rights settings will be created for new User Groups. The user must explicitly **Allow** or **Deny** rights if required.
- **Automatically set to Allow** - All Access Rights for the group will be set to Allow when the group is created. The user must explicitly **Deny** rights if required.

Click **Next**

The Advanced Privileges dialog box appears. Set **Allow**, **Deny** or **Undefined** for Control and Admin Center entities.
14. Modify the privileges of the user group as desired. You can modify the Entities and Functions privileges by selecting the desired mode from the drop-down menu. In the **Entities** mode, you can access the **Advanced** mode by selecting the **Advanced Mode** check box. For more information regarding privileges, see **Privileges**.

15. Click **Next**.

The **Finish** dialog box appears.

16. Click **Finish**.

### 5.10 Tools

In addition to its two primary client applications, ControlCenter and AdminCenter, Latitude comes with a number of client tools used to simplify or enhance system management and configuration.

- **Safrun**
- **Communication Ports**
- **Unified Device Configurator** - a PC-based administration tool which allows end users to configure and work with Value Line, Pro Line, Pro Line A and HD/Quasar edge devices.
- **Scene Tracker**
- **Reporting Tool**
- **Mentor**
5.10.1  **AdminCenter Wizards**
The AdminCenter Side Bar option Wizards contains the following wizard options:

- Quick Configuration wizard
- Camera Wizard
- Copy Configuration wizard
- User Group Wizard

5.10.1.1  **Quick Configuration Wizard**

The Quick Configuration Wizard guides you through the process necessary to set up a basic Latitude system that enables video monitoring and recording.

The Configuration Wizard includes the configuration of the following system components:

- Global Settings
- Archivers
- Discovery and Unit Attachment
- Quality

The Quick Configuration Wizard can be accessed from the Sidebar.

See **Performing the Basic Configuration**

5.10.1.1.1  **Performing the Basic Configuration**

After initializing the AdminCenter for the first time, the Welcome screen of the Configuration Wizard appears.

If you want to change the configuration, add a new Archiver, discover edge devices etc., start the Configuration wizard by selecting **Wizards— Quick Configuration** from the Sidebar.

**To configure the AdminCenter with the Configuration Wizard**

1. On the Sidebar of the AdminCenter, select **Wizards— Quick Configuration wizard**.
2. Click **Next**. The **Welcome** dialog box appears.
3. Click **Next**.

**Global Settings**
The **Global Settings** dialog box appears.

4. The **Default NTP Server** field is not currently supported and will be updated in a future version.

5. From the **System Default Time Zone** list, set the default time zone.

6. From the **Default Video Source Type**, select NTSC or PAL.
   - In **Default Archiver Live Connection Type** select Best Available.
   - In **Default Archiver Recording Connection Type** select Best Available.
   - By default, the **Video Scene Creation** check-box is marked.
   - It is optional to mark the **Audio Scene Creation** and **I/O Scene Creation** check-boxes.

7. Click **Next**.

**Archivers**

The **Archivers** dialog box appears.

1. Click **Add** to create a new Archiver.
   - The **General** dialog box of the **Create Archiver** wizard appears.
2. In the Name field, enter the name of the Archiver.

3. In the Network address field, specify the host name or IP address of the computer on which the Archiver resides.

4. Click Next.
   The Network dialog box of the Create Archiver wizard appears.

5. Click Add to specify a network for the Archiver.
   The Add Network dialog box appears.
6. In the **Base IP** address field, enter the IP address of the network.
7. In the **Subnet Mask** field, enter the subnet mask of the network.
8. In the **Default gateway** field, enter the default gateway of the network. This field is optional.
9. Click **OK**.
10. Select the required network/s from the list, and click **Next**.

The **Storage** dialog box appears.
1. To configure storage for the Archiver, click **Add** and fill in the editable fields in the table.

2. In the **Storage** list, a storage location appears. You can add multiple storage locations.
   
   Set the **Storage** parameters — path, size and capacity — by clicking the respective columns of the table.
   
   Please make sure that the container size is set to 80 MB.

3. To add storage based on system information, wait until your system finishes gathering the information.
   
   The system information appears, including which drive is recommended for the storage location.

4. Select the desired drive (preferably the recommended drive) from the Drive drop-down list and determine its storage size and capacity.
   
   A warning may appear if the selected Storage is not recommended by the system.
Click **No** to change your settings as recommended or click **Yes** to continue.

5. Click **Finish**.

6. Click **Next** to continue to the Discovery configuration

**Discovery and Unit Attachment**

The *Discovery* dialog box appears

Click *Discovery Settings* to enable or disable discovery methods according to the edge devices connected to your system.

For the list of supported edge devices for which discovery methods can be enabled, see [Supported Edge Devices](#).

The *Discovery Settings* dialog box appears.
Enable or disable the discovery and set the parameters of the relevant edge devices
1. To begin the discovery process, click **Start**.
   
   Once your units have appeared in the **Discovered Units** list, click **Stop**.
   
   Alternatively, in the **Discovery** dialog box, click **Discover Units Manually** to attach a specific unit using its IP address.
   
   The **Discover Units Manually** dialog box appears.
   
   Select the unit type and enter the IP address and relevant parameters of the selected unit type, and then click **OK** to attach the selected unit.

2. Click **Next**.
   
   The **Attach Units to Archiver** dialog box appears. Units need to be attached to an Archiver in order to store their recordings.
   
   1. Select the units to be attached to the current Archiver.
   2. Click **Next**. The **Quality** dialog box appears.

**Quality and Recording**

The **Quality** dialog box appears.

1. Select a default Quality Schedule for all cameras, and then click **Next**.
   
   A recording schedule covering all hours of the day has automatically been defined for the cameras.
The Quality Schedule determines the video encoding characteristics of your cameras. This will have an impact on the quality of the video as viewed by the user and the quantity used up in storage.

2. Click Finish.

5.10.1.2 Camera Wizard
The Camera Wizard guides you through the process necessary to
- Discover new units connected to the system
- Configure recently discovered cameras
- (Re)configure an already discovered camera

The Camera Wizard can be accessed from either the Sidebar (to discover and then configure the discovered units) in the View Selection Pane by right-clicking a specific camera scene and selecting Camera Wizard. When accessing the Camera Wizard from a specific unit, the Discovery and Unit Attachment steps are skipped.

The Camera Wizard includes the following components:
- Discovery and Unit Attachment
- Camera Selection and Configuration
- General & Picture Settings
- Live and Recorded Quality
- Recording Settings

For the complete list of supported edge devices, see Supported Edge Devices.

5.10.1.2.1 Performing Camera Configuration Using the Camera Wizard
After connecting new units to the system, you can use the Camera wizard to facilitate the procedure.

Start the Camera wizard by selecting Wizards—Camera Wizard—System or <your system> from the Sidebar or by selecting the desired unit (camera) in the Physical View.

The Camera wizard contains the following components:
- Discovery and Unit Attachment
- Camera Selection and Configuration

Choose Camera, General Settings, Linked Entities, Picture Schedule, Live Schedule, Recording Schedule, Recorded Quality, Camera Actions

You can skip to the relevant part by clicking Next.

To discover and configure a unit with the Camera wizard

1. On the Sidebar of the AdminCenter, right-click Wizards and select Camera Wizard—System or <your system>.
2. On the Welcome screen, click Next.

Discovery and Unit Attachment

1. The Discovery dialog box appears. If you do not need to discover or attach any units, continue with Camera Selection and Configuration
2. Click Discovery Settings tab to enable or disable discovery methods according to the edge devices connected to your system.
For the list of supported edge devices for which discovery methods can be enabled, see Supported Edge Devices.

The Discovery Settings dialog box appears.

Enable or disable discovery and set the parameters of the relevant edge devices:

Note: It is advisable to define the shortest possible IP range and port range to speed up the discovery process of Axis edge devices.

3. After defining the discovery parameters, click OK to return to the Discovery dialog box.
4. To begin the discovery process, click Start.
5. Once your units have appeared in the Discovered Units list, click Stop.
6. Alternatively, in the Discovery dialog box, click Discover Units Manually to discover a specific unit using its IP address.

The Discover Units Manually dialog box appears.
1. Select the unit type and enter the IP address and relevant parameters of the selected unit type, and then click OK to discover the selected unit.
2. Click Next.
3. The Attach Units to Archiver dialog box appears. Units need to be attached to an Archiver in order to store their recordings.
4. Select the units to be attached to the current Archiver.
5. Click Next.
Camera Selection and Configuration

The Choose Camera dialog box appears. This is where you select the camera that will be configured with the wizard.

Select the required camera and click Next.

The General Settings dialog box appears. In the General Settings, the camera name and description are defined.

1. Accept the default settings or modify the settings as needed:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the selected camera.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the camera. This field is optional.</td>
</tr>
</tbody>
</table>

2. Accept the default settings or modify the settings as needed:

Picture Settings

The Picture Settings dialog box appears.

The Picture Setting parameters affect the image quality, such as brightness, contrast and so on.

1. Click the (+) button to select the coverage.
2. The Select Coverage dialog box appears.
3. Select a predefined Coverage range from the top pane (Always or Daytime)
4. Alternatively, define a custom coverage. In the Day and Time pane, a graphical representation, change the coverage by highlighting the periods to be included in the coverage.
5. To configure a complex coverage, click and hold the Control key while marking multiple sections of the table.
6. To configure a complex coverage, click and hold the Control key while marking multiple sections of the table.
7. Click OK.
8. Select a predefined Profile from the Profile drop-down list (Normal, Dark or Bright).
9. Alternatively, select a Custom profile and define or adjust the desired Picture settings.
10. This option is disabled if a predefined Profile setting was selected.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera type</td>
<td>The camera type</td>
</tr>
<tr>
<td>Saturation</td>
<td>The intensity of the colors in the image — Possible values range from 0-100</td>
</tr>
<tr>
<td>Hue</td>
<td>The relative amounts of red, green, and blue in a color — Possible values range from -180 to 180</td>
</tr>
<tr>
<td>Contrast</td>
<td>The range of colors in the image — Possible values range from 0-100</td>
</tr>
<tr>
<td>Brightness</td>
<td>The total amount of light in a color — Possible values range from 0-100</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sharpness</td>
<td>The image sharpness — Possible values range from 0-100</td>
</tr>
<tr>
<td>White balance</td>
<td>The level of white balance of the image</td>
</tr>
<tr>
<td>Noise reduction</td>
<td>The level of noise reduction — Possible values are low, medium, high, plug-in-specific and automatic</td>
</tr>
<tr>
<td>Shutter speed</td>
<td>The level of the shutter speed</td>
</tr>
<tr>
<td>Color enabled</td>
<td>By default, this option is selected</td>
</tr>
<tr>
<td>Exposure area</td>
<td>The area where the camera adjusts the back light compensation</td>
</tr>
<tr>
<td>Input filter</td>
<td>The level of the input filter</td>
</tr>
<tr>
<td>Day Night Mode</td>
<td>Supported for Pro Line A edge devices. These pre-defined settings enable the quick definition of the Picture settings for edge devices used on specific times of the day. The possible settings are Day, Night or Advanced.</td>
</tr>
<tr>
<td>IR filter mode</td>
<td>IR filter mode</td>
</tr>
<tr>
<td>IR filter on threshold</td>
<td>The threshold triggering the IR filter</td>
</tr>
<tr>
<td>Color enabled</td>
<td>In the <em>Advanced</em> Day Night mode -- the Hue parameter is disabled and the Saturation parameter can be enabled by selecting the Color enabled check box. If it is not selected, the scene will appear in black and white.</td>
</tr>
<tr>
<td>Back light compensation</td>
<td>By default, this option is not selected</td>
</tr>
</tbody>
</table>

Save the customized profile by clicking **Save As**.
View the defined Picture Settings by clicking **Picture Settings Summary** in the Preview pane.
Enable on screen display by selecting the **OSD** check box in the Preview pane.
Disable Privacy Mask that is displayed by Right-clicking and selecting **Deactivate privacy mask**. (dependent on user permissions)
9. Click **Next**.
Live Quality Settings

The *Live Quality* dialog box appears.

The Live Quality parameters affect the quality of the video stream used for live display, such as frames per second (FPS) and resolution.

A default Live Quality schedule suitable for the camera type has been added automatically.

1. Click the button to select the coverage. See Coverage settings.
2. Select a predefined Profile that matches your camera type from the *Profile* drop-down list.
3. Alternatively, select a **Custom** profile to define the live quality parameters to best suit your camera.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit rate (kbps)</td>
<td>The maximum number of bits per second generated by the device. Valid bit rates range from 32 to 6000 kbps.</td>
</tr>
<tr>
<td>Frame rate (fps)</td>
<td>The maximum number of frames per second (fps) that will be encoded and transferred by the transmitter. This parameter can be set from 1 to 30 fps.</td>
</tr>
<tr>
<td>Key frame interval in seconds</td>
<td>The key frame interval per seconds. This parameter can be set from 1 to 40 kfps.</td>
</tr>
<tr>
<td>Quality</td>
<td>The video quality. This parameter can be set from 1 to 10.</td>
</tr>
<tr>
<td>Camera type</td>
<td>The camera type</td>
</tr>
<tr>
<td>Compression</td>
<td>The compression used</td>
</tr>
<tr>
<td>Resolution</td>
<td>The measure of how clear and crisp the video image appears. Each resolution corresponds to a specific number of pixels (columns * lines) for each picture of the video sequence.</td>
</tr>
<tr>
<td>Rate control mode</td>
<td>The rate control mode — Possible values are Automatic or manual</td>
</tr>
</tbody>
</table>

You can save the customized profile by clicking **Save As**.

You can view the defined Live Quality Settings by clicking **Live Quality Settings Summary** in the Preview pane.

You can enable on screen display by selecting the **OSD** check box in the Preview pane.

You can disable Privacy Mask that is displayed by Right-clicking and selecting **Deactivate privacy mask**. (dependent on user permissions)

4. Click **Next**.
Recorded Quality Settings

The Recorded Quality dialog box appears.
The Recorded Quality parameters affect the quality of the video stream used for recorded video display.
If the Recorded quality same as live check box is selected, the recorded stream receives the same parameters as the live stream. Therefore there is no need to configure the parameters separately.
If you want to define separate parameters for recorded video stream, clear the Recorded quality same as live check box. This option is disabled if the camera supports single stream only.
1. Define the Recorded Quality parameters the same way as the Live Video Quality parameters. See Live Quality for the list of parameters and their configuration.
   You can save the customized profile by clicking Save As.
   You can view the defined Recorded Quality Settings by clicking Recorded Quality Settings Summary in the Preview pane.
   You can enable on screen display by selecting the OSD check box in the Preview pane.
2. Click Next.

Recording Schedule Settings

The Recording Schedule dialog box appears.
The Recording Schedule parameters determine when the system will record and how long the recordings will be stored.
1. Click the (+) button to a predefined Coverage range from the Coverage drop-down list (Always or Daytime). See Coverage settings to define advanced Coverage settings.
2. Select the Profile (Default Recording Profile) from the Profile drop-down list.
3. Set the desired Recording lifespan.
4. Click Next.

Linked Entities

The Linked Entities dialog box appears. The entities that are linked to the camera are automatically displayed/heard with the camera. For example, when a microphone is linked to a camera, it is possible to hear the audio along with the live or recorded video stream.
1. In the Linked Audio pane, select the check boxes of the desired audio entities to link them to the camera.
2. In the Linked Map pane, select a map from the drop-down list.
   You can toggle the view of the Linked Maps list by clicking Switch View or refresh it by clicking Refresh View.
3. Click Next.

Events and Actions Settings
The *Events and Actions* dialog box appears.
1. Right-click the desired event and select the desired action.
   The relevant *Action Details* pane appears.
2. Set the action parameters. For more details, see *Events and Actions*.
3. Click **Next**
   The *Summary* dialog box appears, displaying the selected settings.
   You can configure an additional camera by clicking **Configure Another Camera**
   or click **Finish**.

### 5.10.1.3 Copy Configuration

The Copy Configuration wizard enables you to copy the configuration settings of a selected entity and transfer the settings to another entity with the same parameters.

**Note:** Using Schedules or Copy Configuration to set up cameras.

When users want all cameras or some groups of cameras to have the same settings, and to have the possibility of changing settings for all cameras in one place, then **Schedules** are used. Settings for all cameras associated with a Schedule can be changed by updating the Schedule itself.

If the users wishes to set up one camera and then just use its settings as a template for others, then the Copy Configuration facility is used. This allows all selected cameras to receive the same settings, but there is no linkage that would allow all camera settings to be changed together by the user.

The wizard can be accessed from either by clicking the **Wizards** button on the Sidebar and selecting the Copy Configuration wizard or by right-clicking a specific entity (in the Physical View, Logical View, System Settings, and so on) and selecting **Copy Configuration**.

**Using the Copy Configuration Wizard**

1. On the Sidebar of the AdminCenter, select **Wizards — Copy Configuration** or right-click the desired entity in the Physical or Logical view, and select Copy Configuration
   Alternatively, select the desired entity and click **COPY** on the View Selection toolbar.
2. From the **Select Type** drop-down list, select the desired entity type.
3. From the **Select Source** drop-down list, select the specific entity whose configuration you want to copy.
4. In the **Select Categories** pane, select the check boxes of the categories you want to copy.
   (The categories offered are limited to those parameters that are available in the selected **Source** entity.)
5. In the **Select Destination(s)** pane, select the specific entity or entities to which you want to paste the configuration settings.
6. Click **Copy**.
7. Click **Close**.

5.10.2 **Communication Ports**

The following are the communication ports supported in Latitude.

**Process Listening and Log Trace Ports**

- **Process** – the name of the Latitude process (service or application)
- **DVComm** – the TCP/IP listening ports of the process
- **Miscellaneous** – additional ports or comments

<table>
<thead>
<tr>
<th>Process</th>
<th>DVComm</th>
<th>Miscellaneous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>4919</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration - Functionality

<table>
<thead>
<tr>
<th>Process</th>
<th>DVComm</th>
<th>Miscellaneous</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDB</td>
<td>4921</td>
<td></td>
</tr>
<tr>
<td>Archiver</td>
<td>5051</td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>5053</td>
<td></td>
</tr>
<tr>
<td>ART</td>
<td>5055</td>
<td></td>
</tr>
<tr>
<td>ARTController</td>
<td>5057</td>
<td></td>
</tr>
</tbody>
</table>
| Transcoder       | 5089   | Video Streaming:  
|                  |        | - HTTP port: 8080  
|                  |        | - RTSP port: 5554 |
| Gateway          | 5099   | Routing TCP port: 7777 |
| AdminCenter      | n/a    |               |
| ControlCenter    | 4931   |               |
| MapBuilder       | n/a    |               |
| SafRun           | 5019   |               |
| Mentor           | n/a    | Default VSIP port 5511 |
| Web Server       | 5061   |               |

### Multicast and Unicast Ports

<table>
<thead>
<tr>
<th>Logger Chatroom</th>
<th>Public</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>266.6.6.6</td>
<td></td>
<td>49374</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Multicast</td>
<td>61454 (&amp; 61455 RTCP)</td>
</tr>
<tr>
<td>Audio Multicast</td>
<td>61456 (&amp; 61457 RTCP)</td>
</tr>
<tr>
<td>Video &amp; Audio Unicast</td>
<td>Configurable Port Range (default 8000-9000)</td>
</tr>
<tr>
<td>VSIP Events</td>
<td>12345</td>
</tr>
</tbody>
</table>
5.10.3 **Discovery**

The Archiver Discovery Service assists the user to attach and configure system elements, by 'discovering' connected hardware. The user can then accept the hardware and use the settings that were automatically entered.

The discovery process is invoked by selecting **Discovery** in the Sidebar, or by navigating to the System/discovery page directly.

The user selects settings that are suitable for the Discovery process, and then can choose whether to run the **Automatic discovery** process - which uses Broadcast Discovery to discover all devices meeting the setting's criteria, or the **Manual Discovery** process, which discovers just a single device meeting the same criteria but at the specified IP address.

Once the selected discovery process has run, the discovered unit/s will appear in the table. Select one or more lines in the table, and choose the archiver to which they must be attached, and click **Save**.

**Method**

Discovery supports two discovery methods:
- **Proprietary**
  - (the system also supports the discovery of Generic cameras that have not been formally integrated into the system
  - See [Generic Camera Discovery](#)

- **ONVIF** (Open Network Video Interface Forum)

---

**Proprietary Method**

This section allows you to choose **Select All**, or to check one or more **Product types** to be discovered.

Each product type selected has a stored set of supplementary information, such as the **IP range** to be used, **Port number**, and **username/password**, which will be used by the Discovery process.

If only one product type is selected, the fields of the supplementary information can be edited and saved. This allows the user to set up an efficient discovery process that will normally scan the product type/s that are in use on the site, using the parameters and username/passwords that the user has set.

These settings are then used successively for each selected product type as the corresponding **software plugin** is used to discover each set of products. Obviously, the selecting fewer product types will result in the automatic discovery process running faster, as fewer alternatives need to be tried.

If the FLIR Product type is selected, all FLIR product types will be discovered. However, there is a **Product Settings** dropdown that allows the operator to isolate a particular model in case some specific change needs to be made only with regard to that model.

---

**Supplementary Information:**

Where supplementary information is required to Discover the units, the right-hand panel shows the default information for that type of unit, and allows modification if required.

- Scan IP range (opens fields for Start and End Addresses)
- Port number
- Username
- Password
Variants (i.e. MJPEG Encoders, etc)

Note: If the user saves the discovery criteria (by clicking after setting the parameters), then the next time the page is accessed it will open with the saved settings.

Proprietary
This method lists the cameras and units according to the company/product name:
See Discovery Proprietary Configuration Information

ONVIF
This method searches for devices that use the Open Network Video Interface Forum standardized communication protocols
To use this method, select the ONVIF radio button in the Cameras and Encoders pane of the Discovery General Tab.
The left-hand window (showing the Proprietary Units) will be cleared, and by default, the Port and User/Password information will be displayed.

In order to select by IP range, click the Scan IP Range check-box, and the corresponding fields will be added.

Networks
1. Click the **Automatic create unit capability scenes** Panel to toggle open the scene creation settings.

**Automatic create unit capability scenes**

![Automatic create unit capability scenes panel](image)

2. Do the following:
   a. For the automatic creation of video scenes for the discovered encoders/edge devices, select Video scene creation enable.
   b. For the automatic creation of audio scenes for the discovered encoders/edge devices, select Audio scene creation enable.
   c. For the automatic creation of relay output and alarm input I/O scenes from the discovered encoders/edge devices, select I/O scene creation enable.

**Notes:**
1. If a Discovery scan doesn't reveal the edge devices on your networks, you can attempt to add them manually.
2. If the unit is on a separate VLAN, you will need to add it manually.

**To Configure Discovery using the Quick Configuration Wizard**

1. In the Latitude **AdminCenter**, click **Wizards** and from the menu that appears, select the **Quick Configuration Wizard**System.
   The Quick Configuration Wizard Welcome dialog appears.
2. Click **Next**, and in the **Global Settings** tab, select the scene types that will be created during the discovery process. Click **Next**.
3. In the **Discovery** tab, click **Start**
   **Note: You can change the default discover unit types by clicking Discover Settings and customizing the setting selections.**
4. The Quick Configuration Discover Wizard will search for units that were configured and connected to the IP network.
   (see **Quick Configuration Wizard**)

**5.10.3.1 Discovery - Proprietary Configuration**

The following manufacturer-specific Configuration panes are displayed when accessing devices in Discovery **Proprietary** mode.

A Generic category is included, to allow the use of Proprietary cameras that may not have been integrated into the Latitude system, but that have generic configuration parameters that can be used by the system.

**Arecont**

![Arecont username and password](image)

**Axis**
Bosch

DVTel 9x20 Series

DVTel Ariel Line

DVTel Pro Line

DVTel Pro Line A
DVTel Quasar + HD Series

DVTel Quasar Gen II

FLIR

FLIR Recorder

Generic Camera
**IOImage**

- **Scan IP Range**: Off
- **Port**: 80
- **Username**: admin
- **Password**: ****

**IQEye**

- **Scan IP Range**: Off
- **Port**: 80
- **Username**: root
- **Password**: ****
- **Discover MJPEG video encoders**: Off

**MMS Plugin Discovery**

- **MMS Plugin Discovery**
- **Camera URL**: http://

**Mobotix**

- **Unit type**: Mobotix
- **Port**: 80
- **Username**: admin
- **Password**: ****

---

December 22, 2019

United VMS 8.0.5 Admin Center Help File
ONVIF

Panasonic

Pelco

Promelit

Sentry 360

Sony
5.10.3.2 Discovery - Generic Camera Configuration

The Generic camera plug-in enables users to configure edge devices which are not integrated into the FLIR VMS system and are not ONVIF Compliant. This plug-in supports any edge device which transmits a standard RTSP H.264 or MPEG4 stream, or alternatively MJPEG over HTTP.

**Note:** Using this plug-in, users are only able to **view live** and **record the stream**. Configuring video or picture settings from Latitude, using motion detection, PTZ and other features are not supported.

**Configuration:**

Discovering a camera via the Generic Camera Plug-in is done manually, in the 'Add unit manually' screen. You can access the screen using one of the following methods:

**Add the Unit to an Archiver manually**

![Add Unit to Archiver](image)

**OR**

**Discover a Unit manually from the Discovery page**
The following steps are required:

1. Open the ‘Add Unit manually’ screen using one of the above methods.
2. Select ‘Generic Camera’ from drop-down.
3. Select required Video Compression from the drop-down.
4. Check settings for video port (and audio port if required)
5. Enter the appropriate suffix information for the device as specified by the supplier, and click ‘Add’.
6. Repeat for each required stream.
   For each stream, the full Unit/Port/URL suffix are displayed in the table.
   This is updated if the user changes the IP address Compression method or URL suffix.

5.10.3.3 Supported Edge Devices

For the updated list of Supported Edge Devices download the Latitude-xx-Supported-hardware from FLIR Inc website:

Supported Edge Devices
5.10.4 DNA Application

DNA lists all devices discovered on the network, and provides a simple interface for required tasks such as setting IP addresses (manually or using DHCP), logging on to the Web interface of devices for changing settings, checking and updating firmware, and updating credentials.

Upon opening DNA, the application has its own embedded Help file.

5.10.5 Export - Background Export

Background Export allows the administrator to configure schedules for exporting large amounts of recorded video and audio from the primary archiving storage to a secondary storage. It is very similar to the way 'Mass Export' works, but offers automation, works incrementally and has some additional options. The exported data is copied into files in a Microsoft Windows folder structure, which later on can be viewed 'offline' using the Latitude ControlCenter client application.

Note: Exported data cannot be restored back into the Archiver and cannot become 'online' again.

Use Cases

The administrator retains the recorded video on the primary online storage (the archiver's).

In one typical use case, the administrator may want to retain the recorded video on the primary online storage (e.g. the Archiver server internal hard drives) for 14 days, and from there export every recorded file to a secondary storage location (e.g. a SAN device) for another 60 days. In this use case, the system will constantly be exporting files from the primary Archiver, once their time has come to move to the secondary storage. Clips will be recycled from the primary storage soon after they expire (14 days) but it will be possible to locate and playback any clip older than 14 days, up to almost 74 days from the time it was originally recorded, by accessing it through the secondary storage folder structure.
In another use case, the administrator may have slightly different requirements:

The Primary recording retention period should be 30 days, and then another 1 year of retention on tape storage. Moreover, only the daytime footage should be copied to tape, from selected cameras only. In order to achieve this, a tape management system has to work side by side with this Latitude feature. Latitude can be configured to export only the selected cameras, and only in the predefined time coverage, but it has to export the files to hard-drive based storage buffer, before the tape management system can copy this footage to the tape device. For playback purposes, the tape management system also has to provide access to the exported footage for the client application in the form of a standard windows drive.

**Architecture**

The architecture of the background export solution is simple:

The same Archiver server that recorded the video or audio data is responsible for performing the background export.

**Configuration**

**To configure Background Export on an Archiver**

1. From Latitude's Admin Center, click the Archiver entity in the Physical View.
2. Select the Background Export tab.
3. In the Background Export dialog box, mark the Enable Background Export checkbox, at the top of the page.
4. Under the **Backup Configuration** section select the coverage from the drop down list. This coverage determines what footage is going to be exported, in terms of the time it was recorded. New coverage can be created via System Settings - Coversages.

5. Select the cameras and/or Microphones that you want to include in the export.

6. Under **Settings**, define the Export location, which is the path to which the Archiver will export the data. This path has to be a local or a network folder that the Archiver has write permissions to. The System Administrator needs to make sure that the ATS.Archiver.RealTime service on the Archiver machine has a log on account with read/write access to the export folder.

7. Once the Export location has been defined, press the **Test** button right next to it, to check if the Archiver has the access permission required. A message will pop up with the test result:
8. You can configure storage Quota limitations by checking the When Quota Exceeds check-box. Define the storage limit capacity and then select the desired behavior upon reaching the quota: either Delete the oldest set, which means that the Archiver will automatically try to free space by deleting the oldest set, or Suspend exporting until storage space becomes available, which means that the Archiver will periodically check to see if there is available space, and this behavior is recommended if there is another mechanism (or manual procedure) that is responsible to free space in the export location. If storage quota limitations are not defined, the Archiver will attempt to write to the storage location without checking how much storage was already used.

9. You can configure the minimal duration that files should be kept on the primary storage before they can be exported to the secondary storage, by checking the Postpone export by check-box and defining the desired duration. If no duration is configured, the Archiver will attempt to export every file as soon as it completed recording it on the Primary storage.

10. Under Advanced, you can define the execution time of the export. By default, this is not restricted (Execution coverage = Always), but you can limit the time window for the Archiver to perform this task, e.g. if there is less activity in the system during the nighttime, background export can be restricted to perform only during that time.

11. Check Export Player to include Quick ControlCenter, the stand alone player, with every export set (24 hours of export).

12. Don't forget to click on the Save button to apply the settings.

13. At the top of the Background Export tab, the Status section provides status information about the background export activity as well as the Pause button that can be used to temporarily suspend the export process.

The Export Sets

The export data is organized in a particular folder structure, under the export location root folder:

- A folder is created for every 24 hours worth of footage, with the data as the folder name, e.g 2010-07-17. Such a folder and its underlying folders and files are considered a set.
- Under that folder, each Archiver creates its own folder with the folder name being the Archiver entity name in the system.
- Under each Archiver folder, a folder is being created for each camera or microphone that is included in the export, with the folder name being the camera/microphone name.
- Inside the camera/microphone folder, the actual files are copied, with each file containing the camera/microphone name, and the date and time of the export.
Reviewing Exported Data

Once the files are exported to the export storage location, the exported copies are no longer referenced in the Latitude Databases. The exported footage should be regarded as an external copy of the information. Currently, the only way to review this information is by accessing the exported folders and playing back the files using Control Center or Quick Control Center, just like one would playback any other exported clip.

Latitude ControlCenter (or the stand-alone version Quick ControlCenter) supports the following features for reviewing offline content:

- It allows the user to browse folders, as long as these folders are accessible from the local OS (e.g. those folders can be browsed using Windows Explorer)
- It allows the user to open a single audio or video clip for playback
- It allows the user to open a folder, containing multiple clips from the same camera. Because the clips are exported such that each camera has its own folder, the user can easily open such a folder and see up to 24 hours of video on the timeline, as if it was a single clip
- ControlCenter also supports Synchronized Playback including regular or smooth reverse playback of footage from multiple sources (audio and/or video)
- Online playback can be set to TCP or UDP protocol
- Playback of an exported clip displays bookmarks that were recorded with it

Note: The playback of exported clips does not support advanced on-line options such as smart search, motion indication, or using the query pane for on-line search.

Deployment with Tape

Latitude doesn't support working directly with tape devices. Hence, any deployment of this feature with a tape device requires a Tape Management system that works independently. The shared buffer between both systems (Latitude and the Tape Management system) is the export storage location, which has to be a hard-drive based storage.
5.10.6 Export - Mass Export

When very large amounts of video data from multiple cameras have to be exported to an external storage location, fastest results are achieved by using Mass Export. It can be used for offline investigations or for creating an offline copy of video data for any other reason.

Regular export can still be performed using the ControlCenter. Since Mass Export is performed in the AdminCenter, the export storage location must be accessible to the AdminCenter.

In order to facilitate the Mass Export procedure, a Job wizard is used. The Job wizard creates one job per Archiver. Each job contains a list of scenes from a single Archiver during a specified time span. It is possible to create more than one job per Archiver but only the first job will be active. All following jobs are queued, awaiting export, until the running job is complete.

In this tab you can perform the following actions:

- Create a Mass Export job from the AdminCenter
- View currently active jobs
- Edit existing jobs
- Stop existing jobs
- Remove existing jobs
- Receive reports per job

To access Mass Export, go the System Mass Export tab.
The following buttons appear in the Mass Export Toolbar:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="start.png" alt="Start" /></td>
<td>Start a selected export job for which the auto start option was not selected or a job that was stopped.</td>
</tr>
<tr>
<td><img src="edit.png" alt="Edit" /></td>
<td>Edit the job settings. The Job Settings dialog box will appear.</td>
</tr>
<tr>
<td><img src="stop.png" alt="Stop" /></td>
<td>Stop a running export job.</td>
</tr>
<tr>
<td><img src="delete.png" alt="Delete" /></td>
<td>Delete an export job. <strong>Note:</strong> This option is disabled during an active export job. The export job needs to be stopped first.</td>
</tr>
<tr>
<td><img src="refresh.png" alt="Refresh" /></td>
<td>Refresh the currently active job list.</td>
</tr>
<tr>
<td><img src="show_report.png" alt="Show Report" /></td>
<td>Display a report of the selected job.</td>
</tr>
</tbody>
</table>

**To create a Mass Export job from the AdminCenter**

1. In the AdminCenter, select Logical View or Physical View from the Sidebar, and then click System.
2. Click the Mass Export tab.
3. Click **Add Job Wizard** to create a mass export job.
4. In the Welcome screen, click **Next**.
5. In the Choose Scenes dialog box, select the check boxes of the desired scenes from which you want to export data from the Navigation tree, and then click **Next**.

![Mass Export Jobs Wizard](image)

**Note**: You can only select scenes from one Archiver for each job.

6. In the Choose Time Period dialog box, select the time frame (time and date) from which you want to export data, and then click **Next**.
In the **Job Settings** dialog box, each job is listed separately.
7. Define the following parameters for each job by selecting the job and then setting the parameters:
   • **Description** - This field is optional. Describe the content or purpose of the job.
   • **Path** - Enter the exact export location path of the job. To make sure the path is valid, click Test.
   • **Include Player** - Select this check box to automatically export and burn an executable player along with exported files that are burnt on a disk.
   • **Stop all recordings while exporting** - Select this check box to stop recordings while exporting files
   • **Auto start** - Select this check box to immediately start the export when completing the Job wizard.

   **In case of existing files:** Skip/Overwrite/Fail - Select what action the AdminCenter should take if the export job already exists. You can choose to skip (the existing files will not be exported again), overwrite (the existing files will be overwritten with the newly exported content) or fail (the export job will stop and will be listed as failed job).

8. Click **Next**.
9. In the **Create Jobs** dialog box, the created jobs are listed, displaying the export location path and job size.
10. Click **Next** to start exporting the defined job or click **Back** to edit the export job (e.g. if the path was not selected).
11. Click **Finish**.
   • The export jobs appear in the **Mass Export** tab, where their name, export location, size and progress appear in a list of all currently active jobs.
   • The job summary of each job appears when selecting it from the list.
   • The job starts exporting at once if the **Auto start** check box was selected.

12. To start the export job manually, click **Play**.

### To view currently active jobs
1. In the AdminCenter, select **Logical View** or **Physical View** from the Sidebar, and then click **System**.
2. Click the **Mass Export** tab.
3. All currently active jobs are listed, along with their name, export location, size and progress.
   The job summary of each job appears when selecting it from the list.

### To edit existing jobs
1. In the AdminCenter, select **Logical View** or **Physical View** from the Sidebar, and then click **System**.
2. Click the **Mass Export** tab.
All currently active jobs are listed, along with their name, export location, size and progress.

3. Select the export job you want to edit, and then click 

4. In the **Job Settings** dialog box, you can edit the following parameters:

   - **Description** - This field is optional. Describe the content or purpose of the job
   - **Path** - Enter the exact export location path of the job. To make sure the path is valid, click **Test**.
   - **Include Player** - Select this check box to automatically export and burn an executable player along with exported files that are burnt on a disk.
   - **Stop all recordings while exporting** - Select this check box to stop recordings while exporting files
   - **Auto start** - Select this check box to immediately start the export when completing the Job wizard.

   In case of existing files skip/overwrite/fail - Select what action the AdminCenter should take if the export job already exists. You can choose to skip (the existing files will not be exported again), overwrite (the existing files will be overwritten with the newly exported content) or fail (the export job will stop and will be listed as failed job).

5. Click **OK**.

### To stop an existing job

1. In the AdminCenter, select **Logical View** or **Physical View** from the Sidebar, and then click **System**.
2. Click the **Mass Export** tab.
   
   All currently active jobs are listed, along with their name, export location, size and progress.
3. Select the export job you want to stop, and then click 

   You can resume the export job by clicking 

### To remove an existing job

1. In the AdminCenter, select **Logical View** or **Physical View** from the Sidebar, and then click **System**.
2. Click the **Mass Export** tab.
3. All currently active jobs are listed, along with their name, export location, size and progress.
4. Select the export job you want to remove, and then click 

   if the job is currently running.
5. After stopping the export job, you can remove the job by clicking 

### To receive reports per job

1. In the AdminCenter, select **Logical View** or **Physical View** from the Sidebar, and then click **System**.
2. Click the Mass Export tab. All currently active jobs are listed, along with their name, export location, size and progress.

3. Select the job for which you want to view a report, and then click Show Report.

5.10.7 MapBuilder

The MapBuilder is a GUI tool for generating HTML and JavaScript code for interactive maps that can be displayed in the ControlCenter. Maps created with the MapBuilder can contain links to cameras, analog monitors, microphones, other maps or web pages, and custom-built JScript or VBScript functions. You can use MapBuilder to create maps from scratch or edit maps previously created by the tool. Existing HTML pages not generated by MapBuilder cannot be modified with it.

The MapBuilder can be accessed from the Admin Center's Applications Menu.

In AdminCenter click Applications - Mapbuilder - Latitude. The Mapbuilder dialog box appears.

Use the Toolbar icons to open an existing map or define a new background. See details below.

Once a map is created, the MapBuilder window will show the workspace panes.

To exit the MapBuilder screen, Save your edited map/s, click Close Map, and then use the Sidebar icons to return to the regular AdminCenter functions.

Workspace

The MapBuilder workspace consists of four panes:
The **Entity Browser** displays the System entities that can be placed in a MapBuilder map. You can drag and drop entities from the Entity Browser into the **Editing Pane**.

The **Toolbar** is used to open an existing map, open a new map, add a button (for triggering JScript/VBScript functions) or add a general image. In addition, you can add Text Label, Save Map, Save as and Close Map. Check the **Auto Scale Map** check-box to open the map in-size with the Control Center tile.

The **Editing Pane** displays the map and allows you to change the location of its elements. Clicking on an element displays its Properties Pane, while right clicking an element allows you to remove it or perform other type-specific functions.
The Properties Pane shows the focused element's properties, such as location, size, tooltip, etc. Element properties vary based on their type, and some properties are not editable and shown for informational purposes only.

Creating a Map

1. From the Admin Center side bar, select Applications, click Mapbuilder and then System.
2. In the Toolbar, select the New Map icon. The New Map- select map's background image dialog box appears.
3. Select the required map image and click Open.
4. The map is generated and appears in the MapBuilder's Editing Pane (see workspace screen shot above). MapBuilder supports most standard image formats, such as jpeg, gif, bmp, etc.
5. Place your cursor on a blank space in the Editing Pane, and click.
6. The Properties Pane displays the map's overall parameters. Two of these are user-modifiable, PutTitle, which controls whether or not the title of the map is shown at the top of the map page (not visible in MapBuilder), and ScriptFile, which can be used to add functionality to the map via a JScript or VBScript script.

Add cameras to the map.
   a. Drag and drop a camera you would like to include in your map from the Entity Browser to the Editing Pane. Place the camera in an appropriate position relative to your background image.
   b. Click the camera to display its properties in the Properties Pane.
   - MapBuilder provides default images for cameras and domes in a number of states (recording, focused, etc.) You can modify any of these images by clicking the "..." button at the right side of the icon's entry in the pane and browsing for and selecting another image.

   c. To add a record button for the camera, right click the camera (in the Editing Pane) and select Add Recording State. As with the camera itself, you can
change the record button images, their size and position and their tooltip text from the Properties Pane.

d. Repeat steps a-c as needed to add cameras to the map and configure them.

8. Add analog monitors to the map. As with cameras, you can change the monitor’s icon, its size and position, and its tooltip text from the Properties Pane.

9. If applicable, you can add links to other maps by dragging and dropping maps from the Entity Browser. As with other entities, you can change a map’s image and its size, position and tooltip through the Properties Pane. Alternatively, a map can also be shown as a button by changing its **CurrentType** parameter from Image to Button.

10. If applicable, add buttons to your map.

   a. Click 🗾 to create a new button or 🌠 to create a new general image. Position it as required in the map.

   b. In the Properties Pane modify its size, position, title and tool-tip as needed.

   c. Enter JScript code into the **OnClick** field in the Properties Pane.

   d. Repeat as needed to create additional buttons.

11. Click **Save** to save your map.

**Adding the Map to the system's entity list.**

See [Map/Create a Map Entity](#).

**Managing Alarms from Maps**

When you create a map in the Latitude MapBuilder, the HTML document of the map is created enabling you to perform the following functions:

- Select the background image (such as the floor plan)
- Drag & Drop camera icons from the camera list
- Drag & Drop alarm icons from the alarm list. These alarm icons display the status of the alarm they represent; either idle, activated, accepted by current user OR accepted by another user.
- Drag & Drop other types of security entities (such as audio devices as well as entities that represent integrated 3rd party systems).
• Create Text Labels, general icons and buttons.

Latitude maps support a java script API which enables programming when advanced functionality is required. Using this API, high level maps can be programmed to show the status of zones. For example, if one or more of the alarms in a zone is active, the zone will flash or show a different color. The user will then be able to click on that zone in order to drill down to a lower level map with more details.

Using Maps in ControlCenter
• To display a camera from the map, double click it or drag and drop it onto a viewing tile.
• To start or stop recording a camera, click its recording button.
• To display a camera on an analog monitor, drag its icon onto the monitor's.
• To display a linked map (on the same tile), click its map icon.

Note: check the autoscale map check-box in Admin Center to enable the map display to fit the tile size in Control Center.

5.10.8 Mentor
Mentor Screen Agent Recording and Training Module is a component of the Latitude video management system. Mentor is an intelligence gathering tool which provides insight about the operations and performance of system users. It provides a view of any networked PC which can be seamlessly synchronized with all of the system's video, audio and data in both live and archived modes.

By running the Latitude Mentor application in the background on the operator's workstation, a video stream is created directly from the graphic card of operator's workstation, enabling access to it as if it were a regular camera in the system.

Latitude can be programmed to record an unlimited number of Mentor channels according to a schedule, upon an alarm, or manually.

Note: Each Mentor channel requires a regular camera connection license.

An authorized Latitude user (normally an Administrator or Supervisor) can view Mentor channels which are available for access using the normal camera tree within the application.

The video stream emulates a ProLine camera with the IP address of the operator's workstation.

Installing and configuring Mentor
Perform the following procedures to install and configure Mentor:

Installing the Mentor Application
Complete the steps below to install the Mentor application on each workstation from which intelligence is to be collected.
1. In order to install Mentor, one needs to enable Mentor in the list of components shown in the Latitude Custom Installation process. This is shown in the normal Installation process when installing for the first time, or by using the Windows Control Center Programs and Features screen to access the Maintenance Wizard.

![Using the Windows Control Panel to access the Latitude Maintenance Wizard](image1)

2. Once the Latitude Maintenance Wizard is running, use the **Custom Installation** option, and select **Mentor** in the component tree. (As this is being installed on a Latitude Client workstation, one would normally have **Control Center** and possibly **Admin Center** selected as well).

![Typical Latitude Workstation Options when Mentor is being installed](image2)

3. Complete the steps in the Latitude Maintenance Wizard.
4. If necessary, make changes to the Mentor Configuration settings.

5. Run the Mentor application by clicking Mentor.exe in the Latitude application folder of Program Files/Program Files (X86), depending on where the Latitude components were installed.

6. Once the application is running on a workstation, the Administrator can use the Add Unit Manually context menu option by right-clicking on the Archiver to which the Mentor’s data stream is to be sent.

7. In the Add Unit Manually dialog box, enter the IP address of the Workstation, and select the unit type ProLine.

A virtual camera will be created in the Admin Center Navigation Tree with the characteristics of a ProLine camera.

8. Complete any required Picture, Video and Recording Settings for viewing and/or recording the stream from the Workstation.
9. Make the appropriate **Access Rights** and **Privileges** settings for the workstations and for the administrators of the system. Typically, the Mentor virtual-camera entities would be moved to a 'Site' that would only be accessible by specifically designated Supervisor/s, so that regular users could not access the Mentor streams of other users.

![Control Center showing a virtual Mentor 'camera' in a tile.](image)

### Configuring the Mentor Application

Using the Mentor configuration, the user may set the exact screen area (rectangle) to be captured, the FR, BR and other video parameters.

In addition, using standard Latitude Camera Settings, the user may define a recording profile to control the times in which recording of the video stream should take place.

There are two levels of configuration of the Mentor application

- Mentor-specific
- Camera-like.

### Mentor-Specific Configuration

The following setting should be made in the Mentor's configuration file (Mentor.exe.config, typically found under C:\Program Files\FLIR\Mentor\Mentor, or ..\DVTEL\.. on an upgraded installation):

- `<add key="ScreenNumber" value="1" />` - Select the screen number to work on, if using more than one screen
- `<add key="SourceX" value="0" />` - The "X" coordinate of the upper left corner of the desired rectangle to be captured in the screen (by default – "0" – the upper left corner)
- `<add key="SourceY" value="0" />` - The "Y" coordinate of the desired rectangle to be captured in the screen (by default – "0" – the upper left corner)
• `<add key="SourceWidth" value="704" />` - The width of the captured rectangle. This value can be set to any value, as long as the sum of SourceX and SourceWidth is not bigger than the screen width in pixels. For example, to capture an entire screen with a resolution of 1024 by 768 this value should be set to 1024. The bigger this value is the more CPU resources will be required by the Mentor service in order to produce the video stream.

• `<add key="SourceHeight" value="576" />` - The height of the captured rectangle. This value can be set to any value, as long as the sum of SourceY and SourceHeight is not bigger than the screen height in pixels. For example, to capture an entire screen with a resolution of 1024 by 768 this value should be set to 768. The bigger it is the more CPU resources will be required by the Mentor service in order to produce the video stream.

• `<add key="DestinationWidth" value="704" />` - The width (resolution) of the 'created' video stream. It is recommended to keep the DestinationWidth and DestinationHeight ratio similar to the SourceWidth and SourceHeight ratio. Any value can be supported but it is recommended to use smaller values to reduce CPU strain by the Mentor.

• `<add key="DestinationHeight" value="576" />` - The height (resolution) of the 'created' video stream. It is recommended to keep the DestinationWidth and DestinationHeight ratio similar to the SourceWidth and SourceHeight ratio. Any value can be supported but it is recommended to use smaller values to reduce CPU strain by the Mentor.

• `<add key="FramesPerSecond" value="5" />` - FPS of the created video

• `<add key="BitRate" value="4000000" />` - BitRate of the created video

• `<add key="KeyInterval" value="25" />` - The Key Frame interval of the created video.

### Camera-Like Configuration

The Mentor application simulates a ProLine camera. From the Admin Center, use the Camera Settings screens to set parameters for each workstation running the Mentor application:

- Picture Settings
- Video Settings
- Motion Detection

### 5.10.9 Rediscovering or Replacing a Unit

It is possible to manually or automatically rediscover and replace a unit. Usually this procedure is necessary when a unit is exchanged physically or when a unit is upgraded or downgraded.

When a unit is rediscovered manually, the unit is removed without deleting its logical configuration, discovered or added manually and then the scenes are attached manually via the ports.
The automatic unit rediscovery performs the same procedure automatically. However, if any acute failure occurs at any point, such as a logical configuration that is not completely compatible, the procedure is canceled and the previous state is reinstated. If any automatic logical changes are made during the automatic unit rediscovery process, a message appears including all necessary information.

- Manual Unit Rediscovery
- Automatic Unit Rediscovery

### Manual Unit Rediscovery

1. In the **Physical View**, right-click the desired unit, and select **Delete Unit**. A confirmation message appears, asking whether or not to remove all child entities. **Note:** If you click yes, the recorded material will no longer be accessible.

2. Click **No**.
3. Go to the **General** tab of System, and access the **Video** panel.
4. Clear the **Automatically create unit capabilities scenes** check box.
5. On the sidebar, click **Discovery**.
6. Click **Start** or **Discover Unit Manually**.
7. If you click **Discover Unit Manually**, select the desired unit type from the Unit type drop-down list.
8. Enter the unit's IP address.
9. Enter other relevant parameters. The parameters vary depending on the selected unit type.
10. Click **OK**.
11. Once the desired unit appears in the list of discovered units, click **Stop**.
12. Select the Archiver to which you want to attach the unit from the Archiver drop-down list, and then click **Attach**.
13. Save your settings.
14. Reattach the unit's child entities manually by right-clicking each port and selecting **Attach existing <child entity>**.
15. Select the desired child entity from the **Select Item** dialog box.
16. Repeat steps 14 and 15 for each child entity.

### Automatic Unit Rediscovery

1. In the Physical View, right-click the desired unit, and select Rediscover Unit.
   The **Add Unit** dialog box appears.
2. Select the desired unit type from the Unit type drop-down list if necessary.
3. Click OK.
4. A confirmation message that the unit has been rediscovered will appear once the process is complete.

5.10.9.1 Time Synchronization

It is important to synchronize the time of the servers in the system for the proper maintenance of all recordings, playbacks and searches.

Note: It is highly recommended that you use a time server to synchronize all United VMS servers connected to your system.

Note: System > General > Time section is not currently supported and will be updated in a future version.
5.10.10 Reporting Tool

The Reporting Tool is an application that provides reports on past Latitude events by querying the audit databases maintained by the Latitude EDBs.

**Audited Events**

<table>
<thead>
<tr>
<th>Report</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Logon</td>
<td>User Logged In, User Logon Failed, User Logged out</td>
</tr>
<tr>
<td>Entity Configuration</td>
<td>Entity Added, Entity Configuration Updated, Entity Removed</td>
</tr>
<tr>
<td>Incident</td>
<td>Incident Created, Incident Updated</td>
</tr>
<tr>
<td>Alarm</td>
<td>Alarm Triggered, Alarm Activated, Alarm Snoozed, Alarm Forwarded, Alarm Acknowledged</td>
</tr>
<tr>
<td>Equipment Failure</td>
<td>Accessibility Lost/Recovered</td>
</tr>
<tr>
<td>Server Monitoring</td>
<td>All events related to all servers. Report displays events in chronological order per server name and server type.</td>
</tr>
</tbody>
</table>

**Limitations**

- If events do not get generated by Latitude, they are not displayed by the reporting tool.
- When exporting reports to .ls format that have more rows or columns than supported by Excel, the reports cannot be displayed in Excel.

Audit Trail feature must be enabled in AdminCenter. For each Report Type, the **Audited Events** pane must include the corresponding **events** required by the tool which are mentioned above.
5.10.10.1 Installing the Reporting Tool

An automated install wizard is provided for the installation of the Reporting Tool software. Insert the application CD into your CD ROM drive. An installer tool will be started and you can click the set up button or copy the files to User folder to your computer and run the REPORTING TOOL INSTALLER.msi

Follow the steps in the installer tool to install the software.

The installer tool will place a shortcut called ATS Reporting Tool in the following locations:

- Desktop
- An ENGINEERING SERVICES folder under Programs in the Start menu

5.10.10.2 Starting the Reporting Tool

To run the Reporting Tool, follow any of the following procedures:

- Desktop
  Locate the REPORTING TOOL icon on your desktop and double-click it.
- Start menu
Navigate the ENGINEERING SERVICES FOLDER via Start/Programs and double-click the Reporting Tool icon

- Installation folder
  By default, the Reporting Tool is installed in the \Program Files\<ENGINEERING SERVICES Folder>\Reporting Tool\ folder. Navigate to this folder, or the installation folder you specified when installing the Reporting Tool software. Double-click the <REPORTING TOOL INSTALLER.MSI>.exe file.

5.10.10.3 Using the Reporting Tool

Directory Login

You need to log in to System Directory in order to be able to use the Reporting Tool. Whenever, you start the application you will be asked to log in.

Directory Login window is displayed every time the application starts and whenever you click on the Login in the File menu.

You need to enter the Host where the directory you want to login to is located, User name, and password. Whenever the Directory Login is displayed, the “Host” defaults to “localhost”, User name to “admin” and Password is blank.

Clicking “Connect” in the Directory Login window logs off the currently logged in user and attempts to log in the user specified in the User name field.

Clicking the “Cancel” button closes the Directory Login window. If the Directory Login window is displayed after running the application, and “Cancel” button is clicked, then the Directory Login closes and Reporting Tool window opens in a disconnected mode.

To reconnect to a different Latitude server, click Login in the File menu.
Reporting Tool Window

Menu

File
- Login – Log in to Latitude as a different user.
- Exit – Hides the application
- Options – Configures database connections. Options menu item is only visible if you are logged in to Latitude.

Help
- About – Displays the version of Reporting Tool application and the Latitude version, the Reporting Tool is to be used for.

Reports
- Provides access to the supported reports (see Preface for list of reports). This menu item is only visible if you are logged in to Latitude and if database connections were set.

Reporting Tool Body

Options Toolbar

Gives you the ability to process the report in various ways:
- **Sort By** – You can sort the report by any column displayed in the report. If you choose to sort by time and the report is also grouped by time, both the group and the subsequent time column will be sorted. To apply the Sort on the report hit “Go” button of the Options toolbar.
**Configuration - Functionality**

- **Filter By/Filter text** – You can filter any column that consists of string/text data by the string provided in the “Filter text” field. To apply the filter, hit “Go” button of the Options toolbar. To cancel filtering, choose “None” in the “Filter by” field.

- **Go** – Pressing the “Go” button will sort and filter the report according to the information provided in the “Sort by”, “Filter by”, and “Filter text” fields.

- **Ascending** – “Ascending Sort” – If this button is disabled when a report is displayed in the report viewer, then the sort direction of the “sort by” field is set to “Ascending Sort”. To perform a “Descending sort” hit the “Dsc” button of the Options Toolbar. *

- **Descending** – “Descending Sort” – If this button is disabled when a report is displayed in the report viewer, then the sort direction of the “sort by” field is set to “Descending Sort”. To perform an “Ascending sort” hit the “Asc” button of the Options Toolbar. *

- **Reload** – reset all Option Toolbar fields to default and refreshes the currently displayed report.

**Report Viewer**

- **Viewer toolbar**
  - Navigate to different pages of the report
  - Export to a pdf or other file format
  - Search for a specific string

- **Report**

**Status Bar**

Displays a message and a progress bar.

**Note:** The sort direction is applied on the already applied sort. If you would like to for example perform an ascending sort on a column, choose the column in the “sort by” field, then hit “go”. Then if the “Asc” is enabled, click it to apply the sort direction. If it is disabled, then the sort direction is already applied. The sort is performed only on items inside groups.

Groups, other than date/time groups cannot be sorted using the Reporting Tool.

5.10.10.4 Configuring the Reporting Tool

Before you can generate reports, you will need to configure its database connection parameters. Database connection parameters must be supplied for both the Directory Database Server and at least one EDB Database Server. To view all reports, please add all EDB Database Servers that were used by Latitude and for which you still have access to.

Any changes to the database connection settings will be applied when you hit **Save** button of the *Database Connection Settings* dialog box. When you login first time to
Reporting Tool, the *Options* dialog box will appear: Both EDB and Directory databases will be reported missing. You need to add these, before you can generate reports.

The *Options* dialog box will appear whenever one of the database types is missing. If you do not want to add database connection at this time, just hit “Cancel” in the “Database Connection Settings” window.

**Adding Database Connections**

1. You have to be logged into Latitude before continuing with the following steps.
2. Go to File>Options.
3. Click Add and enter the connection information for the EDB/Directory database to which you would like to connect (Database Server refers to the server on which the database resides, which may be different than the Latitude> EDB server). If when you installed the Latitude system, you did not change the user name and password to the Directory/EDB databases, leave the DefaultATSUsername & Password checked. This will automatically populate the default user name and password set for Latitude databases. Click OK.
4. To add additional databases, repeat the previous step as needed.
5. The changes to the database connection settings will be applied when you hit “Save” button of the “Database Connection Settings” Windows form.

**Editing Database Connection Settings**

1. You have to be logged into Latitude> before continuing with the following steps.
2. Go to File>Options.
3. Select the Database Connection, which you want to edit. Click Edit and enter the correct connection information for the EDB/Directory database. Click OK.
4. The changes to the database connection settings will be applied when you hit “Save” button of the “Database Connection Settings” Windows form.

**Removing Database Connection Settings**

1. Select the Database Connections which you want remove. To select multiple connections, hold the “Ctrl” key when selecting the connections. Click Remove.
2. The Changes to the database connection settings will be applied when you hit “Save” button of the “Database Connection Settings” Windows form.
Testing Database Connections
1. Select the Database Connections, which you want to test. To select multiple connections, hold the “Ctrl” key when selecting the connections.
2. Click Test. Any changes to the database connection settings will be applied when you hit “Save” button of the “Database Connection Settings” Window form.

Viewing Reports
To be able to view reports, the following conditions must be met:
- You must be logged in to System directory
- Both Directory and EDB database connections are set correctly.

To view a report
1. Navigate into “Reports” menu item and click on a report you want to view.
2. Choose both the starting and ending date and time and click OK. The report will be filtered by the supplied date/time range. Only events that occurred in that date/time range will be displayed.
3. To sort, filter and refresh the report use the “Options” toolbar. See “Using Reporting Tool”
4. To navigate to different pages, search for a text, or export the document, use the toolbar in the report viewer.

The tabs displayed in Report Viewer when a report is displayed do not show the name of the report. The single letter in the report does not represent anything.

Reporting tool has a 5-minute timeout period for generating reports. If a report fails to generate within 5 minutes the above error message is thrown.

5.10.10.5 Reports
The following report types are supported:
- Alarm Report
- Entity Configuration Report
- Equipment Failure Report
- External Event Report
- Incident Report
- Server Monitoring Report
- User Activity Report
- User Logon Report

Each description specifies the default group and sort for the report. You can sort the report by another column using the Options toolbar.

Notes:
1. You can sort only data within a group.
2. Group sort is not supported.
Alarm Report
Overview
Alarm report displays a report about alarm events, such as Alarm Triggered, Alarm
Activated, Alarm Snoozed, Alarm Acknowledged, and Alarm Forwarded that oc-
curred within the date/time which you provide.
Groups
Alarm events are grouped by an Alarm type and then an Alarm Instance.
Sort
Data within a group (per Alarm Instance) are sorted by time in descending order.
Note: You cannot change the sort type and sort order of an Alarm Report.

User Logon Report
Overview
User Logon Report displays User Logged In and User Logged Out events for the
date/time provided by you.
Groups
No groups
Sort
The default sort is by time in descending order.

Entity Configuration report
Overview
Entity Configuration Report displays Entity Added, Entity Updated and Entity Re-
moved events for the date/time range provided by you.
Groups
The report is grouped by day. Group is sorted in a descending order.
Sort
The data in group are sorted by time in descending order.

Server Monitoring Report
Overview
Server Monitoring Report displays all events that occurred for any of the ATS Serv-
ers: Archiver, EDB, Directory, Mail Server, Transcoder, and Gateway Server for the
date/time range provided by you.
Group
The data is grouped by Server type (Ascending Order), then by Server Id (Ascending
Order)
Sort
The data within the inner most group are sorted by time in descending order.
Equipment Failure Report
Overview
Equipment Failure Report displays Accessibility Recovered and Accessibility Lost events for devices for the date/time range provided by you.

Group
The data is grouped by minute in descending order

Sort
The data in the group is sorted by time in descending order.

Incident Report
Overview
Incident Report displays Incident Created and Incident Updated events for the date/time range provided by you.

Group
The data is grouped by day in descending order

Sort
The data in the group is sorted by time in descending order.

5.10.11
Safrun
Safrun is Latitude "Watchdog" component. It is charged with monitoring the Latitude server applications (which run as Windows services) and restarting them if they fail. It can also be used to manually stop and start the Latitude services as well as to view their logs.

Safrun itself consists of two distinct parts: the Safrun service, which performs most of the component's functions, and the Safrun application, which provides a front-end graphical user interface for the service. This application, which is itself monitored by the Safrun service, can be launched from the Windows System Tray by double clicking the icon (similar to the SQL Server Service Manager which provides a front-end interface for managing MSSQL/MSDE services).

The Safrun Application
The Safrun contains two types of views: the Services view, which shows a snapshot of the various services' states, and the Application-specific views (Directory, Archiver, Discovery, EDB, and Transcoder and Gateway), which display the corresponding Latitude services' logs.

You can switch between views with the Views menu and change the overall display mode using the Window menu (the options here only have a visible effect when multiple views are open concurrently).

By default, the Safrun application displays information about the Latitude services running on the local machine on which it is installed. It can also, however, obtain data from a Safrun service running on another Latitude server. You can change the monitored server from the Services view.
The Services View

This view displays vital statistics on the Latitude services running on the computer Safrun is monitoring. To change the machine whose processes are displayed, simply enter the name of a different Latitude server in the Host name field and click Set Host.

Each row in the table represents an Latitude service. The information provided for each of the service is:

- Its name.
- The process state, either Running or N/A.
- The date and time that the process was last started.
- Its memory usage.
- The total CPU time utilized by the process since it last started.

You can use start or stop any of the displayed services by selecting a service and clicking the End Process/Start Process button or by right clicking the service and choosing Kill Process.

Application Specific Views

You can view any of the monitored applications' logs by going to View>[Application]. The level of information detailed in the logs can be set through the applications' .config files (contact ATS Technical Support for more information).

5.10.12 Scene Tracker

Latitude offers full integration to ATS’s SceneTracker application, which is used to “stitch” multiple cameras into a single scene providing a full view of a space covered by multiple cameras. In combination with SceneTracker’s built-in digital PTZ functionality, the application provides users with a highly effective way to monitor multiple cameras.

Following are basic instructions for defining SceneTracker Views and calibrating scenes using the AdminCenter SceneTracker Calibration Wizard.

- Starting Calibration
- **Calibration Wizard**

### 5.10.12.1 Starting Calibration from the AdminCenter

1. In **AdminCenter** (Logical View or Physical View), right-click on the system icon (System) to open the context menu, and select **Add SceneTracker Views**. The SceneTracker screen opens, allowing you to enter a name, an optional description, and the general parameters to be applied.

2. Click to open the **Calibration** tab.

You can create multiple calibrations for a single SceneTracker View but only one may be active at any given time. This feature has two advantages:

- In case a camera already defined in a calibration becomes unavailable, it is easy to create an alternative Calibration.
- It provides a convenient method for trying out a number of calibrations without losing your previous work.

3. Click on **Add Calibration** to open the **Calibration wizard**.
   (see SceneTracker **Calibration Wizard**
4. Once one or more Calibrations have been completed, return to the SceneTracker window. All options in the Calibration window are now enabled.

1. There can be multiple Calibrations for one SceneTracker view. The same cameras will be available for each calibration (but you may opt not to use all of them for some of the Calibrations, for example, if a camera is out of service, you can define a Calibration will does not use that camera.)

2. Choose one calibration and click on Set Active Calibration. (For each SceneTracker view there must be one Active Calibration)

3. Click on the File icon to save the Calibrations.

5.10.12.2 Calibration Wizard

The Calibration wizard consists of four steps. The first three steps are used to select cameras and images to work with, and the last step consists of creating the calibration itself.

Selecting Cameras
Capturing Video
Selecting Frames
Composing the Viewing Area

Selecting Cameras

In this step, you select cameras for your calibration. Up to eight cameras may be used in a single SceneTracker View. To add a camera, highlight it in the Available Items field and move it to the Selected Camera Scenes field with the forward arrow button. Similarly, you can remove a camera with the backwards arrow button.

Note: Once the Next button is pressed, you cannot remove cameras.
Capturing Video

This optional step allows you to capture short video clips from selected cameras to use in creating the calibration.

After selecting the required cameras, click on Next to open the Capture Video Step, and press the record button to capture video.

You can set the number of seconds to record from the Seconds field located to the right of the record and stop buttons. **Note:** You do not need to capture video clips if you want to select the frames to use for stitching directly from live video (see next section).
Selecting Frames
Click Next to open the Select Frames screen.
You need to create and select a set of stills picture frames to use.
To select frames to use in composing the calibration perform the following procedure:

1. Click the Recorded or Live radio button at the bottom left of the window to indicate whether you would like to use frames from currently live video or recorded video. These recordings will the available for replay to capture frames you will pick from.

2. If you selected the Recorded option in Step 1, click the Play button to play the captured clips synchronously.

3. To capture a set of frames (i.e. a frame from each source), click the scissors button at the top right of the window.

   You may repeat this step to capture additional sets of stills.

4. Click the Stills radio button at the bottom left of the window.
5. Select one of the frame sets captured in Step 3 from the drop-down menu to the right of the scissors button.

6. Once you have selected the still frame “Set” from the menu, click Next to go on to the Compose Viewing Area screen.

Composing the Viewing Area

To calibrate a SceneTracker view, you must specify constraints that allow the software to calculate how the frames are spatially connected.

There are two types of constraints that can be configured: **point constraints** (which match a single point between two frames), and **line constraints** (which match a line between two frames).

The procedure below describes the stitching of two cameras. Additional cameras can be added to the scene in the same way - once the cameras in your viewing area are calibrated, a new camera can be stitched to them as if they were a single fixed camera.

1. To add the first camera to the EntireView area.
   a. Expand one of the entries in the Participating Cameras section by clicking its blue, downward-facing arrow.
   b. Click a point in the image shown inside the Participating Cameras section.
   c. Click a point in the blank workspace EntireView area corresponding to the location where you would like to place the point marked in the previous step.
   d. Click the Match current location button. This places the first video on the workspace. The frame will appear in the EntireView area.

2. Add a second camera to the EntireView area.
   a. Navigate to the second camera’s entry in the Participating Cameras section and expand it.
      i. Using the zoomed-in view in the bottom section of the wizard, select an easily identifiable point in the frame that also appears in the first camera’s frame and click it.
      ii. Using the zoomed-in views in the bottom section of the wizard, mark the point in the EntireView area that corresponds to the point selected in the previous step.
      iii. Click the Match current location button. The second camera’s frame will appear in the EntireView area.

3. Repeat this process for each of the participating cameras. Additional reference points can be associated with the pictures to improve alignment.

Various scaling and manipulation options are available in the toolbar above the composition area, to refine the View.
4. Similarly to steps 2.b-2.d, you can add additional constraints, to improve the stitching of the cameras. When doing this, the point added on the Participating Camera view will be followed up by clicking the relative same location on the first camera you added to the EntireView workspace in step 2. To switch to a line constraint, click the Select new constraint button and select the line constraint option. It is recommended to add three or more constraints (points or lines).

5. Similarly to steps 2.b-2.d, you can add additional constraints, to improve the stitching of the cameras. When doing this, the point added on the Participating Camera view will be followed up by clicking the relative same location on the first camera you added to the EntireView workspace in step 2. To switch to a line constraint, click the Select new constraint button and select the line constraint option. It is recommended to add three or more constraints (points or lines).

6. Once you have defined a few constraints (typically at least three), you may want to use the auto-calibration feature to have the software add additional point constraints. To do so, click the Auto button at the pane above the EntireView area. The points created by the auto-calibration are displayed in the Participating Cameras section among the points added manually.

7. You can further adjust the calibrated view by removing and/or adding additional points.
8. If necessary, you can move, crop or rotate individual video sources using the three middle buttons of the toolbar (this should generally be done sparingly, as it may reduce the accuracy of the stitch).
9. Click the Up arrow on the right side of the toolbar.
10. Use the rotation, stretching, zoom and move buttons in the new toolbar to adjust the position, shape and size of the EntireView within the viewing area.

**Tip:** Position and scale the finished View to take into account that the SceneTracker window can include an active pane that acts as a digital PTZ of the whole scene.

11. When the view is satisfactory, click on **Finish.** This will open a window enabling you to choose the final aspect ratio of the view.

12. Click on **Finish** again.
   The final SceneTracker view of this Calibration can be viewed, with the active digital PTZ window, and options for how it should be displayed.
13. Click on Close to exit, and click Finish to return to the main Calibration window, give your calibration a name and save it.

5.10.12.3 Create a New SceneTracker View

To create new SceneTracker Views

Note: Setting up SceneTracker Views is a complex activity, and should be done with guidance from an experienced operator until one is familiar with the tool. The following explanation is an overview only.

1. In AdminCenter (Logical View or Physical View), right-click on the system icon (System) to open the context menu, and select Add SceneTracker Views. The SceneTracker screen opens, allowing you to enter a name, an optional description, and the general parameters to be applied.
2. Click to open the **Calibration** tab.

3. Click on **Add Calibration** to open the **Calibration wizard**. The first step in the Wizard allows the User to select cameras to use for the SceneTracker View.
4. After selecting the required cameras, click on **Next** to open the **Capture Video** Step, and press the record button to capture video.

**Note:** The use of Video is not covered in this Help Material - but a picture must be captured in order to see the Still view (see next frame).
5. When the recording is done, click **Next** to open the **Select Frames** screen.
6. Select **Stills**, and click **Next** to go on to the **Compose Viewing Area** screen.
1. In the **Participating Cameras** panel on the left, pick a camera, mark a calibration points in the camera view. (Use the magnified view at the bottom of the screen to do this accurately).
   Pick a position in the main composition area to which the selected camera image will be aligned.

2. Repeat this process for each of the participating cameras. Additional reference points can be associated with the pictures to improve alignment.
   Various scaling and manipulation options are available in the toolbar above the composition area, to refine the View.
   Position and scale the finished View to take into account that the SceneTracker window can include an active pane that acts as a digital PTZ of the whole scene.
3. When the view is satisfactory, click on **Finish**. This will open a window enabling you to choose the final aspect ratio of the view.
4. Click on **Finish** again.

The final SceneTracker view of this Calibration can be viewed, with the active digital PTZ window, and options for how it should be displayed.
5. Click on **Close** to exit, and click **Finish** to return to the main Calibration window.
Once one or more Calibrations have been completed, all options in the Calibration window are enabled.

6. There can be multiple Calibrations for one SceneTracker view. The same cameras will be available for each calibration (but you may opt not to use all of them for some of the Calibrations, for example, if a camera is out of service, you can define a Calibration will does not use that camera.)

7. Choose one calibration and click on Set Active Calibration. (For each SceneTracker view there must be one Active Calibration)

8. Click on the File icon to save the Calibrations.

### 5.10.13 SNMP

Latitude includes the optional feature of sending SNMP traps to Network Management Systems (NMS).

This is useful for IT administrators who want to monitor the Latitude system in the same way they monitor other systems in their network, using a single, integrated, monitoring solution. In general, Latitude knows how to send traps for every type of event that is available in the software.

**Note:** Latitude does not respond to SNMP queries.
Use Case

In the typical use case the IT organization already has an NMS solution deployed, (e.g. HP OpenView), which is used to monitor multiple sub systems on the IP network of the organization.

Any device or system that supports the SNMP protocol can become an agent of the NMS. In the same way, Latitude with its processes and applications can serve as SNMP agents, and other related components of the Latitude system can also be agents if they support SNMP, for example IP cameras, storage devices, the servers, the workstations, and so on.

In order to make Latitude a part of such a solution, the SNMP feature license should be enabled, and the SNMP feature should be configured in AdminCenter (see below). The IT administrator also needs to configure Latitude as an agent on the NMS, and in order to do that he needs to use the Latitude MIB file which is located under the Latitude installation folder (usually “C:\Program files\<SUPPLIER FOLDER>\MIB\Latitude-MIB.mib”). The configuration of the NMS is not covered here because there are many different solutions with different configuration procedures and options. The end result of a proper configuration would be Latitude sending SNMP traps to the NMS.

General Configuration

To configure SNMP in Latitude (assuming that this licensing feature is enabled) the administrator has to create a new SNMP server in the physical tree of the AdminCenter.

On the Physical Tree, right click on the System entity Add SNMP Manager
**Note:** Multiple SNMP managers can be created in every directory.

A new SNMP manager entity is created
1. In the General tab, under Name and Description define the name and description of the entity and specify the network address.
2. Under Configuration select the SNMP protocol version. In the SNMP version drop-down menu there are two options: SNMPv2 and SNMPv3. To know which version to select consult with the IT administrator in charge of the SNMP manager or NMS.
3. If SNMPv2 was selected, the only other enabled parameter is Community. Unless advised otherwise by the NMS administrator, do not change the default value (public).
4. If SNMPv3 was selected, there are other parameters that can be configured, like User name, Authentication Protocol and Privacy Protocol. In order to decide whether they should be configured and how, please consult with the IT administrator in charge of the NMS system.

**5.10.13.1 Trap Filter**

**Configuring the Trap Filter**

In the Traps Filter page, the administrator can determine which Latitude events will be sent as SNMP traps to the SNMP manager (normally the NMS). Once an event is selected, each time that event is triggered in Latitude, an SNMP trap will be sent to the SNMP manager, with the details of that event.
Notes:
1. There is no way to define that a certain trap type will be sent for some entities and not for others. For example: if ‘Alarm Triggered’ is selected in the filter, it means that a trap will be sent every time an alarm is triggered, for every type of alarm in the system. Similarly it is impossible to configure sending ‘Accessibility recovered/lost’ traps only for some cameras but not for others.
2. The events in the filter are grouped in some cases, such that if a certain type of event has a counter event (e.g. Accessibility lost vs. Accessibility recovered) they must be selected together, or not selected at all.

At the top of the Traps Filter tab, check the **Enable SNMP Traps** check-box

1. In the Application Monitoring panel, use the radio buttons to select that monitoring will be done for servers and/or clients.
2. The selected events appear on the right hand side of the Event Filtering section. Some events are pre-selected by default.
3. You can add event to the selection or remove events from it.
4. When done selecting click the **Save** button

<table>
<thead>
<tr>
<th>Available events</th>
<th>Audited events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility recovered / lost</td>
<td>Admin directory synchronized</td>
</tr>
<tr>
<td>Active Directory activated / deactivated</td>
<td>Application server follower event</td>
</tr>
<tr>
<td>Alarm accepted</td>
<td>Another follower (backup) performed</td>
</tr>
<tr>
<td>Alarm acknowledged</td>
<td>Administering interrupted / resumed</td>
</tr>
<tr>
<td>Alarm activated</td>
<td>ART service accessibility recovered / lost</td>
</tr>
<tr>
<td>Alarm cleared</td>
<td>Background service stopped</td>
</tr>
<tr>
<td>Alarm forwarded</td>
<td>Camera signal status</td>
</tr>
<tr>
<td>Alarm snooped</td>
<td>Case Builder failure</td>
</tr>
<tr>
<td>Alarm triggered</td>
<td>Case do impact failed</td>
</tr>
<tr>
<td>Alarm unaccepted</td>
<td>CaseBuilder storage accessibility recovered / lost</td>
</tr>
<tr>
<td>Analytics - Camera shift</td>
<td>CaseBuilder storage utilization abnormal</td>
</tr>
<tr>
<td>Analytics - Camera shift</td>
<td>Camera storage location detected</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Camera accessibility recovered / lost</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Database accessibility recovered / lost</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Database validation failed / succeeded</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Device IP changed</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Directory breach</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Discovery accessibility recovered / lost</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Failover recording failure occurred</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>PTZ lock overrides</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Server accessibility recovered / lost</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Shutdown failed</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Storage location / backup shared</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Storage location / backup restored</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Storage location was tampered</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>System node recovered</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Temporarily abnormal (back to normal)</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Unit accessibility recovered / lost</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>User login failed</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Vehicle stopped</td>
</tr>
<tr>
<td>Analytics - Advertisement</td>
<td>Vehicle stopped</td>
</tr>
</tbody>
</table>
5.10.14  

**Tile Layout**

**Tile Layouts** allow users to set up predetermined layouts to be used on Control Center Monitors.  

**Note:** Tile Layouts are created and managed in the xx

Creating and Saving Layouts.

Use the **Add Layout** icon in the xx Viewing Pane Toolbar to create a new Layout.

Once a new Layout has been opened, the **Save Layout** icon is enabled. When the user has completed setting up the new Layout (i.e. choosing a tile layout, adding cameras, camera sequences, maps, etc., then the new Layout must be saved so that when it is invoked again, the same content will be available.
6 Configuration - Settings

This section covers the Configuration screens of each of the settings that can be defined in the system.

- Changing IP Address and Computer Name
- Coverages
- Licensing
- Profiles
- Schedules
- Software Components

6.1 Changing IP Address and Computer Name

The Latitude system supports both Computer Name and IP address changes. In general, there is no difference between the two except for the fact that a Computer Name needs to be resolved by either WINS, DNS or the host file.

Using the computer names makes it easier to administer the system when there are IP changes, because the use of IP addresses requires manually changing the addresses in the relevant AdminCenter screens.

Changing Unit IP Addresses

To change the IP addresses of several units:
1. Remove the desired unit from the Archiver.
2. Change the IP address of the unit.
3. Discover the unit(s).
4. Attach the unit to the desired Archiver.

To change the IP addresses of a large number of units:
1. Change the IP addresses of the units via Telnet or the Device Configurator.
2. Change the IP addresses in the AdminCenter.
3. Restart the Archiver.

Changing the Host Names or IP Addresses of Servers

The following process is aimed at systems that are in the installation phase. In case of a live system it might be possible to optimize this process in order to reduce the amount of time that all of the Archivers etc. are down.

To change the host name or IP addresses of servers:
1. Shut down all Latitude applications except for the Directory.
2. Use the AdminCenter to change the Network addresses of the servers to reflect the Host Name/IP address changes.
4. Perform the Computer Name/IP address changes.
5. Delete all FederationHosts.xml files.
6. Check the value of the Server key in the configuration files (i.e. extension .exe.config) of the following applications:
   - **Archiver, Directory, EDB, Gateway, Transcoder**
     a. Configuration files that use the “(local)” convention to denote the host name of the server do not require any changes.
     b. Named references (e.g. `<add key="Server" value=<Systemname/Foldername>`) should be either updated to “(local)” or the new host name.
7. Restart the servers.
8. Use **Safrun** to check that the applications are starting up.
9. Use the **AdminCenter** to check the availability of the Archivers, units, and other components.

**Note:**
1. The Directory’s Network Address must be updated before the change (other servers can also be handled later). Failure to do this will prevent the DB from attaching to the DB after the system is restarted.
2. Changes made to the Computer Name/IP address may take some time to propagate when DNS or WINS are used to resolve them.
   The following commands may be run to update the resolution:
   a. DNS: `ipconfig /registerdns`
   b. WINS: `nbtstat -RR`
3. The Machine ID used for the license is based on the Computer Name of the server running the Directory. Changes to the host name will generate a new Machine ID which will in turn require a new activation of the license to generate a license file with the new Machine ID.
4. Use the Windows search option (i.e “F3”) to find the relevant xml and config files under the relevant directory.

You may access the built-in product manual from any Latitude client/server by launching any of the Latitude applications and pressing the F1 key.

### 6.2 Coverages

A **coverage** is an entity that defines a time span. Along with **super-coverages**, coverages are used as a very common building block when configuring other entities as well as events and actions.

**Coverage**

For each setting type (video, picture and recording settings), only one profile can be defined per coverage. There are 2 predefined coverage settings (Always and Day-time). Customized coverage settings can be added via Coverages in System Settings.

To access Coverages, expand the **System Settings** drop-down menu in the Sidebar, and then select **Coverages**.

To add a coverage, right-click the **Coverages** branch in the **System Settings Root** tree of the **View Selection Pane** and select **Add Coverage**.
The coverage configuration pane is comprised of three sections: Info, which contains the Name and Description fields; Date Range, which is used to specify the Start date and (optional) End date; and Day and Time, which provides a graphical representation of the coverage (the blue boxes). To change the coverage, simply highlight the periods you would like to include in the coverage. To configure a complex coverage, click and hold the Control key while marking multiple sections of the table. You can remove a highlighted period from the coverage by selecting it again.

**Super Coverage**

A super coverage is a coverage defined in terms of other coverages (including super coverages) rather than the basic coverage parameters of dates, days and hours. It is typically used to define periods of time that do not follow weekly cycles, such as Holidays or, conversely, work days.

To access Coverages, expand the System Settings drop-down menu in the Sidebar, and then select Coverages.

To add a super coverage, right-click the Coverages branch in the System Settings Root tree of the View Selection Pane, and select Add Super Coverage.
The pane contains three lists of coverages: positive, negative and available (unused). To add a positive or negative coverage to the super coverage, move it from the available list to the positive or negative list, respectively, using the upper or lower right-arrow buttons. Use the left-arrow buttons to remove a selected positive or negative coverage (and return it to the available coverages list).

### 6.3 Licensing

Details of the license, including real-time usage details, can be viewed in the AdminCenter.

- Go to the AdminCenter
- On the Sidebar, click System Settings
- In the System Settings Navigation window, select License

**Note:** For details of Licensing a system, see below.
License Information
This lists all possible licensed components and features.
**Feature Information column** For each entry, this shows the feature as Not Supported, Supported, Unlimited, or shows the maximum allowed number of licensed instances.
**Usage column** shows the current status for the component/feature ('Not in use', or the number of instances currently in use).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory integration</td>
<td>Enables the option to integrate with Microsoft Active Directory - Supported / Not supported</td>
</tr>
<tr>
<td>Add-on component</td>
<td>Number of permitted Add-On components -- Add-On component licenses will be provided by FLIR Inc with the purchase of engineering service integration modules</td>
</tr>
<tr>
<td>Case Builder</td>
<td>Enables the use of the Case Builder application - Supported / Not supported</td>
</tr>
<tr>
<td>DSF connection</td>
<td>The Direct Show Filter connection - Supported / Not supported</td>
</tr>
<tr>
<td>Failover Directory</td>
<td>The number of failover directory servers in the system, not including the primary directory</td>
</tr>
<tr>
<td>Feature</td>
<td>Comment</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failover video channel</td>
<td>Number of supported camera scenes or analog monitor scenes for which the Archiver failover mechanism is licensed</td>
</tr>
<tr>
<td>GIS Mapping</td>
<td>The GIS Mapping feature - Supported / Not supported</td>
</tr>
<tr>
<td>Global user</td>
<td>Number of global user connection licenses</td>
</tr>
<tr>
<td>Keyboard connection</td>
<td>Number of CCTV Keyboards concurrently configured in the system</td>
</tr>
<tr>
<td>Mobile User</td>
<td>Number of Mobile Users Licensed/Active</td>
</tr>
<tr>
<td>Mobile Video Feed</td>
<td>Number of Mobile Feeds Licensed/Active</td>
</tr>
<tr>
<td>Privacy Masking</td>
<td>Supported / Not supported</td>
</tr>
<tr>
<td>Recorder</td>
<td>Number of supported Recorders</td>
</tr>
<tr>
<td>Redundant Channel</td>
<td>Number of supported camera scenes or analog monitor scenes</td>
</tr>
<tr>
<td>Reporting Tool</td>
<td>Licensed to use Pre-defined Reports - Supported / Not supported</td>
</tr>
<tr>
<td>SceneTracker Channel</td>
<td>Number of SceneTracker user connection licenses</td>
</tr>
<tr>
<td>SDK connection</td>
<td>Number of logins to the Directory server from SDK applications</td>
</tr>
<tr>
<td>SNMP</td>
<td>Enables the administrator to send out SNMP traps to any 3rd party Network Management System and to configure which Latitude events will be sent out as traps - Supported / Not supported</td>
</tr>
<tr>
<td>User session</td>
<td>Number of concurrently active user sessions logged in to the Directory server</td>
</tr>
<tr>
<td>Video channel</td>
<td>Number of supported camera scenes or analog monitor scenes</td>
</tr>
<tr>
<td>Virtual video channel</td>
<td>Number of supported matrix outputs</td>
</tr>
<tr>
<td>Web Client user</td>
<td>Number of concurrently active Web Client sessions logged in to the Directory server</td>
</tr>
</tbody>
</table>

**System Information**

This section shows the Activation Key in use and its Expiration Date, and shows the current server components with their license status.

Selecting a server in the table enables the **Install License** button, which allows the user to add or change licenses, or install licenses on additional servers.
**Licensing a system**

The Licensing process will normally be completed with your representative. Below is a brief overview of the process.

**Getting to the Install License window**

The first time you log on (to an unlicensed system), the system will open the System Settings/Licensing page, and open the Install License window.

If the system is already licensed and you wish to change the license or add a device to the license list, then go to the Systems Settings/License screen, select the device which you wish to license, and click Install License.

This will open the Install License window.

**Get an Activation Key**

In order to install a license, you will need an Activation Key.

This may be

1. Provided by your representative,

2. You (or your integrator) will be invited to register on the Client Portal, to get your keys on the site [https://licensing.flir.com](https://licensing.flir.com)

   The invitation is one-time. Keep a record of the username and password used when you register, so that you can access the site again in the future if needed.

3. Browse to the Client Portal and log in with your username and password.

4. A table will open showing your Activation Key/s.
5. Select the Activation Key to be used

To Generate a License
1. Copy the Activation Key to the Install License window, and click Generate Request.

2. A 'request.txt' file is generated.

3. Save the Request file on your system.

Activating the License File using the Client Portal
1. Go back to the Customer Portal window.
2. Click New Device
3. Click **Browse** and select the request file that was saved.
4. Click **Activate**.
5. A license will be generated and the screen will show a **Download License** Button.
6. Save the file using the Save File dialog.
7. Return to the **Install License** screen
8. Browse to the saved License file.
9. Click **Install License**.

**Licensing Additional Servers or Installing a new license**

When adding additional servers, follow these steps.
1. Right click on the **System** entity and select the server to be added
   (for example, an additional Directory to be used as a Failover Directory, or an additional
   Archiver to control more cameras)

2. Define the new server's address and **Save**.
3. Go to the **System Settings/Licensing** page - the new server will be shown with the
   **IsLicensed** field showing as **False**.
4. Select the server that needs to be licensed, and click **Install License** and follow the in-
   structions above.

**6.4 Profiles**

Profiles are "helper" entities used to simplify and expedite the configuration of other
entities. Profiles are linked to coverage. It is possible to create one profile for each
coverage.
The different profiles are usually added in the respective setting tabs (Video, Picture
and Recording Settings tabs) of a camera in the Physical View. When adding a cov-
erage to a camera, a predefined profile can be selected from the drop-down list or a
profile can be customized. The selected coverage and its profile appear in the Sum-
mary pane of the relevant tab of the Camera entity.

To access generic Profiles directly, expand the System Settings drop-down menu in
the Sidebar, and then select Profiles.

💡 Hint: To see all the entries in the System Setting Tree

To see all Systems Settings entries, use the Filter icon and select No filters.

To add a custom Recording or Video profile, right-click the Profiles branch in the
System Settings Root tree of the View Selection Pane and select Add Recording
Profile or Add Video Profile, respectively. The customized profiles will be access-
ible via the Profile drop-down list of the relevant camera setting tabs.

Note: All possible profiles are listed – The user must check that an appropriate Profile
is chosen.

6.4.1 Picture Profile

A picture profile is used to specify parameters related to how video images are dis-
played. Aside from the standard picture settings such as Saturation and Bright-
ness, you can also specify the amount of Noise Reduction you would like the sys-
tem to perform.
Configuration - Settings

All picture profiles are accessible from the Picture Setting tab of the camera entity. They can be selected from a drop-down list after a coverage type has been selected. Only one profile can be selected for each coverage.

**Note:** All possible profiles are listed – The user must check that an appropriate Profile is chosen.

### 6.4.2 Video Profile

A video profile is used to specify parameters related to how analog video is digitized by an encoder (including the built-in encoder of an IP camera/dome). The profile is used in defining both live video and recording quality schedules. There are a number of pre-configured video profiles with recommended settings for various typical situations, such as full and minimum motion. These cannot be changed but can be used as a reference when creating new video profiles.

All video profiles are accessible from the Video Setting tab of the camera entity. They can be selected from a drop-down list after a coverage type has been selec-
ted. Only one profile can be selected for each coverage. Separate profiles can be defined for live video and recorded video. In order to create separate profiles, the **Recorded quality same as live** check box in the **Recording** tab of the **Settings** pane must be cleared.

In addition, it is possible to add a custom video profile by right-clicking the **Profiles** branch in **System Settings**.

**General**

When creating a video profile via **System Settings**, the **General** tab contains the following information (the Video Settings tab of the camera entity contains the same configuration parameters):

![General tab](image)

This tab is used to configure the following settings:

- **Bit Rate per second** -- The target bandwidth that should be used up by the video stream, in Kbps.
- **Frame Rate per second** -- The number of frames per second, between 1-30 for NTSC and 1-25 PAL.
- **Key Frame Interval (seconds)** -- This setting, also known as the I-Frame Rate, and applicable only to MPEG4 streams, is used to specify the number of seconds between successive frames (or frame areas) that are transmitted by the encoder as full images rather than "delta" functions of the previous frame.
- **Quality** -- This setting is used to specify the image quality of the individual frames.
- **Camera type** -- This non-editable field displays camera type.
- **Estimated storage space** -- This non-editable field displays the estimated storage space necessary for the settings in question.
- **Compression** -- The type of video encoding used.
- **Resolution** -- The resolution of the video image, in CIF or VGA-based units.
- **Rate control mode** -- The rate control mode. Possible values are Automatic or manual.

An encoder may not always be able to produce a video stream that maintains all desired settings. In such cases, it will attempt to find the best compromise between the conflicting requirements.

### 6.4.3 Vendor-Specific Profile

A vendor-specific video profile is used to match the settings of the type of camera in question. The profile is used in defining both live video and recording quality schedules.

The vendor-specific profiles cannot be changed but can be used as a reference when creating new profiles.

The following parameters appear in the profiles, set to match the relevant edge device:

- **Bit Rate** -- The target bandwidth that should be used up by the video stream, in Kbps.
- **Frame Rate** -- The number of frames per second, between 1-30 for NTSC and 1-25 PAL.
- **Key Frame Rate** -- This setting, also known as the I-Frame Rate, and applicable only to MPEG4 streams, is used to specify the number of seconds between successive frames (or frame areas) that are transmitted by the encoder as full images rather than "delta" functions of the previous frame.
- **Quality** -- This setting is used to specify the image quality of the individual frames.
- **Estimated storage space** -- The estimated storage space necessary for this edge device.
- **Compression** -- The type of video encoding used.
- **Resolution** -- The resolution of the video image, in CIF or VGA-based units.
- **Rate control mode** -- The rate control mode, either Constant frame rate or constant bit rate.

### 6.5 Schedules

Schedules are a convenient way to associate a coverage (which answers the question of “when?”) and a profile (“how?”) to multiple applicable entities such as cameras and microphones (“what?”).

**Note:** Using Schedules or Copy Configuration to set up cameras.

- When users want all cameras or some groups of cameras to have the same settings, and to have the possibility of changing settings for all cameras in one place, then Schedules are used. Settings for all cameras associated with a Schedule can be changed by updating the Schedule itself.
- If the users wishes to set up one camera and then just use its settings as a template for others, then the Copy Configuration facility is used. This allows all selected cameras to receive the same settings, but there is no linkage that would allow
all camera settings to be changed together by the user. See Camera, Coverages or Profiles for more information.

Latitude allows the user to attach units to predefined schedules by using the Schedules screen from Systems Settings.

The common procedure is, however, to access the desired camera and select the desired coverage and profile directly in the different Setting tabs. See Camera, Coverages or Profiles for more information.

Four schedule types are used in the system: Picture, Quality of Live Stream, Quality of Recorded Stream and Recording.

When setting up a new Schedule, right-click on Schedules in the System Settings screen. Choose the type of schedule you wish to add from the context menu.

**Note:** Their configuration panes all take the same basic form, with the General tab used to specify a coverage and a profile, and the Attached Entities tab used to apply the schedule to entities.

Schedules are used to associate a coverage (which answers the question of “when?”) to a profile (“how?”) to multiple applicable entities such as cameras and microphones (“what?”). Four schedule types are used in the system: Live Video Quality, Picture, Recording and Recorded Video Quality.

Configuration panes for all Schedule types all take the same basic form, with the General tab used to specify a coverage and a profile, and the Attached Entities tab used to apply the schedule to entities.
6.5.1 Picture Schedule

The picture schedule is used to configure a camera’s picture settings for a particular coverage. Its configuration pane consists of two tabs.

⚠️ If a camera being displayed or recorded is not covered by any picture schedule, it will use the Picture profile by default.

General Tab

The General tab is used to name the schedule, enter an (optional) description for it and select its coverage and profile.

Attached Entities Tab

See Attached Entities
6.5.2 Quality of Live Stream Schedule
The Quality of Live Stream schedule is used to configure a camera’s viewing quality settings for a particular coverage. Its configuration pane consists of two tabs.

⚠️ If a camera being displayed is not covered by any live video schedule, it will use the Normal profile by default.

General
The General tab is used to name the schedule, enter an (optional) description for it and select its coverage and profile.

Attached Entities Tab
See Attached Entities

6.5.3 Quality of Recorded Stream Schedule
The Quality of Recorded Stream schedule is used to configure a camera's recording quality settings for a particular coverage. Its configuration pane consists of two tabs.

⚠️ If a camera being recorded is not covered by any recorded video quality schedule, it will use the Normal profile by default.

General
The General tab is used to name the schedule, enter an (optional) description for it and select its coverage and profile.
6.5.4 Recording Schedule
The recording schedule is used to configure the recording settings of a recordable entity (i.e. camera, microphone, etc.) for a particular coverage. Its configuration pane consists of two tabs.

General
The General tab is used to name the schedule, enter an (optional) description for it and select its coverage and profile.

Attached Entities Tab
See Attached Entities
6.5.5  Attached Entities Tab
The Attached Entities tab is used to attach applicable entities to the schedule. The same structure is used for each of the Schedule types:
- Picture Schedule
- Quality of Live Stream Schedule
- Quality of Recorded Stream Schedule
- Recording Schedule
In the Attached Entities pane, use the arrow buttons to move entities between the Available Entities pane and the Selected Entities pane.

In the Preview pane, you can switch between the different listed entities and preview their live video feed.

6.6  Software Components
The Software Components screen is accessed from Sidebar - System Settings/Software Components
Note:
By clicking on the Grouping Icon, the components will be listed in the groups shown below (i.e. Keyboard drivers, Matrix drivers, PTZ drivers, and Unit drivers.)
If the Grouping Icon is deselected (by clicking again), the list is shown in simple alphabetic order.

The Software Components are the full collection of Plug-ins and drivers used to interface to the different kinds of entities that may connect to the system.

For each component, the Version, Name, and Plug-In Pack version are listed. Where Unit capabilities and/or Defaults are pre-set by the Software Component, these are shown, as in the example of a PTZ driver above.
7 Configuration - Server Components

This section covers the Configuration screens of each of the Server Components that can be defined in the system.

Application Server  Event Distributor (EDB)  Transcoder - Web Publishing
Active Directory  Gateway Server  Web Server Setup
Archiver  Global Admin Server Component  Update Services Server
CaseBuilder  Map Server
Database  Mail Server
Directory  Transcoder

7.1 Application Server

The Application Server is a separate server component that hosts SDK Plug-ins.

The Application Server module is installed by running the Latitude Installation package, and selecting the 'Custom' option. Add a check in the Application Server box.

Click on Change to start the process. A progress bar indicates that the software is being installed.

Once complete, an Application server instance can be added from the Physical View. Right-click on the system icon, and select 'Add Application Server' from the drop-down.

A new Application server icon is added to the tree, with a symbol to indicate that it is still disabled, and the Application Server screen is displayed.

The Application Server's configuration pane contains three tabs, General, Failover and Actions.
General
This tab is used to set the Gateway's Name, optional Description and Host configuration.

When the Network address for the Application Server is entered and the record saved, the Application server icon changes to show that it is enabled.

Failover Tab
The Failover tab allows the user to set separate failover information for the Application servers.
7.2 **Active Directory**

Active Directory integration enables Latitude administrators to centrally manage users.

By using the Active Directory, the administrator can import existing users and user groups instead of having to create a separate set of users and user groups for one or multiple Latitude systems.

In addition, when a new user is added to the organization there is no need to access the Latitude system in order to enable the user to work with Latitude. Configuring the user in the Active Directory configuration suffices. The IT administrator adds the user to one of the existing user groups that is defined both in Latitude and in the Active Directory, thus granting the user permissions of the group. Once added, the users can install Latitude and start working with it seamlessly without the need to log in (assuming that they are logged in to their workstation with their Active Directory user).

- To add an Active Directory entity, access the *Physical View* via the Sidebar, right-click the System icon and then select **Add Active Directory**.
- To connect to the Active Directory, access the *General* tab, enter the connection parameters and click **Activate**.
- To import user groups, access the *Groups* tab, click **Import** and select the desired user groups from the *User Groups* list.
- To import users, access the *Users* tab, click **Import** and select the desired users from the *User Groups* list.
- To set privileges and access rights, go to the *Privileges/Access Rights* tab of the desired user or user group. For more information, see [Privileges and Access Rights](#).

**Note:**
The Active Directory can only be activated when there are no user groups and users defined in the system (except the default Users user groups and the System Admin user). Once the Active Directory is activated, it is impossible to add new users and user groups from within Latitude. They can only be added via the Active Directory entity. This ensures a consistent and reliable user system.

The AdminCenter that configures the Active Directory should be able to communicate directly with the Active Directory. Therefore it is not recommended to configure Active Directory when logged in as a Remote Client.

The Active Directory entity contains the following tabs: General, Groups, Users and Actions.

**General**

The General tab contains the following panes: Name and Description, Connection Parameters, Synchronization and Login.
Information
This pane contains 2 editable fields:
- **Name** -- Enter the name of the Active Directory
- **Description** -- Enter a description - optional.

Connection Parameters
This pane contains the following:
- **Active Directory Network Address** -- The network address of the Active Directory.
- Note that the network address must be a fully qualified DNS name.
- **Port** -- The port of the server on which the Active Directory resides
- **Domain** -- The domain in which the Active Directory resides
- **User name** -- The Windows user name with which the Latitude Directory authenticates against the Active Directory in order to synchronize with it.
- **Password** -- The Windows password of the user who activates the Active Directory
- **Test** -- Click Test to check whether activation parameters enable the activation of the Active Directory
- **Activate/Deactivate** -- Click Activate to activate the Active Directory or Deactivate to disconnect from it.

Synchronization
This pane contains the following:
- **Synchronization Interval** -- How often the Latitude system synchronizes with the Active Directory
- **Automatically Import User** -- Select this check box to import users automatically as they are added to Latitude groups in the Active Directory
- **Last Synchronization Time** -- Displays the last time a synchronization took place

Login
This pane contains the following:
- **Allow Windows Login with Windows Credentials** -- Select this check box to enable users to log in to Latitude using the Windows credentials

User Groups
Via the **User Groups** tab, you can import user groups from the Active Directory into the Latitude.

Users
Via the **Users** tab, you can import users from the Active Directory into the Latitude.
Note: Only users that belong to imported groups can be imported.

**Actions**

See [Events and Actions](#).

### 7.3 Archiver

The Archiver is Latitude’s server component in charge of archiving video, managing units, and proxying video streams between networks (see the System Overview [Archiver](#) section for additional information). Its configuration pane contains the following tabs: [General](#), [Networks](#), [Storage](#), [Redundant Recording](#), [Database](#), [Background Export](#), and [Actions](#).

Latitude allows the user to secure all storage, and to monitor attempts to change Archived data. See [Storage Tampering](#) and [Enable Storage Tampering protection](#).

**General**

The general tab contains the following panes: [Information](#), [Configuration](#), [Failover Configuration](#) and [Child Entities](#).
Information

This pane contains a number of non-editable information fields:

- **Connected** -- Indicates whether the Archiver is communicating with the Directory.
- **Uptime** -- Shows how long the Archiver has been running since it (or its host) was last restarted.
- **Number of supported streams** -- The number of video inputs (i.e. cameras) that the Archiver may be charged with. This value is determined by your license, but is generally never greater than a hundred.
- **State** -- An Archiver's possible states are Active, Failover, Has warnings and Shutdown. Has Warnings indicates there is information available via the Show Detail button. Shutdown state applies to an Archiver that has been intentionally shut down by an administrator.
- **Show Details** -- A button that opens a dialog that provides Archiver Status Check information when the Archiver status shows "has problems". This information is
useful in the initial steps of troubleshooting why an Archiver has problems. For more information, see Archiver Status Check and Notification.

**Configuration**
This pane is used to configure the following parameters:

- **Name** -- The name of the Archiver.
- **Description** -- An optional description of the Archiver.
- **Network address** -- The computer name or IP address of the machine running the Archiver. This field becomes non-editable once the Archiver is first configured.
- **Reported addresses** -- Select from the drop-down list of additional IP addresses that are reported and click Use this to change the network address.

**Failover Configuration**
This pane is used to specify whether the Archiver should act as a failover Archiver. A failover Archiver's **Failover priority** parameter determines which units fail to it under various circumstances. See Archiver Failover for more information.

**Child Entities**
All child entities of the Archiver are listed here. You can perform configuration tasks concurrently on multiple child entities.

See Performing Group Operations for more information.

**Networks**
The **Networks** tab is used to associate networks with the Archiver. An Archiver can only record or otherwise handle streams from units residing in its networks.
To add a network, click the Create button and choose a previously defined network from the drop-down menu that appears under the Name column (the Base Network value is filled automatically by the system).

To remove a network, click its entry in the table and then click the Remove button.

**Storage**

The Storage tab is used to specify and configure the storage locations used by the Archiver and to display the storage usage.

It is possible to define storage on different types of locations - local drive, network map drive and NAS (Network Attached Storage) drive.

**Key storage settings for the Archiver**

Two options set the overall operation of the Archiver:
- **Serve as Media Recorder** - This field is enabled by default. It can be disabled if the user wants to connect cameras that will not be recorded.
  
  **Caution** - if this option is disabled, cameras connected to this Archiver will show warning messages if recording is attempted, and will not be able to be recorded.

- **Tamper-Proof Archiving** - When this field is enabled, Digital Signatures will be generated for all recordings made on this Archiver. This enables the Control Center User to verify that recordings have not been tampered with. (See Query Results Pane in the Control Center Help).

The remaining settings in this tab allow you to:

* Add storage based on system information (recommended)
* Add Network Attached Storage (NAS)
* Phase out storage
* Remove storage
* Set Storage Location for downloaded Edge Recordings
Adding Storage Based on System Information

First add an Archiver and then set the storage. After you finish the initial configuration, you can define the storage of the Archiver. You can define the storage of the Archiver based on system information (recommended) or without preliminary knowledge.

1. To add storage based on system information, wait until your system finishes gathering the information.

   The system information appears, including which drive is recommended for the storage location.

2. Select the desired drive (preferably the recommended drive) from the Drive dropdown list and determine the following parameters:

   ➔ **State** -- This non-editable information field indicates whether the storage is space is configured and available to Latitude.
   ➔ **Path** -- Enter the path of the folder to which you would like to archives.
   ➔ **Storage** -- Enter the amount of disk space that you would like to use for the archives (make sure that the disk has enough free space available).
   ➔ **Container Size** -- The size of the media containers used by the Archiver. Generally, smaller containers provide better performance for systems in which recording is done primarily on events (including manual and alarm-based recording), while larger containers are more efficient in systems that use continuous recording. Please make sure that the container size is set to 80 MB.

3. A warning may appear if the selected Storage is not recommended by the system. This may relate to:
   - the total amount of storage (at least 1000 containers should be available)
   - the blocksize set for the drive/s being used (Blocksize of 64KB is recommended)
   - the arrangement of the drives (IE two storage areas allocated on the same drive)
   - the location of the storage (for example, storage on the C drive is not recommended)

![Warning](image)

4. Click **No** to change your settings as recommended or click **Yes** to continue.

5. When changes have been made to the existing storage, the system will require that the operator performs a manual restart of the Archiver.
Adding Storage without System Information

You can add an Archiver with or without storage. After you finish the initial configuration, you can define the storage of the Archiver. You can define the storage of the Archiver based on system information (recommended) or without preliminary knowledge, as shown below.

1. To add storage without system information, click Add to specify the storage of the Archiver.
2. Fill out the following fields in the row added to the table:
   - **State** -- This non-editable information field indicates whether the storage is space configured and available to Latitude.
   - **Path** -- Enter the path of the folder to which you would like to archives.
   - **Storage** -- Enter the amount of disk space that you would like to use for the archives (make sure that the disk has enough free space available).
   - **Container Size** -- The size of the media containers used by the Archiver. Generally, smaller containers provide better performance for systems in which recording is done primarily on events (including manual and alarm-based recording), while larger containers are more efficient in systems that use continuous recording. Please make sure that the container size is set to 80 MB.
3. Save your settings.

Adding Network Attached Storage (NAS)

Network-attached storage (NAS) is hard disk storage that is set up with its own network address rather than being attached to the local computer. The NAS device is attached to a local area network and assigned an IP address and uses a UNC path.

Since the real-time Archiver (ART) is usually configured for local system access only, its permissions need to be changed to allow for network system access.

The user name of the ART must be configured as one of the users who have permissions to access the NAS by the system administrator based on the local system.

Permissions can be granted in the following ways:
- Granting permissions to all users and then loading the system as usual
- Restricting NAS permissions and setting the ART logon account

Restricting NAS permissions by setting the ART logon account

1. Right-click My Computer and select Manage.
2. Select Services and Applications -- Services, and then right-click the ATS.Archiver.RealTime service and select Properties.
3. In the Properties dialog box, click the Log On tab.
4. Select This account, and set a user name and password of the user who has permission to access the storage.
Note: Define one user only. This user name and password will be used by ART as key to access the storage.
5. Click OK

Storage Phase-Out
A storage location of an Archiver can be phased out before being completely removed. A phased out storage location is read-only and can be restored until the next real-time Archiver (ART) restart. Once the ART has been restarted, a phased out storage is completely removed and cannot be restored. (Phased-out storage may be reactivated before this)
If all storage units of an Archiver are phased out or removed, the Archiver can no longer serve as media recorder. Recordings stored on this Archiver become inaccessible.
The status of the Archiver storage appears in the Storage tab.
Removing Storage

1. Define the Storage Location as Phased Out by selecting the desired storage location and clicking **Phase Out**.
2. Wait long enough until all the remaining available storage re-cycles (e.g. wait for the effective TTL to pass).
   This will cause the clips of the phased out Storage Location to be disconnected from the "live" storage locations.
3. Restart the Archiver (in order to force cutting the clips that exist on the phased out location in case it is defined as always recording).
4. Click **Remove** to remove the Storage Location.
5. Restart the Archiver.

**Note:** *The second restart should take up to 1 extra hour.*

Storage Location for downloaded Edge Recordings

When using Cameras that have Storage-on-the-Edge capability (SOE), the Archiver can recover recordings made during time when communications with the camera have been interrupted. When communications are restored, the Archiver will determine whether the interruption occurred during a time when recordings should have been made. If so, the Archiver downloads the recorded material to a predefined location, and marks the recording trigger as 'Edge' (rather than 'Scheduled', 'Manual', 'Alarm', etc.)

**Note:** *If there were interruptions that affected the Archiver normal functions during this time, the Archiver may download material that would not otherwise have been archived.*

To use this capability, you must define a location to which the Edge Devices can download recordings when communication is restored.

![Enable edge recording download](image)

Check the box **Enable edge recording download**.
Define a location for the storage
Click Test. If the location can be successfully accessed by Latitude, you will get a 'Test Succeeded' message.
Redundant Recording

This tab is used to configure the Archiver to duplicate all recording done by any or all units of other Archivers.

Redundant recording is determined per unit (edge device).

An Archiver is in charge of its own attached units, and then can provide redundant recording of units of other Archivers.

For example, Archiver A can be responsible for units 1, 2 and 3, and at the same time act as redundant Archiver of units 3 and 4 of Archiver B and units 5 and 6 of Archiver C.

Note: In order to use redundant recording, units must have multicast capability, and must be configured as multicast. If you attempt to set up an Archiver to provide redundant recording for units that are defined as unicast, the standard Storage Warning message will be presented, indicating which units must be reconfigured as multicast before the redundant recording setting can be implemented.

Enabling Redundant Recording

1. Access the Redundant Recording tab of Archiver to be used for redundant recording.
2. Select the desired unit(s) which will be recorded by this Archiver from the Available items list and move them to the Attached items list using the arrows. You can select specific units or an entire Archiver.
3. Access each of the scenes of the units added to the redundant recording and set the recording lifespan to the length of time you would like the redundant recordings stored using the Recording lifespan slider.
Note: When selecting an entire Archiver, all units currently attached to that Archiver will be moved to the Attached items list. Any units that will be attached at a later stage are not automatically added to the redundant recording and have to be added manually.

- Redundant recording does not replace the main Archiver’s non-recording functions, such as unit and sequence management. You may therefore wish to configure a failover Archiver as well.
- Redundant archiving supports manual recording.

Database
Latitude provides the end users with the means to view the database size of each of its server applications. For more information, see Database.

Background Export
Background Export allows the administrator to configure schedules for exporting massive amount of recorded video and audio from the primary archiving storage to a secondary storage.
For more information on the Background Export features, see Background Export.

**Actions**

See Events and Actions.

### 7.3.1 Monitoring of Storage Tampering Attempts

Latitude allows the user to monitor attempts to change Archived data. Monitoring can be of a specific Archiver, or system-wide. Once set up, attempts to change data on an Archiver will trigger an Event, which can be used to initiate an appropriate Action.

**Enabling and Disabling Storage Tampering monitoring**

Monitoring of Storage tampering events is activated or deactivated using the check-box Enable storage tampering events in the panel System/Advanced/Maintenance (this check-box is Enabled by default).

**Note:** If the user disables this check box and then re-enables it, monitoring of storage tampering events only resumes after 15 seconds.
7.3.2 Archiver Failover

The purpose of Failover archiving is to increase the availability of the Archiver services. A Failover Archiver is responsible for taking ownership of units from a primary Archiver that fails to function and manage those units, e.g. record them, stream live and archived video from them, provide PTZ and Sequencing services and so on.

Latitude implements a prioritized Archiver failover model that gives a system administrator complete control over how units fail over to other Archivers when the need arises. When an Archiver fails over, the units it controls are distributed to other Archivers based on three criteria: the unit's failover priorities, the failover Archivers' failover priorities, and the failover Archivers' capacities (in the case of camera units only, as each Archiver can control an unlimited amount of other types of entities). Any Archiver can also serve as a Failover Archiver for any primary Archiver, assuming that it is part of the same network since Archiver fail-over only occurs between Archivers on the same network. A failover Archiver can only assume responsibility for units that reside in one of the networks that are configured in the Archiver's network page.

Archiver Capacity

When an Archiver already manages several edge devices, any active camera reduces its available capacity. By setting the **Maximal camera capacity in failover mode** in the Archiver General tab, each Archiver can be set to be responsible for a limited number of cameras.

When an Archiver kicks in as failover, it will assume responsibility for as many edge devices as possible until the 'available units' are all taken up. At this point other failover Archivers, if
they exist, will kick in and continue assuming responsibility for the remaining edge devices from the failing Archiver.

If multiple Archivers have the same failover priority, the system will load-balance between them, trying to split the units of the primary Archiver between them.

**Failed Archiver Indicators - icons**

As part of situation awareness, the AdminCenter provides events and iconic notifications that an Archiver is failing. It allows at-a-glance identification that an Archiver has failed and that a failover situation is currently in place.

This icon notification is triggered by the Archiver Status Check. For more information on the Archiver Status Check, see [Archiver Status Check and Notification](#).

**Archiver Failover Priorities**

The Failover priority of an Archiver, which is set in the General tab of its configuration pane, determines the circumstances under which units from other Archivers may fail over onto it. A unit will always fail over to the highest priority Archiver available to it. Only once this Archiver is working at full capacity (i.e. its Available streams number is equal to zero) will units begin failing over to other failover Archivers until all the Units are in failover mode or until there are no more failover Archivers available. The Failover Priority parameter determines which Archiver is the first to act as Failover Archiver.
Unit Failover Priority

The failover priority of a Unit is directly configurable in the Unit’s General tab using the Priority parameter. During the failover process, a failover Archiver will attempt to assume responsibility for the units with the highest failover priority first, so in case there is not enough capacity to assume responsibility for all the units, the algorithm guarantees that higher failover prioritized units are being served first.

Setting up a Failover Archiver

To set an Archiver to serve as failover, select the Enable failover functionality check box at the bottom of the Archiver General tab in the AdminCenter. You can also set the Failover priority of this Archiver (see Archiver Failover Priority above). At the bottom of the tab you can determine whether failover ends automatically when the primary Archiver is active again (default setting) or not, in case the administrator wants to control such an operation manually.

Failover Groups

It is possible to define a specific Failover Archiver group as the only failover target of a primary Archiver.

For example, if we have a system with two buildings, it is possible to make sure that only Archivers from the same building will serve each other as failover, or in other words, prevent
situations where units from one primary Archiver can failover to an Archiver from the other building. The administrator can define failover groups and assign a single failover group (or none) to any Archiver. When an Archiver fails, its units will only be moved to Archivers belonging to the same failover group (or to any ‘group-less’ Archiver if the failed Archiver does not belong to any group).

7.3.3 Archiver Status Check and Notification
The Archiver server provides a key role for the network video monitoring and archiving. Because this role is so important, the Archiver will notify AdminCenter users if the Archiver is experiencing problems.

An Archiver flashing a yellow alert indicating it has failed a Status Check.

Archiver Status Check
If the Archiver is experiencing problems in the following three areas it will display with a notification icon that alerts the user and helps guide the user/administrator to troubleshoot the problem:

- **Database Accessibility**
  Checks and indicates whether the Archiver can communicate with the SQL database. (E.g. over the network, via the running SQL Services, etc.) If failover is enabled, failover action will be taken.

- **Free Storage Availability**
  Checks and indicates whether the Archiver has available free disk space to write the recordings to. If the Archiver runs out of space and has been configured to stop when the disk space is full, the Archiver will give notice. Although the Archiver cannot continue to record until action is taken, this doesn't represent a failover situation.
• **Storage Accessibility**
  Checks and indicates whether the Archiver can read and write to the specified storage device or media specified. E.g. Problems with the device, network communication to remote storage, no media, removable storage unplugged, storage device offline or turned off, etc. If failover is enabled, failover action will be taken.

When an Archiver fails one of the three checks of a status check, a yellow alert appears on the Archiver and if the actively recording cameras and units/encoders attached to the Archiver are not redirected to a Failover Archiver, they will also show a yellow alert.

**Archiver Notification and Icons**

**The following table shows the icons related to Archiver Check Status failure and their equivalent icons to provide a point of reference for comparison:**

<table>
<thead>
<tr>
<th>Name</th>
<th>OK Status</th>
<th>Archiver Failed (Has warnings)</th>
<th>Archiver Failed with Failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archiver Server</td>
<td></td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Camera</td>
<td></td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>PTZ Camera Recording</td>
<td></td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Camera Recording</td>
<td></td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>

**Archiver Status Check Failed Indicators in AdminCenter**

*Camera List Showing Five Cameras Attached to Archiver that failed a Status Check.*
Archiver Status Check Failed Indicators in ControlCenter

The user of the ControlCenter can be alerted to a problem with the Archiver that is being used for recording cameras. This allows the user to troubleshoot and have awareness that a problem may exist related to the Archiver.

How to view all the cameras that are unable to record due to and Archiver failure (Troubleshooting an Archiver in AdminCenter)

1. From the Latitude AdminCenter Sidebar, click System. The Summary Screen displays in the Dashboard.
2. On the Summary Screen in the Dashboard area, hover the pointer over the Archiver notification to read the tooltip.
3. If the tooltip indicates the Archiver has a problem, click the Archivers link in the Archiver and Storage pane.
The Archiver Status Table displays in the Archiver and Storage pane.

4. From the Archiver Status Table, click on the Archiver entry. A list of attached cameras and devices appears in the table.

5. Scroll through the list and note which Cameras display the Failed Archiver notification and are set for Recording. These are the cameras that currently are attempting to record and cannot. All other cameras that appear "Idle" will not be able to record using the Archiver until the problem is resolved.

**Note:** The status "Recording" only indicates the Camera is suppose to be recording but the failed Archiver notification indicates the device is not being recorded because of the failure. **Note:** There is a delay from the time an Archiver fails or from the time it is restored to all Status OK till the status is refreshed on the user interface. It may take several minutes for the status to update.
How to view the reason an Archiver is failing in the Archiver Status Check dialog (Troubleshooting an Archiver)

1. From the Latitude Sidebar, click Physical View. The Physical View tree appears in the View Selection Pane.
2. From the Physical View tree that appears in the View Selection Pane, click on the Archiver name to display. The selected Archiver settings appear in the View Configuration Pane of the Dashboard.
3. In the View Configuration Pane, if the Status displays "Has Warnings", click Show Details. The Show Details dialog appears.
7.3.4 Export - Background Export

Background Export allows the administrator to configure schedules for exporting large amounts of recorded video and audio from the primary archiving storage to a secondary storage. It is very similar to the way 'Mass Export' works, but offers automation, works incrementally and has some additional options. The exported data is copied into files in a Microsoft Windows folder structure, which later on can be viewed 'offline' using the Latitude ControlCenter client application.

**Note:** Exported data cannot be restored back into the Archiver and cannot become 'online' again.

**Use Cases**

The administrator retains the recorded video on the primary online storage (the archiver's).

In one typical use case, the administrator may want to retain the recorded video on the primary online storage (e.g. the Archiver server internal hard drives) for 14 days, and from there export every recorded file to a secondary storage location (e.g. a SAN device) for another 60 days. In this use case, the system will constantly be exporting files from the primary Archiver, once their time has come to move to the secondary storage. Clips will be recycled from the primary storage soon after they expire (14 days) but it will be possible to locate and playback any clip older than 14 days, up to almost 74 days from the time it was originally recorded, by accessing it through the secondary storage folder structure.

In another use case, the administrator may have slightly different requirements:

The Primary recording retention period should be 30 days, and then another 1 year of retention on tape storage. Moreover, only the daytime footage should be copied to tape, from selected cameras only. In order to achieve this, a tape management system has to work side by side with this Latitude feature. Latitude can be configured to export only the selected cameras, and only in the predefined time coverage, but it has to export the files to hard-drive based storage buffer, before the tape management system can copy this footage to the tape device. For playback purposes, the tape management system also has to provide access to the exported footage for the client application in the form of a standard windows drive.

**Architecture**

The architecture of the background export solution is simple:

The same Archiver server that recorded the video or audio data is responsible for performing the background export.
Configuration

To configure Background Export on an Archiver

1. From Latitude's Admin Center, click the Archiver entity in the Physical View.
2. Select the Background Export tab.
3. In the Background Export dialog box, mark the Enable Background Export checkbox, at the top of the page.
4. Under the Backup Configuration section select the coverage from the drop down list. This coverage determines what footage is going to be exported, in terms of the time it was recorded. New coverage can be created via System Settings - Coverages.
5. Select the cameras and/or Microphones that you want to include in the export.
6. Under **Settings**, define the Export location, which is the path to which the Archiver will export the data. This path has to be a local or a network folder that the Archiver has write permissions to. The System Administrator needs to make sure that the ATS.Archiver.RealTime service on the Archiver machine has a log on account with read/write access to the export folder.
7. Once the Export location has been defined, press the **Test** button right next to it, to check if the Archiver has the access permission required. A message will pop up with the test result:

![Test Successed](image)

8. You can configure storage Quota limitations by checking the **When Quota Exceeds** check-box. Define the storage limit capacity and then select the desired behavior upon reaching the quota: either Delete the oldest set, which means that the Archiver will automatically try to free space by deleting the oldest set, or Suspend exporting until storage space becomes available, which means that the Archiver will periodically check to see if there is available space, and this behavior is recommended if there is another mechanism (or manual procedure) that is responsible to free space in the export location. If storage quota limitations are not defined, the Archiver will attempt to write to the storage location without checking how much storage was already used.
9. You can configure the minimal duration that files should be kept on the primary storage before they can are exported to the secondary storage, by checking the **Postpone export by** check-box and defining the desired duration. If no duration is configured, the Archiver will attempt to export every file as soon as it completed recording it on the Primary storage.
10. Under **Advanced**, you can define the execution time of the export. By default, this is not restricted (Execution coverage = Always), but the you can limit the time window for the Archiver to perform this task, e.g. if there is less activity in the system during the nighttime, background export can be restricted to perform only during that time.
11. Check **Export Player** to include Quick ControlCenter, the stand alone player, with every export set (24 hours of export).
12. Don't forget to click on the **Save** button to apply the settings.
13. At the top of the Background Export tab, the **Status** section provides status information about the background export activity as well as the **Pause** button that can be used to temporarily suspend the export process.

**The Export Sets**

The export data is organized in a particular folder structure, under the export location root folder:
- A folder is created for every 24 hours worth of footage, with the data as the folder name, e.g. 2010-07-17. Such a folder and its underlying folders and files are considered a set.
- Under that folder, each Archiver creates its own folder with the folder name being the Archiver entity name in the system.
- Under each Archiver folder, a folder is being created for each camera or microphone that is included in the export, with the folder name being the camera/microphone name.
- Inside the camera/microphone folder, the actual files are copied, with each file containing the camera/microphone name, and the date and time of the export.

**Reviewing Exported Data**

Once the files are exported to the export storage location, the exported copies are no longer referenced in the Latitude Databases. The exported footage should be regarded as an external copy of the information. Currently, the only way to review this information is by accessing the exported folders and playing back the files using Control Center or Quick Control Center, just like one would playback any other exported clip.

Latitude ControlCenter (or the stand-alone version Quick ControlCenter) supports the following features for reviewing offline content:
- It allows the user to browse folders, as long as these folders are accessible from the local OS (e.g. those folders can be browsed using Windows Explorer)
- It allows the user to open a single audio or video clip for playback
- It allows the user to open a folder, containing multiple clips from the same camera. Because the clips are exported such that each camera has its own folder, the user can easily open such a folder and see up to 24 hours of video on the timeline, as if it was a single clip
- ControlCenter also supports **Synchronized Playback** including regular or smooth reverse playback of footage from multiple sources (audio and/or video)
- Online playback can be set to TCP or UDP protocol
- Playback of an exported clip displays bookmarks that were recorded with it

**Note:** The playback of exported clips does not support advanced on-line options such as smart search, motion indication, or using the query pane for on-line search.

**Deployment with Tape**

Latitude doesn’t support working directly with tape devices. Hence, any deployment of this feature with a tape device requires a Tape Management system that works independently. The shared buffer between both systems (Latitude and the Tape Management system) is the export storage location, which has to be a hard-drive based storage.
7.4 CaseBuilder

The CaseBuilder feature allows a ControlCenter user to collect together materials for investigations and documentation of events that are of interest to the users of the system. For example, collecting all the documentation and video clips of a burglary or accident. This collected content can then be exported into portable files called cases that are compressed and ready to be distributed as needed. For example, sending a case of evidence to the local police.

Note: The CaseBuilder feature requires the installation and addition of the CaseBuilder server to the System system. If you did not install the CaseBuilder when you installed Latitude, you can add it at any time. CaseBuilder can be included or licensed separately. You can check the status of the CaseBuilder license status in the System Settings. For more information, see Licensing.

Note: There can only be one CaseBuilder server per System system.

CaseBuilder Case

A case is a collection of materials the user has grouped together regarding a specific occurrence or matter requiring discussion, decision, or investigation. A case can be saved on the system or exported and opened for viewing.

Example: A CaseBuilder-created case could include a collection of materials, such as video clips that were recorded, snapshots taken by the ControlCenter, the meta data that describes this material, as well as and their meta-data digital files scanned into the computer, document files, still photographs, miscellaneous files, and links to website URLs.

The case may then be stored, and when needed, exported and sent to recipients such as officials or law-enforcement for use as evidence in investigations and prosecution, such as for a court case.

The ControlCenter is the client application of the CaseBuilder and it works with the files saved to the centralized location specified by the CaseBuilder server. Case Builder is useful for creation of cases by collecting and exporting data and Meta data from Latitude and from external sources, to achieve several things:

1. Organize and assemble the information by cases for simplified and focused reviewing process
2. Protect important information – the cases copy of the relevant information can be stored and protected separately to avoid accidental deletions or recycling (overwriting), that can happen to files stored in Archiver locations on the system.

3. Allow easy porting of the cases to remote investigation locations that don't have fully licensed systems Latitude installation, such as courts and police stations.

7.4.1 Cases - CaseBuilder Features

The features of the CaseBuilder allow users to gather together items and put together supporting documentation and video clips into a single entity for research and investigative purposes. A Case can have the following types of contents added to it:

- **Clips**: Archiver Recorded Video Clips
- **Bookmarks**: Existing video bookmarks (with text) and the video before and after the bookmark
- **Incidents**: Information about existing incidents and related content
- **Alarms**: Alarms and the supporting alarm information, descriptions (resolution) and procedures if they exist
- **URLs**: Allows the inclusion of hyperlinks to HTTP content.
- **Snapshots**: Allows the inclusion of snapshots (frame capture to image file) from a clip being viewed in the CaseBuilder Layout.
- **Files**: Allows including user selected files in a case. No restriction on file types. For example, material might include exported DVT files, readme instructions, letters to the user, audio clips, previously captured snapshots (from the Default Layout), etc.

The following image shows the CaseBuilder Mode interface and its features:
For more information about these features, see the CaseBuilder topics in the Control Center Help.

7.4.2 Adding a CaseBuilder Server

The CaseBuilder server (and database) manage cases the user creates. Only one instance of CaseBuilder Server may be defined per System.

See To add a CaseBuilder server.

Note: The CaseBuilder Server will only be shown as available (Available) once the settings are saved and the system has verified that the Shared Path set in the CaseBuilder tab is available, and has full Read/Write permissions.

The Application Server's configuration pane contains four tabs - General, CaseBuilder, Database and Actions.

General Tab

This tab is used to set the CaseBuilder's Name, optional Description and Host configuration.
**Connected**: The Connection Status icon that indicates the server in online, accessible and working or inaccessible.

**Uptime**: Indicates how long the CaseBuilder server has been consecutively online without failure or restart

**Name**: The short descriptive name of this instance of a CaseBuilder server. This description shows in the `<ControlCenter>` and in events and logs

**Description**: An optional description for the server

**Network Address**: The Host name or IP address for communication to the CaseBuilder server

**Reported Address**: The drop-down will indicate alternative addressing for the server, if available
**Case Builder Tab**

**Data Location**

**Path:** This is the path to a shared folder on the network to which the CaseBuilder server has access. It is used for saving CaseBuilder cases.

**Note:** This folder must have Read/write file system permissions set. For more information, see CaseBuilder Data Location Folder Setup.

**Maximum size:** This is the maximum allowable size for storage of cases in the default CaseBuilder data location (folder) as specified in Data Location Path field.

**Data location size:** This is free space of the location specified.

**Cases**

**Processing Cases table**

The Processing Cases table displays all Cases that the ControlCenter clients are *currently* using the CaseBuilder server and database to process. For example, when a Control Center client starts the process of saving a case, the details of the case will appear in the table. As soon as the Save operation is complete, the entry will be removed from the table. Thus, in most cases, the table will be empty.

**Table Headings:**

- **Name:** The short descriptive name of the case.
- **Serial Number:** The unique number that identifies a case
Creator: The user name of the ControlCenter client who created the case.

Creation Time: Creation Date & Time, generated by the server on creation.

Start Time: The time the case processing started

End Time: The time processing ended

Custom Fields

When a Control Center user enters the details of a case, there is provision for entering descriptive information about each case. However, it may be important that the user always enters some general information. To assist in prompting the user to remember to add such information, four custom fields are provided for guiding the Control Center operator to enter specific information as part of a case. Whatever values are provided in this screen for these field contents will appear in the Control Center Case screen as field definitions.

Example of using the Custom Fields

Define the fields in Admin Center

<table>
<thead>
<tr>
<th>Field 1</th>
<th>Agency requesting Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field 2</td>
<td>Branch/Department</td>
</tr>
<tr>
<td>Field 3</td>
<td>External Reference No.</td>
</tr>
<tr>
<td>Field 4</td>
<td>Name of requester</td>
</tr>
</tbody>
</table>

How the fields appear in Control Center

<table>
<thead>
<tr>
<th>Custom Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency requesting Case: Metropolitan Police</td>
</tr>
<tr>
<td>Branch/Department: Florencio Detective Unit</td>
</tr>
<tr>
<td>External Reference No.: Docket 2015/Jan 2015/1389</td>
</tr>
<tr>
<td>Name of requester: Sgt. Waberga</td>
</tr>
</tbody>
</table>

Text entered as data in Custom Fields

Text becomes Field definitions to guide the user

Database Tab

The Database tab displays all the settings related to the SQL or compatible database used to store the CaseBuilder content and related information.

In general, the information in this table is updated by the system, and does not need User input.
**Database name:** The name of the database table that stores the CaseBuilder data. This is complementary data that is coupled with the data components stored in the Data Location Path.

**Database Network Address:** The host name address where the database for the CaseBuilder server resides.

**Use trusted connection:** This setting indicates that the connection to the Database is trusted. Selecting this will disable the use of database authentication settings of Database User Name and Database Password.

**Database User Name:** The user name required for authentication when connecting and using the database.

**Change Password:** Enables the change password field.

**Database Password:** The new password to use.

**Custom Backup Path/Test button:** A setting that allows the enabling and entry of a path which will be used for backup. The test button checks that the destination folder specified allow write privileges. When a user backs up the database to the server, this path will be used. For more information, see [Backing up a Server Database](#).

**Actions tab**

The Actions tab of the CaseBuilder server allows the configuration of event and actions to work together in automating actions for CaseBuilder functionality and more. For more information, see [Events and Actions](#).
To add a CaseBuilder server

1) In the AdminCenter from the Side-Bar menu select Physical View.
2) In the Navigation Tree, right click on the System and from the shortcut menu, select Add a CaseBuilder Server.
   The CaseBuilder server appears in the Navigation Tree with an unavailable CaseBuilder icon (offline).
3) In the General tab do the following:
   a) In the Name field, enter a name for the CaseBuilder server. (It is recommended to include "CaseBuilder" in the name to help users identify the server type.)
   b) Optionally, enter a description.
   c) In the Network Address, enter the domain name or network IP where the server is installed.
      -OR-
      From the Reported address menu, select from the optional networking addressing value that will be viewable in the case files for this location and click Use this.
   d) Click Save.

   You may need to stop (Kill Application) and restart the Casebuilder service using SafRun.
   Continue after the CaseBuilder service restarts,
4) Click the CaseBuilder tab and do the following:
   a) In the Data Location Path field, enter the path to the shared folder to which the Case materials will be written, and click Test.
      A message will appear indicating if the folder location was accessible and writable for the CaseBuilder server. If the test failed, check the path is correct and that full permission to read and write have been granted to everyone.
      Note: This is the location to which the <ControlCenter> clients and the CaseBuilder server will read and write content. If you have not configured a share folder, you will need to do this now.
      For more information, see CaseBuilder Data Location Folder Setup.
   b) In the Maximum size field enter the number and the unit for the maximum size of CaseBuilder storage that can be used at the Data Location Path location.
   c) In the Custom Fields Field 1-4 fields, enter the respective optional descriptive name for each of the fields.
   d) Click Save.

5) Click the Database tab and do the following:
   a) If the Database Connection Configuration correctly identified your database and created the CaseBuilder table, you do not need to change the default values.
      Note: If the values are incorrect, make changes in the appropriate Database name (SQL table), Database network address (the network path) and either select Use Trusted connection, or enter the database login credentials.
   b) If you want the Backup to the server to write to a different location other than the default location, expand the Backup area, select Custom Backup Path. Enter the full path in the Custom Backup Path field and click Test.
   c) Click Save.

6) To configure option Event/Actions, click the Actions tab and configure as needed.
   For more information, see Events and Actions.
Note: You will need to configure CaseBuilder privileges for Users and User Groups as needed. For more information, see Privileges and Access Right Configuration.

7.4.2.1 CaseBuilder Data Location Folder Setup

Before you configure the CaseBuilder server you may need to prepare a folder with the permissions and access needed for the CaseBuilder server to write to when the ControlCenter clients create cases. If you are not sure or do not have privileges to the files system to create folders, grant permissions and sharing, contact your system IT administrator for assistance.

A Shared folder must be configured so that it can be accessed from the machine on which the CaseBuilder server is operating. The folder needs to be specified as Share with full permissions for the server (everyone users) for any client.

The following is an example of creating and changing permissions on a Share folder

1. Open Windows Explorer and navigate to the location where you want to create the folder.
2. From the main menu, select File ► New ► Folder.
   A new folder appears in the file system with the folder name selected for editing.
3. Type the name of the folder and press Enter.
   The folder name is applied.
4. Right mouse-click on the folder and select Properties.
   The properties dialog appears.
5. In the properties dialog do the following:
   a. Click the Sharing tab and in the Sharing tab, select Share this folder.
   b. In the Sharing tab, click Permissions.
      The permissions dialog appears.
   c. In the permissions dialog, select the Group Everyone, then mark Allow next to Full control and click OK.
   d. In the Properties dialog, click OK.

7.5 Database

Latitude provides the end users with the means to view the database size of each of its server applications.
For backing up a Database, see Backing Up a Server Database

In the Archiver/Database tab, clicking on the Database component entry displays a table of the space available and occupied for the selected type of data.
The statistics or pie chart of the used space of the data file and log file can be accessed by selecting each from the mini-tree in the left Information pane.
Use the Legend to interpret the respective color-coded slices of the pie chart representation of database allocation and used sizes.

### 7.5.1 Backing Up a Server Database

You can backup a Server Database to a local drive or associated server. When you back up to a local drive, you can browse and enter a path to write the backup files to. When you select backup to a server, the default backup path or custom backup path as specified in the Database tab of the server will be used.

**To Backup a Server Database Locally**

1. In the AdminCenter from the Side-Bar menu select Physical View.
2. In the Navigation Tree, right click on the server (in this example it is a Directory server) and from the shortcut menu, select *Backup database on the local machine*. The Client side database backup dialog appears.

3. In the Client side database backup dialog, do the following:
   a. If you want to change the default backup file name, in the File name field type a file name for the backup file.
   b. In the Path field, enter the path to the location where you want the backup file written to or click Browse and in the Browser for Path dialog that appears, select the folder you want to use and click OK.
   c. In the Client side database backup dialog, click **OK**. A progress indicator appears and when finished, a backup complete prompt appears.
d. In the Backup Complete dialog, click OK.

**To Backup a Server Database to the Server**

1. In the AdminCenter from the Side-Bar menu select Physical View.
2. In the Navigation Tree, right click on the server and from the shortcut menu, select Backup database on the server.
   The Backup database on the server dialog appears.
3. In the Backup database on the server dialog, do the following:
   a. If you want to change the default backup file name, in the File name field type a file name for the backup file.
   b. In the Backup database on the server dialog, click **OK**.
      A progress indicator appears and when finished, a backup complete prompt appears showing the path to the backup.
c. In the Database backup on the server dialog, click **OK**.

### 7.6 Directory

The Directory is the final arbiter of control in an Latitude system, charged with managing access to the various applications and maintaining a repository of all system settings (see the System Overview Directory section for additional information). Its configuration pane contains four tabs: **General**, **Failover**, **Database** and **Actions**.

#### General

The **General** tab consists of two panels: **Information** and **Configuration**.

#### Information

This section contains non-editable information fields:

- **Connected** -- Indicates whether the Directory is running.
- **Uptime** -- Shows how long the Directory has been running since it (or its host) was last restarted.
- **State** -- Indicates whether the Directory is acting as the Primary or Failover Directory.
- **Is Licensed** -- Indicates whether or not there is a license for the directory.

#### Configuration

This section is used to configure the following parameters:

- **Name** -- The name of the Directory entity.
- **Description** -- An optional description of the entity.
- **Network address** -- The computer name or IP address of the machine running the Directory. This field becomes non-editable once the Directory is first configured.
Failover

This tab is used to enable the Directory for failover and set its failover priority. When the primary Directory fails, the highest priority non-primary Directory becomes primary. The tab also provides information about when the Directory's state last changed and when it was last synchronized.

Database

The Database tab displays informational fields about whether the database is valid and when its validity was last checked.

Action

See Events and Actions.

7.6.1 Directory Failover

The purpose of a Failover Directory is to increase the availability of the Directory services. A Failover Directory is responsible for taking ownership of entities from a primary Directory that fails to function and manage those entities.

Latitude implements a prioritized Directory failover model that gives a system administrator complete control over how units fail over to other Directories when the need arises. When the primary Directory fails, the highest priority non-primary Directory becomes primary. Failback occurs when the Archiver is backed up.

You must obtain and activate a license for a Failover Directory.
**Directory Failover Priorities**

The Failover priority of a Directory is set in the Failover tab of its configuration pane. The priority determines the circumstances under which units from other Directories may fail over onto it. An entity will always fail over to the highest priority Directory available to it.

**Note on Synchronization:**

*Failover Directory Automatically invoked* - The primary Directory database is backed up automatically, according to the schedule defined in the Directory Backup Schedule panel of the System/General screen. In the event of a failure of a Directory, a Failover Directory (if one exists) will be invoked automatically, and will use the most up-to-date backup of the Directory database.

*Manually switching to Failover Directory* - If an operator wishes to take a Directory out of service (i.e. for maintenance or replacement etc.), then the 'Unchanged since last synchronization' field will indicate whether the saved database is up to date and the change can be undertaken, or whether the operator should first manually synchronize the database before making the change.

*Last successful / Last failed synchronization* - When manually switching between the Directory and a Failover Directory, these fields allow the user to check whether the database has captured recent changes before proceeding.

**7.7 Event Distributor (EDB)**

The Event Distributor is used as an interface for passing events and actions between different Latitude components, as well as between the system and external devices and programs. For more information on the Event Distributor, see Overview of the Event.

**7.8 Gateway Server**

The Gateway Server is an intermediary between client stations connected from outside the LAN and the rest of the server applications. Since remote clients can only receive media content from the Transcoder, the two applications work closely (and are often installed on a single server).
By default, the Gateway Server uses port 7777. The port used by the Gateway, along with the one used by the Transcoder, must be opened on any firewall protecting the network.

The Gateway Server's configuration pane contains three tabs, **General, Mobile Viewing, TruWitness** and **Actions**.

### General

The General tab consists of two panels:

**Information**

The three fields in this panel show the current connectivity status.

**Configuration**

The user can set a name and description for the Gateway.

- **Name** - The name of the Gateway Server.
- **Description** - An optional description of the Gateway Server.
- **Network address** - The computer name or IP address of the machine running the Gateway Server. This field becomes non-editable once the Gateway Server is first configured.
- **Reported addresses** - Select from the drop-down list of additional IP addresses that are reported and click Use this to change the network address.

### Mobile Viewing

Here, the user configures how the application communicates with devices using the mobile application.
TruWitness
This pane is used to set up connections for the TruWitness Android/iOS feature.

Actions
See Events and Actions.
7.9 Global Admin Server Component

The Global Admin Server, if available in your system, is a separate server set up to allow multiple Latitude systems to share User and User Groups. This means that a user or user group may be created on any of the connected systems, and that the credentials of that user or group will be valid on all of the connected systems.

Installing and Configuring the Global Admin Server

1. Set up the Global Admin server
   Run the application `GlobalAdminServer_x.x..exe`, and follow the instructions provided in the InstallShield.
   Once a server has had the software installed, and is connected to the network, continue with the steps below.

2. Configure the Global Admin server
   Using the Physical View, right-click on the System icon to open the Context menu, and select Add Global Admin Server.

   ![Add Global Admin Server](image)

   The Global Admin Server page is opened.
3. The user may provide a **Name** and **Description**.
4. Enter the **Connection Parameters** for the Global Admin Server.
   a. **Global Server Network Address** - The network address of the server must be entered.
   b. **User Name, Password** - The user name and password allowing remote access to the computer running the Global Admin Server application must be entered.

   **Important Note:** This User Name/Password pair is stored on the local machine, and used to establish connection to the Global Admin server. If the user changes these credentials on the local machine, connection to the Global Admin Server will be lost unless the corresponding credentials are changed on that machine. There is no automatic update.

5. Click the **Save** icon to update these parameters in the system.
6. Test the connection by clicking the **Test Server** button.

   **Note:** The Test button is not enabled until the user completes the above steps and the information is updated in the system.

   The system will signal a successful test or give a relevant error message.
7. The user may optionally change the **Synchronization** setting. If it is changed, the new setting must be **saved**.
8. Once the Global Admin Server is set up and running, User and User Groups can be set to **Global** using the **User** and **User Group** pages.

   Subsequent changes to the Global Admin Server parameters can be made by accessing the server from the Sidebar **Physical View** setting.
Global Server Test Error Messages

<table>
<thead>
<tr>
<th>Condition</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized</td>
<td>Username/Password incorrect – Please check your credentials.</td>
</tr>
<tr>
<td>Internal Server Error</td>
<td>Global Admin Server internal error. Please contact your administrator.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Global Admin Server timeout. Please check that the server is up and that it is accessible via the network.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Global Admin Server is inaccessible. Please check that the server is up and that it is accessible via the network.</td>
</tr>
</tbody>
</table>

7.10 Map Server

The Map Server is a separately-licensed component that allows the user to define GIS-based maps and link them to the system. The maps can show the position of system entities using Google Maps. This can include displaying the position of alarms and, when using the TruWitness mobile phone application, to show the position of mobile phones/cameras that are connected to the system, display alarms generated from those mobile phones, and preview live video or playback from those devices.

Installing and configuring the Map Server

The Map Server is not a separate entity like Archiver or Directory – it runs as part of the Web Services running under the Windows Internet Information Server (IIS) component.

In order to run the Map Server, the user must have an appropriate License, and the Mapping Services Server must be installed using the Custom Installation process, by checking the appropriate box in the Custom Setup Dialog box.
The Mapping Services Server is normally installed on the Directory Server, but a different host can be chosen - see System Entity/Advanced/Mapping Services).

Full information on installing and configuring the Mapping Services Server is given in the Latitude 6.3 Release Notes.

### 7.11 Mail Server

The mail server is responsible for dispatching notifications when actions or events occur.

In order to enable email notifications, a mail server and a user with a valid email address must be defined. In addition, email notification must be defined in the desired action or event.

You can only define one mail server for each system.

**Defining a Mail Server**

1. Click the **Physical View** button in the Sidebar.
2. Right-click the desired system, and then select **Add Mail server.**
3. In the **Configuration Pane**, define the name, SMTP server, SMTP port and sender address of your mail server.
Defining an Email Notification

See Actions/Send Email

7.12 Transcoder

The Transcoder is a server application that trans-codes the MPEG4 video generated by encoders/IP cameras (and archived by Latitude) to standards-compliant MJPG-over-HTP and standard video streams over RTSP/TCP, for transmission over the Internet. Like the other Latitude server application, it runs as a Windows service and can be stopped or started using the Safrun watchdog application.

The Transcoder is particularly useful in providing good quality video images over limited bandwidth connections. Typically, there will be three main uses for the Transcoder:

- **Video streaming to Remote Clients who connect through the Gateway**
- **Video streaming to remote networks in 'Mixed mode'**
- **Video streaming to Web Clients**

**Video Streaming to Remote Clients That Connect Through the Gateway**

Remote Clients are client applications that are connected to the system through the Gateway server, instead of connecting directly to the directory.

In this mode, video streams requested by such remote clients will always be provided by the Transcoder.
Video Streaming to Remote Networks in ‘Mixed Mode’

In this mode, the system is usually comprised of multiple networks, with cameras and Archivers.

If some of the network connections have limited bandwidth, the administrator can add Transcoders to support good quality video transmission over those connections.

When the check-box 'Enable Dynamic Transcoding' on the System/General Tab’s Video panel is checked, then, upon request for a stream from a client, the system will determine whether the video should be sent through the Transcoder or directly from the Archiver (or from a multicast camera). The client application will receive video from Transcoders if the source of the video is located over a connection that is not part of the Archiver’s network list, but still receive it directly where the requesting client is part of the list.

Video Streaming to Web Clients

Web Clients can receive live or recorded video from a transcoder. In the case of multiple transcoders, allocation of a transcoder is the same as for Mixed Mode (above).

Transcoder Configuration Pane

The Transcoder configuration pane contains the following tabs: General, Archivers, Capture Devices, and Actions.
General

- **Information** - provides information about the current state of the Transcoder
- **Server configuration** - allows setting the Transcoder settings
- **Transcoded stream configuration** – controls the output characteristics of the Transcoder
- **Global performance limits** – set parameters that will limit the load imposed by the transcoder on other processes that may be running on the same server (i.e. in an All-in-One installation).

Aside from **Name** and the optional **Description**, the Transcoder's configurable parameters are in the following panels:

**Server Configuration**

- **Network Address** -- The IP address of the computer on which the Transcoder resides.
• **External IP** -- The external IP address at which the Transcoder can be accessed if different from that of the Gateway Server (if the two use the same external IP address, this field can be left blank).

• **External Port** -- **Internal Port** -- These are the ports used by the system to communicate with the Transcoder. Both must be set to the same port.

• **Secured Port** -- This port is assigned for encrypted communications with Web Clients

• **RTSP Port** -- For connecting to the transcoder when requesting a stream over RTSP protocol

• **Default Transcoder** -- Select the check box if the Transcoder acts as default transcoder.

**Transcoded Stream Configuration**

• **Compression Quality** -- The relative accuracy of the JPEG encoding (from the original MPEG4 video)

• **Default Transcoder** -- Select the check box if the Transcoder acts as default transcoder.

• **Default Quality** -- The relative accuracy of the JPEG encoding (from the original MPEG4 video).

• **Maximum Frame Rate** -- The maximum total frame rate for each video stream trans-coded by the Transcoder.

• **Maximum Resolution** -- The maximum resolution of the trans-coded video stream (streams with higher resolutions are "trans-coded down").

• **Compression** -- The compressed format that this transcoder will output - H264, MJPEG, or MPEG4

**Global Performance Limits**

![Global performance limits](image)

• **Total CPU % Limit** - Threshold value for Transcoder loading. Default value 60%.

• **Check-box: 'Above limit, enable 'Key Frame only' mode. Default status Disabled (unchecked). See Transcoder CPU Power Saver mode**

• **Max. concurrent trans-coded frames per second** – the maximum number of frames per second that the Transcoder may encode and send to the client. Default value 180.

• **Max. concurrent client streams** – maximum number of client streams that may be served by the Transcoder at once. Default value 20.

**CPU Power Saver Mode**

Transcoding video is a CPU-intensive task, which can lead to overloading the server running the transcoding function. In an 'All-in-One' configuration, this can degrade the performance of the whole system. The Latitude system provides two ways to protect the system from such overloading. The check-box 'Above limit, enable "Key-Frame only" mode' allows the user to set which method to use.
• **Default mode** - When total CPU % limit is exceeded, further requests are declined. (Default behavior)
  The following message is displayed:
  "Transcoder service has passed the CPU limit".

• **Key-Frame only Mode** - When Total CPU % limit is exceeded, the Transcoder will start changing the mode of transcoded sessions, and it starts moving existing transcoded sessions to 'key-frame-only' mode, starting with the latest session. The Transcoder will stop moving sessions to that mode, once the CPU loading goes below the CPU % limit.

**Notes:**
1. When using the CPU Limit option, all units connected to the affected Transcoder should have their Key Frame Interval set as low as possible in order to get adequate video quality (i.e. 1 fps).
2. If a new request for a scene that is already being transcoded is made, and the limit is exceeded, any existing streams of that scene will also be limited to 'key frames only'. This can have the result that a user who is watching a scene will see it change to 'key frames only', and motion in the scene will not be shown smoothly.
3. Streams being output in 'key frame only' mode remain in that mode. Only by reducing the Transcoder load until it is below the Total CPU % limit and then restarting those streams will they return to normal mode.
4. Users should keep in mind that 'key-frame-only' mode may be applied to exported streams.
5. CPU Limit Setting is per Transcoder, not global.

**Archivers**

This tab contains two panes -- the **Archivers** pane and the **Summary** pane.

In the **Archivers** pane, all existing Archivers in the system are listed and can be attached to the Transcoder.

Each Archiver should be attached to a Transcoder to ensure the transcoding of video streams both for internal and remote clients.

The **Summary** pane lists all attached Archivers and the Transcoders to which they are attached.
To attach an Archiver to the Transcoder
1. In the Archivers tab, select the desired Archiver from the list of Available Items
2. Click the arrows to move the Archiver to the Attached Items list.
3. Save your settings.

Capture Devices
The Transcoder Capture Devices tab allows the user to create Capture Device definitions for any available video source. It consists of two panels:
- **CaptureDevicesProperties** - the Transcoder general settings related to the CaptureDevice feature.
- **Selected Cameras** - select cameras/sources to be defined as Capture Devices
CaptureDevicesProperties pane

Two parameters may be set:

- **Serve as Streaming Server** - Enable / disable the Transcoder functionality that allows working with Capture Devices.
- **Should Run Batch** - Enable / disable the execution of the Command lines in the “Selected Cameras” grid

Selected Cameras pane

Cameras/sources that are available to be defined as Capture devices are shown in the left-hand column. Sources that are not available are shown as grayed out. Select the source/s by clicking on them and then clicking on the right-hand arrow to move them to the Capture Devices table on the right.

Once a camera is added, enter a Publish name that will be used as a label in the published content and any Command Line start commands for third party broadcast-
ing applications. These devices then become available to the client machine. Capture Devices that have been defined may be removed by selecting them in the right-hand column and clicking the left arrow.

**Actions**
See [Events and Actions](#).

### 7.13 Transcoder - Web Publishing

Latitude Web publishing enables streaming of live video from Latitude cameras to external (non-Latitude) video over TCP/IP without requiring the end-users to run Latitude client application or SDK applications. Latitude can now interface with common Media publishing software solutions, allowing them to receive live video from Latitude and transmit it to their clients. Examples of Media publishing software are Microsoft Expression Encoder 4, VLC, and legacy version of Windows Media Encoder.

![Diagram of Transcoding Process](image)

**Applications**

- **Web publishing**, e.g. end users connecting to a public web site to read traffic reports and view traffic cameras. The video from the traffic cameras comes from a Windows Media Encoder/Server, which acquires the video stream from Latitude. Note that the users do not need to login to Latitude or be defined as Latitude users and other than viewing the live stream, they have no control over the camera (PTZ, Playback).

- **Provide 'common' or 'standard' video streams to 3rd party systems**, e.g. video analytics engines that can only analyze specific type of video streams, receive the video from the Media publishing software rather than directly from Latitude. Most Media publishing solutions are capable of 'Transcoding' the video form one format to another as well as providing the stream in various streaming methods (HTTP, RTP) but for specific details it is best to consult with the specific media publishing software documentation.

**Note:**

1. FLIR Inc is only responsible for the functionality of the interface with the Media publishing software, since there are many different Media publishing solutions available in the market, each with various features, options and configuration requirements, it is then the responsibility of the end-user to find out which Media publishing solution meets his or her requirements and to learn how to deploy and configure the Media publishing solution.

2. Video with Privacy Mask configured will include the mask embedded in the image at the Transcoder and cannot be disabled from the streaming video.
Basic Configuration
For an overview of Transcoder modes and settings, see the Transcoder section.

1. In order to enable web publishing the system should have 1 or more Transcoder servers configured.

2. A Transcoder can possibly publish any of the cameras in the system, but if the Transcoder was assigned to specific Archivers, it can publish cameras only from those Archivers. To assign the Transcoder to specific Archivers use the Archiver Tab of the Transcoder entity.

3. To publish cameras, go to the Transcoder Capture Devices tab and do the following:
   a. Under the Capture Devices Properties section mark the Serve as Streaming Server check box.
   b. Under the Selected Cameras section select the cameras that you want to publish.
   c. Click Save.

At this point the Transcoder creates the ‘Capture Device’ elements for each camera selected.
Now, in order to stream that camera the administrator is required to configure the Media publishing solution and use the ‘Capture Devices’ that were created by the Archiver.

**Advanced Configuration**

Since the Transcoder is a service and is monitored by Safrun, it is considered robust. For example it will automatically resume after the server went through a power cycle. However, some of the Media publishing solutions are just simple applications which will not resume automatically upon restart, so the Capture Devices tab in AdminCenter offers a helper: the ability to create a command line script that the Transcoder will execute every time it initializes. You can enter the command line script in the Command Line column, for every camera that appears in the Selected Cameras table under the Capture Devices tab.

Because the Transcoder automatically runs the Command Line on start-up, you may want to create a batch file and call it by `pathname`. The batch file can contain multiple commands that close any existing instance of your chosen application for encoding the broadcast streams. A `bat` file can be created with Notepad and saved with an extension `".bat"`.

For example the following instructions are represented in the example that follows:

1. send a stop (kill) signal to associated
2. pause for 10 seconds to wait for devices to become available again
3. run a second stop to force quit
4. start the encoding

   Taskkill /im encoder.exe /t
   Choice /t 10 /c ync /d y
   Taskkill /im encoder.exe
   "C:\Program Files\Microsoft Expression\Encoder 4\Encoder.exe" "C:\Users\josh\Documents\Expression\Expression Encoder\Jobs\Camera 2 streaming.xej"

   The command line definition itself depends on the Media Publishing solution. Two examples are provided below.

**Publishing with Microsoft Expression Encoder 4**

Download and install Microsoft Expression Encoder and any needed prerequisites. This example, assumes you have added a Transcoder in the AdminCenter and that you have configured one or more camera scenes in the Capture Devices tab and saved your settings.

In this example you will:
1. Create a live broadcast project and save it.
   This will identify the streaming settings for the Transcoder camera you select.
2. Modify the saved live broadcast project.
   This will change the project file for automation to start when opened rather than requiring manual clicking of Start by a user.. If you do not modify this, the Transcoder call will only open the application but encoding will not start without human intervention.
3. Enter the command line in the Transcoder.
   Configure the Transcoder that when it starts (or restarts) to run your live broadcast project (to go online)
To Create a Live Broadcast Project

1. Run the Microsoft Expression Encoder 4 application and on the splash dialog click **Live Broadcast Project**.
2. In the Preview window, click **Add a Live Source**.
   A Live source window will appear in the Live Source panel.
3. On the Live Source panel, click the **Video Device** menu arrow, select the camera (Capture Device) that you want to use for your video source, and then click **Cue**.
   The live video appears in the Live source video window.
4. On the Presets panel, expand the nodes of either **Standard Encoding** or **Wide screen encoding**, select the type of encoding you want and click **Apply**.
   **Note**: If you hover the mouse over the options, the encoding parameter default values are displayed.
5. If not already displayed, click the Output tab and then mark to enable **Streaming**.
6. In the streaming options, select **Broadcast** and modify the values for Ports and Max Connections as needed.
7. In the Preview pane, click **Start** and in the Output tab, click **Launch Preview**.
   The streaming video link opens in the default web-browser and displays the streaming video.
   **Note**: If prompted, allow installation of browser components.
8. In Microsoft Expression Encoder 4, click **File>Save As** and in the dialog that appears, enter the name you want to save the project as.

To modify a live broadcast project to auto-start encoding

1. Locate the xej live broadcast file on your file system and open it in Notepad or similar text editor.
2. Go to line of the project file that has the text **AutoStart="False"** and change the to **AutoStart="True"**.
3. Save changes and close the file.
   Now every time the file is opened it will automatically start encoding.

**Entering the command line in the Transcoder for a Microsoft Expression Encoder 4 live broadcast**

1. In AdminCenter, on the Side Bar, click **Physical View**.
2. In the Navigation Tree, click the Transcoder the capture device you selected for your live broadcast project.
   The General Tab settings for the Transcoder appear.
3. Click the **Capture Devices** tab.
   The Capture Devices settings appear in the display area.
4. In the **Selected Cameras** table, click the **Command Line** field for the camera (Capture device) and enter the Microsoft Expression Encoder 4 command line for calling the modified xej project file. Use the following syntax:
   
   ```
   [path encoder.exe] [path xej file]
   ```

   Where `[path encoder.exe]` is the full path to the Microsoft Expression Encoder 4 executable file and `[path xej file]` is the full path to the Microsoft Expression Encoder 4 Broadcast Project file. Use quote marks if there are spaces in the file path and file name.

   For example:
   ```
   "C:\Program Files\Microsoft Expression\Encoder 4\Encoder.exe" "C\camera 1 my-broadcast.xej"
   ```

**Publishing with Windows Media Encoder 9**

This shows how to publish a single camera using Windows Media Encoder 9, and view it using Windows Media Player.

**Note:** In this example we will install WME (Windows Media Encoder) on the same machine with the Transcoder Service.

If you do not already have a legacy copy of Windows Media Encoder, you may be able to download it from [here](#).
Install WME follow the simple installation instructions (use defaults)

   If the New Session Wizard does not appear, click New Session.

2. In the New Session Wizard, double-click Broadcast a live event.

3. In the Device Options screen, if not selected, select Video. From the menu, choose the capture device name as you configured it in the Transcoder settings and click Next. (Transcoder does not support audio - deselect it)
   If you do not see the capture device in the options, make sure you saved your settings in the AdminCenter and that the local servers are running.

4. In the Broadcast Method screen, select Pull from the encoder (indicates the server or the player will initiate the connection) and click Next.

5. In the Broadcast Connection screen, if you need to use a specific port, enter the new port number in the HTTP port field, and click Next.
   The Encoder Options screen appears.

6. In the Encoder options dialog, do the following:
   a. From the Video menu, select the option category for the type of purpose you will be streaming for.
      The Bit rate table will update options based on this selection.
   b. In the Bit Rate list, select the option that best suits your bit rate, frame rate and resolution (output size) for the stream you want, clear any settings you do not want, and then click Finish.
      Note If you do not see the resolution you want, return to step a) and check other menu options.

   These settings can be adjusted and even cropped in the Video Size tab of the Properties screens after you create the session file for this procedure.

   Caution: In order to make this a completely automated encoding (our goal) and to avoid the need for human intervention, you should avoid encoding to a file.
   Because the session file only allows specifying a static video file name to write to, the auto run feature will not start encoding because a prompt opens asking if you want to overwrite the existing file. On this prompt you will need to select "Don't show me this again".
   Additionally, if you are streaming for long periods using default settings, these files can consume the memory of the local machine and create large unmanageable files.

7. Click Start Encoding.

8. Open a video player that supports streaming from a URL.
   For example: Open Windows Media Player, right click on the navigation header and select File > Open URL. In the dialog that appears enter your computer IP, the streaming port you entered in the wizard in an HTTP URL.
9. In Windows Media Encoder, click **File > Save** as and in the Save As dialog, enter the file name and click **Save**.

**Entering the command line in the Transcoder for a Windows Media Encoder 9 live broadcast**

1. In AdminCenter, on the Side Bar, click **Physical View**.
2. In the **Navigation Tree**, click the Transcoder of the capture device you selected for your live broadcast project.
   The General Tab settings for the Transcoder appears.
3. Click the **Capture Devices** tab.
   The Capture Devices settings appear in the display area.
4. In the **Selected Cameras** table, click the Command Line field for the camera (Capture device) and enter the Windows Media Encoder command line for calling the modified wme project file. Use the following syntax:
   
   \[ \text{[path \text{wmenc.exe}] [path \text{wme file}] /Start} \]
   
   where \[ \text{[path \text{wmenc.exe}] is the full path to the Microsoft Media Encoder 9 Series executable file, [path \text{wme file}] is the full path to the Windows Media Encoder saved session file and /Start is the command line switch that tells the encoder to open and automatically start encoding immediately without user intervention. Use quote marks if their are spaces in the file path and file name.} \]
   
   For example:
   
   "\text{C:\Program Files\Windows Media Components\Encoder\wmenc.exe} "\text{C:\camera 1 my-broadcast.wme}} /Start"}

### 7.14 Web Server Setup

United VMS 8.0.5 The Web Server is not a separate entity like Archiver or Directory – it refers to the Windows Internet Information Server (IIS) component. This is added automatically during an All in One installation, or the component may be checked in the list of components to be installed during a Custom installation.
The Web Server entry in the Admin Center allows the system to take advantage of the ability to rename the Web server, and to assign it to an alternative port. These steps may be required when other Web Servers are in use for other applications.

### Web Server

The default Web Server entry is shown below, with the virtual directory as defined during IIS setup.

![Web Server GUI](image)

Should the user wish to use a different virtual directory setting, this can be done by changing the virtual directory name, or by removing the use of a virtual directory all together by un-checking the **Web site is located in a virtual directory** check-box.

![Virtual Directory Configuration](image)

### IIS Setup

The IIS is normally set up by the installation process in a specific path in the Web Client virtual directory (application). This is done in the **Internet Information Services (IIS) Manager** screen.

(Windows Control Panel ▶ All Control Panel Items ▶ Administrative Tools ▶ Internet Information Services (IIS) Manager)
7.15 Update Services Server

The Update Services Server provides a central location from which client applications may download new versions of the Latitude software when required, and install them automatically.

In the event of new major releases of Latitude being installed, any computers running the client applications Admin Center and Control Center will indicate that the main system is running new software. Operators of the client applications can then request that the updated client applications be downloaded to their machines. The process is run automatically, and the client machines will restart with the new version running. See Updating for major releases.

If minor updates are installed centrally, updates of client machines may only be required in order to use new functionality. In these cases, operators can query whether new versions of the client applications are available, and they can choose whether or not to allow the automatic update process to run. See Updating for minor releases.

See below for information on Installing and configuring the Update Services Server.

Updating for major releases (Mandatory)

When an operator opens a client application (Admin Center or Control Center), and attempts to log on, the system checks that the client application software matches the version running on the central system. If a mismatch is detected, the system displays a message offering to...
update the client software from the Update services server. If the operator selects **Update Now**, the new version will be automatically installed. If not, the application will terminate.

If the system detects that allowing the operator to proceed would allow the user to connect to more than one system, then a warning message is posted, because the two systems may not be on the same software release. Upgrading to connect to one might prevent connection to the other.

You must then take appropriate steps to upgrade the ‘other’ system/s.

**Updating for minor releases (Optional)**

If minor updates are installed centrally, updates of client machines may only be required in order to use new functionality. In these cases, operators can query whether new versions of the client applications are available, and they can choose whether or not to allow the automatic update process to run.

**To query for a new version of the client:**

In Control Center, click **Help** in the **Main Menu**, and select **Check for Updates**. **Note:** The **Check for Updates** option is only enabled if the system has detected that the Server version is different from the Client version.

In Admin Center click **System** in the **Sidebar**, and select **Check for Updates**.
Note: The Check for Updates option is only enabled if the system has detected that the Server version is different from the Client version.
If a newer version is available, the following message will be displayed:

**Automatic Update Process**

Once the operator chooses the upgrade, the system will start the process of downloading the files to the client machine. A progress bar is displayed.

When all the files have been downloaded, the updates will be applied - this process can take 7-10 minutes. When completed, a message will be displayed.

Click on Finish, and the application will re-open.

**Installing and configuring the Update Services Server**

The Update Services Server is not a separate entity like Archiver or Directory – it runs as part of the Web Services running under the Windows Internet Information Server (IIS) component.

The Update Services Server must be installed using the Custom Installation process, by checking the appropriate box in the Custom Setup Dialog box.
The Update Services Server is normally installed on the Directory Server, but a different host can be chosen - see System - Advanced/Automatic Client Updates.

Full information on installing and configuring the Update Services Server is given in the Latitude 6.3 Release Notes.
Access Rights 211
Accessibility lost 152
Accessibility recovered 152
Activating the License 313
Activation Key 313
Add Serial Device 152
Alarm Configuration 137
Alarm Management 137
Analytic Rules 75
Analytics 75
Analytics - Camera shift 152
Analytics - Fence detection 152
Analytics - Intrusion ended 152
Analytics - Intrusion started 152
Analytics - Loitering detected 152
Analytics - Object removed 152
Analytics - Tripwire detection 152
Analytics - Unattended object 152
Analytics - Vehicle stopped 152
Analytics device 152
Application Server 17
Archived stream switch off 152
Archived stream switch on 152
Archiver Server 15
Archiving resumed 152
Archiving stopped 152
ART lost 152
ART recovered 152
Audit Log purged 152
Background Export 255, 354
Backup started 152
Binding Cameras 144
Bookmark created 152
Bookmark updated 152
Camera Sequence 81
Camera signal lost event 152
Camera signal recovered event 152
CaseBuilder Server 19
Change Password 113
Changing passwords 107
Client Portal 313
Clip locked 152
Clip unlocked 152
Connection to database lost 152
Connection to database recovered 152
Containers initialized 152
Database corrupted event 152
Database valid event 152
Defective containers percentage abn 152
Directory Backup 103
Directory Failover 371
Directory server licensed 152
Directory server unlicensed 152
Discovery 245
Discovery - Proprietary 248
Discovery lost 152
Discovery recovered 152
DNA Application 255
Edge Device Security Settings 113
Edge Recording 71
Edge Security Settings 107
Event Distributor (EDB) Server 17
Events 152
Export 255, 354
failed synchronization 371
Failover Directory 14, 371
Failover ended 152
Failover started 152
Generate Self-Signed Certificate 113
Global Admin Server 19
Intrusion Area 75
Keyboard 99
- L -
Licensing a system 313
Licensing Additional Servers 313
Linked 73
Live stream switch off 152
Live stream switch on 152

- M -
Masking Area 75
Mass Export 260
Mass export job added 152
Mass export job removed 152
Mass export job updated 152
Master recording ended 152
Master recording failed 152
Master recording started 152
Media snapshot exported 152
MMS 168
Motion Detection 75

- P -
Password Change 107
Password Rules 107
Picture Settings 62
Pin set to abnormal state 152
Pin set to normal state 152
Primary Directory 14
Privacy Mask 78, 189
Privileges 211
PTZ Configuration 74
PTZ locked 152
PTZ locked overridden 152
PTZ moved to preset 152
PTZ movement ended 152
PTZ movement started 152
PTZ pattern ended 152
PTZ pattern started 152
PTZ session ended 152
PTZ session started 152
PTZ unlocked 152

- R -
Recording clip export ended 152
Recording clip export started 152
Recording ended 152

- S -
Scene motion off 152
Scene motion on 152
SD card restore session ended 152
SD card restore session started 152
Security Actions 113
Security Mode 113
Server Entity Events 1
Shut down 152
Source Filter streaming started 152
Source Filter streaming stopped 152
Storage location corrupted 152
Storage location down 152
Storage location restored 152
Storage location tampered 152
Storage utilization abnormal 152
Storage utilization back to normal 152
Supported Edge Devices 254
Synchronization 1, 371
System Security 107

- T -
Tampering camera event 152
Technician session ended 152
Technician session started 152
Thermal Settings 65
TLS 107
TLS Certificate 107
Transcoder & Gateway Servers 17
Tripwire 75

- U -
Unit Security Status 113
Update Services Server 19
Updating Firmware 107
Updating Firmware on Quasar Gen II and TRK-101 units 107
User Group 224

- V -
Video Settings 58
- **W** -
  
  Web Security     107  
  Web Server       18  
  Wizards          229  

- **Z** -

  Zone motion off  152  
  Zone motion on   152